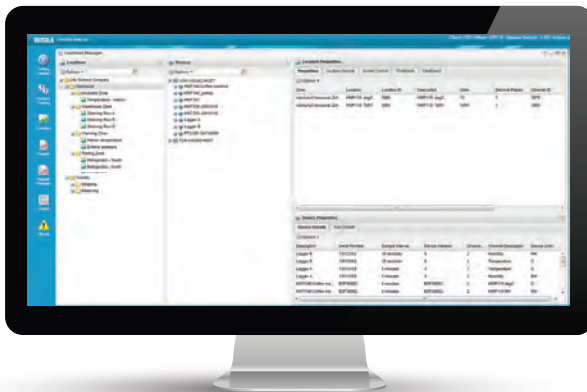


USER'S GUIDE

Vaisala Veriteq viewLinc Software viewLinc 4.3



PUBLISHED BY

Vaisala Oyj

Vanha Nurmijärventie 21, FI-01670 Vantaa, Finland

P.O. Box 26, FI-00421 Helsinki, Finland

Phone (int.): +358 9 8949 1

Fax: +358 9 8949 2227

Visit our Internet pages at www.vaisala.com.

© Vaisala 2014

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.

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.

Software License

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 on any other applicable media, depending on each individual product and the product items delivered to you.

Contents

CHAPTER 1: GETTING STARTED	1
What's New	1
Who Should Use this Manual	4
Conventions Used in this Document	4
How this Manual is Organized	5
Device Installation Documentation	5
Overview	5
How Does it Work?	6
System Components	6
viewLinc System Requirements	7
Default Application File Locations	9
Hardware Installation Options	10
Connecting Devices	11
Method 1: Using vNet Devices	12
Method 2: Using Digi Devices	14
Method 3: Using USB Port	16
Method 4: Using Serial Port	17
Method 5: Wireless Devices	17
Configuring Devices	18
Installing viewLinc	19
Logging in to viewLinc	22
Setup Road Map	24
Optional Setup Tasks	24
Getting Help	24

CHAPTER 2: SYSTEM SETTINGS	27
Choosing System Preferences	27
Device and Channel Aliases	28
Comments	29
MKT Activation Energy	29
Temperature Measurement Units	30
Remote Acknowledgement	30
Security Key	31
Technical Support	31
Session Expiry Time	31
viewLinc Aware Service	32
Unit Descriptions	32
Enabling Scheduling Functionality	33
Setting Language Option	34
Discovering Devices	35
Adding Hosts	37
Controlling Access to viewLinc	38
Assigning Rights	39
Access Control Permissions	40
Creating Groups and Adding Users	42
Editing Users and Passwords	47
Setting Up Schedules	48
Email & SMS Notification Settings	49
Define Email Notification Settings	49
Define SMS Notification Settings	51
Templates	52
Email & SMS Templates	52
Alarm Templates	53
Threshold Templates	58
Single Threshold Template	59
Multi-threshold Template	60
Using Preconfigured Comments in Templates	62

System Maintenance	63
CHAPTER 3: VIEWING DATA	65
viewLinc Desktop Orientation	65
Managing Locations & Zones	69
Organizing Locations	70
Creating Zones	71
Adding Locations to Zones	72
Linking Location Channels	74
Unlinking and Relinking Location Channels	74
Renaming Locations and Zones	76
Deleting Zones	77
Editing Location Properties	78
Assigning Access to Locations & Zones	79
Setting Up Location Thresholds	80
Disabling Threshold Alarms	82
Deactivating and Reactivating Threshold Alarming	83
Building Dashboards	83
Adding a Dashboard Image	84
Adding Zone and/or Location Data Items	85
Changing the Appearance of Dashboard Items	85
Setting Up User-specific Views	86
Creating a New View	87
Working with the Locations window	88
Searching for Zones and Locations	89
Using the Locations Dashboard	90
Monitoring Alarms	90
Building a Trend	91
Viewing Pop-up Trends	94
CHAPTER 4: MANAGING DEVICES	97
Viewing Devices and Hosts	97
Viewing Device Properties	98
Editing Device and Channel Properties	99
Editing Channel Properties	102
Setting Channel Temperature Units	104

Adding New Devices	105
Setting Up Device and Host Alarms	105
Communication Alarms	105
Device Alarms	108
Calibrating Devices	109
Removing Devices	110
Deactivating/Reactivating a Location	112
Swapping a Device	112
Permanently Delete a Location or Zone	114
CHAPTER 5: MONITORING ALARMS	117
About Alarms	117
Types of Alarms	118
Threshold Alarms	118
Communication Alarms	118
Event Validation Alarms	118
Device Configuration Alarms	119
Device Status Alarms	119
System Alarms	120
What Happens When an Alarm is Triggered?	120
Viewing and Acknowledging Alarms	121
Refreshing the Alarms Window	121
Receiving and Acknowledging Alarms	122
Ways to Acknowledge Alarms	122
Pausing Alarms	126
Managing Alarms View	127
Alarm Reporting	128
CHAPTER 6: EVENTS	131
Viewing Events	132
Adding Comments to Events	133
Adding Custom Events	134

Printing and Exporting Event Logs	135
CHAPTER 7: REPORTING	137
Types of Reports	137
Default viewLinc Reports	138
Custom Reports	138
Generating and Printing Reports	138
Reviewing Report Progress	140
Creating New Reports	140
Creating an Alarm Report	140
Creating a Location History Report	143
Creating a System Report	148
Cloning an Existing Alarm, Location or System Report	149
Deactivating and Deleting Reports	149
On-Demand Reports	150
Transferring Data	151
Using Transferred Data in Reports	151
Creating Transfer Schedules	151
Performing an Immediate Data Transfer	153
Editing Transfer Schedules	154
Deactivating Transfer Schedules	154
Disabling Transfer Schedules	155
CHAPTER 8: REMOTE & MOBILE DISPLAY	157
Using a Remote Display	157
Remote Display Requirements	158
Creating a Default User and View	159
Setting up the Remote Display	159
Changing the Remote Display View	160
Viewing Data on the Remote Display	161
Using viewLinc Mobile	161
Viewing Data with viewLinc Mobile	162
Acknowledge Alarms with viewLinc Mobile	164

APPENDIX: FAQs & TROUBLESHOOTING	167
Installing viewLinc	167
Setting Up Devices	176
Moving Vaisala Veriteq Devices	180
Troubleshooting Tips	182
Logging In	182
Alarms	183
Managing Data and Devices	184
Predefined UI Settings	185
Need More Help?	188
Index	189

CHAPTER 1

GETTING STARTED

Welcome to viewLinc, a key element in the Vaisala Veriteq Continuous Monitoring System (CMS). Easily monitor Device readings locally on a PC, across a network using a supported version of Microsoft® Internet Explorer®, or from mobile Devices like the iPhone® or Google Android®.

This chapter introduces you to the key concepts and setup requirements for your Vaisala Veriteq Continuous Monitoring System:

- What's New
- Overview
- Connecting Devices
- Configuring Devices
- Installing viewLinc
- Logging in to viewLinc
- Setup Road Map
- Getting Help

What's New

With the release of Vaisala Veriteq viewLinc 4.3, many new features and functions have been added to improve and simplify your network monitoring capabilities.

Instant Alarm Notification

- **Immediate SMS notification:** Ensure your team members receive immediate notification of changes in alarm conditions with SMS text messages (requires an SMS modem). Recipients can also take immediate action and acknowledge alarms remotely.
- **Accommodate fluctuating work schedules:** Create alarm notification schedules, to specify who needs to be notified of alarm condition changes for specific time periods (for example, day shift or night shift, alternating shift work, or 4-day work weeks).
- **Schedule system reminders:** Receive automatic notification of upcoming calibration service dates, and receive system configuration alarms whenever the server system time is changed.
- **Create escalating notifications:** If for some reason there is no response to a primary alarm notification, ensure subsequent alarm notifications or more severe alarm condition notifications are sent to additional team members, with multi-level threshold templates.

Easier Setup and Configuration

- **Save time installing vNet PoE devices:** viewLinc can now automatically identify newly installed vNet devices with the viewLinc Aware Service.
- **Customize measurement units:** Change device-defined unit measurement descriptions to more user-friendly terms. For example, a relative humidity Channel could display on screen as %RH, or a temperature Channel could read, Celsius.
- **Create Email and SMS templates:** Specify whether you want to send an SMS or Email notification for an alarm, and specify the contents of the message.
- **Quickly identify Access to Locations:** With the Access Control Inspector function, you now have an easy way to determine which Users or Groups have View or higher Access to Locations and Zones.

- **Easily restart viewLinc:** Any Admin Group User can restart the viewLinc service, if needed. A system notification is sent to all Admin Group members.

Comprehensive Reporting

- **Generate complete system reports:** Easily review your overall system details, such as a list of all Users, Groups, Access Rights, system-wide or Location-specific data reports.
- **Instantly distribute On-Demand reports:** Generate and email reports all in one step.
- **Reduce long report lists:** Distribute report management tasks by assigning ownership of a report to specific Users or Groups.
- **Add more report details:** viewLinc 4.3 reporting capabilities now include custom options: specify minimum and maximum excursions, add comments and/or signatures to reports, generate separate system and threshold alarm reports.

Flexible Alarm and Threshold Templates

- **Include notification lists:** Your alarm templates can now include automatic notifications to Groups (as well as Users).
- **Apply templates to multiple Locations:** Save time by setting up templates for Locations with identical threshold limits, even if different Groups need to be notified (templates are customizable by Location).

More Intuitive User Interface

- **Review data trends at any time:** Any viewLinc User can quickly create data trends, with easy to assemble graphs created on the Trend tab (accessible by all Users in the default Locations window).
- **More control over Dashboard display:** Adjust the font size and color of Location data appearing on your desktop Dashboard, and specify how you want data to display on a remote display terminal.
- **Flexible access control:** Depending on the Rights assigned to a User or Group, the desktop Options menu displays only those

windows which the User or Group has permission to view. Additionally, you can specify the Locations you want a User or Group to Access, and control access permission level.

- **Access training online:** viewLinc training videos are instantly available from your desktop, so you can get your team comfortable using viewLinc today!

Who Should Use this Manual

This manual is for both Administrators and Users.

- **Administrators:** Learn how to install and configure viewLinc Server software and its associated components (see Chapters 1 through 4).
- **Users:** Learn how to operate viewLinc standard tasks, such as viewing and monitor Device readings across a network (see Chapters 3 through 8).

Conventions Used in this Document

This document uses the following conventions:

- A sequence of actions is indicated by a list separated by a vertical line. For example:
“In viewLinc, choose **Options | System Configuration | Locations Manager**”
- Menu selections, items you select, and the names of buttons are shown in **bold**.
- Keys on the keyboard are shown in [square brackets].
- Vaisala Veriteq Loggers, Vaisala Wi-Fi Data Loggers (HMT140), and 300 Series Transmitters are referred to as Devices throughout this manual.
- vNet and Digi Devices are Network Devices.

How this Manual is Organized

The Vaisala Veriteq viewLinc 4.3 User's Guide includes the information you need to install, configure and operate the viewLinc system, and reference step-by-step procedures for the standard tasks performed using viewLinc.

For a graphical overview of installing viewLinc, refer to the Quick Start Guide.

Device Installation Documentation

Vaisala Devices are installed and configured for your network using vLog or HMT140 Utility software (shipped with your Device).

To set up and configure your Devices, refer to the specific Vaisala product User Guide for more information.

Overview

The viewLinc system features triple-redundant data retention ensuring that data is immune to power outages, network interruptions, and human error. It provides complete data protection and allows you to:

- **Monitor** remote conditions in multiple languages from multiple Devices (and different time zones!) from any PC connected to your network.
- **Identify** Devices and the areas where they operate.
- **Create** preconfigured comments for alarm notifications and reusable alarm threshold templates.
- **View** real-time data in a customizable graphical format.
- **Receive** visual or email alarms when conditions you are monitoring are out of compliance or if there is a network communication problem.
- **Acknowledge** alarms from your mobile Device.
- **Generate** historical data and alarm reports.
- **Swap** a Device for calibration or replacement purposes without breaking the data audit trail.

How Does it Work?

viewLinc runs as a Windows service which is launched automatically. If and when you reboot the viewLinc Server, the viewLinc service starts automatically. Depending on your network setup, you may want to set up an Enterprise Server and one or more Device Hosts:

- viewLinc **Enterprise Server**: Gathers data from Devices, performs scheduled transfers, watches for alarms, executes any associated actions, manages Users, and controls system-wide and user-specific settings.
- viewLinc **Device Host**: Runs as a service on a Host computer. It acts as a data collection point for Devices located in the remote server area. It functions in the same way as the Enterprise server, except it forwards the collected data to the Enterprise server for processing and storage.

System Components

The Vaisala Veriteq CMS is comprised of both software and hardware components:

- **Software**: Device drivers (if required to connect your Devices to a network), vLog and/or HMT140 Utility (to configure your Devices), and viewLinc (for data monitoring).

Note: The software shipped with your Device allows you to set sample timing, maintain audit trail, and clear history; viewLinc then allows you to monitor and manage the data transferred or transmitted from the Devices.

- **Hardware**: Veriteq Loggers, HMT140 Wi-Fi Loggers, or 300 Series Transmitters, one or more PCs with a supported Internet browser, and, depending on how you connect the Devices to your PC, various cables, Vaisala Veriteq vNet or Digi network Devices.

viewLinc System Requirements

Before you install and set up Vaisala Veriteq viewLinc 4.3, you will need:

- One or more Vaisala Veriteq Loggers, Vaisala Wi-Fi Data Loggers (HMT140) or 300 Series Transmitters.
- A PC (will be referred to in the rest of this document as the viewLinc Server).
- (optional) Additional PCs, if you plan to manage Devices at multiple locations (will be referred to in the rest of this document as a Host PC).
- (optional) Remote Display terminals, if you plan to provide additional monitoring opportunities in locations without PCs.
- Vaisala cables, for connecting Loggers and setting up wireless Transmitters.
- (optional) vNet Devices, for connecting Veriteq Loggers to a viewLinc Server using an Ethernet connection
- (optional) Digi Devices, for connecting Veriteq Loggers to viewLinc Server using an Ethernet connection

viewLinc Server and viewLinc Host PC Requirements

For optimum performance, your viewLinc Server PC requires 200KB available per Channel per day for storing data.

Note: The historical database (where data is stored) and configuration files are located in the Public Documents folder.

In addition, the viewLinc Server PC and any viewLinc Host PCs, must meet the following requirements:

- Be available 24 hours a day, 7 days a week.
- Have 350 MB free application disc space.
- Use one of the following Microsoft® operating systems:
 - Windows Server 2012 R2 (64 bit)
 - Windows 7 Pro (64 bit)
 - Windows Server 2003 (32 bit)
 - Windows Server 2008 R2 (64 bit).

- Have a supported Internet browser installed (Microsoft® Internet Explorer® v8, 10, or 11 are recommended). Only required on the Server PC if you plan to use it to run viewLinc.

Additional Server Requirements

Depending on the number of Device Channels you plan to activate and monitor, the viewLinc Server should also meet the following requirements:

Installation Size	viewLinc Server Requirements
<p>Large installation (400-5000 Channels)</p>	<ul style="list-style-type: none"> • a dedicated machine • 3.2 GHz, Quad Core • 4 GB RAM • sufficient HD space to support 200KB/Channel/day <p>For example, if you have 400 Channels, you will need approximately 30GB (400x200x365) per year.</p> <p>For large size installations, it is recommended to run a 64-bit OS for optimum performance.</p>
<p>Medium installation (20- 400 Channels)</p>	<ul style="list-style-type: none"> • machine may be shared with other applications • 1.6 GHz Dual Core • 4 GB RAM • sufficient HD space to support 200KB/Channel/day <p>For example, if you have 40 Channels, you will need approximately 3GB (40x200x365) per year.</p>
<p>Small installation (<20 Channels)</p>	<ul style="list-style-type: none"> • 1.6 GHz • 2 GB RAM • sufficient HD space to support 200KB/Channel/day <p>For example, if you have 4 Channels, you will need approximately 300MB (4x200x365) per year.</p>

End User PC Requirements

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

- 2.4 GHz
- 2 GB RAM
- Microsoft Internet Explorer 8, 10 or 11.

Default Application File Locations

It is strongly recommended that you use these default installation folders for data file storage, as other folders may have special security restrictions placed on them.

Note: The default location for the viewLinc application is in the Program Files folder.

For example, Windows 2008 does not allow files in the Program Files folders to be deleted by non-admin Users.

Platform	Default File Storage Location
Windows 2012	Program files: C:\Program Files(x86)\Vaisala\Vaisala Veriteq viewLinc Data files: C:\Users\Public\Documents\Vaisala\Vaisala Veriteq viewLinc
Windows 2008/ Windows 7 Pro	Program files: C:\Program Files(x86)\Vaisala\Vaisala Veriteq viewLinc Data files: C:\Users\Public\Documents\Vaisala\Vaisala Veriteq viewLinc

Platform	Default File Storage Location
Windows 2003	Program files: C:\Program Files\Vaisala\Vaisala Veriteq viewLinc Data files: C:\Documents and Settings\All Users\Documents\Vaisala\Vaisala Veriteq viewLinc

Hardware Installation Options

How you connect Veriteq Loggers, HMT140 Wi-Fi Loggers, or 300 Series Transmitters to your PC is a very important administrative decision. There are five methods and each requires certain hardware connections.

Method 1: vNet Device

Configuration software: Web interface

How connected: Ethernet

- Connect Devices to the PC across an Ethernet network.
- PC and Devices can be separated by large distances within a facility.
- Requires installation of vNet drivers (provided).
- Requires use of vNet Device.

Method 2: Digi Device

Configuration software: vLog

How connected: Ethernet

- Connect Devices to the PC across an Ethernet network.
- PC and Devices can be separated by large distances within a facility.
- Requires installation of Digi driver software (provided) and Digi Device.
- Digi Device only required for Vaisala Veriteq Loggers.

Method 3: USB Port**Configuration software:** vLog**How connected:** Vaisala Veriteq USB cable

- Connect Devices directly or over an Ethernet network (when a Device Host PC is installed) to the viewLinc server.
- Requires installation of USB drivers (provided) and uses a USB connection on a PC.
- Requires a USB-to-logger cable.

Method 4: Serial Port**Configuration software:** vLog**How connected:** Serial cable

- Connect Devices directly or over an Ethernet network (when Device Host is installed) to the viewLinc server.
- Requires a Serial Port on a PC.
- Requires a Serial cable.

Method 5: Wireless**Configuration software:** HMT140 Utility (HMT140 Wi-Fi Data Loggers); Web UI (300 Series)**How connected:** 802.11b/g Wi-Fi

- Connect Devices wirelessly to the viewLinc server.
- Vaisala Wi-Fi Data Logger HMT140: Requires configuration with an HMT140 Configuration Cable.

It is also possible to use a mix of these methods depending on your system requirements.

Connecting Devices

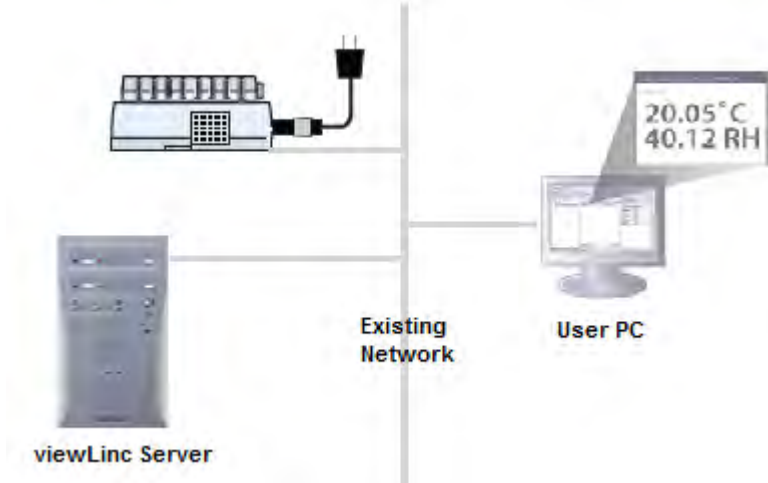
This section outlines the five methods Loggers and Transmitters (Devices) can connect to your viewLinc CMS.

For a graphical representation of how to install Devices, see the Vaisala Veriteq viewLinc Quick Start Guide.

To obtain a copy of the Quick Start Guide, see <http://www.vaisala.com/viewLinc>, or call to request a copy of the guide from your sales representative.

Method 1: Using vNet Devices

The following procedure describes how to use vNet Devices to connect Vaisala Veriteq Loggers to your network.



Hardware: Attach Logger to vNet Device

- 1 Remove protective label on the bottom or back of the Logger.
- 2 Connect the Logger to the vNet Device.
- 3 Connect the vNet Device to the Ethernet outlet and (if not using Power Over Ethernet) power supply. When power is supplied to the vNet Device, the red power LED light will blink for 7-8 seconds, then stay solid. When a network connection is made, the red LNK LED should light up and stay solid, and the green ACT LED should blink occasionally.

Note: To ensure a secure connection, insert the power supply barrel-end connector into the Device and turn 1/4 to the

right. If your network supports PoE, you do not need to connect to a power supply.

For more information about installing vNet Devices, refer to the vNet User Guide.

Drivers: Connect Logger to your Network

This section describes how to install the drivers for vNet Devices to connect Vaisala Veriteq Loggers to the network using an Ethernet connection.

If you are installing vNet Devices with the latest Firmware installed (v1.4 or higher) on the same subnet as viewLinc, device drivers are installed automatically when you enable the viewLinc Aware Service (see “viewLinc Aware Service” on page 32). Full details are available in the vNet User's Guide.

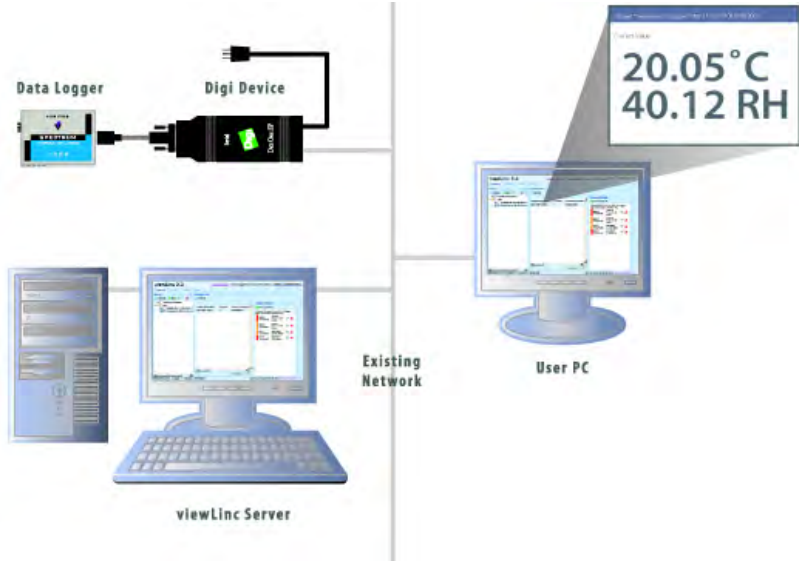
Note: Follow these steps only if you are installing vNet Devices with a serial number 1411xxxx or Firmware v1.3x or earlier.

- 1 Insert the vNet Device driver CD into the viewLinc Server.
- 2 Run the Device Setup Wizard.
- 3 Identify your vNet Device using the MAC address found on the side of your vNet Device.
- 4 Enter an IP address (provided by your IT department).
- 5 Select RealPort Settings and ensure the option, **Install RealPort on this computer**, is selected.
- 6 Complete the Wizard accepting all remaining default options.

Repeat Steps 1 and 2 for each vNet Device.

Method 2: Using Digi Devices

The following procedure shows how to use Digi Devices to connect your Vaisala Veriteq Devices to the network.



Hardware: Attach Device to Digi

- 1 Connect your Vaisala Veriteq Device to a Digi Device using a Vaisala Veriteq cable.
- 2 Connect your Digi Device to power supply and Ethernet outlet.

Note: These instructions focus on the Digi One SP. For other Digi models, see <http://www.vaisala.com/en/lifescience>.

Drivers: Connect Devices to your Network

This section describes how to install the drivers for Digi Devices to connect Vaisala Veriteq Devices or Vaisala 300 Series Transmitters to the network using an Ethernet connection. Repeat all of these steps for each Digi Device you'll use.

Step 1: Discover the Digi Device

- 1 Obtain a reserved (recommended) or static IP address for your Digi Device from your IT department. If your networking policy requires you to reserve IP addresses using DHCP, see <http://www.vais-ala.com/en/lifescience> for instructions.
- 2 Insert the Digi driver CD into viewLine Server.
- 3 The Digi Device Setup Wizard launches automatically. Click **Next**.
- 4 Select the Device that matches the MAC address from the bottom of your Digi Device. Click **Next**.

If your Device is on a different subnet from the server, you will need to know the IP address of the Digi Device and launch the RealPort installer on the Digi Driver CD.

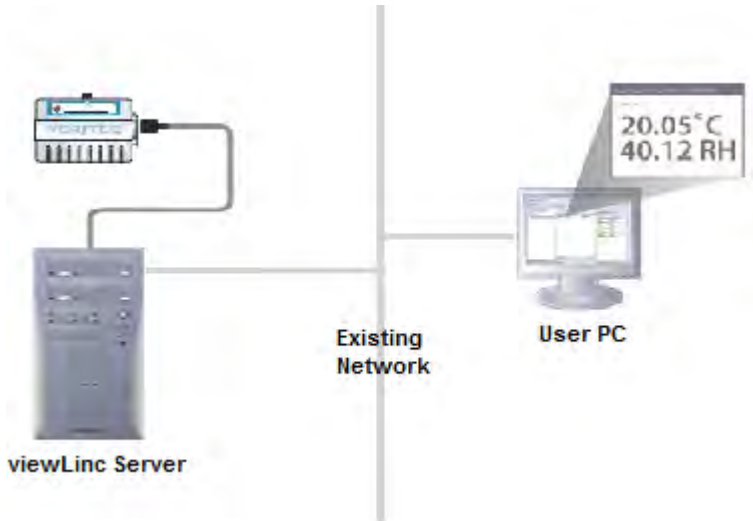
Step 2: Configure RealPort and Install Drivers

- 1 In the Configure Network Settings screen, enter an IP address (provided by your IT department). Click **Next** two times.
- 2 In the Configure RealPort Settings screen, select **Install Digi RealPort on this computer**. Click **Next**.
- 3 Click **Next** again. The settings are saved.
- 4 Click **Finish**.

Repeat Step 1 and Step 2 for each Digi Device.

Method 3: Using USB Port

You can connect Vaisala Veriteq Devices directly to PCs using a USB Port:



Drivers: Install USB Drivers

Using the supplied Vaisala Veriteq USB cable driver CD and Quick Start Guide, install USB drivers on every PC you plan to attach Devices to.

Hardware: Connect Hardware

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

Method 4: Using Serial Port

You can also connect Devices to PCs using a Serial Port. The configuration using a Serial Port is very similar to using USB (refer to the diagram shown in, Method 3: Using USB Port).

Hardware: Connect

- 1 Connect your Device to a Vaisala Veriteq Serial Port cable.
- 2 Connect the Serial Port cable to your viewLinc Server or Host (ensure this computer is attached to your network).

Repeat these steps for all Devices.

Method 5: Wireless Devices

To set up a wireless connection for HMT140 Devices, first connect each Device to your computer with the HMT140 Configuration Cable and configuration software, HMT140 Utility). For complete instructions, refer to the HMT140 Wi-Fi Data Logger User's Guide.

Hardware: Set Up HMT140

- 1 Ensure the HMT140 Configuration Cable is disconnected from your PC.
- 2 Open the HMT140 case to ensure the power switch on the Device is in the OFF position.
- 3 Install three 3.6V lithium batteries, and turn power switch ON. Setup process completes in 5 seconds.

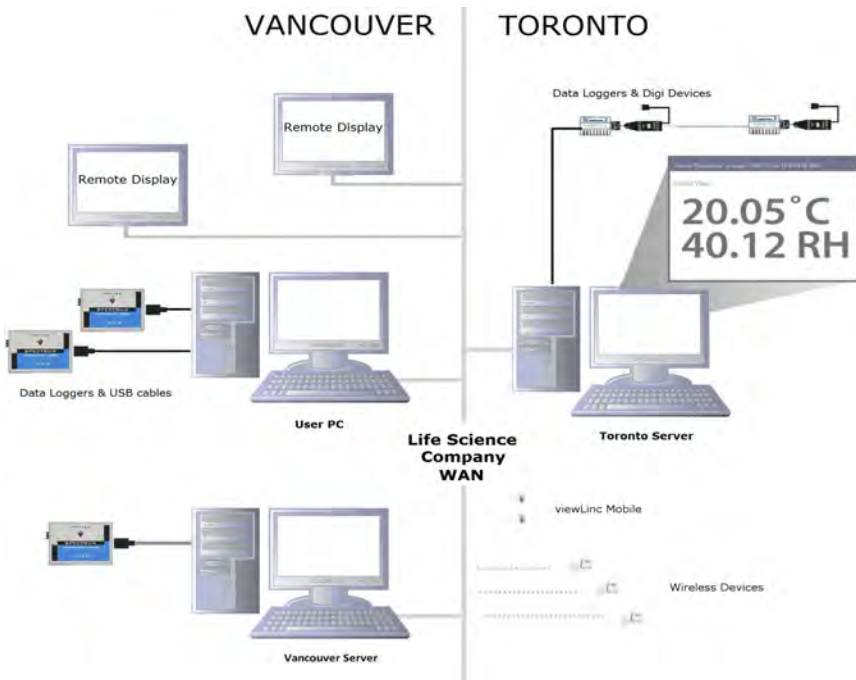
Note: Use only part # 236318SP Vaisala 3.6V Lithium Thionyl Chloride batteries.

Software: Install Connectivity Software

- 1 With the HMT140 Device case removed and the Device turned ON, connect the USB connector on the HMT140 Configuration Cable to your PC.
- 2 On your desktop, start the HMT140 Utility.

- 3 Connect the HMT140 Configuration Cable to the 4-pin HMT140 CONFIG header.
- 4 On the HMT140 Utility **Setup** tab, click **Retrieve**. To make configuration changes, refer to the HMT140 Wi-Fi Data Logger User's Guide.
- 5 Disconnect the configuration cable from the Device, wait 8 seconds, then press the SERVICE button.

If you have a combination of Devices and set up configurations, your network may look similar to this combination diagram:



Configuring Devices

Once your Devices are installed, you are ready to configure your Devices with vLog software, or, if you are using wireless Devices,

HMT140 Utility software. These software programs allow you to confirm the successful installation of the Port and change Device settings as required (depending on your Device).

Refer to your specific Vaisala Device User Guides for installation and configuration instructions.

Configuration activities include:

- set sample intervals
- enable or disable Channels
- specify Device and Channel descriptions
- store historical data for backup purposes

Note: Depending on the Devices you have installed, some of these properties can be adjusted within viewLinc. See “Editing Device and Channel Properties ” on page 99.

Installing viewLinc

Now you are ready to make Device monitoring, alarming and reporting activities available across your network.

There are two options available to you:

- **Install viewLinc software on a network server** (install option: Enterprise Server). This installation method allows the viewLinc server PC to monitor and administer all Devices connected to it, wired and wireless. If you are monitoring less than 20 Devices, you may decide that you only require one installation of viewLinc; however, if you want additional control and network stability, or have a medium or large installation, it is recommended that you connect some of your Devices to a Host PC.
- **Install viewLinc software on a Host PC** (install option: Device Host). Setting up viewLinc on additional, dedicated PCs allows automatic communication with the viewLinc Server while offering protection from bandwidth and network communication issues, and greater flexibility when managing Device configuration.

Refer to the Host and Server requirements for different installation sizes, to determine which option is best for your needs (see “viewLinc System Requirements” on page 7).

Note: All Users can access viewLinc from their own PC or mobile Device, without having to install the 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 (see “Controlling Access to viewLinc” on page 38).

To install viewLinc on the Enterprise Server PC (new install):

- 1 On your viewLinc Server PC, insert the viewLinc CD and run viewLincSetup.exe.
- 2 Select the installation language, then click **OK**.
- 3 To start the Setup Wizard, click **Next**.
- 4 Review and accept the License Agreement, then click **Next**.
- 5 Choose a destination for the viewLinc program files, then click **Next**.
- 6 Choose a destination for data files, then click **Next**.
- 7 Select **Enterprise Server** from the **Select Components** window, and click **Next**.
- 8 Enter the installation key purchased from Vaisala, then click **Next**.
- 9 Select Non-secure, Secure server (SSL) or Both (depending on your company’s security policies).
- 10 Review the install options and click **Install**.
- 11 Click **Finish** once the application is finished installing.

Note: You must reboot the server for the viewLinc services to start running.

To install viewLinc on an Enterprise Server PC (upgrade from 3.5.1 or higher):

- 1 On your viewLinc Server PC, insert the viewLinc CD and run viewLincSetup.exe.
- 2 Select the installation language, then click **OK**.
- 3 To start the Setup Wizard, click **Next**.

- 4 Review and accept the License Agreement, then click **Next**.
- 5 Enter the installation key purchased from Vaisala, then click **Next**.
- 6 Choose your Import settings.
Note: If you did not use custom Channel descriptions in the earlier version of viewLinc, it is highly recommended that you select the option to create Locations based on existing Device and Channel descriptions. This will ensure you can easily identify your Device Channels in the viewLinc 4.3 Locations navigation tree.
- 7 Review the install options and click **Install**.
- 8 Click **Finish** once the application is finished installing.

Note: You must reboot the server for the viewLinc services to start running.

You can 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.

To install viewLinc on a Host PC:

Note: If you are installing viewLinc on a PC running Windows 7, 2008 or 2012, you may need to adjust your Firewall settings to specify Public/Private/Domain exceptions. Contact Vaisala customer support if you require assistance.

- 1 Insert viewLinc CD and run viewLincSetup.exe.
- 2 Select the installation language from the box list. Click **OK**.
- 3 Start the Setup Wizard by clicking **Next**.
- 4 Review and accept the License Agreement, then click **Next**.
- 5 Choose a destination for the viewLinc program files, then click **Next**.
- 6 Select **Device Host**, then click **Next**.
- 7 Click **Install**.
- 8 Click **Finish**.

Note: You must reboot the server for the viewLinc services to start running.

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


Logging in to viewLinc

When you are ready to start using viewLinc, log in to viewLinc from any PC with an Internet browser using the default “admin” account (this is a User account with Full Control). The username and password are both “admin”.

Note: The default Admin User is part of the default ADMIN Group. For security purposes, it is important to change the admin password as soon as possible (see “Editing Users and Passwords” on page 47).

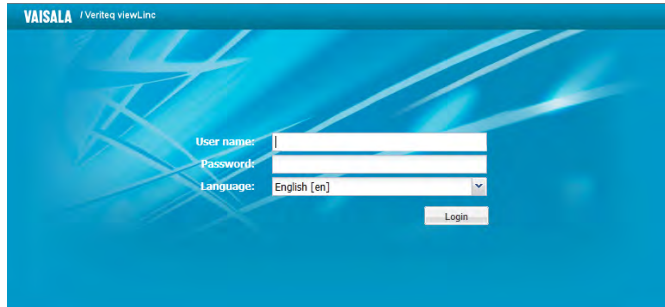
You also need to create accounts for other Users, specifying their username, their Email address, availability schedule (times they should receive alarm notification), their Rights and Access Control Permissions, the Channels they can view, and their authentication method (if they will use a viewLinc login or use the same login as their Windows login). For more information see, “Controlling Access to viewLinc” on page 38.

To log in to viewLinc:

- 1 Double-click the desktop icon .
- 2 Or, in the address box of a supported Internet browser, enter the name or address of the machine where viewLinc is installed, and the Port number. Your administrator will provide the correct address.

For example, `http://computername:portnumber` or `https://-computername:portnumber` if secure (if no Port number is specified, 443 is used by default). Save this address to your favorites or set as your homepage to easily access viewLinc from your browser.
- 3 In the login screen, select your language from the language list. When a new language is selected, the page will automatically refresh and update accordingly.

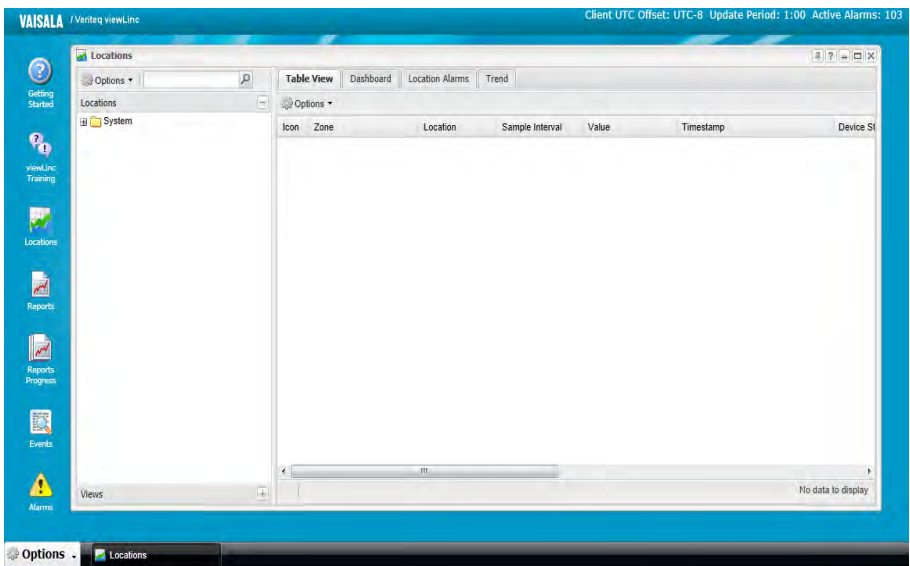
The default administrator User name and Password are both “admin”.



Note: To save your language setting, ensure that your browser is not set to automatically delete cookies upon exit.

- 4 Enter your User name and Password. Click **Login**. viewLinc starts and displays the Locations screen.

The first time you log in to viewLinc, the Locations window appears in the browser. This is the primary entry point for all Users.



Setup Road Map

Once your viewLinc system is installed, Administrators may find the following Road Map a useful overview of the setup and configuration activities required to get your team started using viewLinc. Once these set up activities are complete, you are ready to start monitoring Device readings, viewing events and printing reports.



Optional Setup Tasks

Depending on the types of Loggers you are using, you may want to set up a transfer schedule to view and analyze Vaisala Veriteq Logger data in vLog software (see “Transferring Data” on page 151). Data collected by HMT140 Loggers and 300 Series Transmitters is automatically available for viewing and analyzing in viewLinc.

Getting Help

If you need help, technical support is available:

North America

Contact Vaisala, 8 am to 4 pm PST Monday to Friday.

Phone: 1-888-VAISALA

Email: helpdesk@vaisala.com

Web: www.vaisala.com/en/lifescience

For assistance calibrating Devices, contact the Vaisala Calibration Service Center. (Visit <http://www.vaisala.com/en/services/maintenance/Pages/depotcalibration.aspx>.)

Outside of North America:

Email: helpdesk@vaisala.com

Web: www.vaisala.com

Vaisala Headquarters (Finland)

Vanha Nurmijärventie 21

01670 Vantaa

FINLAND

Industrial Instruments

Phone: +358 9 8949 2658

Fax: +358 9 8949 2227

Japan Service Center

42 Kagurazaka 6-Chome

Shinjuku-ku

Tokyo 162-0825

JAPAN

Phone: +81 3 3266 9611

Fax: +81 3 3266 9610

China Service Center

Floor 2, EAS Building

No. 21, Xiao Yun Road, Dongsanhuan Beilu

Chaoyang District

Beijing 100027

CHINA

Phone: +86 10 5827 4100

Fax: +86 10 8526 1155

CHAPTER 2

SYSTEM SETTINGS

There are several important settings screens in viewLinc, which are all accessible from the System Configuration menu (from the viewLinc desktop, select **Options | System Configuration**). System settings define the overall ‘backbone’ of your viewLinc system, and allow you to define how Devices connect and display data.

This section reviews key Administrator tasks:

- Choosing System Preferences
- Discovering Devices
- Controlling Access to viewLinc
- Setting Up Schedules
- Email & SMS Notification Settings
- Templates
- System Maintenance

Choosing System Preferences

viewLinc includes several system options that affect the behavior and display of viewLinc windows. You have the option of making these changes:

- Adding Device and Channel Aliases
- Configuring Comments
- Defining MKT Activation Energy
- Enabling Scheduling Functionality
- Changing Temperature Measurement Units

- Setting up Remote Acknowledgement
- Specifying a new Security Key
- Changing reporting options for the Technical Support Log
- Controlling Session Expiry Time
- Setting up viewLinc Aware Service
- Modifying Device Unit Descriptions
- Setting Setting Language Option

Device and Channel Aliases

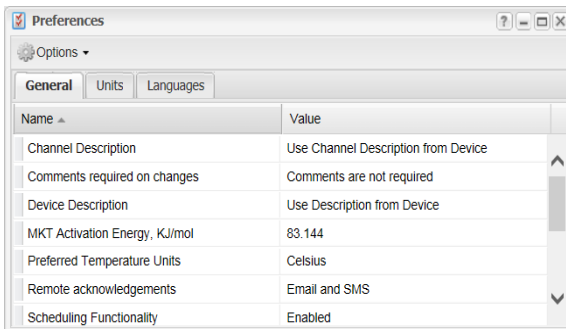
Vaisala Veriteq Devices have descriptions stored inside them that have a maximum length of 16 characters (300 Series Transmitters do not store descriptions). These descriptions can be defined and modified using the specific Device configuration software (vLog or HMT140 Utility), or viewLinc.


For easier reference, you can configure viewLinc to display a longer, more informative description for a Device or a Channel, up to 64 characters. This longer description is called an Alias.

Events-, Alarms-, Reports windows, and Email messages all use the designated descriptions for Channels and Devices.

To set the Channel or Device Description display preference:

- 1 On the viewLinc desktop, choose **Options | System Configuration | Preferences**.






- 2 On the **General** tab, click in the **Channel Description** Value field to select your preference from the list.
- 3 Select your preference in the **Device Description** field.
- 4 Save your changes (**Options** |  **Save**).

Comments

Comments can provide valuable reference information about changes made to your system by Users, or network Events. Depending on your Comments preference setting, manually entered or preconfigured Comments appear in the Events window (Event details pane), generated in Reports, and added during the acknowledgement of alarm notifications.




To set up preconfigured comments, see “Email & SMS Templates” on page 52.

To set Comments preference:

- 1 On the viewLinc desktop, choose **Options** |  **System Configuration** |  **Preferences**.
- 2 On the **General** tab, click in the **Comments required on changes** Value field to select an option from the list. Choose whether comments are required on changes; if it is up to the User to enter a Comment; if they are required, or if only preconfigured comments are required.
- 3 Save your changes (**Options** |  **Save**).

MKT Activation Energy

The default value for MKT Activation Energy is used in Reports and Pop-up Trends.

- 1 On the viewLinc desktop, choose **Options** |  **System Configuration** |  **Preferences**.
- 2 On the **General** tab, select the **MKT Activation Energy** row, then click in the **Value** column to enter a new value.
- 3 Save your changes (**Options** |  **Save**).




Temperature Measurement Units

When viewLinc is installed, temperature is 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 the Device measures temperature, it simply alters the units in which temperature is displayed (except for Channels which already have preferred unit settings assigned).

Note: To set measurement units on individual Device Channels, see “Editing Device and Channel Properties ” on page 99.




To choose global temperature measurement unit preference:

- 1 On the viewLinc desktop, choose **Options |  System Configuration |  Preferences.**
- 2 On the **General** tab, select the **Preferred Temperature Units** row, and then click in the **Value** column to choose either **Celsius (C)** or **Fahrenheit (F)** setting.
- 3 Save your changes (**Options |  Save**).

Remote Acknowledgement

For team members who are required to acknowledge alarm notifications, specify whether you want to allow remote acknowledgement, and the method which you want used to issue acknowledgement, by Email, SMS or Email and SMS.




To set remote acknowledgement preference:

- 1 On the viewLinc desktop, choose **Options |  System Configuration |  Preferences.**
- 2 On the **General** tab, select the **Remote acknowledgements** row, and then click in the **Value** column to choose your acknowledgement preference.
- 3 Save your changes (**Options |  Save**).

Security Key

Enter the Security Key you were provided by Vaisala. 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.

To set or update the security key:

- 1 On the viewLinc desktop, choose **Options** |  **System Configuration** |  **Preferences**.
- 2 On the **General** tab, select the **Security Key** row, then click in the **Value** column to enter your security key (the code is hidden from view when you click outside the field).
- 3 Save your changes (**Options** |  **Save**).

Technical Support



The **Technical support log** field specifies the amount of information detail included in the support log file. If you ever require viewLinc technical support, your Vaisala Technical Support representative may ask you to change the Technical support log setting temporarily, to better understand the issue you may be encountering.


Session Expiry Time

Use the **Users must confirm their identify** field to choose a session expiry time after which a User must reconfirm their identity (by reentering their password). This prevents non-authorized Users from making changes to viewLinc. This setting is applied universally to all viewLinc Users and Administrators.

You can choose to set this expiry time as **Never**, **Always** (User is required to enter password before making any change to the system), or intervals of **1, 5, 10, 15, 30** or **60 minutes** after logging in or reconfirming their password.

To set the session expiry:

- 1 On the viewLinc desktop, choose **Options** |  **System Configuration** |  **Preferences**.




- 2 On the **General** tab, select the **Users must confirm their identity** row, then click in the **Value** column to choose an expiry time.
- 3 Save your changes (**Options** |  **Save**).

viewLinc Aware Service

Choose whether to enable or disable the **viewLinc Aware Service**. This service automatically permits viewLinc to search for and communicate with vNet Devices on your network or subnet.

Note: Only one viewLinc Server per subnet can have this option enabled.

To enable/disable viewLinc Aware Service:

- 1 On the viewLinc desktop, choose **Options** |  **System Configuration** |  **Preferences**.
- 2 On the **General** tab, select the **viewLinc Aware Service** row, then click in the **Value** column to enable or disable the service.
- 3 Save your changes (**Options** |  **Save**).



To learn more about how to set up vNet Devices with viewLinc, refer to the vNet PoE Device User Guide.

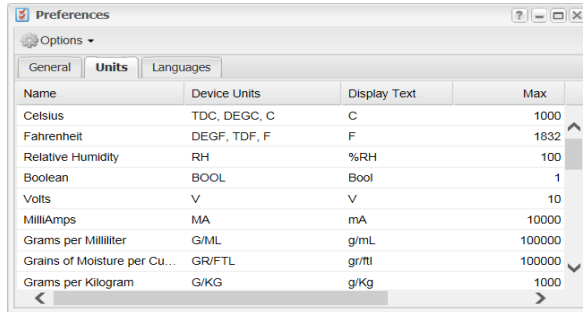
Unit Descriptions


For each Device you monitor, the information tracked on the Channel is preset. However, if you want the information displayed differently onscreen, use the Unit Preferences screen to make your changes.

For example, if your Channel tracks MilliAmps, you could change the display text to read, mA.

To specify unit descriptions:

- 1 On the viewLinc desktop, choose **Options** |  **System Configuration** |  **Preferences**.






- 2 Select the **Units** tab. The list displays all standard Device Channel unit types, but some of your Devices may be preconfigured with custom unit descriptions.
- 3 To add custom Device units to this table, ensure viewLinc can recognize the unit type and assign correct threshold settings:
 - In the **Name** column, identify and select the row for the channel type.
 - Double-click the **Device Units** field in the selected row, and click **Add Units**.
 - Enter the units (max. 4 characters), then click **Apply**.
 - Double-click in the **Display Text** or **Decimal Places** column to choose how you want information units to display.
- 4 Save your changes (**Options** |  **Save**).

Enabling Scheduling Functionality

The viewLinc Scheduling function allows you to specify specific times of day or days of the week when you want a User or Group to be notified of alarm conditions. It is also used to schedule times when you want Location threshold alarming active. By default, this option is disabled.

To enable/disable scheduling functionality:

- 1 On the viewLinc desktop, choose **Options** |  **System Configuration** |  **Preferences**.

- 2 On the **General** tab, select the **Scheduling Functionality** row, then click in the **Value** column to enable or disable scheduling.
- 3 Save your changes (**Options** |  **Save**). A new Schedules option appears on the System Configuration menu.

Refer to “Setting Up Schedules” on page 48, for information about how to define schedules for Users and Locations.

Setting Language Option




If your company operates in more than one country, you may want to provide Users the option to view the viewLinc desktop in their native language.

Note: Report contents are generated in the language preference selected during viewLinc installation.

Languages supported in viewLinc 4.3 are:

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

To specify Languages available to Users:

- 1 On the viewLinc desktop, choose **Options** |  **System Configuration** |  **Preferences**.
- 2 On the **Languages** tab, select the language(s) you want available when Users log in.
- 3 Save your changes (**Options** |  **Save**).





Discovering Devices

When new vNet Devices, Loggers and Transmitters (they are all referred to as Devices) are connected to your network, most model types are automatically identified by viewLinc; however, if a Device does not display in the **Devices** navigation pane in the **Locations** window, you can run the viewLinc Discover Devices function to look for a missing Device.

Note: 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).

It is also easy to add more Host machines as your monitoring network grows (see “Adding Hosts” on page 37).

To discover recently attached Vaisala Veriteq Devices:

- 1 From the viewLinc desktop, choose **Options** |  **System Configuration** |  **Locations Manager**.
- 2 In the center **Devices** pane, select the Host machine to which the Device is connected, then right-click and select  **Discover Devices**, or, on the Device tab **Options** menu, select **Host** |  **Discover Devices**.





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

Adding Devices Manually

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

- discovering Devices is taking too long
- you are adding a 300 Series Transmitter or HMT140 Wi-Fi Logger
- you want to add a variety of Device types at one time

To add a Vaisala Veriteq Device:

- 1 From the viewLinc desktop, choose **Options** |  **System Configuration** |  **Locations Manager**.
- 2 In the **Devices** pane, select a Host, then select **Options** |  **Host** |  **Add Device**.





- 3 On the **Add Device** screen, in the **Device Class** box list, select your Device type.
- 4 Enter the COM Port number.
- 5 Click **OK** to save.

To add a 300 Series Transmitter:

- 1 Ensure no other Users are logged on to the Transmitter you want to add.
- 2 From the **Locations Manager** window, on the **Devices** pane, select a Host, then select **Options** | **Host** | **Add Device**.
- 3 In the **Add Device** screen, from the **Device Class** box list, select **300 Series Transmitter**.
- 4 Enter the following:
 - **Timeout:** To ensure continuous monitoring, do not change (default 30 seconds).
 - **Disconnect After Scan:** To maintain a persistent connection to the Device, choose **Yes**.
 - **Connection Type:** If the transmitter has a LAN or WLAN module, select Network. If you use an external Digi 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).
- 5 Click **OK** to save.



To add an HMT140 Wi-Fi Data Logger:

- 1 Ensure no other Users are logged on to the HMT140 you want to add.

- 2 From the **Locations Manager** window, on the **Devices** pane, select a Host, then select **Options** |  **Host** |  **Add Device**.
- 3 In the **Add Device** screen, from the **Device Class** box list, select **HMT140**.
- 4 Enter the following:
 - **Timeout:** To ensure continuous monitoring, do not change (default 30 seconds).
 - **Serial number:** Enter the HMT140 serial number.
 - **UDP Port:** Auto-generated, 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).

Note: Do not change the ‘Max blocks per beacon’ value for HMT140 Devices without first consulting your technical support department as changes to this setting may impact battery life.
- 5 Click **OK** to save.

To add several Devices or a combination of Device types:

- 1 Create a definitions file, see the FAQ on page 176.
- 2 From **Locations Manager**, on the **Devices** pane, select a Host, then select **Options** |  **Host** |  **Add Device**.
- 3 On the **Add Device** screen, in the **Device Class** box list, select **Upload Definitions File**, then enter or browse to the correct file.
- 4 Click **OK** to save.

Adding Hosts


For larger installations, viewLinc provides the option of adding multiple Host machines. This allows you greater control over specific Devices (group management), and ensures more network stability.

For example, you may want to monitor Devices in multiple offices. Rather than connecting all Devices at each office location to the

Enterprise viewLinc Server network, set up Host machines at each office to which local Devices are connected. This setup allows you to:

- Manage Devices more effectively (such as pausing alarming at one office, rather than trying to pause alarming on specific Devices on a remote server).
- Ensure that network traffic is distributed more evenly throughout your network (Host machines can manage smaller groups of Device data, before sending to Enterprise viewLinc Server).

To add a host machine:

- 1 From **Locations Manager, Devices** pane, select **Options |  Add Host**.
- 2 On the **Add Host** window, enter the hostname or IP address.
- 3 Click **OK**. The viewLinc system discovers the Host and all Devices residing on it. Device Discovery 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.
- 4 Click **Yes** when prompted to refresh.

Controlling Access to viewLinc

Administrators define who has access to viewLinc functional areas by creating Users and Groups, and assigning an access permission hierarchy. This hierarchy provides flexibility when assigning specific Users or Groups viewLinc tasks they need to perform, and which Locations or Zones you want them to access.

Each User and Group is assigned a permission hierarchy which is made up of:

- **Rights:** Defines **access** to functional areas in viewLinc (windows).
- **Access Control:** Grants **permission** to a Location or Zone.

For example, if a User is assigned the Right, Manage Devices, in order to perform the tasks in the Locations Manager window, the

User must also be added to the Access Control list for specific Locations. Setting up access controls in viewLinc involves these tasks:

- Assigning Rights
- Setting Access Control Permissions
- Creating Groups and Adding Users
- Editing Users and Passwords
- Setting Up Schedules

Assigning Rights

Rights are assigned to Users or Groups, and give individual Users or all Users in a Group the ability to perform certain functions in viewLinc.

Note: By default new Users are automatically part of the default Everyone Group with the Right, Manage Events (allows you to see **Events** window).

Right	Description
Manage Alarm Templates	Configure Alarm Templates
Manage Comments	Define preconfigured Comments
Manage Devices	Edit Device settings, swap Devices, deactivate/reactivate, set Device alarm settings, pause/resume, edit Channel description and alias. Edit and set up Transfers, and deactivate scheduled Transfers.
Manage Events	Add custom Events, add comments to events, print event reports, export event details to a spreadsheet for analysis
Manage Locations	Add, cut, delete, rename, unlink or deactivate Locations and Channels.

Right	Description
Manage Reports	View and configure Reports.
Manage System	Configure system settings: Email & SMS settings, Users & Groups, Schedules, Email templates.
Manage Threshold Templates	Configure Threshold Templates.
Manage Views	Create new views, add zones, rename zones, define access to the zone, add dashboard images, monitor trends.

Once a User is assigned a Group and Rights, the Rights of that User is actually a combination of the assigned User rights plus his/her Group rights.

For example, if User1 has Manage Devices Rights and is assigned to Group1, which has Manage Locations Rights, the Rights for User1 are Manage Locations and Manage Devices.

Note that access to Locations is permitted by Access Control List (ACL).

Access Control Permissions

After being granted Rights to access specific tasks within viewLinc program windows, the Administrator can then grant Users or Groups Access Control permission.

This permission allows the Administrator to specify which Users or Groups have access to view or perform tasks for specific Zones or Locations.

viewLinc offers several Access Control privileges, as outlined in the following table:

Permission	Definition
Hide	All Access Control permission disabled. Since Access Control is inherited from the top Zone down, the Administrator can use this permission to hide specific Locations within a Zone or Sub-zone.
Full Control	User can view the Zone/Location, acknowledge alarms, and, if assigned Manage Locations Right, can configure custom Threshold alarm settings and apply alarm schedules.
Configure Alarms	User can view the Zone/Location, acknowledge alarms, and, if assigned Manage Locations Right, can also apply alarm schedules.
Configure Custom Thresholds	User can view the Zone/Location, acknowledge alarms, and, if assigned Manage Locations Right, can configure custom Threshold settings.
Acknowledge Alarms	User can view a Location, and acknowledge alarms at Location.
View	Basic view permission.

With this combined control system, the Administrator can define specific activities that can be performed by each User or Group.

Important notes about assigning Access Control

- Admin Users and Users that belong to the Admin Group automatically have full access to all functions and Locations in viewLinc; Access permissions are ignored.
- If you assign a User **Full Control** for a Zone, all sub-zones and Locations inherit the **Full Control** setting.
- The effective User Access Control permission, with multiple User- and Group-level permissions defaults to the highest setting. For example: If you assign a User **View** permission to a Location, but one of the Groups that the User belongs to has Full Control for the

same Location, the User would have Full Control to the top-level Location, System.

Note: Use the Access Control Inspector tool to quickly determine which Users or Groups have access to your Zones and Locations.




- The **Hide** permission overrides all other Access Control permissions. It is available to help you handle exceptional cases, such as when you want to give a Group Full Control to a Location, but want to Hide the Location from a specific User in that Group.

Access Control Inspector

For large organizations with multiple Zones or Locations and specific access control requirements, the Access Control Inspector provides you with a quick way to view and modify the currently applied permissions.

Note: You require Manage Locations Right to use the Access Control Inspector.

To open the Access Control Inspector:

- 1 From the viewLinc desktop, select **Options** |  **System Configuration** |  **Locations Manager**.
- 2 In the **Location Properties** pane, select the **Access Control** tab, then choose **Options** |  **Access Control Inspector**.
- 3 In the **Available Groups/Users** column, select a Group or User. Assigned Zones/Locations and the permission level appear in the Locations panel.
- 4 To filter the Available Groups/Users list, choose a selection from the Options menu (All, Groups, Users).

Creating Groups and Adding Users

Groups functionality allows the viewLinc Administrator to assign Rights to multiple Users at one time. This is a quick method of

configuring access rights for multiple Users, and permits the addition of individual User rights as needed.




Even if you have less than 10 Users in your viewLinc system, defining tasks by Group is recommended. Once a Group is set up, the Rights assigned to the Group define which areas of viewLinc the Users in the Group can access.

By default there are two default Groups available when you first install viewLinc, with default Rights preassigned:

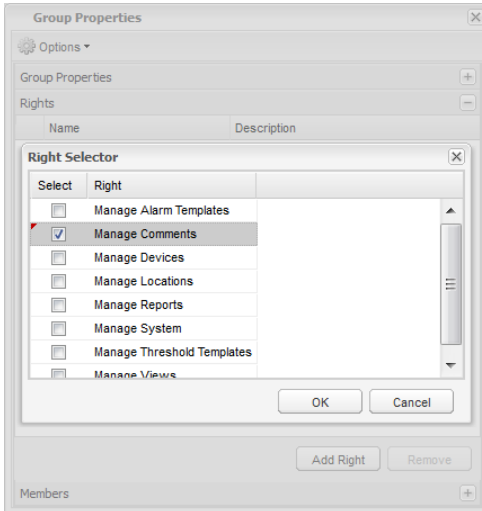
- **Admin:** A User set up as the Administrator is automatically assigned to the default Admin Group. This User, and anyone else assigned to the Admin Group, has the Right to access all windows, perform any function within viewLinc, and manage any Location.
- **Everyone:** All non-admin Users are automatically assigned to the second default Group, Everyone. This Group has the Right to access the Locations and Events windows, but have not been assigned Access Control to perform any functions or manage any Locations.

Create a Group

To create a Group:

- 1 From the viewLinc desktop, select **Options** |  **System Configuration** |  **Groups**.
- 2 On the **Options** menu, select  **Add Group**.
- 3 Complete the **Group Name** and **Description** fields.
You may want to use the Description field to indicate the Rights that will be assigned to the Group, or the primary job function of the Group, such as Threshold Monitoring.
- 4 To define Group Rights, click the plus sign on the lower bar labeled **Rights**, then click **Add Right**. If no Rights are assigned, these Users are automatically only able to view Events in the Events window.
- 5 Choose from the following options (see page 39 for a complete description of each Right):
 - Manage Alarm Templates
 - Manage Comments
 - Manage Devices

- Manage Events
 - Manage Locations
 - Manage Reports
 - Manage System
 - Manage Threshold Templates
 - Manage Views
- 6 Click **OK** to add the Right to the Group Properties list, then click **Add Right**.







- 7 To assign Users to this Group, expand the Members view (+) then click **Add User**.
- 8 Select the Users you want to include in this Group, then click **OK**. The members of the selected Groups and their group rights now appear in the Member section.

Deactivate/Reactivate a Group

With Groups functionality, you may find it useful to deactivate a Group, rather than deactivating the Rights and Access Control Permissions of Users individually.

To deactivate or reactivate a Group:




- 1 From the viewLinc desktop, choose **Options** |  **System Configuration** |  **Groups**.
- 2 Select the Group you wish to deactivate/reactivate.
- 3 Select the **Options** box in the Groups window and select  **Deactivate Group**.
- 4 To reactivate a Group, select **Options** | **Show Deactivated Groups**. Follow steps 1 to 3 then select  **Reactivate Group**.

Add a User

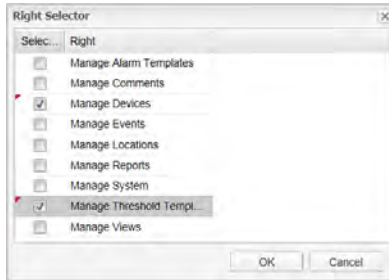
Before you add Users to your system:


- Determine whether you need to set up Group.
- Determine which Rights you want to assign to the User.

To add a new viewLinc User and assign access rights:

- 1 From the viewLinc desktop, choose **Options** |  **System Configuration** |  **Users**.
- 2 To check that the User does not already exist, perform a search on the User Name or Full Name:
 - In the Search field at the top of the window, enter the User Name or Full Name, then click the Search icon (magnifying glass).
 - Click the 'x' to clear the field and display the full list of Users.
- 3 On the **Options** menu select  **Add User**.
- 4 In the **User Properties** window, complete the following:
 - **User Name** and **Full Name**: Enter the User name for login, and a full name, if required.
 - **Email, Mobile number** and **PIN**: Use these fields to include additional contact details (for receiving reports, alarm notification or acknowledgement).
 - 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).
 - Enter a PIN number with 4 to 6 digits, between 1000 and 999999.
 - **Schedule:** Click the **Schedule** box to select a specific time period to contact this User. To define a Schedule, see “Setting Up Schedules” on page 48.
- 5 Set the password manually by entering and confirming it, or select **Windows Authentication** to use Windows authentication instead.
 - 6 To define the User’s system rights, expand the Rights view.
 - a Click **Add Right** and select the rights required for this User.
 - b Click **OK**.



- 7 To assign the User to a Group, expand the Groups view.
 - a Click **Add Group** and select the Group for this User by clicking the checkboxes in the **Select** column.
 - b Click **OK**.
- 8 Click **Options** |  **Save**.





Note: You can require that Users re-confirm their identity (re-enter their user name and password) whenever a change is made, or after a set number of minutes. To set this preference, see “Session Expiry Time” on page 31.

Editing Users and Passwords

After creating new User accounts (see “Creating Groups and Adding Users” on page 42), you can modify account settings (such as password), or deactivate Users temporarily (useful for Users who may be going on holiday).




Note: To preserve your data history, Users cannot be deleted permanently.

To edit user accounts and passwords:





- 1 From the viewLinc desktop, choose **Options** |  **System Configuration** |  **Users**.
- 2 Select the User you want to edit, then choose **Options** |  **Edit User**.
Or, double-click the row containing the User you want to edit.
- 3 On the **User Properties** window, edit settings as needed.
- 4 Select **Options** |  **Save**.

Note: You can only edit passwords in viewLinc if you are not using Windows authentication.

To deactivate a User:

- 1 From the viewLinc desktop, choose **Options** |  **System Configuration** |  **Users**, select the User you want to deactivate.
- 2 Select **Options** |  **Deactivate User**.
- 3 Click **Yes** to confirm the change.

To reactivate a User:

- 1 From the viewLinc desktop, choose **Options** |  **System Configuration** |  **Users**, click **Options** |  **Show Deactivated Users**. All deactivated Users appear in grey text.
- 2 Select the User you want to reactivate, then choose **Options** |  **Reactivate User**.

Setting Up Schedules




There are two ways to use the Schedules function: to specify when you want Users to receive alarm notifications, and to schedule when you want Location threshold alarming active. Three status options are available (selected in the **State** field on the **Schedules** window):


- **Always:** Users are notified of alarm conditions at all times/Threshold alarming is continuously active.
- **Never:** Alarm notification is turned off (applies to User only).
- **Enabled:** Use a custom schedule. A custom schedule allows you to define specific times you want a User to receive alarm notifications, or a specific Zone or Location's Threshold alarming to be active. This could be a schedule of times and rotating dates to accommodate a User's availability. For example, to set up a User to receive alarm notifications only between 7 am and 7 pm (07:00-19:00) on a 4-day on, 5-day off rotation. Or, set up a Threshold Alarm schedule to only be active for specific shifts.

Alternatively, if a User goes on holiday, you can deactivate the User account temporarily (see “Editing Users and Passwords” on page 47), or, if a monitored area will be shut for maintenance temporarily, see “Deactivating and Reactivating Threshold Alarming” on page 83.

Note: To use Schedules, enable this feature in the **Options | System Configuration | Preferences** window. Schedules must then be set up before applying to a User's account.

To create a custom schedule:

- 1 From **Options |  System Configuration |  Schedules**, click **Options |  Add Schedule** (or use right-click menu option).
- 2 In the **Schedules** window complete the following:
 - **State:** Choose **Enabled**.
 - **Start Date:** Choose a start date by typing in the text box or choosing a date from the calendar.
 - **Repeat Days:** To repeat the schedule every 7 days, enter **7**. For 9 days, enter **9**. The maximum value is 99 days.

- **Time Zone:** Set the schedule times for the local time of the selected time zone.
 - **Time Periods:** Enter a time period in 24-hour time, in the following format: **xx:xx-yy:yy**, where **xx:xx** is the start time and **yy:yy** is the end time.
 - To send notifications during intermittent periods on a single day, separate time periods by a comma (for example, 08:00-12:00, 13:00-16:00).
 - To send notifications all day, enter 00:00-24:00.
 - If you do not want notifications sent at anytime on a specific day, leave the time period blank.
- 3 By default, your schedule is named **New Contact Schedule**. To rename it, double-click the row or select **Options | Rename**.
 - 4 Click **Options |  Save**.



Email & SMS Notification Settings

Alarm notifications are sent via Email or SMS. Administrators can define your system Email and SMS settings, such as the mail server and Email delivery addresses.

- To specify the contents of Email and SMS messages, see “Email & SMS Templates” on page 52.
- To control who receives alarm notifications, see “Setting Up Schedules” on page 48.
- To create an alarm threshold setting, see, “Threshold Templates” on page 58.

Define Email Notification Settings

To configure default Email settings for notifications:

- 1 From the viewLinc desktop, choose **Options |  System Configuration |  Email Settings**.

- 2 Enter the Administrator's Email address. This address receives all system notifications. You can specify who should receive email notifications at different times of day, and tiered email notification for multiple email notifications.



Note: The Administrator's Email address does not have to be a company email address. For convenience, viewLinc can issue emails to external email addresses, such as Administrator@gmail.com.

- 3 Enter a valid "From" address. Email notifications from viewLinc will be "from" this address, so the email address must exist within your company. Contact your IT administrator to create a "From" address if needed.

For example:




viewlinc_system@yourcompany.com or
controlroom47@yourcompany.com

- 4 In the **Outgoing Server** area, enter:
 - an outgoing SMTP mail server name (e.g., mail.yourserver.com)
 - an outgoing mail server Port (a number between 1-65535). Your IT Administrator will have this information.

- 5 If your outgoing mail server requires authentication, select the **SMTP Authentication** check box and enter the username and password to send mail on that server.
Note: viewLinc automatically uses secure SMTP if it is supported by the SMTP server.
- 6 If your outgoing mail server requires confirmation through a POP3 connection before sending mail (contact your IT network administrator for assistance), configure the following settings:
 - a Select **POP3 connection is required**.
 - b **POP3:** Enter the incoming POP3 mail server name.
 - c **Port:** Enter the incoming mail server port.
 - d Select **POP3 Authentication**, then enter a username and password for a valid POP3 account for the viewLinc system to use.
- 7 Select **Options** |  **Test Email** to test your settings. If they are OK, continue. If not, adjust the administrator Email address and verify the settings until the test Email is sent successfully.
- 8 Select **Options** |  **Save** to save the Email settings.

Define SMS Notification Settings

To configure default SMS settings:

- 1 From the viewLinc desktop, choose **Options** |  **System Configuration** |  **SMS Settings**.
- 2 Enter the **Administrator's mobile number**.
- 3 Enter your modem **SMS COM port** number.
- 4 Select an option from the **SMS port baud rate** box list. Select the rate which is best supported by your modem.
- 5 Enter the **SIM Card PIN** number (if required).
- 6 Select **Options** |  **Save**.

Templates

Templates are used to quickly define the information required for distribution in standard email and SMS messages, alarm notification requirements, and Location threshold values:

- **Email & SMS Templates:** Defines standard email or SMS notification content for a viewLinc alarms.
- **Alarm Templates:** Defines how alarm notifications display on a User's PC, when an alarm should activate, whether acknowledgement is required for a specific type of alarm.
- **Threshold Templates:** Defines units of measure (temperature only), Threshold values for single or multi-threshold alarms, display parameters for specific types of Thresholds. Threshold templates are applied to Locations.

Email & SMS Templates

Alarm notifications are issued by Email and/or SMS, and contain information about alarm conditions in your network (see "Types of Alarms" on page 118). viewLinc provides you with more than 40 Email and SMS templates to use as is, or you can create custom message content.

When creating custom Email and SMS templates, you can choose to include or not include specific content items, for example:

- Device description
- Event Type
- Details of Alarm
- Date
- Time
- Channel
- Comments (custom or preconfigured comments)

Note: Message content options differ between templates.

To create custom Email or SMS template messages:

- 1 From the viewLinc desktop, choose **Options | System Configuration | Templates | Email/SMS Templates**, then select the row containing the template you want to assign a custom template.

Using Custom	Template Name	Default Email Subject	Default Email Body	Default SMS Text	Custom Email Subject	Custom Email
No	Device Communication Alarm	viewLinc - Communication Alar	There has been a communication alarm on [Ala	Communication Alarm on [Device		
No	Device Communication Repeat Alarm	Repeat viewLinc - Communicat	Repeat message: There has been a communic	Repeat: Communication Alarm on		
No	Device Communication Repeat Alarm	viewLinc - Communication Res	Communication received on [AlarmCharacter	Communication Alarm received in		
No	Heat Communication Alarm	viewLinc - Communication Alar	There has been a communication alarm on [Ala	Communication Alarm on Heat [E		
No	Heat Communication Repeat Alarm	Repeat viewLinc - Communic	Repeat message: There has been a communic	Repeat: Communication Alarm on		

- 2 On the **Options** menu, select **Edit Email Template**, or double-click the row to open the template window.
 - The standard template contents appear in the **Default Messages** area (no changes are permitted to default message content).
 - Items in [square brackets] are variables that are generated automatically.
- 3 To add new message content, go to the **Custom Messages** area and start typing in the **SMS Text:** field or **Email Subject/Body:** fields.
- 4 To add auto-generated variables, move the cursor to the location where you want to add the variable, then select **Options | ★ Macros**.
Select a variable from the box list (different macros are available depending on the template). For a complete list of Macro definitions see page 186.
- 5 Select the **Enable Custom Messages** checkbox (top right corner of window).
- 6 Click **Options | Save**.

Alarm Templates

An Alarm template allows you to configure and apply similar alarm settings to multiple Locations. With the Manage Alarm Templates Right, you can create new templates, or modify the default templates provided for these alarm types:

- Communication

- Configuration Changed
- Device Calibration
- Device Configuration
- Device Validation
- Event Validation
- Threshold

Note: Alarm templates (standard messaging and notification) work in conjunction with Threshold templates (reusable condition limits).





Alarm Template Options

When creating alarm templates, there are many ways to define how Users view alarm conditions on their desktop, the contents of an alarm notification message, and when you want to send an alarm notification to a single or multiple Users.



For example, you could create a notification for the first recipient with a short delay period, perhaps 1 minute. Create another email notification for 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.

To create or modify alarm templates, User must have Manage Alarm Templates Right assigned. To apply alarm templates to specific Locations, User must have Manage Locations Right and Configure Alarms permission assigned for on all Locations where you want to apply the template.

To create a new alarm template:



- 1 From the viewLinc desktop, choose **Options** |  **System Configuration** |  **Templates** |  **Alarm Templates**, select **Options** |  **Add Alarm Template**.
- 2 Click in the title to enter a specific title, then press **[Enter]**.
- 3 On the **General Parameters** tab, define the following:
 - **Color:** Choose the color to display as the background color for a row in Locations window. This color is also used as the background color for a Location Value in a

Pop-up Trend, as a threshold line color, or as a dashboard Location color. Use color codes to indicate alarm severity, starting with blue for less serious alarm conditions, escalating to red for the most serious alarm conditions.

- **Alarm Message:** If you want an Email or SMS notification sent out when an alarm is triggered (as set up on the Notifications tab), enter the message you want to appear in the alarm notification. The contents of the Alarm Message field appear in the body content area of the default Email notification template for the specific type of alarm (using the AlarmMessage macro - see “Email & SMS Templates” on page 52).
 - **Delay Before Activating Alarm (HH:MM):** If desired, specify a delay period, in hours and/or minutes, from when a condition exists and you want the alarm triggered.
 - Notification delays are also set on the Notification tab. If you enter a time delay on the General Parameters tab, ensure the combined time delay does not interrupt your alarm notification requirements.
 - **Acknowledgement Required:** Select this option if you require an individual to acknowledge an alarm (by responding to an acknowledgement request appearing on the viewLinc screen, remote display, in an Email or SMS text). If you select this option, the alarm will remain active until it is acknowledged. If the alarm condition is no longer present, the unacknowledged alarm notification remains in the Alarms window.
- 4 To make an alarm notification open in a pop-up window on a User’s viewLinc desktop or remote display, click the **Notifications** tab, then click  **Add**, then select  **Add Pop-up Notification**. Complete the following field:

Delay before popping up: Indicate a delay, in hours and/or minutes (HH:MM), before you want the pop-up to display. This delay starts after the delay on the General tab finishes (if one is specified).

Note: We recommend that you use this feature sparingly. If many pop-ups are triggered at the same time, it can disrupt your browser operation and you may need to restart your browser.

- 5 To send an alarm notification by email, on the **Notifications** tab click  **Add**, and then select  **Add Email Notification**. Complete the following fields:

Delay before sending first notification: Indicate a delay, in hours and/or minutes (HH:MM), before you want the first email sent. If you specified an alarm trigger delay on the General tab, ensure the combined time delay does not interrupt your alarm notification requirements.

Send email to: Enter one or more addresses that are not pre-configured in viewLinc. Separate multiple email addresses with commas.



IMPORTANT: If you enter a preconfigured viewLinc User's email address in the **Send email to** field, viewLinc ignores assigned schedules.

User List: Click in this field to open the **Group/User Selection** window, then drag viewLinc Users or Groups across to the **Selected Groups/Users** column. You can reorganize the list order using the arrow buttons, for easier display. Click **OK**.

Repeat email notification: Choose an appropriate interval for the frequency emails are resent while the condition still exists. You may want to use the **Maximum Number of Repeats** field to specify a maximum number of repeat emails that should be sent (enter zero, 0, to allow infinite repetition).

Pause notifications after acknowledgement: Select an option to allow, pause or prevent repeated distribution of Email and/or SMS alarm notifications.

Notify....: Select the corresponding check box to send an email when an alarm is acknowledged, or when the condition no longer exists.

- 6 To trigger a command on the viewLinc Server, on the **Notifications** tab click  **Add**, and then select  **Add Command Notification**. Complete the following fields:

Delay before running first notification command: To specify a delay before the command runs, enter a delay period in hours and/or minutes (HH:MM).

Note: If you have set the Delay Before Activating Alarm option (on the General Parameters tab), ensure the combined time delay does not interrupt your alarm notification requirements.

Run command text fields: Enter DOS commands to run different commands when an alarm is triggered, a notification is repeated, an alarm is acknowledged, or an alarm condition is no longer true.

For example:

```
C:\Program Files\Veriteq Instruments\viewLinc\python\python" -m
viewLinc.scripts.SwitchBbRelay <number of com
port where relay Device is attached>
```

Option as specified in script documentation. See the script documentation in, "APPENDIX: FAQs & TROUBLESHOOTING" on page 167. The example above shows a Python script specific to a Digital Relay I/O Device. Different parameters apply to different commands or scripts.

- 7 To add specific comments to the alarm notification, click the **Comments** tab. Select a comment from the **Preconfigured Comments** drop-down list, if any are available, or enter a new comment.

Note: How comments appear in an Email notification is defined by the Email template associated with the Alarm event (**System Configuration | Templates | Email Templates**). For more information see "Email & SMS Templates" on page 52).

- 8 When alarm settings are complete, select **Options |  Save**.





You can now apply this alarm template to one or more Devices or Locations (see "Threshold Templates" on page 58 or "Using Pre-configured Comments in Templates" on page 62).

Note: To list all Locations and Devices currently using the selected Alarm template, select Options | Devices and Locations Using Template.

To edit a default or custom alarm template:

Note: User requires Configure Alarms permission for the Location to which the alarm template is assigned.

IMPORTANT: Before making changes to a template, check which Devices and Locations are using the template (in the Alarms window, right-click on an alarm template to select **Devices and Locations using template**).

- 1 From the viewLine desktop, choose **Options** |  **System Configuration** |  **Templates** |  **Alarm Templates**, select the Alarm template you want to modify.
- 2 Make the required changes as outlined in steps 3 to 8 starting on page 54.
- 3 Select **Options** |  **Save**.

Threshold Templates

Threshold settings are assigned to Locations, to define the conditions that trigger alarms. For example:

- Greater than 23.00 C for more than 1 minute, or,
- Less than 37.76 RH for more than 15 minutes

Threshold settings can be applied with or without templates, but a Threshold template makes it easy to apply similar parameters to several Locations, with single or multiple-threshold settings.

Users with can create a new Threshold template, or simply modify one of the two default templates, High Temp and Low Temp.

Note: If threshold settings are applied to a Location, and conditions exceed these settings, the Default Threshold Alarm Template is automatically activated. To learn about Alarm Template settings, see “Alarm Templates” on page 53.





Alarm settings can indicate whether the alarm is a mild concern (indicated with a yellow bar, perhaps when conditions are nearing

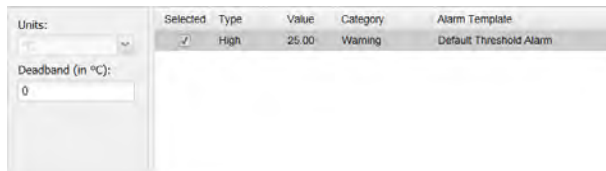
Threshold) or an extreme concern (indicated with a red bar, when a condition exceeds Threshold).

For example, you could set a yellow alarm to trigger first, automatically sending an email to someone who needs to know within a few minutes of the minor condition alert. For a red alarm, you could set the alarm condition to a longer time (15 minutes out of threshold) and send the email to a lab manager, or a distribution list of people who need to be notified to take action.


Single Threshold Template

To create a single-threshold template:

- 1 From the viewLinc desktop, select **Options** |  **System Configuration** |  **Templates** |  **Threshold Templates**.
- 2 To modify an existing default High or default Low templates, select the template and then set the threshold condition as in steps 4 to 6.
- 3 To create a new template, click **Options** |  **Add Single-Threshold Template** (or use the right-click menu). Double-click anywhere in the title to change it.
- 4 Set the Threshold conditions:



- **Units:** Select the Channel's measurement units.
- **Deadband:** Specify the measurement range you want viewLinc to ignore (this range accommodates minor fluctuations which you do not want to trigger an alarm).
- **Type:** Identify the threshold as a High limit (High or HighHigh), or Low limit (Low or LowLow), or, indicate the rate of change in units (ROC Units). 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 refrigerator door is opened.





- **Value:** Enter the threshold limit.
 - **Category:** For reporting purposes, specify whether a Warning message or an Alarm notification is issued when threshold condition is met.
 - **Alarm Template:** Choose an existing Alarm Template you want assigned to the Threshold Template (the Alarm Template defines how the Threshold Alarm displays, and who is notified when a Threshold is reached). Choose Private to create custom Alarm settings you want applied to a single Location to which you have been granted Access Control permission.
- 5 To define a custom (Private) Alarm template, or modify existing Alarm Template settings, complete the fields in the General Parameters, Notifications, and Comments tabs.
- Note:** You require Manage Alarm Templates Right to modify existing Alarm Templates. For more information, see “Alarm Templates” on page 53.
- 6 When you finish creating your Threshold template, click **Options** |  **Save.**

To apply the Threshold template to a Location, see “Setting Up Location Thresholds” on page 80.

Multi-threshold Template

A multi-threshold template can have up to five threshold settings.

To create a multi-threshold template:

- 1 From the viewLinc desktop, select **Options** |  **System Configuration** |  **Templates** |  **Threshold Templates.**
- 2 In the Threshold Templates window, click **Options** |  **Add Multi-Threshold Template.**
- 3 Double-click anywhere in the title to change it.
- 4 Set the Threshold conditions:




- **Units:** Select the Channel's measurement units.
- **Deadband:** Specify the measurement range you want viewLinc to ignore (this range accommodates minor fluctuations which you do not want to trigger an alarm).
- **Type:** Identify the threshold as a High limit (High or HighHigh), or Low limit (Low or LowLow), or, indicate the rate of change in units (ROC Units).

Note: Rate of change measures the amount of variation recorded in one (1) minute. For example, you may want to know how quickly the temperature in a refrigerator rises when the refrigerator door is opened.

- **Value:** Enter the threshold limit.
- **Category:** For reporting purposes, specify whether a Warning message or an Alarm notification is issued when threshold condition is met.
- **Alarm Template:** Choose an existing Alarm Template you want assigned to the Threshold Template (the Alarm Template defines how the Threshold Alarm displays, and who is notified when a Threshold is reached). Choose Private to create custom Alarm settings you want applied to a single Location to which you have been granted Access Control permission.

- 5 To define a custom (Private) Alarm template, or modify existing Alarm Template settings, complete the fields in the General Parameters, Notifications, and Comments tabs.

Note: You require Manage Alarm Templates Right to modify existing Alarm Templates. For more information, see “Alarm Templates” on page 53.

- 6 When you finish creating your Threshold template, click **Options** |  **Save**.

To apply the Threshold template to a Location, see “Setting Up Location Thresholds” on page 80.




Using Preconfigured Comments in Templates

Email/SMS templates using the [Comments] variable, automatically include either preconfigured comments, or custom comments. The type of Comments retrieved are defined in an Alarm Template (see “Threshold Templates” on page 58).

For example, if you set up a Communication Alarm (Alarm Template) with a notification requirement to send an Email to a specific User when it is triggered, the preconfigured or custom comment assigned to the Communication Alarm template appears in the Email notification.

Note: Preconfigured comments can also be used in the Event Log to provide more information in reports. See “Adding Comments to Events” on page 133.




To create a preconfigured comment:

- 1 From the viewLinc desktop, choose **Options** |  **System Configuration** |  **Comments**, select **Options** |  **Add Comment**.



- 2 In the box that contains the text, **New comment**, enter your comment and press **[Enter]**. The new comment is saved automatically.

To delete preconfigured comments:

- 1 From the viewLinc desktop, choose **Options** |  **System Configuration** |  **Comments**, highlight the comment to delete.
- 2 Click **Options** |  **Delete**.

To use preconfigured comments in an alarm template:

- 1 From the viewLinc desktop, choose **Options | System Configuration | Templates | Alarm Templates**, highlight a template, then click the **Comments** tab.



- 2 On the Comments tab, select a comment from the **Preconfigured Comments** drop-down list. Your preconfigured comments appear in the Comments field, allowing you to make additional changes to the text, if required. Alternatively, enter your own message in the Comments field.
- 3 Click **Options | Save**.

To use preconfigured comments in an Email template:

- 1 From **Options | System Configuration | Templates | Email/SMS Templates**, double-click the Email template you want to edit.
- 2 In the Custom Messages area, in the Email Message Body field, ensure the [Comments] variable is present. To add it to your template, select **Options | Macros | Comments** (see “Email & SMS Templates” on page 52). The preconfigured comment you selected in Communication Alarm settings is inserted in the Email message when it is sent.
- 3 Click **Save**.

For information on setting Device and Host communication alarms, see “Setting Up Device and Host Alarms” on page 105.

System Maintenance



Occasionally, you may want to take viewLinc offline, or complete a reboot of your system (this does not affect the data tracking of your Devices).

You can choose to restart or stop the viewLinc service temporarily (see APPENDIX: FAQs & TROUBLESHOOTING).



These system changes are recorded in the Event Log.

Note: Only a member of the Admin Group can perform this task.

To restart viewLinc service on the Server machine:

- 1 From the viewLinc desktop, choose **Options |  System Configuration |  Preferences**.
- 2 Click **Options | Restart viewLinc Service**. An event message is generated and an email is sent to the viewlinc Administrator (according to the email address specified on the Email Notification Settings window).

To restart a viewLinc Logger service on a Host machine:

- 1 From the viewLinc desktop, choose **Options |  System Configuration |  Locations Manager**.
- 2 In the **Devices** tree, select a Host.
- 3 In the **Device Properties** pane, select the **Host Details** tab.
- 4 Click **Options | Restart Host Service**. A system-wide message alerts all logged in Users that viewLinc is about to restart.

CHAPTER 3

VIEWING DATA

In viewLinc, each data collection point (Device Channel) is mapped and identified as a Location. These data collection points are viewable in the viewLinc Locations window.

For organizations with several Devices in multiple locations (offices, laboratories, warehouses), you may want to create Zone and sub-Zone folders to help you easily identify the areas where data is collected.

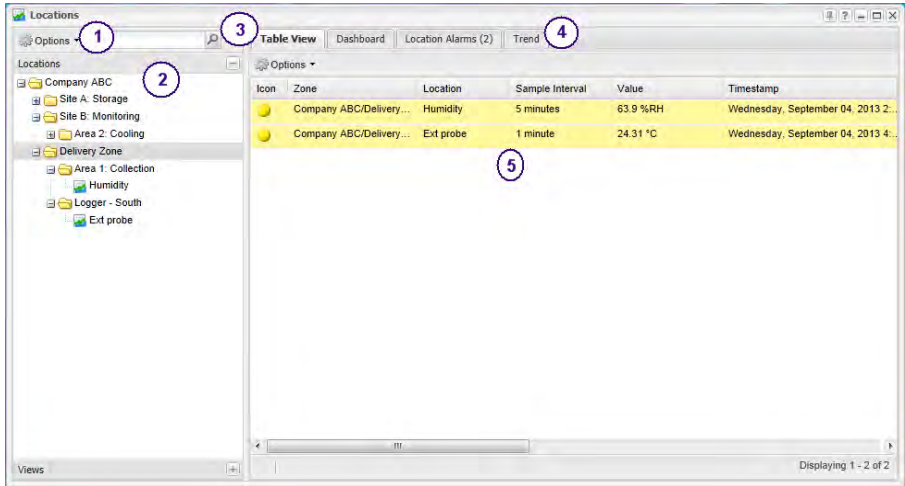
This chapter provides you with information about:

- viewLinc Desktop Orientation
- Managing Locations & Zones
- Editing Location Properties
- Building Dashboards
- Setting Up User-specific Views
- Working with the Locations window

viewLinc Desktop Orientation

When you first log in to viewLinc, the **Locations** window appears automatically. All Users can view this window and access the window elements and tabs.

In the left Locations pane, Users view a list of the Locations, and Zones that they have been authorized to view (set up by the Administrator). This navigation pane can be expanded or collapsed to reduce visual clutter, and can be customized so a User only views specific areas of interest (see “Setting Up User-specific Views” on page 86).



Item	Details
① Options	Context-sensitive menus. The menus change depending on which tab is open and which item is selected within the tab. There is also an Options menu for the Locations tree/navigation pane.
② Locations	Navigation pane (tree view): <ul style="list-style-type: none"> • Zones display as 📁 • Locations display as 🏠 (if you have a small installation, Zone folders may not be required, and you only see a list of Locations). • To view Locations in alphabetical order, select Options Sort Ascending/Descending.
③ Search	Search for Locations. Enter a search term in the text box and then click 🔍 (hover your mouse over the icon for search tips).

Item	Details
④ Tabs	<p>Main viewLinc function tabs.</p> <ul style="list-style-type: none"> • Table View: View and monitor data from Zones and/or Locations • Dashboard: View a graphic interface (imported image) identifying your Devices (to add an image see “Adding a Dashboard Image” on page 84). • Location Alarms: View active alarm events. • Trend: Combine, contrast and compare Location history in visual graphs with real-time data (see “Building a Trend” on page 91).
⑤ Location Details	The Table View tab displays Location details: alarm status, configuration, path, current data reading, latest timestamp, and threshold information.


Working with Columns

Most columns in the Table View, Location Alarms and Trend tabs are self-explanatory; however, here are a few column definitions to help you get more familiar with viewLinc columns.

To see all column options available, see page 68.

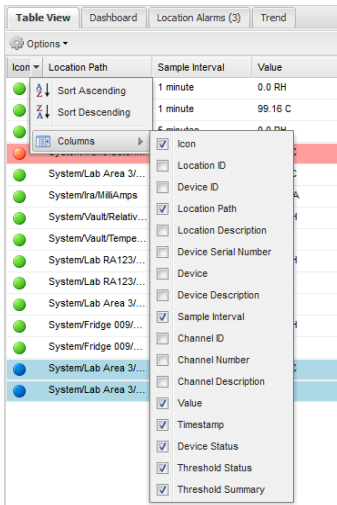
Column	Displays
Icon	The color coded icon associated with the alarm status of the Location. See “Alarm Templates” on page 53.
Timestamp	Time that the last reading was taken.
Device Status	The current status of the Device. Displays errors if the Device is inactive.
Threshold Status	“OK” appears if there are no currently active alarms. Changes to indicate if a threshold alarm condition has been detected.

To re-sort column display order:

- 1 In the **Locations** window on the **Table View**, **Location Alarms** or **Trend** tabs, right click on a column heading (Trend tab columns are: **Locations**, **Group Statistics**, **Scale** in lower half of screen).
- 2 On the menu that appears, click the  to select **Sort Ascending** or **Sort Descending**, or, click on any column header to sort all the rows using that column (up/down arrow indicates direction). Click again on the column header to sort the list in the opposite order.

To hide columns:

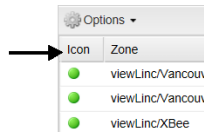
- 1 From any tab in the Locations window, let your mouse hover over a column heading, then click the black down arrow that appears.



- 2 Select **Columns**, then select the columns you want to display or deselect columns you want to hide.

For example, to show a column with colored icons representing alarm status, select **Icon**.

Click the heading to sort in ascending or descending order.



- 3 Click outside the list, or press **[Esc]** to hide the options list.

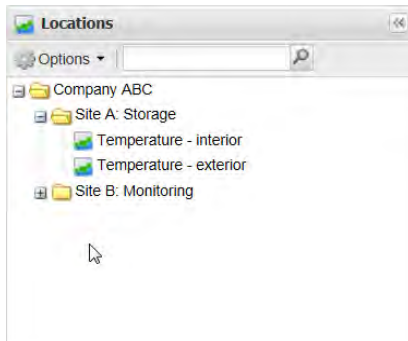
Managing Locations & Zones

In general, each Vaisala Device is set up to monitor a specific physical location; however, depending on your Device configuration, you could use one Device to monitor multiple physical locations.

For example if your Device has more than one Channel, (Devices have up to five active data collection points), using Location and Zone folders, you can control how this information displays on the viewLinc desktop.

Note: 300 Series Transmitters Output Quantities are displayed as Locations.

For example, if you have a Device with two temperature Channels, you might view these data points in the Locations navigation tree as:



By identifying Locations in Zones you can also:

- Ensure that reporting is consistent for a specific Zone, regardless of the Logger used to monitor that data location.

- Swap a Device easily from one Zone to another (perhaps when sending a Logger out for calibration).

Organizing Locations

To organize your viewLinc screen and keep a closer eye on the Locations that matter to you, organize your data into relevant Zones using the Locations Manager. Users assigned Manage Locations Right can access the Locations Manager window. Users can only organize the Locations and Zones to which they have been assigned Full Control Permission (see “Access Control Permissions” on page 40).

Use specific areas of the Locations Manager window to organize and view your data:

- **Locations** (left pane): Add or delete Locations, and link or unlink Channels to Locations. Location details are viewed in the Location Properties window.
- **Devices** (middle pane): View and configure Devices currently connected to the viewLinc system, and the Channels associated with each Device.
- **Location Properties** (upper right pane) tabs:
 - **Properties:** Displays extended information regarding a selected Location. It allows you to edit Location properties, and sort and group Locations (useful for larger Zones).
 - **Location Devices:** Lists the Device Channels connected to a selected Zone or Location. Use the Options menu to select, **Include Link History**, to identify all Locations to which the Channel has been linked, and for which period of time.
 - **Access Control:** Allows you to view currently assigned User and Group access permissions (see “Assigning Access to Locations & Zones” on page 79), and add individual User or Group access permission to a specific Zone or Location. This functionality compliments the User and

Group Rights, allowing for greater customization and flexibility.

- **Thresholds:** Allows you to view and add Thresholds (less than or greater than values for associated measurements) to selected Locations. See “Setting Up Location Thresholds” on page 80.
- **Dashboard:** Allows you to load an image for a physical location, such as a facility map. Data readings from Locations where data is being collected can be dragged over to the image for a more accurate visual display of where data is being recorded. See “Adding a Dashboard Image” on page 84.
- **Device Properties** (lower right pane) tabs:
 - **Device Details:** View and modify specific Channel properties.
 - **Host Details:** Use the Options menu to restart the Host Service (as required), or modify communication properties. With the right-click menu on a selected Host, you can also test network communications (ICMP Ping Host), or activate automatic identification of vNet devices (Enable viewLinc Aware Service).

Creating Zones




By default, there is one Zone folder created automatically, System. It can be renamed at any time, perhaps with your company name.

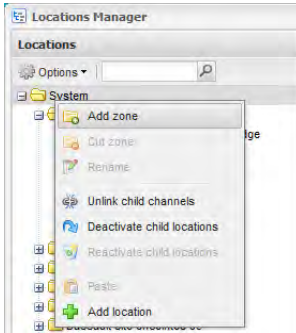
Additional Zones are created manually. You can quickly add a Location to a Zone with the right-click menu option, **Add Location**, or drag a Channel or Device to the new folder.


Note: If no Devices display in the middle **Devices** pane, your Devices may not be connected properly. For Vaisala Veriteq Devices, try Discovering Devices - see “Discovering Devices” on page 35, or contact your network administrator.

For more information about connecting Devices and enabling or disabling Channels, refer to the specific Device User Guides.

To add a Zone:

- 1 From the viewLine desktop, choose **Options** |  **System Configuration** |  **Locations Manager**. Right-click the System folder and select  **Add Zone**.



- 2 When the New Zone folder appears, enter a name for the Zone and press **[Enter]**. To create a sub-Zone, select the Zone parent, then complete steps 1 and 2 for each sub-Zone you want to create.
- 3 Select **Options** |  **Save**.



Adding Locations to Zones

Because viewLine recognizes Devices regardless of their assigned Zone, Devices and Channels can be moved from one Zone to another, without losing any data history.

For example, if you need to move a monitored refrigeration unit to another physical location, in viewLine, simply move the Device Location data point to a different refrigeration Zone.

Note: Channels can only be linked to one Location at a time.

To add a Location to a Zone:

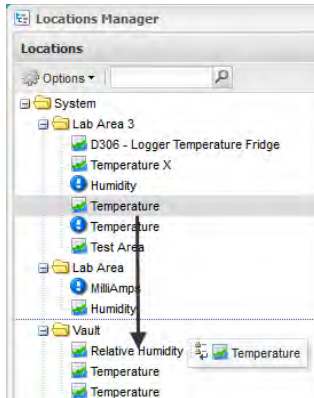
- 1 From the viewLine desktop, choose **Options** |  **System Configuration** |  **Locations Manager**.

- 2 In the **Locations** navigation pane, select a Zone (or the default zone, System), then right-click to select, **+ Add Location**.
- 3 In the **New Location** text box, enter the Location name, then press **[Enter]** or click outside the box. When a Location has no data source associated with it, a blue exclamation mark icon appears next to the Location title, **!**.
- 4 In the **Locations** navigation pane, select **Options | Save**.

To link a Channel to this new Location, see “Linking Location Channels” on page 74.


To move a Location:

- 1 Ensure a Zone is created for the Location data point (see “Creating Zones” on page 71).
- 2 To move a Location with drag and drop, simply select the Location you want to move, then drag the Location to the new Zone.







- 3 To move a Location manually:
 - a Right-click on the Location you want to move, and select **+ Cut Location**.
 - b Right click on the Zone you'd like to move the Location to, and select **+ Paste**.
- 4 Click **Options | Save**.

To create a Zone and Locations from a single Device:

- 1 Ensure a Zone is created for the Device (see “Creating Zones” on page 71).
- 2 Browse the Devices tree to select the Device you want, then drag the Device into the Zone.
- 3 At the prompt, select whether you want to automatically create a sub-zone based on the Device name, or simply paste all of the Device Channels to the Zone.
- 4 Click **Options** |  **Save**.

Linking Location Channels

To link an unlinked Channel to a new Location:

- 1 From the viewLine desktop, choose **Options** |  **System Configuration** |  **Locations Manager**, and ensure you have created a Location that you want linked to a Device Channel.
- 2 Navigate the **Devices** pane to locate the Channel. If you do not see any Devices listed, check the Options filter to ensure all Devices and Channels are visible. If you still don't see any Devices, contact your system administrator.
- 3 Drag the Channel (represented by the  **Channel** icon) from the **Device** pane and drop it into an unlinked Location in the Locations tree, identified with, .

The Channel is now linked with the Location you dragged it to.




Unlinking and Relinking Location Channels

If you want to link a Channel to a different Location, or if you no longer want a Channel associated with a particular Location, you can unlink it using the Locations Manager.

Channels can be unlinked individually, or you can unlink all Channels within a Zone. This option saves you time when you want to delete a specific Zone (the monitored area may no longer require monitoring).



For some organizations, the list of Locations and Zones is lengthy, and the first step is to identify to which Location a Channel is linked.

To find a Channel's linked Location:



- 1 From the viewLinc desktop, select **Options** |  **System Configuration** |  **Locations Manager**.
- 2 In the **Devices** tree, navigate to a linked Channel, identified with the checked graph icon, .
- 3 Right-click to select **Find Linked Location** (alternatively, select a Location, right-click and select **Find Linked Channel**). The 'found' Location is highlighted with a yellow bar in the Locations tree.

Note: If you do not see a yellow highlight bar, the Location may already be selected (grey highlight bar), or you do not have the required Access Control permission to view the linked Location.

To unlink a Channel:


- 1 Navigate the **Locations** tree in **Locations Manager** to find the Location with the Channel you want to unlink.
- 2 Right-click and select  **Unlink Channel**.
- 3 A prompt appears asking you to confirm that you want to unlink the Location. Click **Yes**. The Channel is now available to link with another Location.
- 4 On the Locations pane, select **Options** |  **Save**.

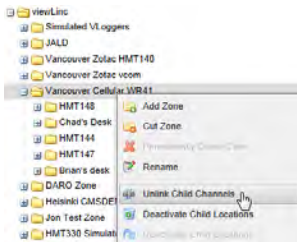
To relink a Channel

- 1 To display available unlinked Channels, in **Locations Manager** on the **Devices** pane, select **Options** | **Show Unlinked Only**.
- 2 Select an available Channel, and drag it over to the unlinked Location (indicated by a .
- 3 On the Locations pane, select **Options** |  **Save**.

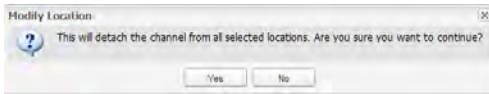
To unlink all child Locations in a Zone:


Note: These steps are required if you want to delete a Zone (see page 77).

- 1 In **Locations Manager**, navigate the **Locations** tree to find the Zone with the Locations you want to unlink.
- 2 Right-click to select  **Unlink Child Channels**.



- 3 A prompt appears. Click **Yes** to confirm the change.



- 4 In the Locations pane, select **Options** |  **Save**.




To view the link history of a Channel:


- 1 In **Locations Manager**, navigate the Locations tree to select a Location to view.
- 2 On the **Location Properties** pane, select the **Location Devices** tab.
- 3 Select **Options** | **Include Link History**.

The Start and End columns display the link history. If the Start value is blank (o), this Channel has remained linked to the current Location since it started monitoring data.

Renaming Locations and Zones

To rename a Zone or Location:

- 1 From the viewLinc desktop, choose **Options** |  **System Configuration** |  **Locations Manager**, and then highlight the Location or Zone you want to rename.
- 2 Right-click the Location or Zone and select  **Rename**.

- 3 With the existing name highlighted, enter the new name.
- 4 Press **[Enter]** or click outside the dialog box, then select **Options** |  **Save**.

Note: Renaming Zones edits the Zone name only; it does not change the Locations assigned within it. To link or unlink Locations to a Zone, see “Adding Locations to Zones” on page 72.



Deleting Zones

To delete a Zone, first move all child Zones and/or Locations to a different Zone (use your mouse to select a Zone or Location, then drag-and-drop to the new Zone).



Note: Locations cannot be deleted if they have been used to collect data. If you want to hide them from view they can be deactivated.


To delete a Zone:

- 1 In **Locations Manager** on the **Locations** tree, select the Zone to delete.



Note: You cannot delete the System zone.
- 2 Right-click to select  **Permanently Delete Zone**. This option is only available when all child Locations have been moved.
- 3 Select **Options** |  **Save**.

To deactivate a Location:

- 1 In **Locations Manager** on the **Locations** tree, select a Location to deactivate.
- 2 Right-click to select  **Deactivate Location**.
- 3 Select **Options** |  **Save**.

Note: To view all deactivated Locations, select **Options** |  **Show Deactivated Items**.

To reactivate a Location:


- 1 In **Locations Manager** on the **Locations** tree, select **Options** | **Show Deactivated Items**.
- 2 Select a Location, then right-click to select  **Reactivate Location**.
- 3 Select **Options** |  **Save**.

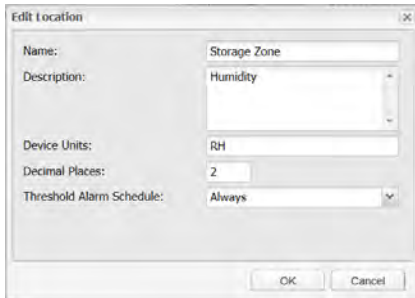
Editing Location Properties

In the Locations Manager window, use the Properties tab to review Location information, such as how data is measured, and whether the Location uses a Threshold alarm schedule.

To make changes to Location properties, you require Manage Locations Right, and have Full Control Permission assigned to you, for the Location.


To modify Location properties:

- 1 From the **Locations Manager** window, **Locations** tree, select the Location you want to edit.
- 2 Right-click to select  **Edit**. The **Edit Location** window appears.
- 3 Enter the name, description, units and decimal places as you would like them to appear in viewLinc.



Note: The name, description, units and decimal places control the way your Location appears throughout viewLinc. If you enter a smaller number of decimal places than your

Device reads, viewLinc will automatically round the data it receives from the Device to the nearest decimal point.

- 4 Choose a Threshold Alarm schedule from the box list, then click **OK**. See “Setting Up Schedules” on page 48.
- 5 In the **Locations** navigation pane, select **Options** |  **Save**.



Assigning Access to Locations & Zones

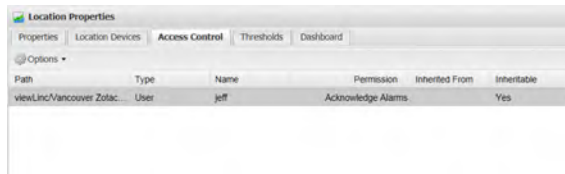
Users and Groups are set up by the Administrator (see “Controlling Access to viewLinc” on page 38). To grant other Users or Groups access to a specific Location or Zone, you require Location Manager Rights, and Full Control Permission for the Location.

When authorizing access to a Location, consider the following:

- It is easier to manage access control on Zones and Groups, rather than on Locations and Users.
- Build access control starting at System root folder (top down).
- To check currently assigned Access Control permission, use the Access Control Inspector “Access Control Inspector” on page 42.

To authorize access to a Zone or Location:

- 1 From the viewLinc desktop, choose **Options** |  **System Configuration** |  **Locations Manager**.
- 2 Navigate the Locations tree to select a Zone or Location.
- 3 In the **Location Properties** pane, click the **Access Control** tab to see the current permissions for a Zone or Location.



To see permissions inherited from the parent Zone, go to the **Access Control** tab, then click **Options** | **Show Inherited**. The list updates to show inherited permissions, and existing permissions for the Zone or Location.

Path	Type	Name	Permission	Inherited From	Inheritable
viewLinc/Vancouver Zotac...	User	cend	View	viewLinc	Yes
viewLinc/Vancouver Zotac...	Group	Administrators	Full Control	viewLinc	Yes
viewLinc/Vancouver Zotac...	User	anri (Andrey N...	View	viewLinc/Vanco...	Yes
viewLinc/Vancouver Zotac...	Group	display	View	viewLinc	Yes
viewLinc/Vancouver Zotac...	User	testack	View	viewLinc	Yes
viewLinc/Vancouver Zotac...	User	jeff	Acknowledge Alarms		Yes

- 4 On the **Access Control** tab, select **Options** | **Add**.
- 5 On the **Create Access Control** window, specify the following:
 - **Type:** Select User or Group.
 - **Name:** Select User or Group name.
 - **Permission:** Select an option from the list. For permission descriptions, see “Access Control Permissions” on page 40.
 - **Inheritable:** Select this option if you want the User or Group to view all subfolders for a Zone/Location.

Note: You can assign access to subfolders on an individual basis.

- 6 Click **Save**.

The new permission appears in the Access Control list (Name column) and access to the Location is assigned accordingly. To see current permissions for other Zones, select a Zone or Location in the Locations tree and the Access Control list updates automatically.

Setting Up Location Thresholds

You can configure one or more Thresholds for each Location, and the Alarm settings to activate if a Threshold is reached.

Threshold settings can be applied with or without template, but a Threshold template makes it easy to apply similar parameters to several Locations. To create a single or multi-threshold template, see “Threshold Templates” on page 58.

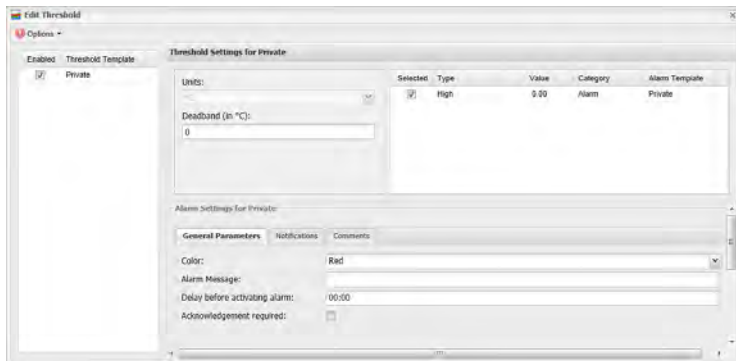
To set a threshold for a specific Location:

- 1 From the viewLinc desktop, choose **Options** | **System Configuration** | **Locations Manager**, then select the Location or

Locations you want to set the threshold alarm for.

Note: To select multiple Locations at one time, hold down the **[Ctrl]** key while you select each Location. To select a group of Locations in a list, hold down the **[Shift]** key and select the first and last Locations. The Locations Properties pane updates automatically.

- 2 Select the **Thresholds** tab, click **Options | + Create X Threshold** (where X represents the unit reading measured at this Location or group of Locations, such as C or RH or mA).



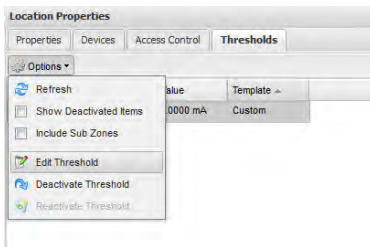
- 3 On the **Edit Threshold** screen, select a template in the Threshold Template column (check the selection box), or create specific alarm settings on the General Parameters, Notifications, and Comments tabs, following steps 3 through 8 in “Threshold Templates” on page 58.
- 4 Click **Options | Save**, or, if you are editing an HMT140 Wi-Fi Data Logger, choose **Options | Save and update device alarm**.

To edit a threshold:

When a Location Threshold or Threshold template is modified, all associated active alarms are acknowledged and terminated automatically. viewLinc applies the new Threshold settings once the next data scan completes.

- 1 From the viewLinc desktop, choose **Options | System Configuration | Locations Manager**, and select a Location.

- 2 On the **Location Properties** pane, select the **Thresholds** tab.



- 3 Select **Options** | **Edit Threshold**. The Edit Threshold window displays.
- 4 Edit threshold settings as desired.
- 5 Click **Options** | **Save** or, for an HMT140 Device, click **Options** | **Save and update device alarm**.

Disabling Threshold Alarms

You can temporarily disable alarms without deleting the Threshold settings (for example, when you want to move a Device from one physical location to another).

To temporarily disable a threshold alarm:

- 1 In **Options** | **System Configuration** | **Locations Manager**, highlight the row of the Location for which you want to disable thresholds.
- 2 On the **Location Properties** pane, **Thresholds** tab, select **Options** | **Edit Threshold**.
- 3 In the Edit Threshold screen, deselect **Enable Threshold Alarm**.
- 4 Click **Save**.





Note: To pause all Host or Device alarms for a temporary period, up to 24 hours, see “Pausing Alarms” on page 126.

Deactivating and Reactivating Threshold Alarming





You may want to deactivate a Device's Threshold because it is no longer required. A deactivated Threshold “disappears” while deactivated, and can be reactivated at any time.

Note: To pause all Host or Device alarms for a temporary period, up to 24 hours, see “Pausing Alarms” on page 126.

To deactivate a Threshold:

- 1 Select **Options** |  **System Configuration** |  **Locations Manager**.
- 2 In the **Locations** pane, select the Location.
- 3 In the **Location Properties** pane, on the **Thresholds** tab, highlight the Threshold you want to deactivate.
- 4 Click **Options** |  **Deactivate Threshold**.
- 5 Click **Yes**, then save the change (**Options** |  **Save**).

To reactivate a Threshold:

- 1 Select **Options** |  **System Configuration** |  **Locations Manager**.
- 2 In the **Locations** pane, select the Location.
- 3 In the **Location Properties** pane, on the **Thresholds** tab, click **Options** then select **Show Deactivated Items**.
- 4 From the list of Thresholds that appear, highlight the Threshold you want to reactivate, right-click and select  **Reactivate Threshold**.
- 5 Click **Options** |  **Save**.

Building Dashboards

A Dashboard gives the User a visual display of the current readings at various points. Simply upload a custom image for any Zone or View and place Locations on the Dashboard image (**Locations** window, **Dashboard** tab).

For example, upload a floor plan or map of a building being monitored, then drag data Locations listed in the Locations tree to their corresponding real life locations on the map. These data points display




the most current readings and can be easily selected to display Pop-up trends. See “Building a Trend” on page 91.


Here are some general tips about how to read Location data on the Dashboard:

- Zones display as folder icons that can be double-clicked to navigate Locations.
- A Location with data associated to it automatically displays and refreshes this data on your Dashboard (real-time).
- To reposition items on the dashboard simply drag and drop them around the Dashboard image. This does not change the reading, only the way the Location appears on your desktop.
- You can double-click a data point to display the Pop-up Trend. Alternatively, you can right-click on the Location and select **Pop-up Trend**.
- To view the Location properties, right-click and select **Properties**.
- You require Manage Locations Right to add Dashboard images.

Adding a Dashboard Image



To create a new Dashboard image:

- 1 From the viewLine desktop, choose **Options |  System Configuration |  Locations Manager**.
- 2 Select a Location from the **Locations** tree.
- 3 On the **Location Properties** pane, select the **Dashboard** tab.
- 4 Click **Options |  Upload Image**.
- 5 Enter the file location or use the **Browse** button to navigate to the image you wish to use, then click **OK**.

Note: The **Options** button turns red to indicate that the current dashboard is being edited. If it is necessary to resize the image, select **Options |  Resize Image**. A grey border appears around the image allowing you to adjust the size in a window.

Adding Zone and/or Location Data Items

To add Zones or Locations to the Dashboard:

- 1 From the viewLinc desktop, choose **Options** |  **System Configuration** |  **Locations Manager**
- 2 Select a Location from the **Locations** tree.
- 3 On the **Location Properties** pane, select the **Dashboard** tab.
- 4 Select the Location or Zone you would like to add to your Dashboard image, then drag and drop from the Locations tree to the image.




Note: It is only possible to place Locations on the dashboard that are a part of the Zone being edited, and are not in the current Dashboard.

The current reading at the Location appears on the image.

Changing the Appearance of Dashboard Items

There are a variety of ways to display data points on your dashboard. You can select Numeric and Zone item preferences, create overriding default preferences for specific items, and arrange items as tiles on the screen (for easier sorting on a User's desktop, or to improve Point-of-Sale (POS) display functionality).

To change Dashboard data point appearance:


- 1 From the viewLinc desktop, choose **Options** |  **System Configuration** |  **Locations Manager**.
- 2 Select a Location from the Locations tree.
- 3 On the **Location Properties** pane, select the **Dashboard** tab.
- 4 Click **Options** |  **Dashboard Preferences**, then choose to modify **Numeric Items**, **Zone Items** (font size only), or **Tiling**.

You can choose to display Location data in up to 4 columns - the greater number of Locations may require a greater number of columns). Test each option to determine which display suits your needs most effectively.

Note: A single-column list is most effective for rotating POS display purposes.


- 5 Click **Options** |  **Save**.

To delete a Dashboard data point:

- 1 To delete Location data from the Dashboard, click on the desired item to select it.
- 2 From the **Options** menu click **Delete** (or right-click to select Delete from the menu).
- 3 Click **Yes**.
- 4 Click **Options** |  **Save**.

To erase the Dashboard image and all data points:

IMPORTANT: The erase operation cannot be undone.

- 1 To erase the current dashboard, select **Options** |  **Erase Dashboard**.
- 2 At the confirmation message, click **Yes**.

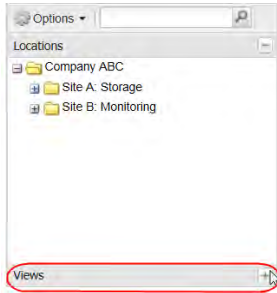
Setting Up User-specific Views

The Locations screen can display User-specific Views, an easy way for non-administrative Users to view only those Locations that matter to them/their job function. Note that you require Manage Views Right to create Views.

For example, you could create a View of all humidity or all temperature Locations a User is permitted to view, regardless of the Zone in which Devices are located. Once a new View is saved, the Administrator assigns access to that View to a User or Group.

If you plan to use a remote display terminal, note that the displayed content is defined by the View assigned to the User logged in, and the Locations the User is permitted to access. For more information about setting up a Remote Display, see “Using a Remote Display” on page 157.

Once a View is set up, the User or Group can access their View in the Locations window, by clicking in the dark grey bar labeled, **Views**, at the bottom of the Locations tree pane.

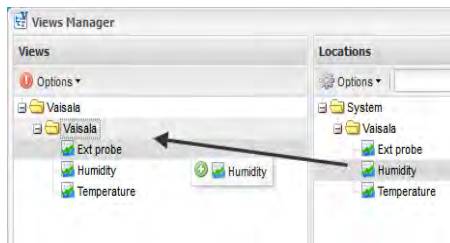


Creating a New View

You require Manage Views Right to access the Views Manager window.

To create a View:

- 1 Select **Options** | **System Configuration** | **Views Manager**.
- 2 In the Views pane, click **Options** | **New View**.
- 3 Enter a name for the View.
- 4 Right-click the View to add Zones or rename.
- 5 In the Locations tree in the center pane, select a Location or Zone (you may need to expand the tree), then drag it to your View (or right-click on the Location or Zone, and select Copy & Paste). Note that when you drag and drop a Location or Zone, all child Locations are included in the View.



- 6 Click **Options** | **Save**.

To specify who can access the View:

- 1 In the **Views Manager** window, on the **View Properties** pane, select the **Access Control** tab.
- 2 On the **Access Control** tab select the View, then select **Options | Add**. The **Create Access Control** window appears.
- 3 Specify the access control type, User or Group, the name of the User or Group, and select the permission you wish to give:
 - **Hide:** Use this permission for exceptions.
 - **View:** User or Group can see this Location in the Locations window.
 - **Full Control:** User or Group can modify the View using the Views Manager window.
- 4 Click **Save**. The new permission appears in the Access Control tab. When selected, access to the view is provided with 'Full Permission' by default.

Note: To share this View with multiple Users who are not in the same Group, you can either create a new Group and assign specific Users to the Group, or complete steps 1 through 4 for each specific User.

Working with the Locations window

All viewLinc Users have access to the Locations window; however, Locations that a User can view differ depending on the Locations the User or Group is permitted to view. Permissions are assigned by the viewLinc Administrator (see “Controlling Access to viewLinc” on page 38).

As described in the “viewLinc Desktop Orientation” on page 65, the Locations window contains a navigation pane and four tabs with various options and control buttons to help you customize, manage and display data.

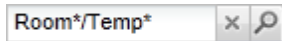
Searching for Zones and Locations

For some Users, the list of Locations they can view is long, and finding a specific Location may be time-consuming. Using the toolbar search field at the top of a navigation tree, a User can conveniently target their search with a filter.

For example:

- To search for all Zones starting with the term, 'Room', use the following syntax: **Room***.
- To include all Zones starting with the term, 'Room', and all Locations that start with the term, 'Temp', enter the search string as: **Room*/Temp***.

Click the magnifying glass icon to activate the filter. An 'x' icon appears next to the icon to indicate the filter is active:




While the filter is active, only Zones and Locations that match the search criteria display. Click the 'x' to deactivate the filter.

Finding a Linked Location

If you are having difficulty finding which Location is linked to a Zone, viewLinc offers a quick way to show the corresponding Location.

To find a Location Linked to a Specific Zone:

- 1 In the **Locations** window, on the **Table View** tab, select the Location.
- 2 Right-click and select  **Find Location** (or use the right-click menu option).
- 3 A yellow highlight bar appears in the Locations tree to indicate the corresponding Location.

Note: If the yellow highlight does not appear, you may already have selected the linked Location, and the yellow highlight is hidden behind the grey selection bar, or you do not have permission to view the Location.

Using the Locations Dashboard

Dashboards allow you to view a custom image of a physical space, and identify where Zone and Location data readings are monitored. This gives you a quick, at-a-glance display, of current readings at various points at a monitored site.



You can also use the Dashboard area to display Location data without a background image.

To set up a Dashboard image and data points, see “Building Dashboards” on page 83.

Monitoring Alarms

All active alarms for the current Location or Zone and sub-zones display in the Locations Alarms tab. You may be required to act upon an alarm in one of several ways:

- If acknowledgement is required on an alarm, the alarm will be listed in this window, whether it is on or off.

- If acknowledgement is not required on an alarm, the alarm will be present in this window only if it is currently on.
- A User can acknowledge threshold alarms if they have Acknowledge Alarms permission on that Location.
- Device alarms can be acknowledged if the User has Acknowledge Alarms permission for at least one Location referencing that Device.

For specific instruction on acknowledging alarms, or viewing Alarms in the Alarms window, see “Viewing and Acknowledging Alarms” on page 121.

Building a Trend

The Trend tab enables you to compare live data for multiple Locations for display as a trend graph, and save the trend data as a View or as a Location History Report for future reference.

- To share a View with other Users or Groups, you require Manage Views Right.
- To view a single Location’s data trend in a graph format, you may find it quicker to view the Location in a Pop-up Trend window.

Trend Tab Functions

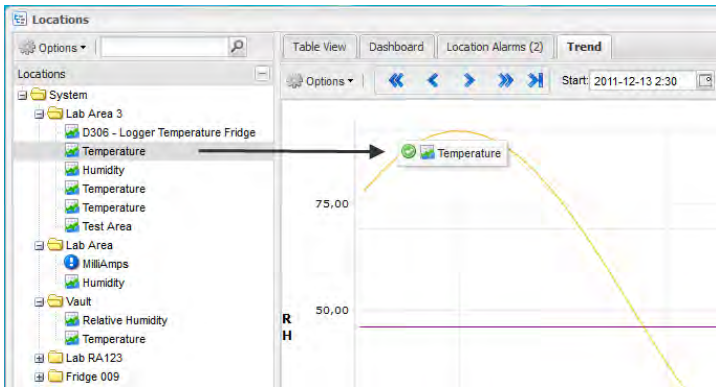
Use the Trend tab Options menu to:

- **Refresh:** Reload data from server.
- **Clear:** Clear all Channels from the trend.
- **Save as View:** Displays a window to save the current trend as a View. This function requires ‘Manage Views’ right.
- **Save as Report:** Displays a window to save the current trend as a single page Location History Report.
- **Include Realtime Samples:** When checked, this option includes real time samples along with the logged data.
- **Show Data Markers:** When checked, this option adds small markers on the trend graph, indicating exactly where the readings took place.

Note: If you don't have permission to perform a function you need, speak to your administrator.

To create a new trend:

- 1 In the **Locations** window, navigate the Locations tree to find a Location you would like to graph as a trend.
- 2 Drag and drop one or several Locations (maximum 16) from the Locations tree onto the graph pane on the right.



- 3 If you have been assigned the Right to Manage Views, you can save the trend as a View. Select **Options** | **Save as View**, then enter a name (description) and click **Save**. This View is now available in the Views area and can be accessed any time.



You can continue to build upon and modify your Trend at any time by simply dragging more Locations onto the graph and saving again.

Note: You can add up to 16 Locations (lines) per Trend.

Navigating a Trend View



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

- **Forward and Back arrows** (↔): Click to adjust the start time.

- **Double forward and back arrows:** Click to adjust the start time by a greater distance.
- **Live button** : Click to fetch the most recent data according to the specified **Duration** value.
- **Auto Refresh On:** Click on or off to toggle the auto refresh option. Uncheck it to stop periodic updates, or check it to have the same effect as pressing the  **Live** button.

Note: Navigating or zooming within the trend will automatically uncheck the “Auto Refresh On” option, because when you navigate within the trend, you are then viewing historical data.

To change the contents of the Trend View:



- 1 In the **Locations** window, select the **Locations** tab below the Trend chart.
- 2 To select Locations you want to view, in the **Selected** column, check or uncheck the Locations you want to view.
- 3 To include Threshold values, in the **Threshold lines** column, check or uncheck the Thresholds you want to view. The pane displays statistics information for each graph line.
- 4 Click the **Live** button, , or click **Options** |  **Refresh** to refresh the graph to display only the data you have selected.

To view Trend max/min statistics:

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

To adjust scale values:


- 1 In the **Locations** window, select the **Locations** tab below the Trend chart.
- 2 Click the **Scale** tab. The default low/high range is set to Auto. To enter new values, click on the Auto text field and enter new values.

- 3 Click the **Live** button, , or click **Options** |  **Refresh** to refresh the graph to display the new values.

To select a specific time period to view:

- 1 With a Trend graph open, click anywhere on the graph and drag your cursor to the right to highlight the time period you want to magnify, then release. The magnified area displays until the next live update.
- 2 To return to full view, double-click anywhere on the graph (or to zoom out, select an area, drag cursor to the left, then release).

To save a View as a Report:

- Click **Options** |  **Save As Report** and enter a name for your report. The report is available with the name you specified in the Reports section.

To learn more about reports, see “Types of Reports” on page 137.

Viewing Pop-up Trends

A Pop-up Trend is a window displaying the most current data reading for a specific Location, any related threshold settings, a graph representation of recent historical data readings, and an area to indicate an active alarm. To view a trend which includes data for multiple Locations, see “Building a Trend” on page 91.

You can manually open the Pop-up Trend view from the **Locations** window, or configure an alarm to automatically display a Pop-up Trend due to an alarm condition (see “Alarm Templates” on page 53).

The Pop-up Trend view contains most of the same functionality as a graph created using the Trend tab, with the addition of a large yellow banner indicating the most recent data reading. In this window you can view the most recent historical trends, and hover over specific data points for more detailed readings.

Note: You can view a particular Location’s data reading in a single pop-up window, or you can open multiple Location pop-up 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 | Tabs | Settings**).

Here is a description of the key elements in the Pop-up Trend graphing area:

Item	Description
Title bar	Displays the name of the Zone and type of location data reading (humidity, temperature, voltage or current).
Header bar	Indicates the date and time of latest reading; the time zone is based on the time zone setting of the PC running the browser. The graph header bar also displays the number of data points being measured.
Numerical display area	Displays most current data values in units being measured, as defined by the User (see "Editing Device and Channel Properties " on page 99to change).
Graph area	A graphical representation of data history is displayed here.
Left-side Y-axis	Shows the scale for the data displayed in the graph.
X-Axis time scale	Shows the reporting time frame (if you use Internet Explorer, you can only view the last 300 data points; all other browsers display the last 1000 points).
Graph Line	Indicated by a line to show 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.
Threshold Line	Indicated by a 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.

Item	Description
Active Alarms area	Displays active alarm details: Threshold value and amount exceeded; alarm date and time; whether the alarm was acknowledged, and by whom. Permits User to acknowledge an alarm. If you don't see the active alarm area, there may be no alarms to display. It can still be shown using the double arrows on the right hand side of the pop-up trend.
Status bar	Indicates channel monitoring status (OK or Alarm/Alarm condition type).

To open a Pop-up Trend:

- 1 From the viewLine desktop, select **Options** |  **Locations**.
- 2 In the **Locations** window, browse the Locations tree and select a Location you want to view as a Trend.
- 3 On the **Table View** tab or **Locations** navigation tree, right-click on the selected Location, then choose  **Pop-up Trend**. A new resizable window appears, containing information about the selected location.
- 4 Repeat steps 1 to 3 to view multiple Pop-up Trend views, which you may want to display on various monitors.

To close a Pop-up Trend window, click **Close (x)** in the top right corner.

To acknowledge an alarm, see “Ways to Acknowledge Alarms” on page 122.

CHAPTER 4

MANAGING DEVICES

During viewLinc setup, your Vaisala Veriteq Devices are discovered automatically, and display in the Locations and Locations Manager windows (see “Discovering Devices” on page 35).

Administrators, and Users assigned Device Manager Rights, use the Locations Manager window to manage how Devices display in viewLinc, define Host and Device Alarm settings, specify Device Calibration settings, deactivate or reactivate Host machines, and pause or resume alarming.

- Viewing Devices and Hosts
- Adding New Devices
- Setting Up Device and Host Alarms
- Calibrating Devices
- Removing Devices

Viewing Devices and Hosts

All Device Channels currently linked to Locations display in the Locations window (note that Locations a User can view depends on their Access Control permission level - see “Access Control Permissions” on page 40).

To view currently connected Devices and Hosts, you must be an Administrator or be assigned Manage Devices Right. Devices and Hosts are viewed in the **Locations Manager** window, **Devices** pane (middle).

Viewing Device Properties

To view Device properties:

- ▶ On the viewLine desktop, select **Options | System Configuration | Locations Manager** and select a Device from the middle **Devices** pane. Device and Host details appear in the **Device Properties** area, lower right of the screen.

Column	Displays
Device Details tab	
Description	Device Description.
Serial Number	The serial number associated with the Device.
Sample Interval	The interval between samples taken from Device.
Device Address	Address of Device with protocol type.
Channels	Number of Channels associated with Device.
Channel Description	Description entered for Channel.
Device Units	Units measured (RH, C, mA, mV, etc.).
Host Details tab	
Hostname	Displays name of the Host of the selected Device/Channel.
Resolved Name	For administrative purposes.
Host IP Address	Host's IP Address





Column	Displays
Localhost	Identifies whether the selected Host is running viewLinc (viewLinc server machine).
Devices	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.
Alarming	Alarm state.

Editing Device and Channel Properties

To save time, you can view and edit Device information, such as Description, Alias, Timeout seconds, UDP Port, Password, and data transfer parameters (depending on the Device options) from within viewLinc (see “Device and Channel Aliases” on page 28).

Depending on the Vaisala Veriteq Devices you have installed, you can modify these properties in viewLinc; however, if your Device is linked to the vLog audit trail, edit the Device properties in vLog or first disable the link to the audit trail to modify properties in viewLinc.

To edit Device properties:

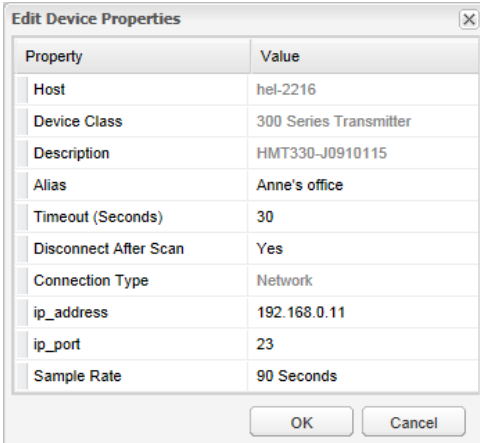
- 1 From the viewLinc desktop, choose **Options** |  **System Configuration** |  **Locations Manager**.
- 2 On the **Devices** pane, select the Device you want to edit.
- 3 Select **Options** |  **Device** |  **Edit Device** (or use the right-click menu).
- 4 In the **Edit Device Properties** screen, edit the properties fields.

For Vaisala Veriteq Loggers you can specify:

- **Description:** Enter a short Device description (maximum 16 characters for Vaisala Veriteq Devices only). viewLinc allows you to edit a Vaisala Veriteq Device description (maximum 16 alpha-numeric characters stored within the Device), as well as its alias (maximum 64 alpha-numeric characters, not stored within the Device). You can only edit a 300 Series Transmitter alias in viewLinc.
- **Alias:** Enter a more descriptive Device description, if needed (maximum 64 characters). The Alias is used instead of a Description, if the option is set up in system settings (see “Device and Channel Aliases” on page 28).

For 300 Series Transmitters, you can also specify:

- **Alias:** A more descriptive Device description, if needed.
- **Timeout:** Specify the number of seconds to wait for data before canceling a transmission.
- **Disconnect After Scan:** Choose whether you want the Device to disconnect automatically after scanning.
- **Sample Rate:** The frequency that data samples are saved to the Transmitter.



The screenshot shows a dialog box titled "Edit Device Properties" with a close button (X) in the top right corner. The dialog contains a table with two columns: "Property" and "Value". The table lists the following properties and values:

Property	Value
Host	hel-2216
Device Class	300 Series Transmitter
Description	HMT330-J0910115
Alias	Anne's office
Timeout (Seconds)	30
Disconnect After Scan	Yes
Connection Type	Network
ip_address	192.168.0.11
ip_port	23
Sample Rate	90 Seconds

At the bottom of the dialog box, there are two buttons: "OK" and "Cancel".

For HMT140 Wi-Fi Data Loggers you can also specify:

- **Timeout:** Number of Seconds to wait for a data transmission before failing the 'Add' operation.
- **UDP Port:** Auto-generated, can be modified if required.
- **Password:** Change the assigned password, if using.
- **Max Blocks per Beacon:** Specify 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 as changes to this setting may impact battery life.
- **Retry Count:** Number of times data transmission is attempted by the Device if it fails to receive an acknowledgement.
- **Transmit Period:** The frequency of data transmissions.
- **Sample Rate:** The frequency that data samples are saved to the Device.

Property	Value
Host	VAN-WWLNC-HOST
Device Class	HMT140 Series Transmitter
Description	HMT140 #44
Alias	
Timeout (Seconds)	70
Serial number	E0D8E004
UDP Port	6767
Password	
Max Blocks per Beacon	64
Retry Count	3
Transmit Period (Mins)	15
Sample Rate (Mins)	2

Buttons: Set Calibration Date, OK, Cancel

- 5 Click **OK** to save.




Note: To modify Calibration settings, see “Calibrating Devices” on page 109.

Editing Channel Properties

To easily identify a specific Channel onscreen, you can edit a channel’s description, alias, and preferred temperature units, if applicable.

Note: Depending on the Device you use, not all Device channels can have their descriptions modified. Refer to the specific Device User Guide for more information.

To edit channel properties:

- 1 From the viewLine desktop, choose **Options** |  **System Configuration** |  **Locations Manager**.
- 2 In the **Devices** tree pane, select a Device Channel to edit.
- 3 On the **Devices** | **Options** menu, select Channel, then  **Edit Channel** (or use the right-click menu).
- 4 In the **Edit Channel Properties** window, modify the following fields as required.
 - **Description:** Enter a short Device description (maximum 16 alpha-numeric characters for Vaisala Veriteq Loggers; maximum 32 characters for HMT140 Wi-Fi Loggers; this is not an option for 300 Series Transmitters).
 - **Alias:** Enter a more detailed Device description (maximum 64 characters). The Alias is used instead of a Description, if the option to use Aliases is set up in system settings (see “Device and Channel Aliases” on page 28).

Additional options are available for HMT140 Wi-Fi Loggers:

Property	Value
Device	E0F2E08C
Device Class	HMT140 Series Transmitter
Description	Channel: HMP110 degC
Alias	
Password	
Channel Type	HMP110 Temperature
Units	C
Decimal Places	0
Presentation Scale	1.0000
Presentation Offset	0
Engineering Scale	0.0122
Engineering Offset	-200.0000
Calibration Scale	1.0000
Calibration Offset	0
High Alarm Value	200.0000
High Alarm Time (15 Sec)	255
Low Alarm Value	-200.0000
Low Alarm Time (15 Sec)	255

OK Cancel




For HMT140 Wi-Fi Loggers (with HMP110 Probes):

- **Decimal Places:** Enter the number of decimal places to display.
- Refer to the Vaisala Wi-Fi Data Logger HMT140 User Guide to modify the calibration settings:
- **Presentation Scale/Offset:** The final scaling ($x = \text{Scale} * V + \text{Offset}$).
- **Engineering Scale/Offset:** The intermediate scaling ($x = \text{Scale} * V + \text{Offset}$)
- **Calibration Scale/Offset:** The primary calibration scaling ($x = \text{Scale} * V + \text{Offset}$)
- **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.


Setting Channel Temperature Units

If you do not want to use the system default temperature units for temperature Channels (set on the **Options | System Configuration | Preferences** tab), you can modify the temperature units for a specific Channel. This setting does not alter how the Channel measures temperature, it alters the units in which temperature is displayed.

To set Channel temperature units:

- 1 From the viewLinc desktop, choose **Options |  System Configuration |  Locations Manager**.
- 2 In Locations Manager, on the **Devices** tree, select a Channel to edit.
The current unit measurement for the selected Channel appears on the right, in **Device Properties** area on the **Device Details** tab.
- 3 On the **Devices | Options** menu select **Channel |  Edit Channel** (or use the right-click menu).
- 4 In the **Edit Channel Properties** window, make the required change to the **Units** field.

To use system default temperature settings:

- 1 From **Locations Manager**, use the **Locations** tree to select a Location to edit.
- 2 On the **Locations | Options** menu select ** Edit Location** (or use the right-click menu).
- 3 In the **Edit Location Properties** window, in the **Preferred Units** field, select the option, **Use System Default**.

The screenshot shows a dialog box titled "Edit Location". It contains the following fields and values:

- Name: Temperature
- Description: Temperature
- Device Units: C
- Preferred Units: Use System Default (dropdown menu)
- Decimal Places: 2

Buttons: OK, Cancel

Adding New Devices

As your network monitoring needs increase, viewLinc makes it easy to expand your monitoring capabilities with the addition of new Devices and Hosts.

Refer to “Discovering Devices” on page 35 to learn how to add additional Devices and Hosts to expand your viewLinc system.

Setting Up Device and Host Alarms

Communication between Devices and the viewLinc Server is essential for real-time monitoring of conditions. Because of this, viewLinc allows you to configure both Host and Device Communication Alarms, as well as Device Alarms (Device Calibration, Configuration and Calibration).

Communication Alarms

Communication alarms notify Users if communications are down at any point – the alarm controls how the alarm displays on a User’s screen, who is notified, when the alarm notification is initiated, and whether acknowledgement is required.

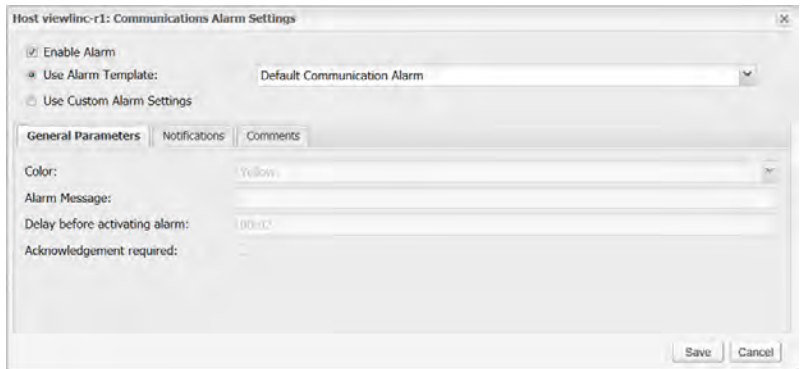
By default, there is one communication alarm preconfigured for each Host and each Device. You can specify whether you want the Device or Host to use the default communication alarm template or your own custom communication alarm template (see “Templates” on page 52), or

apply specific communication alarm settings to individual Hosts and Devices.

To set a communication alarm:

- 1 From the viewLinc desktop, choose **Options | System Configuration | Locations Manager**, then navigate the **Devices** tree to select a Host or Device.
 - To set up a Host Communication alarm, right-click the Host, then choose **Host Communication Alarm Settings**.
 - To set a Device communication alarm, right-click the selected Device and choose **Device Alarm Settings | Device Communication Alarm Settings**.

The Communications Alarm Settings screen appears.



- 2 Select **Enable Alarm** (an alarm is not active until it is enabled).
- 3 To set up a communication alarm to use an existing alarm template, select **Use Alarm Template**, then select the template from the drop-down list.
- 4 To set custom alarm settings for this Host/Device, select **Use Custom Alarm Settings**.
- 5 Set your alarm settings on the General Parameters, Notifications, and Comments tabs following steps 3 to 8 in “Alarm Templates” on page 53.

- 6 Click **Save**.






Editing Communication Alarms

Communication alarm settings can be modified for Hosts or Devices individually, or applied globally when set up as a custom Communication Alarm template.

Note: The default Communication Alarm template cannot be modified.

To edit a custom Communication Alarm Template, see “Alarm Templates” on page 53.

To edit communication alarm settings for a single Device or Host:

- 1 From the viewLinc desktop, choose **Options** |  **System Configuration** |  **Locations Manager**, navigate the **Devices** tree to select the Host or Device.
 - To edit a Host communication alarm, right-click the Host, then choose  **Host Communication Alarm Settings**.
 - To edit a Device communication alarm, right-click the selected Device and choose **Device Alarm Settings** |  **Device Communication Alarm Settings**.
- 2 Edit alarm settings as desired.
- 3 Click  **Save**.




Disabling Communication Alarms

You can temporarily disable (deactivate) Communication Alarms for a specific Host or Device, without deleting all the setting information. You may want to do this when you need to perform maintenance on a Host or Device.

Note: To pause all Host or Device alarms for a temporary period, up to 24 hours, see “Pausing Alarms” on page 126.

To disable alarms:

- 1 From the viewLinc desktop, open the **Locations Manager** and use the **Devices** tree to select the name of the host or Device with an active communication alarm you want to disable.

- To edit a Host communication alarm, right-click the Host, then choose  **Host Communication Alarm Settings**.
 - To edit a Device communication alarm, right-click the selected Device and choose **Device Alarm Settings** |  **Device Communication Alarm Settings**.
- 2 Deselect the **Enable Alarm** option.
 - 3 Click  **Save**.

Device Alarms

By default, there are three types of Device alarms (in addition to the Device Communication alarm) preconfigured for each Device: Calibration, Validation, and Configuration Alarms. These alarms are enabled automatically when a Device is added.





Device Alarms cannot be deleted; however, you can specify the Alarm Template to use, or create custom Alarm settings.

Editing Device Alarms

Device alarm settings can be modified for specific Devices by modifying the settings or the custom template applied to the Device.

Note: Default Device alarm templates cannot be modified.

To edit a Device alarm:

- 1 From the viewLinc desktop, select **Options** |  **System Configuration** |  **Locations Manager**, and use the Devices pane to locate and select a Device.
- 2 On the Devices **Options** menu, select  **Device** |  **Device Alarm Settings**, then select the Device alarm type you want to edit.
- 3 Edit alarm settings as desired (refer to steps 3 through 8 in “Alarm Templates” on page 53).
- 4 Click **Save**.





Disabling Device Alarms

During system maintenance periods, or if you are replacing a Host Server and it will be out of operation for any length of time, you can disable Host Communication Alarming, individual Device alarming (one Device alarm at a time), or Pause all alarming for a Host or a Device.

Alternatively, you may want to deactivate a Device or a Host (all monitoring and alarming is stopped). See “Removing Devices” on page 110.

Note: To pause alarming on a Host or Device for a temporary period, up to 24 hours, and have it start up again automatically, see “Pausing Alarms” on page 126.

To disable or enable a Device alarm:

- 1 From the viewLinc desktop, select **Options** |  **System Configuration** |  **Locations Manager**, and use the Devices pane to locate and select a Device.
- 2 On the Devices Options menu, select  **Device** |  **Device Alarm Settings**, then select the Device alarm type you want to disable or enable.
- 3 Deselect or Select the **Enable Alarm** check box.
- 4 Click **Save**.

Calibrating Devices

Calibration ensures that the data produced by the measurement equipment (Loggers, Transmitters, Probes) is reliable and accurate.




For example, most people are used to adjusting their watches to the correct time, whenever necessary. 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, we 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 the following procedure when you need to update calibration values for your Device (if it was calibrated by the Vaisala Calibration Services team), or you are performing an onsite calibration.

Note: Only the calibration properties of HMT140 Wi-Fi Data Loggers with RTD, voltage or mA channels can be edited in viewLinc. Refer to the HMP110 User's Guide for information about calibrating HMP110 Humidity/Temperature probes.

To edit calibration properties:

- 1 Make sure a Device which supports calibration properties is selected.
- 2 Ensure the initial calibration values have been downloaded from the Device to viewLinc (automatically discovered).
- 3 On the viewLinc desktop choose, **Options |  System Configuration |  Locations Manager**, and then use the Devices tree to select a Channel to edit.
- 4 On the **Options | Channel** menu select  **Edit Channel** (or use the right-click menu).
- 5 In the **Edit Channel Properties** window, edit the calibration properties for Calibration Scale and Calibration Offset (provided by Vaisala or collected from your onsite calibration testing).
- 6 Click **OK**.
- 7 When the calibration property is changed, confirm the change and ensure the correct calibration date is entered.
- 8 Click **OK**.

Removing Devices

When a Device is removed from the viewLinc system, or transferred to a new monitoring area, viewLinc needs to be notified to prevent system alarms.




You may want to remove a Device when:

- a Device requires maintenance (such as recalibration)
- a Device is no longer required
- a Device needs to be disabled temporarily






To ensure consistency in monitoring, you can choose to deactivate a Device, deactivate a Location, swap a device or permanently delete a Location. Before you can swap a Device you must first unlink any linked Channels.

IMPORTANT: If a Device is removed without being deactivated, this will trigger a Communication Alarm.

To deactivate a Host or Device:

- 1 From the viewLinc desktop, choose **Options |  System Configuration |  Locations Manager**.
- 2 In the **Devices** pane, select the Host or Device you want to deactivate.
- 3 On the **Devices | Options** menu, click **Host | Deactivate Host or Device | Deactivate Device**.
- 4 A message appears, asking that you confirm removal of the Host/Device. Click **Yes**. The Host/Device is no longer visible on the Devices tree, but the network connection is still intact, allowing you to reactivate the Host/Device when needed.
- 5 Click **Options |  Save**.



To reactivate a Host or Device:

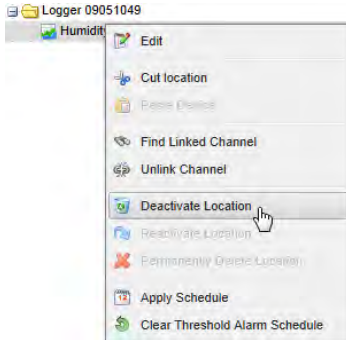
- 1 From the viewLinc desktop, choose **Options |  System Configuration |  Locations Manager**.
- 2 On the **Devices | Options** menu, select the option, **Show Deactivated Items**.
- 3 Select the deactivated Host/Device in the Devices tree (indicated by an ) , then right-click to select  **Reactivate Device**.
- 4 Click **Options |  Save**.

You can now drag the Host/Device to a Location in the Locations tree, if required.

Deactivating/Reactivating a Location






To deactivate a Location:

- 1 From the viewLinec desktop, choose **Options** |  **System Configuration** |  **Locations Manager**.
- 2 In the Locations pane, select the Location you want to deactivate.



- 3 At the Modify Location prompt, click **Yes**.
- 4 Click **Options** |  **Save**.

To reactivate a deactivated Location:

- 1 From the viewLinec desktop, choose **Options** |  **System Configuration** |  **Locations Manager**.
- 2 On the **Locations** | **Options** menu, select the option, **Show Deactivated Items**.
- 3 Select the deactivated Device in the Devices tree (indicated by an ) , then right-click to select  **Reactivate Device**.
- 4 Click **Options** |  **Save**.

Swapping a Device

When a Device is swapped, 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.


To swap a Device:

Note: Only a Device with the same settings may be swapped.





- 1 To check if you have any existing Devices connected to the network that could be used for the swap, go to **Locations Manager | Devices | Options**.
- 2 Right-click on the Device you want to swap, then select **Swap This Device With**. If no Devices appear in the Swap Device Selector window, use vLog to find a Device with the same settings.

Note: Each Vaisala Veriteq Device must be reviewed separately using vLog, and the COM Port to which they are connected must be selected.

The following settings must be present:

- **COM port/IP address.** Device is on the same COM Port (attached to the same cable). If you are swapping a 300 Series Transmitter connected as a network Device, ensure the new transmitter has the same IP address.
 - **Name.** Device is not retired or deactivated.
 - **Status.** Device is not in active alarm mode.
 - **Sample Interval.** Devices have the same sample interval.
 - **Channels.** Devices have the same channels enabled and be using the same units of measure for each matching channel.
 - **Audit Trail.** Vaisala Veriteq Devices are not linked to a vLog Audit Trail.
- 3 In **Locations Manager**, navigate the Devices pane to select the Device you want to swap. Right-click and select  **Pause Device Alarming**.
 - 4 In the **Pause Device Alarming** window, you can add a comment, or select a preconfigured comment, to indicate why alarming is paused, and specify the expected duration for the pause. This will ensure no communication or threshold alarms are triggered when disconnecting the Device.

Note: When a Device is paused any active alarms at the time of the pause are turned off. Any event logs and emails sent out will not indicate they were turned off due to a pause.

- 5 Click **OK**.
- 6 Disconnect the Device you want to swap, and connect the new Device. If you are swapping a 300 Series Transmitter, unplug the power source and plug it in again.
- 7 Select **Devices | Options | Refresh** to update the Device list (you may have to wait a few minutes for the Device to appear). If the new Device has been previously swapped it will be found in the list of deactivated Devices in the Device Properties pane (to view, select **Devices | Options | Show Deactivated Items**).
- 8 From the **Devices** pane, select the Device you have removed.
- 9 Right-click and select  **Swap This Device With**.
- 10 Select a Device, then click **OK**. viewLinc reassigns the Device.
- 11 If you want the new Device to resume alarming, navigate the system tree from **Options | Locations** to find the Device you want to resume (indicated with a ). Right-click and select  **Resume Device Alarming**.
- 12 On the Locations pane, select **Options |  Save**.

Hide or Show Deactivated Locations/Devices

- ▶ In **Locations Manager**, on the **Devices** or **Locations** pane, select **Options | Show Deactivated Items**.

Permanently Delete a Location or Zone

As your company grows, and monitoring needs change, you may find that you no longer need a Location or Zone displayed on your desktop. If you simply want to move a Location to a new Zone, see “Managing Locations & Zones” on page 69.

You require Administrator or Manage Locations Right to permanently delete a Location or Zone.

To delete a Location or Zone permanently:

- 1** In the Locations Manager window, select the Location or Zone you want to delete.
- 2** Ensure no Channels are linked to the Location, and no Locations are linked to the Zone.
- 3** Right-click to select **✖ Permanently Delete Location** or **✖ Permanently Delete Zone**.

CHAPTER 5

MONITORING ALARMS

Alarms and Alarm Acknowledgement are the keys to success with the Vaisala Veriteq Continuous Monitoring system.

During system set up, you would have defined alarm notification settings (who receives alarm notification), created alarm templates (standard Email messaging and alarm parameters), and specified Threshold templates (conditions which will trigger alarms).

This section provides you with information you need to understand different types of alarm conditions, how to activate alarm settings, ways to view and acknowledge alarms, how to pause alarming, and generate alarm reports.

About Alarms

There are several types of alarms in viewLinc which indicate:

- Condition changes in a monitored environment (Threshold Alarms)
- Communication issues (Communication Alarms)
- Possible problems with data collection (Event Validation Alarms)
- Interruptions in tracking data history (Device Configuration Alarms)
- Issues with device validation or calibration reminders (Device Status Alarms).
- System configuration warnings (System Alarms)

Using viewLinc, you can customize the information that is issued for Threshold, Communication and Device alarms (using default or custom Email & SMS Templates), and specify when and how Users should be

notified of alarms (using default or custom Alarm Templates and Threshold Templates).

All alarm events are recorded in the Event Log.

Types of Alarms

Most viewLinc Alarms are issued automatically. It is up to you to set condition limits, and decide how you want to view, be notified of, and acknowledge different types of alarms.

Threshold Alarms

Threshold Alarms notify Users when conditions (such as temperature and relative humidity) are outside acceptable limits. When conditions exceed these limits (preconfigured by an Administrator), a Threshold Alarm is triggered. You can configure single or multi-level threshold alarm settings for each Location.

Communication Alarms

Communication Alarms automatically notify Users when communication between a Host or viewLinc Server PC, and its supported Devices, is interrupted. Example conditions which might prompt a Communication Alarm are:

- viewLinc Server can not communicate with a Device
- Device connection to a Host has been severed.

Think of Communication Alarms as a system health test, alerting you if there is a problem that might disrupt viewLinc monitoring and alarming.

Event Validation Alarms

Event Log Validation Alarms are used to ensure database security, and require acknowledgement. They indicate whether changes have been made to the Event Log from outside the viewLinc system.

If any changes have been made, or any missing records or files are discovered, an alarm is automatically triggered, rendering data non-validatable.

Device Configuration Alarms

If you receive a Configuration Alarm, this indicates that your Device has stopped recording data history or was configured incorrectly.

This could be the result of:

- Device settings set to stop when full.
- A delayed start (as set on a Vaisala Veriteq Logger).
- An internal Device error.
- A Channel has been disabled in the Device, manually or with the Device configuration software.
- IR sensor sending too many transmissions (may drain battery)

Note: You can verify or modify the Vaisala Veriteq Device settings using vLog or HMT140 Utility software; however, if the problem persists, contact your Vaisala technical support representative.

The default delay for most configuration alarms is 60 seconds (this delay can be modified in viewLinc). However there is no delay for certain alarm types such as missing Channel Alarms, configuration changes and probe changes (cannot be changed).

Device Status Alarms

If your system uses VL-type data loggers (on a validated system), you may receive these alarms:

- **Device Validation Alarms:** Sent if the validation memory in the Device is corrupted or has been modified. Contact your Vaisala technical support representative for assistance.
- **Device Calibration Alarms:** An intermittent notification sent when your Device is due for calibration. You receive notifications at the following intervals: 3 months and 1 month before the calibration due date, then again on the data logger's scheduled recalibration date. This alarm remains active until the Device is recalibrated (for more information contact Vaisala Calibration Service Center).

System Alarms

System Alarms occur automatically when viewLinc detects a change in the database made outside standard desktop interaction. It is issued to warn of possible database tampering.

What Happens When an Alarm is Triggered?

When an alarm is triggered, several things can happen, depending on your system configuration settings:

- **Pop-up:** A pop-up notification can appear on your desktop indicating a description of the condition, and an alarm message. If pop-ups are blocked in your browser, an error message appears, prompting you to enable pop-ups for viewLinc.
- **Email or SMS:** An Email or SMS notification can be sent once or repeatedly, based on how the alarm properties are set, and according to a User's work schedule. If configured, an Email can automatically be sent to an email address, or multiple email addresses. If issuing an SMS notification, a text message is sent to a mobile Device.
- **Command:** An application can be launched or an external Device turned on. If configured, an external Device (such as a light or buzzer) or a computer application (such as batch file which can page or phone a particular number) can be triggered when an alarm condition occurs.

Alarms should be dealt with as soon as possible by acknowledging them in viewLinc, on a remote display, or with a reply to an email or SMS notification. If configured to require acknowledgement, an alarm notification will persist unless acknowledged.

IMPORTANT: Alarm notification is sent only for Devices with Channels currently linked to active Locations.

Do Alarms Require Acknowledgement?

Alarms can be configured so they do not require acknowledgement.

Viewing and Acknowledging Alarms

The Alarms window displays a list of all active alarms on your viewLinc system. Only alarms for the Locations which you have permission to view are visible. You require permission to Acknowledge Alarms for a specific Location.

You can view active alarms in the Locations window (Location Alarms tab), or in the Alarms window. For information about viewing alarms in the Locations window, see “Monitoring Alarms” on page 90.

Refreshing the Alarms Window

The Alarms window updates automatically or on demand. The automatic Auto Refresh function ensures you are viewing the most current alarms; however, when reviewing a long list of alarms you can disable this functionality to prevent the window from updating before you are ready.

To disable Auto Refresh, uncheck the **Auto Refresh On** button in the top right corner.

To force refresh manually, select **Options | Refresh**.

Alarms Window Orientation

Color	Description	Location	Device Description	Device Serial Number	Zone	Timestamp	Duration	State	Acknowledgement
Red	High Threshold location val...	HMP110 degC (36...	HMT140 #270 2/...	EGD1E104	viewLinc/Vancouver	Tuesday, October 3...	10 months, 11 days...	Off	Required (not acknowl...
Blue	Low Threshold location val...	Channel1 RTD deg...	HMT140	EGP3606C	viewLinc/Vancouver	Friday, February 9S...	9 months, 6 days, 1...	On	Not required (not ackn...
Blue	Device Calibration Reminde...	Temperature (21452)	Logger 09051049	09051049	viewLinc/Vancouver	Friday, July 25, 201...	3 months, 15 days, ...	On	Required (acknowledge)
Yellow	Communication Alarm: Defa...	Voltage (00024)/Vol...	ovens logger	10104019	viewLinc/Vancouver	Monday, October 5...	1 month, 5 days, 6...	On	Not required (acknowle...
Blue	Device Calibration Reminde...		HMT140 #64 E000...	E006902C		Thursday, October 5...	25 days, 3 hours, 4...	On	Required (acknowledge)
Red	Configuration Changed Alar...					Tuesday, October 2...	20 days, 1 hour, 55...	On	Required (not acknowl...
Red	Configuration Changed Alar...					Wednesday, Octobe...	19 days, 10 hours, ...	On	Required (not acknowl...
Red	Configuration Changed Alar...					Wednesday, Octobe...	18 days, 20 hours, ...	On	Required (not acknowl...
Red	Configuration Changed Alar...					Monday, October 2...	14 days, 8 hours, 1...	On	Required (not acknowl...
Red	Configuration Changed Alar...					Tuesday, October 2...	13 days, 2 hours, 5...	On	Required (not acknowl...

- ① **Color code:** Used to help identify severity of condition.
- ② **Duration:** Indicates how long condition has been present.
- ③ **State:** Indicates whether alarm condition is in effect.
- ④ **Auto Refresh On:** With this option selected, Alarm listing updates automatically whenever there is a change. Turn off this option if you are

reviewing a long list of alarms, as it may delay the alarm selection process.

⑤ **Location ID:** The number after the Location name (for example, 15494) is the unique location ID. In case more than one Location has been given the same name, this number provides a unique ID so you can differentiate between them.

Receiving and Acknowledging Alarms

All viewLinc Users can receive alarm notification via Email or SMS text, whether or not they are logged in to viewLinc. However, only viewLinc Users with the Right to Acknowledge Alarms (or higher) and Access to the Location where the Alarm is occurring can acknowledge alarms (for information about User Rights and Access Control permissions, see “Controlling Access to viewLinc” on page 38).

An acknowledgement indicates to the viewLinc system that the alarm condition is recognized. Whatever steps are taken to correct the issue is stored as Acknowledgement information, such as the action taken and any comments, and is tracked in the Event Log.

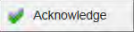
If your system requires alarm acknowledgement, alarm notifications must be acknowledged. An alarm notification message can be configured to be sent continuously by the viewLinc server until it is acknowledged.

Ways to Acknowledge Alarms

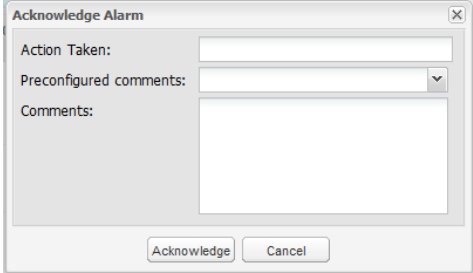
There are four ways to acknowledge alarms:

- In the viewLinc **Locations** window, on the **Location Alarms** tab (for Location-specific alarms).
- In the viewLinc **Alarms** window (displays all active alarms on viewLinc network, to which the User has assigned access permissions).
- On a Pop-up Trend graph.
- On an Email or SMS on your mobile device (see also, “Acknowledge Alarms with viewLinc Mobile” on page 164).

To acknowledge alarms from the Location Alarms tab:

- 1 With the **Locations** window open, select a Location or Zone in the Locations tree.
- 2 Click the **Location Alarms** tab, select the active alarm, then right-click to select .

The **Acknowledge Alarm** window appears:



- 3 In the Acknowledge Alarm window, enter the actions taken and your comments. You can select a comment from the preconfigured comments drop-down, if there are any available.


For example, if you receive a high temperature alarm for a refrigeration facility, but you are not in the facility where the alarming is happening, you may need to notify a person working at the Location to investigate the problem. In this case, if a refrigerator door had been left open, the facility operator would close the door and add this action to the Acknowledge Alarms window.

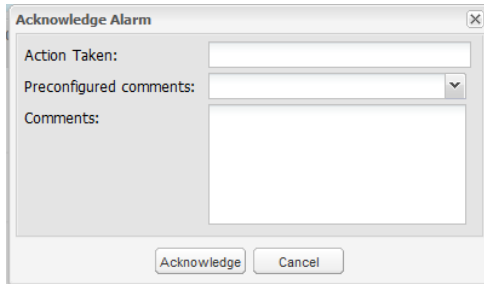
- 4 Click **Acknowledge**. Your comments and actions are added to the Event log and the Acknowledge Alarm box closes. Locations are updated with this change in status, as well as the Acknowledgement column in the Alarms window.

To acknowledge alarms from the Alarms window:

- 1 On the viewLinc desktop, select **Options | ⚠ Alarms** to view the list of all active alarms.
- 2 Select the Alarm you wish to acknowledge. If you wish to acknowledge multiple alarms, press the **[Ctrl]** or **[Shift]** keys while you click multiple Locations.


Note: When selecting multiple Locations, it is recommended that you de-select the **Auto Refresh On** option, as this feature can delay the selection process.

- 3 Right-click on a selected Location and select , or click **Options | Acknowledge**. The Acknowledge Alarm window appears, prompting you to enter the actions taken and comments.



- 4 Click **Acknowledge**. Your comments and actions are added to the Event log and the Acknowledge Alarm window closes. Locations are updated with this change in status.

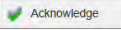
To acknowledge all inactive alarms:

- 1 On the viewLine desktop, select **Options |  Alarms**.
- 2 Select **Options | Acknowledge All "Off" Alarms**. Multiple Location selection is not required.

Note: The acknowledgement column reads, **Not required**, for all active alarms that do not require acknowledgement. Inactive alarms (the alarm condition is no longer present) that were not acknowledged, will read **Off**.

- 3 In the **Acknowledge All "Off" Alarms** window, indicate any action taken, select a preconfigured comment, if available, or enter any additional comments about why you are acknowledging an 'Off' alarm.
- 4 Click **Acknowledge**.

To acknowledge an alarm from a Pop-up Trend graph:

- 1 With the **Pop-up Trend** window open, click the **Location Alarms** tab.
- 2 Select the active alarm, then right-click to select . The **Acknowledge Alarm** window appears, prompting you to enter the actions taken and comments.
- 3 Click **Acknowledge**.

To acknowledge an Alarm by Email or SMS text:

- 1 Open alarm Email (the From address will be your server administrator account). For example: viewlinc.boulder@companyemail.com
- 2 Depending on which template you use, the default Email and/or SMS message displays with a standard format. Here is an example default Threshold Alarm:

Subject: [Ticket ###] viewLinc -
Description of condition and [Location],
[Zone]

Body: There has been a Threshold alarm on
[data] at [Location], [Zone].
[Event Details]
[Device information]

- 3 To acknowledge an Email, send a Reply message which includes the default Subject line (with Ticket number), and enter your PIN in the Body of the message.

Note: Sending a Reply without content in the Body area or the ticket number in the subject line does not acknowledge the alarm.

Subject: RE: [Ticket ###] viewLinc -
Description of condition and [Location],
[Zone]

Body: PIN####

- 4 To acknowledge an SMS message, send a reply message which includes:

Ticket### PIN####


Pausing Alarms

To avoid receiving unnecessary alarm notifications, you may want to pause alarming on one or more Devices or a Host (requires Manage Devices Right and Configure Alarms Permission for the Location).


This feature is useful if you need to move several Devices (which trigger communication alarms), or if a certain known situation may result in conditions exceeding set thresholds (which trigger Threshold alarms).

You can pause Threshold alarms for a specific Location or a Zone, or pause all alarm conditions for all Channels on a Device or all Devices connected to a Host, for up to 24 hours. Pausing alarms is more convenient than disabling individual alarms on specific Devices, temporarily; however, if you need to stop alarming for a longer period, use the disable alarming function (see “Disabling Device Alarms” on page 109).

To pause Threshold alarming at a single Location:



- 1 In **Locations**, on the **Table View** tab, select the alarm, then click **Options** |  **Pause Threshold Alarming**. The active Alarms list continues to refresh and show the most current alarms while the **Auto Refresh On** option remains checked.
- 2 In the **Pause Alarming** window, enter a reason for pausing alarming, using a preconfigured comment (if available), or enter your own notes in the Comments text box.
- 3 Click **OK**.

To pause Threshold alarming for a Zone:

- 1 In **Locations**, navigate to a Zone in the Locations tree, then click **Options** |  **Pause Threshold Alarming**.
- 2 In the **Pause Alarming** window, enter a reason for pausing alarming, using a preconfigured comment (if available), or enter notes in the Comments text box.
- 3 Click **OK**.



To pause all Channel alarming on a Device:

Note: This function requires Manage Devices Right.

- 1 In **Locations Manager**, on the **Devices** pane, select the Device, then click **Options** |  **Device** |  **Pause Device Alarming**.
- 2 In the **Pause Device Alarming** window, enter a reason for pausing alarming (select a preconfigured comment, if available, or enter notes in the Comments text box).
- 3 Click **OK**.

To pause all Device alarming on a Host:

Note: This function requires Manage Devices Right.

- 1 In **Locations Manager**, on the **Devices** pane, select the Host, then click **Options** |  **Host** |  **Pause Host Alarming**.
- 2 Click **Yes** to pause Host alarming.
- 3 In the **Pause Alarming** window, enter a reason for pausing alarming, using a preconfigured comment (if available), or enter notes in the Comments text box.
- 4 Click **OK**.

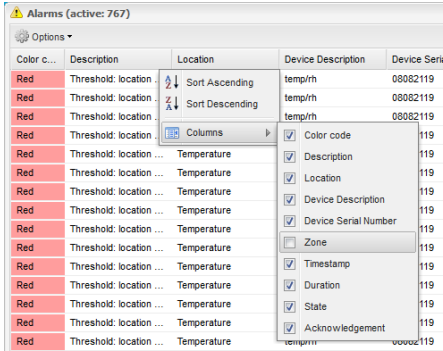
Managing Alarms View

All Users can change which columns display on their desktop, and the column sort order.

Note: The color of an Alarm row is defined by the Alarm template.

To re-arrange the sort order of Alarm table:

- 1 Select any column heading, click the arrow drop-down, and select **Columns**.



- 2 Select or deselect the columns you want to view. New columns appear automatically, and removed columns disappear automatically.
- 3 Click anywhere in the window to close the Column content options.

Alarm Reporting

For historical record-keeping purposes, you may want to print a hard copy of specific alarm conditions for a specified time period.

In viewLinc, you can print alarm data directly to your printer (.pdf format), or export alarm data to a spreadsheet (.xls). In the spreadsheet format, you can control how the information displays, to meet your company’s reporting requirements.


Refer to Chapter 7: Reporting and Historical Data, for more information on Alarm, Location History and System Reports.

To print a report on all active alarms:

- 1 In the viewLinc **Alarms** window, select **Options | Print** . A new browser tab appears displaying a printer-friendly list of alarms.

- 2 In the **Print** window, choose your desired print settings, then click **Print**.

To export alarms to Excel format:

- 1 Select **Options** |  **Export to Excel**. This will export all alarms in this list to a .tsv format file.
- 2 At the prompt, choose to **Save** (file is saved to your default Downloads folder) or **Open** this file. If you receive an error message stating Windows cannot open the file, select MSExcel to view the file and make changes.

CHAPTER 6

EVENTS

All viewLinc system activity is treated as an Event, and all Events are tracked in an Events log (**Options | Events**).

Data tracked as an Event is different from the monitoring data logged in a Device. Here are some key differences:

- Events occur within the viewLinc system: alarms, transfers of data from Devices, 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 history, Event Validation Alarms notify you if the viewLinc Event Log has been tampered with externally. For more about Event Log validation alarms, see, “Event Validation Alarms” on page 118.

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

In this section, you’ll learn about:


- Viewing Events
- Adding Comments to Events
- Adding Custom Events
- Printing and Exporting Event Logs

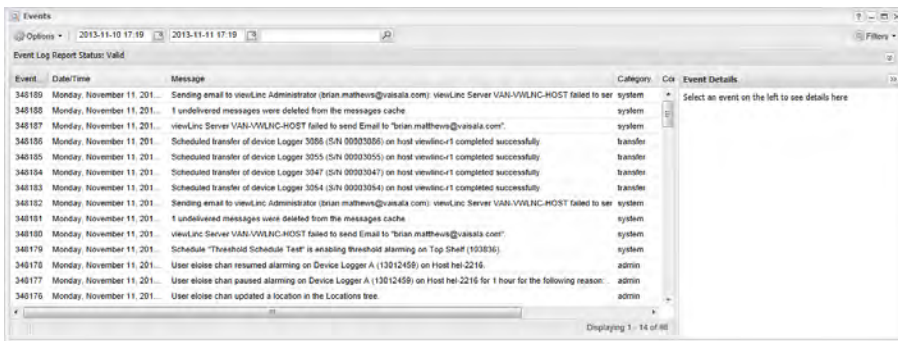
Viewing Events


Events are viewed in the Events window as an Event Log, a text-based listing of all system events occurring with the Devices on your system.

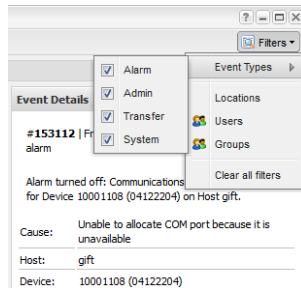
Note: An Alarm Event is issued if there is a system time change.

To view Events:

- 1 From the viewLinc desktop, select **Options** |  **Events**. The Event Log appears, displaying a numbered list of events, and, if available, comments on the Event in the Event Details area to the right of the event listing.



- 2 To ensure the Events Log is intact, review the comments listed in the **Event Log Report Status** area, at the top of the screen. Additional details may be available when you click the expand icon, .
- 3 To view Events during a specific period, use the calendar fields at the top of the window to enter a date (using format YYYY/MM/DD HH:MM), or use the calendar button to specify a date range.
- 4 To view specific types of Events, use the **Filters** box list in the upper right corner. Select or deselect different event types (Alarm, Admin, Transfer and System Events).



You can also filter the list to view Events acknowledged by specific Users or Groups or Events occurring at a specific Location.

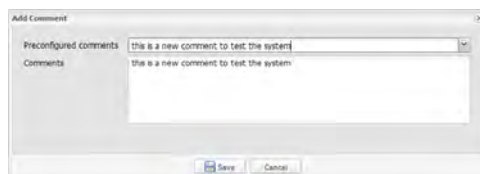
- 5 Click outside the Filters dropdown and the list refreshes automatically (or click **Options** | **Refresh** to refresh the list manually).

Adding Comments to Events

You may want to add comments to an Event Log, perhaps to outline why an event occurred or what was done in response to an event or problem. Comments added to an Event Log can be used to provide additional notes about a specific Event, such as an Administrator providing clarification about a change affecting a specific Group of Users or a Location.

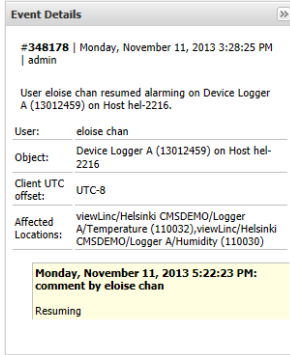
To add a comment to the Event Log:

- 1 From the viewLinc desktop, select **Options** | **Events** (or click the Events shortcut on the viewLinc desktop).
- 2 Select an Event, then click **Options** | **Add Comment**. The **Add Comment** window appears.



- 3 Enter a preconfigured comment (if available), or enter your own comments, then click **Save**.

- 4 To view a comment for a particular event, highlight the row containing that event and look for the comment in the **Event Details** area. Comments added in the Events Log appear in a yellow box after Event Details.





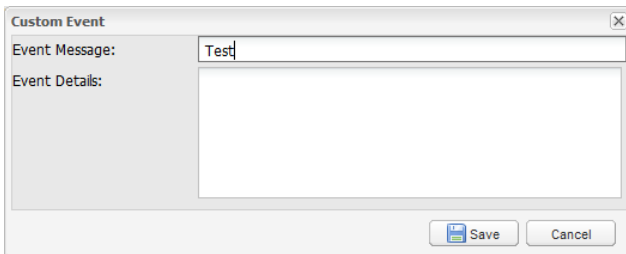
These additional comments also appear in the Event Log Report.

Adding Custom Events

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

To add a custom Event:




- 1 From the viewLinc desktop, select **Options** |  **Events** (or click the Events desktop shortcut).
- 2 In the Events window, select **Options** |  **Add Custom Event**.
- 3 Fill in the custom event PM message and details, then click **Save**.



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.

To print the event log:




- 1 From the viewLinc desktop, select **Options** |  **Events**.
- 2 Specify the parameters for the report:
 - In the date/time fields, enter a date and/or time in 24-hour notation, or click the calendar icons to make your selection.
 - Use the **Filter** button to include the types of Events, and from whom/where they were generated.
- 3 To update the Event log, click **Options** |  **Refresh**.
- 4 Click **Options** |  **Print**.
- 5 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.mathews@vivaala.com): viewLinc Server V100-V10LINC-HOST failed to send Email to 'Brian.mathews@vivaala.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 V100-V10LINC-HOST failed to send Email to 'Brian.mathews@vivaala.com'.	system	Email text: [Ticket 128790] viewLinc - Communication Alarm on Device 'WRT14XGAB0'		admin	System
Recipients: Brian.mathews@vivaala.com Error: Message pruned Destination: C:\Users\Public\Documents\viewLinc\viewLinc\write\viewLinc\events\Logger_3086-00003086-2013-11-11 17:43:15.tsv Device: Logger 3086 (S/N 00003086) on host viewLinc-01							
348186	Monday, November 11, 2013 4:53:51 PM	Scheduled transfer of device Logger 3086 (S/N 00003086) on host viewLinc-01 completed successfully.	transfer			admin	Logger 3086
Destination: C:\Users\Public\Documents\viewLinc\viewLinc\write\viewLinc\events\Logger_3055-00003055-2013-11-11 17:44:38.tsv Device: Logger 3055 (S/N 00003055) on host viewLinc-01							
348185	Monday, November 11, 2013 4:46:29 PM	Scheduled transfer of device Logger 3055 (S/N 00003055) on host viewLinc-01 completed successfully.	transfer			admin	Logger 3055
Destination: C:\Users\Public\Documents\viewLinc\viewLinc\write\viewLinc\events\Logger_3086-00003086-2013-11-11 17:43:15.tsv Device: Logger 3086 (S/N 00003086) on host viewLinc-01							

- 6 Set your print parameters and print the Event Log (**File** | **Print**).

To export an Event log:

- 1 From the viewLinc desktop, select **Options** |  **Events**.

- 2 In the header date/time boxes, enter a date and/or time in 24-hour notation, or click the calendar icons beside each box to make your selection.
- 3 Click the  **Filters** box list to the right of the date and time selector, to choose different event types by checking or unchecking **Alarm**, **Admin**, **Transfer**, and/or **System Events**.
- 4 Click **Options** |  **Refresh**.
- 5 Click **Options** |  **Export to Excel**. A file download window opens, prompting you to open or save the events .tsv file (in Microsoft Excel format).

CHAPTER 7

REPORTING

Using the historical data collected by Vaisala Devices, you can automatically create graphs and reports to analyze changes in data over a specific period of time, or compare conditions recorded by different Devices.

Historical data from Vaisala Veriteq Loggers can also be transferred to a local directory on a set schedule. Once transferred, data can be exported or printed, depending on your reporting needs.

This chapter reviews:

- Types of Reports
- Generating and Printing Reports
- Creating New Reports
- Deactivating and Deleting Reports
- On-Demand Reports
- Transferring Data




Types of Reports

viewLinc provides a set of default reports to help you easily view data trends or alarm statistics. No specific Rights are required to generate default or custom reports – any User can generate a report for a Location to which they have access permission.

Administrators or Users with the Manage Reports Right can also create custom reports.

Default viewLinc Reports

The standard reports available in viewLinc are:

-  **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 values (presented in both graphical and tabular format).
-  **System reports** provide overall snapshots of specific system information, such as system configuration, transfer schedules, and lists of available templates. You can also generate a system report to list current Users and Groups, Locations and Access Control details.

Custom Reports

When creating a custom report (Administrators or Users with Manage Reports Right) you can include information about the report owner (a User or Group authorized to modify the report), time zone to use for generating data, individuals who receive the report by email and the schedule for generating the report, if required, and report contents (content options change depending on the type of report).

Generating and Printing Reports

The reports available for Users to generate and print are listed in the Reports window. You can select an available report format to generate and print at any time, or your Administrator may set you up to receive reports by Email according to a set schedule.

Reports are current as of the moment they are generated. This means that the list of reports you see in the Reports window is in fact a list of report 'shells', waiting to be populated with generated data.

Note: Reports can also be set up to be available at any time, meaning that any User (not only the report owner), with access permission to a specific Location, can generate an On-demand report (see “On-Demand Reports” on page 150).

All available generated reports are viewable in the Reports Progress window.

To generate an existing report:


- 1 From the viewLinc desktop, choose **Options | Reports** and then select the report you want to generate from the **Report Definitions** tree.



The report parameters appear in the **General, Content, Source Data, and Page Layout** tabs.

Note: Users or Groups can only view the report parameters for reports they create, or reports to which they have been granted owner access.

- 2 On the **Report Definitions | Options** menu, select:
 - **Generate PDF Report:** Available for Alarm and Location History reports. Choose this option to generate the report according to PDF settings specified in the Scheduled Generation parameters.
 - **Export to Excel:** Generate the report in .tsv format.
 - **Generate and Email Report:** Email report to predetermined list of Users/Groups as a PDF file, according to Scheduled Generation parameters.

- 3 In the **Reports Progress** window, the most recently generated report appears at the top of the report list (if Reports Progress does not display automatically, open it from the task bar ). Once report generation is complete, open or save the report by clicking the link, **Download report**, in the **Progress** column.

Generated reports are available to download from the Reports Progress window for 1 hour. Scheduled reports are available for 12 hours, to ensure that any reports auto-generated during off-peak hours remain available in regular work hours.

Reviewing Report Progress

Each time you generate a report, the Reports Progress window displays automatically. Note that if the Reports Progress window is already open, it remains hidden behind the currently active window (to open the Reports Progress window, click the taskbar,



To open the Reports Progress window:


- ▶ Choose **Options** |  **Reports Progress**, or click the Reports Progress icon on your viewLinc desktop, .

Creating New Reports

There are two ways to create new Alarm, Location History or System reports: create a new report using the Reports window parameters tabs, or create a copy of an existing report (cloned report).

Creating an Alarm Report

To create a new Alarm report:

- 1 In the **Reports** window, select **Options** |  **New Alarm Report**.
- 2 Enter the name of the new report.
- 3 Complete the **General** tab:

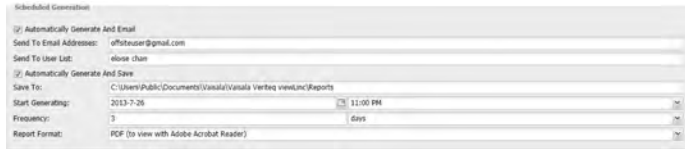
- **Report Owner:** Select a User or Group you want to have access to modify or generate this report.
 - **Range Type:** Specify the period you want the report to include using the default option, **Most Recent Events**, or a specific date range. If you choose a fixed date range from the Range Type box, calendars will appear to indicate from/to dates. This option is available for Alarm and Location History reports.
 - **Duration:** 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 box. This option is available for Alarm and Location History reports.
 - **Time Zone:** Change this value only if a specific time zone adjustment is required for the report, otherwise leave it as the default and it will report for your server time zone. If you do select a different time zone, all report dates, scheduled generation and printed timestamps will be relevant to the selected time zone.
 - **PDF Font:** Choose the format for the report output. If you want to generate a report in Chinese, select **Chinese character support**. This option is available for Alarm and Location History reports.
- 4** In the **Scheduled Generation** area of the **General** tab, choose one of the following:

Note: A report can be generated at any time manually, or automatically generated on a set schedule.

- **Automatically Generate and Email:** Choose this option to send the report directly to specific Email addresses, or to a viewLinc Group.
- **Automatically Generate and Save:** Choose this option to generate the report automatically according to a set schedule, and save it to a specific file location:
 - **Save To:** Specify where you want the report saved.
 - **Start Generating:** Enter the start date and time you want the report generated.

- **Frequency:** Specify whether you want the report generated hourly, daily, weekly, or monthly.



For example, to run the report every 3 days at 11 pm, the field would look like this:



- **Report Format:** (PDF for viewing in Acrobat, or tab-separated, for Excel), to automatically generate and save the report to a specific file location, or send the report to an email address or a list of addresses (use a comma to separate email addresses). You can also schedule when you want the report to generate, and how frequently you want it generated.



Note: For large report data sets, we recommend that you schedule report generation at a time when few Users are logged into the system.

- 5 On the **Content** tab, select options according to the report type:
 - **Detail Level:** Select whether to print a brief report (displays one line for each alarm), or a Detailed report (displays details about all alarm activities).
 - **Include Device Alarms:** Specify the types of Device Alarms to include in the report.
 - **Include Location Threshold Alarms:** Select this option to include threshold alarm data, then specify the threshold category to include, Alarms or Alarms and Warnings.
 - **System Alarms:** Choose whether to include system alarm information (threshold types).
- 6 On the **Source Data** tab define the report content scope, **All Locations**, or **Selected Locations And Zones**.
 - To select all Locations in a Zone, select the checkbox corresponding to the Zone name.

- To select a specific Location in a Zone, expand the tree to find and select the Location.
- 7 On the **Page Layout** tab define your report display options:
 - **Page Header/Page Footer** options: choose the pages on which you want a Header or Footer displayed. To define the content of the Header or Footer, enter text in the Left Header/Footer, Center Header/Footer or Right Header/Footer fields. Use the Footer field to select Signature box or Comments boxes.
 - You can also choose a customized icon in the left header section by clicking “Upload” or select from a list of provided icons by clicking the Image File dropdown.
 - Choose the type of paper you want to print on and the orientation.
 - 8 From the **Reports** window, select **Options** |  **Save** (the  exclamation point icon indicates when you have made changes that need to be saved).

Creating a Location History Report

To create a new Location History report :

- 1 From the viewLinc desktop, select **Options** |  **Reports**.
- 2 In the **Report Definitions** tree, select **Options** |  **New Location History Report**.
- 3 Enter the name of the new report.
- 4 Complete the **General** tab:
 - **Report Owner:** Your viewLinc User name appears automatically. If you have Admin access, you can select a different User to have access to modify this report. If a User does not appear in the list, you may need to create a User account (see “Controlling Access to viewLinc” on page 38).
 - **Range Type:** Specify the period you want the report to include using the default option, **Most Recent Events**, or a specific date range. If you choose a fixed date range from the

Range Type box, calendars will appear to indicate from/to dates.

- **Duration:** 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 dropdown list. This option is available for Alarm and Location History reports.
 - **Time Zone:** Change this value only if a specific time zone adjustment is required for the report, otherwise leave it as the default and it will report for your current time zone. If you do select a different time zone, all report dates, scheduled generation and printed timestamps will be relevant to the selected time zone.
 - **PDF Font:** Choose the format for the report output. If you want to generate a report in Chinese, select **Chinese character support**. This option is available for Alarm and Location History reports.
- 5 In the **Scheduled Generation** area of the **General** tab, choose the following:
- **Automatically Generate and Email:** This option is used to send the report directly to specific Email addresses (including non-viewLinc Users), or to a viewLinc Group.
 - **Automatically Generate and Save:** Use this option to save report data automatically according to a set schedule:
 - **Start Generating:** Enter the start date and time you want the report to generate
 - **Frequency:** Specify whether you want the report generated hourly, daily, weekly, or monthly.
 - **Report Format:** PDF (for viewing in Acrobat), or tab-separated (for Excel). To automatically generate and save the report to a specific file location, or send the report to an Email address or a list of addresses (use a comma to separate email addresses). You can also schedule when you

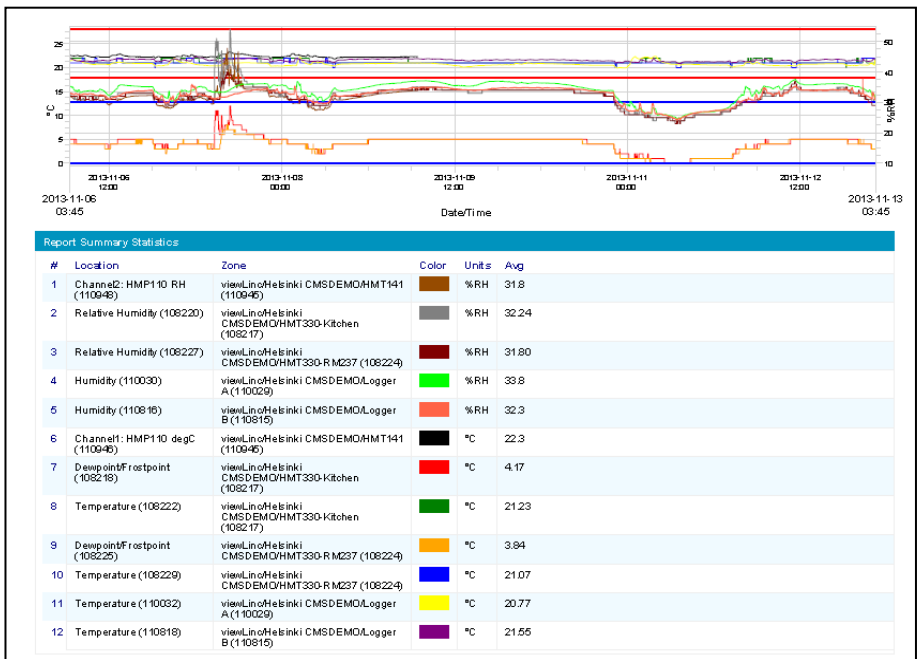
want the report to generate, and how frequently you want it generated.

Note: 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.

6 On the **Content** tab, identify the data you want included in the report:


- **Title Page:** Reviews contents of the report.
- **Include Trend Graph:** If you select this option, a graphical display of the data is included in the report.

You can also choose to include threshold lines, a statistics summary (selected on the Statistic Settings tab), and all Location data on a single graph (by default all Location data, according to measurement unit, is included on a single graph). You can also choose to group measurement units together on the same graph (a single graph can only include up to 4 measurement unit types).




- **Include Interval Statistics Graph:** Select this option if you want to define how information will display on your report, then choose options on the **Statistics Settings** tab (see step 7).
 - **Tabular Data:** Choose to include additional data tables in the report. If you choose to include Historical Samples, specify the timestamp data period you want used, and whether to use the last sample timestamp that reflects the closest timestamp to the specified data period (every 5, 15, 30, or 60 minutes), or the closest reading to the period interval timestamp. This option is useful when reporting Locations have different sample rates.
- 7 If you chose the option, **Include Internal Statistics Graph** (on the **Contents** tab), complete the following:
- **Include Statistics At Intervals:** To intermittently generate statistics within the time frame of a report. For example, if your report generates data based on a seven day (weekly) interval, you may want to view statistics daily by selecting the Specify Duration radio box and specifying 1 day, 0 hours.
 - **Include:** Select the types of statistical data you want to add to the report, including maximum value, average value, minimum value, standard deviation, sample count.
 - **Mean Kinetic Temperature (MKT):** Specify the activation energy as KJ/mol.
- 8 On the **Source Data** tab define the report content scope, **All Locations**, or **Selected Locations And Zones**.
- To select all Locations in a Zone, select the checkbox corresponding to the Zone name.
 - To select a specific Location in a Zone, expand the tree to find and select the Location.
 - To specify a color to highlight a specific Location's data, select the Location, then select an option from the color dropdown. If you select Auto, viewLinc chooses a color according to the default color spectrum.

Description ^	Type	Color	Lo
System/Lab Area 3/Humidity	Location	Auto	At
System/Lab Area 3/Temperature	Location	Auto	At






Note: When Location line colors are set to **Auto**, viewLinc assigns the next free color from a built-in palette of colors (see page 185 for the color spectrum sequence).

Repeat the colour selection for each Location you want to include on the report.

- **Default Scaling:** Enter the Low and High values to define the graph measurement range.
 - **Show Markers:** Choose this option to identify graph lines with numbers (this is useful if you do not plan to print graphs in colour).
- 9 Use the **Page Layout** tab to define the headers, footers, paper size and orientation:
- a 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.
 - b To define the content of your header or footer, enter text in the Left, Center or Right fields, or use the Footer field to select Signature box or Comments boxes.
 - c Choose the paper size you want to print on and the orientation (portrait or landscape).
 - d Select a header image by using the Image File dropdown (for previously used images) or upload a new image file by clicking the **Upload** button and clicking **Browse** to locate the file.
- 10 Select **Options** |  **Save**.

Creating a System Report



To create a new System report:

- 1 From the viewLinc desktop, select **Options** |  **Reports**.
- 2 In the **Report Definitions** tree, select **Options** |  **New System Report**.
- 3 Enter the name of the new report.
- 4 Complete the **General** tab:
 - **Report Owner:** Your viewLinc User name appears automatically. If you have Admin access, you can select a different User to have access to modify this report. If a User does not appear in the list, you may need to create a User account (see “Controlling Access to viewLinc” on page 38).
 - **Time Zone:** Change this value only if a specific time zone adjustment is required for the report, otherwise leave it as the default and it will report for your current time zone. If you do select a different time zone, all report dates, scheduled generation and printed timestamps will be relevant to the selected time zone.
- 5 In the **Scheduled Generation** area of the **General** tab, choose the following:
 - **Automatically Generate and Email:** This option is used to send the report directly to specific Email addresses (including non-viewLinc Users), or to a viewLinc Group.
 - **Automatically Generate and Save:** Use this option to save report data automatically according to a set schedule:
 - **Start Generating:** Enter the start date and time you want the report to generate.
 - **Frequency:** Specify whether you want the report generated hourly, daily, weekly, or monthly.
- 6 Select **Options** |  **Save**.

Cloning an Existing Alarm, Location or System Report

If you want to define a new report which is similar to an existing report, save time and use the Clone Report feature.

To clone an existing report:

- 1 In the **Reports** window, select an existing report you want to copy.
- 2 Choose **Options** |  **Clone Report**.
- 3 Modify the report parameters, as required.
- 4 To assign a new name for the report, right-click on the title to make the text editable, and enter the report name.
- 5 Select **Options** |  **Save**.


Your new report is saved and appears alphabetically in the report list.

Deactivating and Deleting Reports


You can deactivate or permanently delete a report. When you deactivate a report, you prevent it from being used or auto-generated for a specific period of time.

If you no longer want a report, simply delete the report.


To deactivate a report:

- 1 In the **Reports** window, select the report you want to delete from the **Report Definitions** tree.
- 2 Select **Options** |  **Deactivate Report**.

To reactivate a report:

- 1 In the **Reports** window, select **Options** | **Show Deactivated Reports**.
- 2 Select the report you want to reactivate from the **Report Definitions** tree.
- 3 Select **Options** |  **Reactivate Report**.

To permanently delete a report you no longer use:


- 1 In the **Reports** window, select the report you want to delete.
- 2 Select **Options** |  **Permanently Delete Report** (or use the right-click menu).
- 3 Click **Yes** to confirm.

On-Demand Reports


Setting up On-Demand reports allows you to quickly generate a report from the Locations window, using any Location as the data source.

Administrators, Users assigned Manage Reports Right, and Report Owners can specify which of their reports can be accessed on-demand by other Users.

To make an on-demand report available to other Users:

- 1 In the **Reports** window, select a report from the **Reports Definitions** tree.
- 2 On the **General** tab, select **Available as On-demand Report**.
- 3 Click **Options** |  **Save**.

To generate an on-demand report:

- 1 Open the **Locations** window, select a Location or a Zone.
- 2 Select **Options** |  **On-demand Reports** (or use the right-click menu), then select an available report.
- 3 Select the output method. If report is being sent by Email, complete the **Generate and Email Report** window:
 - Choose the report format.
 - Enter Email address of recipient, and any viewLinc Users or Groups to whom you want the report sent.
 - Add additional notes to the **Subject** and **Body** fields.
- 4 Click **OK**.

Transferring Data

In addition to being able to view Device history in viewLinc, you can transfer Vaisala Veriteq Device data for viewing, generating reports, and exporting to an external spreadsheet program or other data analysis tool.

Using Transferred Data in Reports

For convenience, your system administrator can set up viewLinc to automatically transfer Vaisala Veriteq Device data according to a set schedule, allowing you to use the data for additional reporting needs (.xls spreadsheets).

Since transfers can be scheduled in advance, you do not need to be available when a transfer occurs. And no matter how frequently (or infrequently) you schedule data transfers, data in a Device remains intact and is recorded indefinitely (or until the Device reaches its memory capacity).

When Should I Transfer Data?

It is recommended that you transfer Vaisala Veriteq Device data on a regular basis for backup purposes, and to ensure no data is overwritten due to a full memory.


To avoid overwritten data, all Vaisala Veriteq Devices are assigned a default transfer schedule when each Device is discovered by viewLinc (during set up of your viewLinc system). The transfer schedule is enabled and scheduled for a seven-day period; however, if you expect that your Device will reach its storage capacity before this period is over, you can adjust the period to ensure no data is lost.

Note: Refer to your device-specific User Guides for more information on managing device data storage capacity.

Creating Transfer Schedules

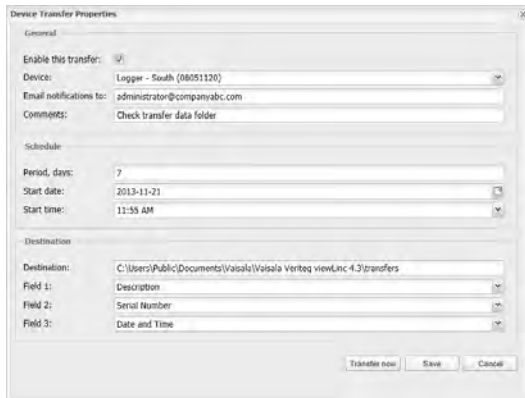
To create a transfer schedule for a Vaisala Veriteq Device:

Note: Administrator or Manage Devices Right is required.

- 1 From the viewLinc desktop menu, select **Options |  System Configuration |  Transfers.**

- 2 In the **Transfers** window, select **Options** | **+ New Transfer**.
- 3 On the **Device Transfer Properties** window, in the **General** area select **Enable this transfer** and complete the following fields:
 - **Device:** Click in the field and choose the Logger for which you want to set the transfer.
 - **Email notifications to:** Enter an Email address for the individual you want to receive notification, should the transfer fail. You can choose a single Email address, a list of Email addresses separated by commas, or a distribution list created on your mail server by the IT administrator (see “Choosing System Preferences” on page 27).
 - **Comments:** Enter any specific comments you want to associate with this transfer, such as its purpose, and to whom Email notifications should go.
- 4 Ensure correct mail server settings have been set. See “Choosing System Preferences” on page 27.
- 5 In the **Schedule** area, choose a transfer schedule interval and start date and time.

For example, you could set up a data transfer every 7 days, beginning 2013-11-21 at 11:55 PM. It would look like this:



- 6 In the **Destination** area, complete the fields:
 - **Destination:** Choose the destination directory for the saved data (.spl) file (do not use a mapped drive path).
 - Sample directory paths could include: c:\Device_files or \\<machinename>\<destination_dir>. We recommend you use a directory on the viewLinc Host Server (for example, c:\<destination_dir>).

Note: During a data transfer, you may be prompted to enter a valid username and password to save the file to a target directory or shared directory. You also need to ensure that the account which installed viewLinc (that is, which runs the viewLinc Enterprise Server service) has sufficient permissions to write to the directory where you want the transferred data to go. For more on Services with viewLinc, see “APPENDIX: FAQs & TROUBLESHOOTING” on page 167.

 - **Field 1/2/3:** Specify the order you want used to identify the three fields which will make up the transfer filename. Filenames for .spl files are created from combinations of the Device's description, serial number, and the date and time the file was saved.

For example, Device ID-08094523-2011-04-22 16-30-01.spl.
- 7 To test that the transfer will complete as defined, click **Transfer Now**. Use Windows Explorer to ensure the data file transferred to the specified file location.
- 8 Click **Save** to save these settings for a scheduled transfer.

Note: If comments are enabled from system preferences, the Add Comment window appears. Select a preconfigured comment or enter your own. A row containing information on the scheduled transfer for each Device you've set up appears in the Event Log.

Performing an Immediate Data Transfer




You may be required to initiate an immediate transfer, before a scheduled transfer is due, perhaps after receiving an alarm that Logger memory is running low.

To transfer data now:

- 1 Follow steps 1 through 8 in “Creating Transfer Schedules” on page 151 (or edit an existing transfer schedule), and then click **Transfer Now** (or use the right-click menu). The data transfers immediately.
- 2 Click **Save** to save the scheduled transfer settings, or click **Cancel** to close.

Editing Transfer Schedules

To edit a scheduled transfer:



- 1 From the viewLinc desktop, select **Options |  System Configuration |  Transfers**.
- 2 Select the row containing the scheduled transfer(s) to edit.
- 3 Select **Options |  Edit Transfer**.
- 4 The **Device Transfer Properties** screen appears. Edit the transfer details as required.
- 5 Click **Save**.

Deactivating Transfer Schedules

When a Device is deactivated, all associated transfers are automatically deactivated; however, you may want to deactivate a specific transfer schedule, independent of the Device.

A deactivated transfer is automatically hidden from view.

To deactivate a scheduled transfer:




- 1 Open the Transfers window (viewLinc desktop **Options |  Transfers**).
- 2 Select the row containing the scheduled Transfer you want to deactivate. Click in a column heading to sort alphabetically, in ascending or descending order.
- 3 Click ** Deactivate Transfer** (or use the right-click menu).
- 4 To confirm the deactivation, click **Yes**.

To check that you deactivated the correct transfer, select **Options | Show Deactivated Transfers**; all deactivated transfers appear in your list in grey text.

Disabling Transfer Schedules

Disable a transfer schedule when you want to deactivate a transfer schedule temporarily. A disabled transfer remains in view, marked with an **X**.

To temporarily disable scheduled transfers:

- 1 From viewLinc, select **Options |  System Configuration |  Transfers**.
- 2 In the **Transfers** window, select the row containing the scheduled transfer to edit.
- 3 Click **Options |  Edit Transfer**.
- 4 From the **Device Transfer Properties** screen, deselect the option, **Enable this transfer**.
- 5 Click **Save**.

CHAPTER 8

REMOTE & MOBILE DISPLAY

With viewLinc's touchscreen functionality, it is easy to view and access viewLinc with a remote display terminal, or using a mobile device.

- **Remote Display:** Set up a conveniently located visual display for a specific monitoring environment. A remote monitor is best for areas requiring a larger visual display, without having to set up a complete workstation (with tower or keyboard).

Note: For display purposes only, viewLinc also supports Point-of-Sale (POS) terminals.

- **Mobile Display:** Perform key monitoring and acknowledgement tasks from your smartphone or tablet.

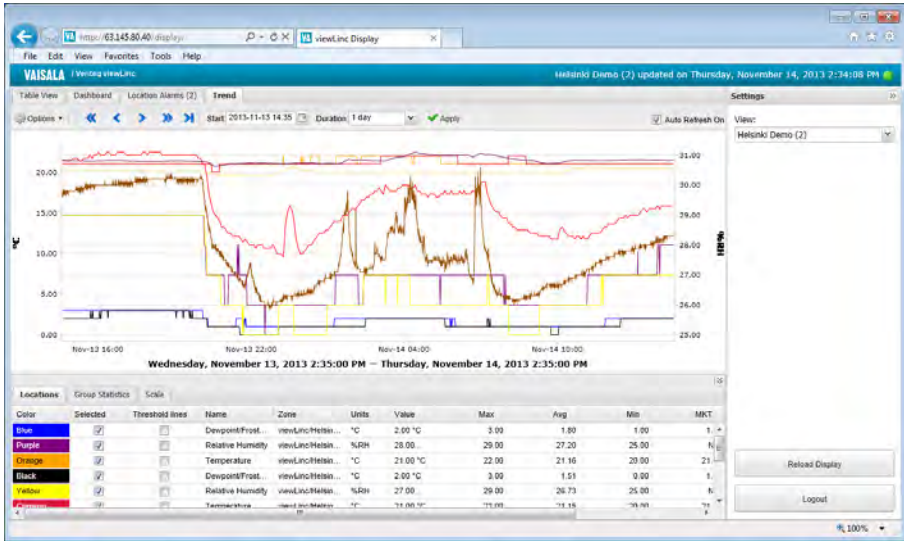
You can access the viewLinc Mobile UI from Apple® iOS 3+ and Android® 2.1+ mobile devices.

This chapter describes:

- Using a Remote Display
- Using viewLinc Mobile
- Viewing Data with viewLinc Mobile

Using a Remote Display

For areas where you want to display monitoring information for increased visibility, viewLinc allows you to set up a touch-screen display terminal, without having to use a full workstation or full desktop setup.



The remote display screen contains the same information as found in the **Locations** window, without the Locations navigation tree. Locations available for monitoring are defined by the default View selected at initial login.

Remote Display Requirements

Before setting up a remote display (perhaps you want to set up an easily visible terminal for a specific laboratory), ensure the display is running Windows (see “viewLinc System Requirements” on page 7), and can connect to a wired keyboard, or display an onscreen keyboard.


Any viewLinc User can log in to the remote display; however, the displayed data is defined by the View and Access Control settings assigned to their User account. By creating a default remote display User View, you can define what you want viewable on the Remote Display.

Note: To change the View, simply log in as another User with different View options (see page 160).

Creating a Default User and View

Administrators can set up a User account as the default log in for the Remote display. The Administrator also defines the Locations available to view, and whether alarms can be acknowledged. The only viewLinc window visible on the remote display is the Locations window.

To set up a User-assigned View for remote display:

- 1 Create a default User account:
 - a In the **System Configuration | Users** window, create a new User (for example, Remote Display User).
 - b Do not assign the User to any Groups.
 - c Do not assign any Rights to the User.
- 2 Assign User Access Control:
 - a In the **Locations Manager** window, select the top level Zone you want displayed on the terminal. Then, on the **Location Properties | Access Control** tab, select **Options |  Add**.
 - b Identify the default User account, and assign required Permission (if the terminal will only be used to view data, select **View**; if the terminal will be used to view and acknowledge alarms, select **Acknowledge Alarms**).
 - c To ensure the User has access to all inherited Locations, check the option, **All children inherit permission**.

For complete instructions on how to create a viewLinc View, see “Setting Up User-specific Views” on page 86.

Setting up the Remote Display

To set up a remote touch-screen display terminal:

Note: You require viewLinc Admin Rights to set up a remote display. Contact your IT network administrator if you require assistance.

- 1 On the viewLinc Server, ensure you have created a User account with access to the View you want displayed on the terminal.

- 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 (“viewLinc System Requirements” on page 7). This will ensure 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, and then choose a View.


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 the last User.

Changing the Remote Display View


To change the View displayed on a remote terminal, you can either select a different View assigned to the User currently logged in, or log in as a new User.

To change the terminal display View:

- 1 On the viewLinc remote display, expand the **Settings** pane (click the Expand icon if required, .
- 2 In the **View** box, select another available View.

The display updates automatically to the new View.

To log in as a new User:

- 1 On the viewLinc remote display, expand the **Settings** pane (if required, click the Expand icon, .
- 2 Click **Logout**.
- 3 At the viewLinc log in prompt, log in as a new User.
- 4 Select a View from the list of available Views for this User.

The display updates automatically to the new View.

Viewing Data on the Remote Display

All viewLinc functions are available on the remote display, as a User would find in a desktop View.

To learn more about using the **Table View**, **Dashboard**, **Location Alarms** and **Trend** tabs, see “Working with the Locations window” on page 88.


To learn more about acknowledging alarms, see “Viewing and Acknowledging Alarms” on page 121.

Using viewLinc Mobile

If you have team members working away from your viewLinc network, they can continue to access viewLinc data with viewLinc Mobile.

With any supported mobile Device, simply enter your viewLinc IP address using the Internet browser on your mobile Device.

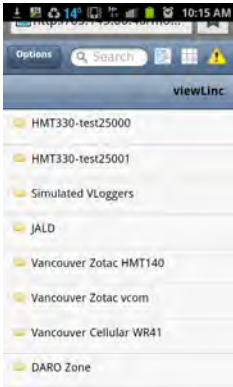
To start viewLinc Mobile the first time:

- 1 Start the Internet browser on your mobile Device, .
- 2 Enter your viewLinc IP address followed by **/mobile** (for example: **##.###.##.##/mobile**).
- 3 Log in with your viewLinc User name and password.
- 4 Select the language you want to display. When changing to a language other than English, the page automatically refreshes to display the new language.


Viewing Data with viewLinc Mobile


The initial screen that appears after you log in, is the primary **Locations** window navigation tree.

Tap the name of a Zone to reveal the Locations below it, then press the top left **Options** menu to view the commands available.





There are three selectable Views available:

 **Locations pane View:** The default View. Use this View to display Pop-up Trends, change Pop-up Trend graph settings, or acknowledge alarms. When a Location is tapped, the contents view expands.

- To go up a folder, tap . Do not use your Back button, it will end the browsing session.
- To get further information on a Location, select it, then select **Options | Pop-up Trend**.

Note: If the Pop-up Trend does not appear, check that your mobile Device is not set to block pop-ups.

 **Locations Table View:** Displays detailed Location information for whichever Location was selected from the Locations pane view.

- To go up a folder, select the **Locations pane View** icon,  (do not tap the Back button, as this will exit the browser and you will have to log in again).



- To view Location information, select the Location, then double-tap to view details. Click the X to return to view previous screen.

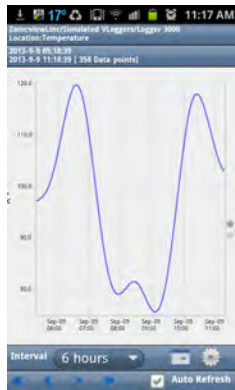
⚠ Alarm Grid View: Displays alarm information for whichever Location was selected from the Locations pane view (or all Location alarms, if none selected).

- 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.

To view a Pop-up Trend:

Note: Before you can view Pop-up Trends on a mobile Device, ensure the Device option to Block pop-ups is disabled. Refer to your Device-specific User Guide for more information.

- Tap the  **Locations pane View** icon, then navigate to a specific Location (may need to open a zone folder), and select the Location ().
- Tap **Options | Pop-up Trend**. The Pop-up Trend window appears.




This window is controlled using the same buttons and checkboxes as a desktop Pop-up Trend window. See “Navigating a Trend View” on page 92.

Acknowledge Alarms with viewLinc Mobile

If you are authorized to acknowledge alarms for the Locations you can view on your desktop display, you are also authorized to acknowledge those alarms remotely.


To acknowledge an alarm:

- 1 Tap the  Alarms button.
- 2 Highlight the alarm you want to acknowledge.
- 3 Tap **Options | Acknowledge**.

A window appears prompting you to enter the action taken, pre-configured comments (if required) and extra User comments (if required).

- 4 Fill in the required information and tap **Acknowledge**.

To pause or resume alarming using the mobile UI:

- 1 From the default Locations Tree view, tap  Locations Table view.
- 2 Select the Location you want to pause or resume alarming, then click **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**.

APPENDIX: FAQs & TROUBLESHOOTING

This section contains answers to frequently asked setup questions and information for troubleshooting common problems with viewLinc, Vaisala Veriteq Devices, and vNet or Digi Devices. It also contains more technical information for viewLinc Administrators and your network support staff.

Installing viewLinc

Q: Which Transmitters can I use with viewLinc?

A: Here is the list of supported 300 Series Transmitters:

- HMT-331, -332, -333, -334, -335, -337, -338
- DMT-342, -344, -345, -346, -347, -348
- PTU-301, -303, -307
- MMT-332, -337, -338

Q: What is the lowest viewLinc version where an update to 4.3 is possible, including transfer of all data and settings?

A: viewLinc 3.6.1 is the official (QA tested) lowest version which can upgrade to viewLinc 4.3 directly. If you want to upgrade from an earlier version, you must first upgrade to 3.6.1.

Q: How does viewLinc upgrade my data for use in viewLinc?

A: viewLinc automatically detects your existing version and converts your data. This is done transparently when you install viewLinc.

The data is treated as follows:

- 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 4.3 Access Control permissions are applied, according to the following procedure:
 - a** All Users are assigned to the Group **Everyone**
 - b** The Group **Everyone** is assigned View permissions on the top-level Zone, without inheriting any permissions.
 - c** Restricted Users: If previously authorized access to a Zone, have their historical permission level automatically assigned; If previously authorized access to a Channel, have their historical permission level automatically assigned.
 - d** Users are assigned to Groups according to their historical permissions.
 - e** Regular Users: Automatically assigned access permission allowing them to acknowledge alarms.
 - f** Operators: Automatically assigned access permission allowing them to configure Thresholds.
 - g** Supervisors: Automatically assigned access permission allowing them to configure alarms.

- h** Everyone: Automatically assigned access permission allowing them to View all Locations.
 - i** Users with Full Control are automatically added to the default Administrators Group.
- 4** Thresholds configured on active Channels are applied to new Locations.
 - 5** Reports are upgraded to retrieve data from the new Locations/Zones.
 - 6** POS displays are upgraded to use retrieve data from the new Locations.

Q: How do I install viewLinc 4.3 on a new server, and transfer all data and settings from an old server machine running an older version?

A: Here is the recommended procedure for viewLinc versions 3.6.1 and higher:

- 1** Stop the watchdog and viewLinc services on the old system.
- 2** Install viewLinc 4.3 on the new server. Accept all system default settings for the installation and data file locations.
- 3** In the data file locations for the earlier version refer to the Administrator Guide for the default location for the old version, then delete all files under the **XXX** folders.
- 4** Copy:
 - a** Files from the **db** folder on the old system into **Vaisala\Vaisala Veriteq viewLinc\db**
 - b** Files from the **\log** folder on the old system into **Vaisala\Vaisala Veriteq viewLinc\log** EXCLUDING any files under **Vaisala\Vaisala Veriteq viewLinc\log\debug** folder and any files named **log\watchdog*.***
 - c** Any reports and transfer folders into the **Vaisala\Vaisala Veriteq viewLinc** folder.
- 5** Open the **Vaisala\Vaisala Veriteq viewLinc\config\viewlinc.cfg** file and set the **level = debug** (in the [logging] section).

- 6 Restart viewLinc and verify the upgrade. It may take a few minutes to start.
- 7 Log in as admin, and select **Options | System Configuration | Preferences**. In the Preferences window, set the Technical Support Log to **Informational**.
- 8 Select **Options | Save**.

Q: How do I configure the viewLinc Web server for SSL security?

A: Enabling SSL (https://) on the viewLinc web server requires completion of the following steps:

To set up the SSL Port on a new installation:

When installing viewLinc for the first time, the install wizard prompts you to provide information on the web server:

Select the mode:

- The web server can run in **Secure** mode, **Non-secure** mode or **Both**.
- If available, the default ports are applied (80 = Non-secure and 443 = Secure).
- If the default ports are not available, provide alternative Port numbers.

To set up the SSL Port on an existing installation:

The viewLinc configuration file contains the Port numbers. The file is located in: <datadirectory>\config\viewlinc.cfg

The following section contains the viewLinc ports:

```
[web]
port=80
https_port=443
```

- 1 Set the ports as desired:
 - Setting the Port to zero (0) disables non-secure access.
 - Setting **https_port** to zero (0) disables secure access.

Note: The defaults of 80 and 443 are preferred.

- 2 Restart the viewLinc service.

To set up SSL Security:

viewLinc is installed with a default Security Key. The default Security Key is for testing and initial validation only, it is not to be used on a live system. Before using viewLinc, the default Security Key must be replaced with either a self-signed key, or a key signed by a Certificate Authority (CA).

The examples here use the Open source tool, OpenSSL, to generate Security Key files. It must be downloaded and installed if it is not already available. Check with your IT department first:

<http://www.slproweb.com/products/Win32OpenSSL.html>.

- 1 Locate the Certificate and Security Key files in the following folders:
 - <datadirectory>\config\keys\viewlinc.key
 - <datadirectory>\config\keys\viewlinc.crt

Note: These files should be left as they are (they may be replaced during upgrades). Do not replace them with similarly named files.

The names of the files that viewLinc will load at startup are found in the viewlinc.cfg configuration file:

```
<datadirectory>\config\viewlinc.cfg
[web]
privatekeyfile = viewlinc.key
certificatefile = viewlinc.crt
```

When you have created your own files, the entries in viewlinc.cfg must be modified.

To create a Security Key and self-signed certificate:

The Security Key names should use the domain name of the server convention. If the URL to access the server is,

<https://viewlinc.bigpharma.com/>, then the filenames should be:

- viewlinc.bigpharma.com.key
- viewlinc.bigpharma.com.crt

- 1 Create a private key. The file created by the following command contains the private RSA key to be used by viewLinc:

```
openssl genrsa -out viewlinc.bigpharma.com.key  
2048
```

- 2 Create a Certificate Signing Request (CSR) file.

Note: This file contains the certificate request details, and is not required by viewLinc (it is only an intermediate step in the Security Key generation procedure).

- 3 Create a configuration file called SSLConfig.txt containing your certificate details.

For example:

```
[ req ]  
distinguished_name= req_distinguished_name  
prompt = no  
[ req_distinguished_name ]  
countryName = CA  
stateOrProvinceName = British Columbia  
localityName = Vancouver  
organizationName = Big Pharma Inc.  
organizationalUnitName = Big Pharma Unit  
commonName = viewlinc.bigpharma.com  
emailAddress = support@bigpharma.com
```

- 4 Run this command:

```
openssl req -new -key viewlinc.bigpharma.com.key  
-out viewlinc.bigpharma.com.csr -config SSLCon-  
fig.txt
```

- 5 Create a Certificate (CRT) file:

Note: This file contains the signed certificate that viewLinc requires.

```
openssl x509 -req -days 365 -in viewlinc.big-  
pharma.com.csr -signkey viewlinc.big-  
pharma.com.key -out viewlinc.bigpharma.com.crt
```

- 6 Copy `viewlinc.bigpharma.com.crt`, and `viewlinc.bigpharma.com.key`, into the `config\keys` folder. The `viewlinc.cfg` should be updated with the new names.
- 7 Restart viewLinc. The https web server will be available to use with the new SSL certificate files.

To create a key and certificate signed by a Certificate Authority (CA):

Note: The key names by convention should be the domain name of the server. If the URL to access the server is `https://viewlinc.bigpharma.com/` then the filenames should be: `viewlinc.bigpharma.com.key`, and, `viewlinc.bigpharma.com.crt`

- 1 Create a private key. The file created by this command contains the private RSA key to be used by viewLinc:

```
openssl genrsa -out viewlinc.bigpharma.com.key 2048
```

- 2 Create a Certificate Signing Request (CSR) file.

Note: This file contains the certificate request details, and is not required by viewLinc (it is only an intermediate step).

- 3 Create a configuration file called `SSLConfig.txt` containing your certificate details, for example:

```
[ req ]
distinguished_name= req_distinguished_name
prompt = no
[ req_distinguished_name ]
countryName = CA
stateOrProvinceName = British Columbia
localityName = Vancouver
organizationName = Big Pharma Inc.
organizationalUnitName = Big Pharma Unit
commonName = viewlinc.bigpharma.com
emailAddress = support@bigpharma.com
```

- 4 Run this command:

```
openssl req -new -key viewlinc.bigpharma.com.key  
-out viewlinc.bigpharma.com.csr -config SSLCon-  
fig.txt
```
- 5 Create a Certificate (CRT) file. The file must be sent to the Certificate Authority (CA). This may be your own IT department, or it may be a commercial CA, such as Thawte or Symantec. The CA will produce a signed, trusted certificate file, `viewlinc.bigpharma.com.crt`.
- 6 Copy `viewlinc.bigpharma.com.crt`, and `viewlinc.bigpharma.com.key`, into the `config\keys` folder. The `viewlinc.cfg` should be updated with the new names.
- 7 Restart viewLinc. The https web server will be available.

To connect to viewLinc:

For the example previous, the URL connection would be:

`https://viewlinc.bigpharma.com/`

or , if Port 2443 was used instead of the default,

`https://viewlinc.bigpharma.com:2443/`

If the certificate file was signed by a CA, the viewLinc login page should appear and the site should be trusted. If it is a self-signed certificate, the browser will issue a warning. You can continue to the site, and then install the client certificate. The browser will always flag it is not trusted.

Useful diagnostic commands:

- ▶ Run these commands and compare the outputs:

```
openssl req -noout -modulus -in viewlinc.big-  
pharma.com.csr | openssl md5
```

```
openssl rsa -noout -modulus -in viewlinc.big-  
pharma.com.key | openssl md5
```

```
openssl req -noout -modulus -in viewlinc.big-  
pharma.com.csr | openssl md5
```

The outputs should be identical if the files are related.

- ▶ Run this command to connect to viewLinc and display the certificate information:

```
openssl s_client -connect viewlinc.bigpharma.com:443
```

Note: Minimum requirements are OpenSSL 0.9.8h-1 or higher for Windows installed.

Q: How can I use the Mobile Application when my Smart Phone does not have VPN access to the company network?

A: Ask your IT department to set up Port forwarding for the internal address of the CMS server on the corporate firewall, and specify the TCP Port that the CMS has been set up to use. This Port may be changed in the viewLinc.cfg file if required.

```
[web]
# port for insecure (http) communications
port = 80
# port for secure (https) communications
https_port = 443
```

A service restart is required following this change (**Options | System Configuration | Preferences: Options | Restart viewLinc Service**)

Q: Can I turn off the Mobile Application?

A: The viewLinc.cfg file contains the entry to enable/disable Mobile applications. Add a # to the start of line that contains mobile_agent_ids. Eg #mobile_agent_ids.

Q: How do I keep my Security Key files when upgrading from viewLinc 4.0 to viewLinc 4.3?

A: There is an installation bug in viewLinc 4.0. For this version viewLinc will load the key files from this location:

```
<installdir>\Python\Lib\site-packages\viewlinc\config\keys
```

When creating your replacement key files, always put them in the above folder AND in the documented folder

```
<datapath>\config\keys.
```

The keys need to go in both is because upgrading viewLinc will destroy the <installdir>\Python folder tree, thereby deleting your key files. viewLinc 4.3 uses the correct location, so you will find your key files in the folder.

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.

Setting Up Devices

Q: My network uses a combination of Vaisala Veriteq Devices, 300 Series and HMT140 Wi-Fi Data Loggers. How can I add them quickly?

A: To add multiple Transmitters or a combination of Devices and Transmitters at one time, create a .txt definitions file with one Device or Transmitter defined per line. Add fields to identify the Device class and Device properties (separating each field with a tab). To set vcom type Devices (Vaisala Veriteq Devices), define the COM Port number to which your Device is connected. For example:

```
vcom com_port=101  
vcom com_port=102  
vcom com_port=103
```

To set HMT330 type Devices (300 Series Transmitters), 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 (i.e. for HMT140 Devices)
- 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, 12h, 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)

To set HMT140:

```
hmt140 serial_number
```

Q: How do you add IP addresses for Vaisala Veriteq Devices using Digi or vNet Devices?

A: You don't. However you do assign IP addresses to your communication Devices, Vaisala Veriteq Devices. Because viewLinc communicates using COM ports, attaching Vaisala Veriteq Devices to the network using Ethernet/IP addresses requires the use of a networking Device, vNet or Digi Devices.

vNet or Digi Devices create virtual COM ports that allow Vaisala Veriteq Devices to communicate with viewLinc using Ethernet.

We recommend that you do not use dynamic IP address for your Devices; instead, use a reserved or static IP address (obtained from your IT department). IP addresses are assigned to vNet or Digi Devices during driver configuration. Refer to the Vaisala Veriteq Quick Start Guide for vNet or Digi Devices for installation instructions.

- For more about vNet Devices, see <http://www.vaisala.com/en/lifescience>.
- For more about Digi's, see www.digi.com.

Q: How can I connect via wireless or ethernet with 300 series Devices?

A: Internal LAN-1 Module (Ethernet): Allows single PTU300*, HMT330, DMT340 or MMT330 transmitter to connect to the 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 WIFI): Allows single PTU300*, HMT330, DMT340 or MMT330 Device to connect to the viewLinc host computer via standard 802.11b/g wireless networks. WLAN-1 Module is internally powered by the Transmitter.

Single Port Digi Device (Ethernet): Allows single PTU300, HMT330, DMT340 or MMT330 Device to connect to the viewLinc host computer via standard TCP/IP Ethernet network. Requires installation of Digi Device drivers (included) and configuration of virtual COM ports on viewLinc host computer. Digi Device available with 802.3af Power over Ethernet (PoE) (Optional) Digi Device 9-30VDC powered (AC adapter included). Requires transmitter configured with DB9 serial cable. Requires DB9-serial cable connection between Digi Device and Transmitter.

Multi-port Digi Device (Ethernet): Allows multiple PTU300, HMT330, DMT340 or MMT330 Devices to be connect to the viewLinc host server via standard TCP/IP Ethernet network. Requires installation of Digi Device drivers (included) and configuration of virtual COM ports on viewLinc host computer. Allows for multiple PTU300, HMT330, DMT340 or MMT330 to connect to the host server through a common TCP/IP network interface module. Digi Device available with 802.3af Power over Ethernet (PoE) (Optional). Digi Device is 9-30VDC powered (AC adapter included) Requires transmitter configured with DB9 serial cable. Requires DB9-serial cable connection between Digi Device and Transmitter.

Single Port Digi Device (802.11b/g WIFI): 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 Digi Device drivers (included) and configuration of virtual COM ports on viewLinc host computer. Requires transmitter configured with DB9 serial cable. Digi Device is 9-30VDC powered (AC adapter included)

Multi-port Digi Device (802.11b/g WIFI): Allows multiple PTU300, HMT330, DMT340 or MMT330 Devices to be connect to the viewLinc host server via standard 802.11b/g wireless networks. Requires installation of Digi Device drivers (included) and configuration of virtual COM ports on viewLinc host computer. Allows for multiple dataloggers to connect to the host server through common 802.11b/g wireless networks. Requires transmitter

configured with DB9 serial cable. Digi Device is 9-30VDC powered (AC adapter included).

Note: PTU300 can only support WLAN-1 and LAN-1 modules when no datalogger modules are installed.

Q: How do I enable or disable HTTPS?

A: Set the `https_port` to 0 in the `viewlinc.cfg` file, or select the Port during installation. To enable after installation, set required Port (usually 443) in `https_port` and restart `viewLinc`.

Q: How does viewLinc know which Vaisala Veriteq Devices are connected to it?

A: It doesn't. Your network Devices aren't 'assigned' to `viewLinc`; rather, `viewLinc` monitors the network for Devices attached to COM ports (`viewLinc` software communicates via COM ports, or the virtual COM ports created by `vNet` or Digi Devices).

To see which COM ports (virtual or other) are assigned to a vNet or Digi Device:

- 1 From the Windows **Control Panel**, open the **Device Manager**.
- 2 Once **Device Manager** is open, 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`; Digi Devices are named `Digi xxxxx` (where `x` is the serial number of the Device).
- 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.

Moving Vaisala Veriteq Devices

Q: I'm using vNet/Digi Devices to connect my Vaisala Veriteq Devices to the network. I want to move one of my Vaisala Veriteq Devices from one location to another within the same subnet. What do I need to do?

A: If you've used a reserved or static IP address for your Device (as recommended), here are the steps to follow:

- 1 Pause alarming on the Device (you may experience communication alarms while performing these steps if you do not pause alarming - see page 126).
- 2 Unplug the vNet or Digi Device from the network (with Vaisala Veriteq Device still attached).

Note: You do NOT need to uninstall the Digi RealPort software from the viewLinc Server machine. In fact, doing so will potentially cause problems when you reattach the Digi to the network.

- 3 Move the Vaisala Veriteq Device to another location.
- 4 Plug the vNet or Digi Device into the network again.
- 5 Resume alarming. viewLine will reconnect with the Vaisala Veriteq Device and allow you to see the Device in the **Locations Manager** window, **Devices** pane.

Q: I'm using vNet/Digi Device to connect my Loggers to the network. I want to move my Device from one subnet to another. What do I need to do?

A: If you've used a reserved or static IP address for your vNet or Digi Device (as recommended) and you're moving from one location to another in a different subnet, there are several configuration steps:

- 1 Pause alarming (you may experience communication alarms while performing these steps if you don't pause alarming – see page 126).

- 2 You do NOT need to uninstall the Device software from the viewLinc Server machine; but, you do need to make some configuration changes:
 - Reserved IPs: Remove the reservation from the DHCP scope for the original subnet and create a new reservation in the DHCP scope for the new subnet. Proceed to step 6.
 - Static IPs: With the vNet or Digi Device still connected at its original location, log into the vNet or Digi web interface. In the address bar of a web browser, type the IP address of the Device. (The IP of your Device can be found using Device Discovery, if you are on the same subnet as the Device.)
 - At the login screen, login as 'root' user and supply the password. The default password is 'dbps'. If you have not changed the password, use the default.
 - From the navigation bar, choose Network. In the Network Configuration screen, enter the new IP address, subnet mask and gateway for the new subnet. Click **Apply**.
 - Reboot the Device.
- 3 Move the Device to its new location.
- 4 Configure viewLinc to look for the Device in the new subnet:
 - a On the viewLinc machine, from the Windows **Start** menu, open the **Device Manager** .
 - b Select **Device Manager | Multiport Serial Adaptors**, then right-click on the row for your Device.
- 5 On the **Properties** screen, choose **Advanced | Properties | Network**.
- 6 On the **Network** screen, enter the network settings to reflect the Device's new IP address. Click **OK**.
- 7 Resume alarming. viewLinc will reconnect with the Vaisala Veriteq Device and allow you to see the Device in Locations Manager.

If viewLinc cannot connect to the Device after performing the above steps, a Port may be blocked on the router connecting the subnets. Try the following:

- 1 Determine if the Device in the new subnet is accessible from the viewLinc computer. From a command prompt on the viewLinc

computer, type **ping <IP address>**. If there are successful responses to the ping, this test will prove that routing exists between the subnets. Go to the next test.

- 2 For Digi Devices:
 - a In the command prompt, type **telnet <IP address>**. If you receive a login prompt, this test will prove that the Device is able to respond to requests. Press **[Ctrl]+[C]** to abort the login. Go to the next test.
 - b In the command prompt, type **telnet <IP address> 771**. If you receive an error message (and the previous tests were successful) then Port 771 is blocked between the local computer and the Device. This Port must be opened before the Device can be used with Vaisala viewLinc software. This Port may be blocked by network Devices (such as routers, firewalls or layer 3 switches) or PC software (such as the Microsoft Windows Firewall, 3rd party firewalls, or security software suites). Unblock this port.

A successful connection is indicated by sets of three (3) horizontal lines (≡≡≡...) appearing on your screen. Note that one set of lines will appear every 10 seconds.

Troubleshooting Tips

Logging In

Q: Why can't I log in to viewLinc using the correct username and password?

A: Ensure the viewLinc Enterprise Server service is running:

- ▶ In Windows Control Panel, choose **Administrative Tools | Services**, then find "viewLinc Enterprise Server" on the list and right-click to select **Start**. (If Enterprise Server isn't running you cannot view the Login screen).

Alarms

Q: I'm receiving communication alarms in viewLinc. I think my network Device or Vaisala Veriteq Device has stopped responding. What do I do?

- 1 Ensure your Vaisala Veriteq Devices are plugged in and/or batteries charged (HMT140).
- 2 Ensure your network Devices are connected to a power supply and the power supply is plugged in. On a Digi or vNet Device, the power light on the front of the Device should be solid red.
- 3 Ensure the Device is connected to and communicating with the network. Try to ping the Device by typing the following at a command prompt: `ping <IP address of the Device>`.
- 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. Ensure your Device has been configured to use RealPort (see <http://www.vaisala.com/en/lifescience> for more). 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 the 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, you should see an entry for the Device with the address you configured. If you don't see the Device, try connecting another working Device, or reinstall the Device.
- 6 If the light on the cable is not working properly, open vLog and determine if the cable can communicate with the Vaisala Veriteq 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.

Managing Data and Devices

Q: I'm in viewLinc and trying to transfer Device data files to a network location but it isn't working. What do I do?

A: First, ensure you are using the full network path to the network directory (for example, \\ComputerName\etc.), not a mapped drive letter. Also, ensure that the account that's running viewLinc has write permissions to the folder where you're attempting to transfer the Device files. The account that's running viewLinc was set during installation. See information on installing viewLinc in Chapter 1 of this guide, or online help.

Q: If I wish to back up the files associated with viewLinc, what are their locations and file sizes?

A: viewLinc configuration text files: <installdir>\config* (small text files)

viewLinc security keys for https: <installdir>\config\keys* (small binary files)

viewLinc operational configuration: **app_data_root\db\Viewlinc.sqlite** (up to 100MB on very large systems)

viewLinc historical data files: **app_data_root\db\hist\YYYY-MM*** (up to 10GB per month on very large systems)

viewLinc event logs: **app_data_root\log\Events\Events-YYYY.sqlite** (up to 100MB per year on very large systems)

viewLinc Repository files, uploaded dashboard images, report logos etc: **app_data_root\db\repository\images*.*** (under 5 MB)

Note: It is recommended that all viewLinc services be stopped before performing a backup.

Q: I've made some changes in viewLinc, such as new Thresholds and Device descriptions, but they're not showing up. What's wrong?

A: Location information is updated and refreshed depending on the refresh rate set in viewLinc. Click the Refresh button in viewLinc, or determine the refresh rate viewLinc is using and wait the allotted time.

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, the sampling is resumed. The sample timestamps will start off when the cable is removed, and will not be 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, the configuration alarms will 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) will work.

Predefined UI 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** Ecrú (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?

A: Content variables are added to a notification Email or SMS using the following macros. Note that not all macros are available for all Email/SMS templates:

Alarm acknowledgement messages:

[Acknowledger] = Person who acknowledged the alarm.

[AcknowledgerAction] = What was done in response to the alarm.

[AcknowledgeTimestamp] = Time alarm was acknowledged.

[AlarmID] = Alarm ticket ID (used for remote acknowledgements).

Alarm-related messages:

[AlarmMessage] = Message associated with the alarm.

[AlarmObject] = Description of where alarm was triggered, from a Channel, a Logger or Host.

[AlarmType] = Type of Alarm, Communication or Threshold.

[AlarmTimestamp] = Time alarm occurred.

[AlarmDeactivationTimestamp] = Time alarm turned off.

Threshold Alarms:

[AlarmOffValue] = Channel Value when alarm turned off.

[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.

[LocationName] = Description of Location.

[LocationZone] = Description of Zone in which Location resides.

[LocationTimestamp] = Location alarm value timestamp when email issued.

[LocationValue] = Location alarm value when email issued.

[ThresholdCondition] Summary of the threshold condition.

All Alarm messages:

[Comments] = Comments entered (manual or preconfigured) with corresponding alarm or Logger transfer settings.

[Date] = Date of alarm

[Details] = Alarm-specific details

[Server] = Name of the PC viewLinc is installed on.

[Time] = Time of alarm event.

[User] = Name of User who acknowledged the alarm (Acknowledgement messages)

[WorkerName] = Name of viewLinc worker which caused the error.

[Port] = Port number

[URL] = URL used for viewLinc (for system error messages)

Device Communication Alarm

[LocationSummary] = List of Logger Channels in alarm state.

Device Host Communication Alarms:

[DeviceHostDevicesSummary] = Brief description of all Loggers on a Host, associated with the alarm event.

[DeviceChannelsSummary] = Brief description of all Logger Channels associated with the alarm event.

Logger Alarms:

[DeviceAddress] = Logger address (for example, COM Port or serial number).

Logger Communication alarm messages:

[DeviceComPort] = COM Port the Logger is attached to.

Logger Communication and Threshold messages:

[DeviceDescription] = Description of the Logger.

[DeviceSerialNumber] = Serial Number of the Logger.

Communication alarm messages:

[DeviceHostName] = Name of the Device Host.

Logger recalibration alarm messages:

[DeviceNextCalDate] = Next calibration date for the Logger.

Transfer messages:

[TransferDirectory] = Destination directory for transferred Logger data.

[TransferFile] = Destination file for transferred Logger data.

Reporting:

[ReportName] = Name of report affected.

[Error] = Description of the error that caused the report failure.

Need More Help?

If you require additional assistance with any of these issues, contact Vaisala at 1-888-VAISALA (within North America) or send an email to helpdesk@vaisala.com.

Index

- 3**
- 300 Series Transmitters 167
 - adding 36
 - alias 100
 - output quantities 69
 - sample rate 100
 - swapping 113
 - timeout 100
- A**
- Access Control 38
 - defined 38, 40
 - for remote display
 - terminal 159
 - inherited 79
 - setting for a Location 79
- Access Control Inspector 42
- access to viewLinc 38
- acknowledging alarms 123, 164
 - Alarms window 123
 - by Email or SMS 125
 - configuration settings 30
 - inactive alarms 124
 - Pop-up Trend 125
 - viewLinc mobile 164
- activating threshold alarming 48
- active alarms
 - viewing 67, 96, 121
- adding
 - 300 Series Transmitters 36
 - commands to an alarm template 57
 - comments 57
 - comments box to a report 143, 147
 - dashboard images 83-84
 - Email notification to an alarm template 56
 - HMT140 Wi-Fi Devices 36
 - Hosts 37
 - Locations to a dashboard 85
 - multiple 176
 - multiple devices 37
 - Upload Definitions file 37
 - signature box to a report 143, 147
 - users 45
 - variables to Email or SMS templates 62
 - Zones 72
- adjusting
 - scale value in a trend 93
- Administrator's Email address 50
- alarm notification
 - command 120
 - comments 57
 - email 120
 - launching an application or device 120
 - pop-up 120
 - receiving 122
 - schedules 48
- alarm status
 - icons 67
- alarm templates 58
 - adding preconfigured comments 63
 - commands 57
 - defined 52-53
- Alarms
 - about 117
 - acknowledging 123
 - active
 - viewing 96
 - Communication 105, 118
 - disabling 107
 - editing 107
 - email notifications 56
 - pop-up notification 55

-
- troubleshooting 183
 - Configuration
 - configuration alarms 119
 - defined 118
 - Device 108
 - Device Validation and Calibration 119
 - editing 108
 - monitoring 90
 - multiple notifications 54
 - pausing 126
 - reporting 128
 - setting acknowledgment preferences 30
 - single threshold condition template 59
 - templates 54
 - templates, editing 58
 - Threshold 118
 - deactivating/reactivating 83
 - disabling 82
 - email notifications 56
 - multiple notifications 58
 - pop-up notification 55
 - Validation 118
 - viewing active 90
 - Alarms window
 - arranging column order 128
 - auto refresh 121
 - orientation 121
 - refreshing 121
 - alias
 - 300 Series Transmitters 100
 - aliases for Devices and Channels 99
 - application folder location 9
 - applying
 - threshold settings 80
 - assigning
 - Rights 39
 - auto refresh on/off 121
 - B**
 - blocks per beacon
 - HMT140 Wi-Fi Data Loggers 101
 - browsers
 - supported 1, 8
 - building
 - dashboards 83
 - trends 91
 - C**
 - calibration
 - Device settings 109
 - Calibration alarms 119
 - celsius or fahrenheit 30
 - changing
 - Channel units 32
 - columns
 - Alarms window 128
 - dashboard
 - appearance 85
 - Device descriptions 28
 - trends 93
 - Zones 73
 - Channels
 - changing unit display 32
 - description
 - editing 102
 - editing properties 102
 - finding linked Location 75
 - linking to Locations 72, 74
 - naming 28
 - properties 102
 - unlinking 74
 - unlinking/relinking
 - Locations 75
 - viewing link history 76
 - clear unit preferences 104
 - cloning reports 149

-
- color
 - selecting for reports 146
 - color of alarms 127
 - color palette 185
 - columns
 - Alarms window 128
 - Device status 67
 - hiding 68
 - Locations window 67
 - sort order 68
 - Threshold status 67
 - Timestamp 67
 - COM Ports
 - viewing 179
 - commands
 - adding to alarm templates 57
 - comments
 - adding on a report 143, 147
 - adding to alarm notification 57
 - adding to Events/event
 - logs 133
 - preconfigured 62
 - deleting 62
 - setting preferences 29
 - viewing 134
 - Communication Alarms 105, 183
 - about 118
 - adding email notifications 56
 - adding pop-up notification 55
 - disabling 107
 - editing 107
 - pausing 126
 - templates 54
 - templates, editing 58
 - troubleshooting 183
 - Configuration Alarms
 - defined 119
 - configuring
 - Devices 18
 - connecting
 - Devices 11
 - options 11
 - contact information 24
 - Continuous Monitoring System (CMS) 6
 - controlling access to viewLinc 38, 42
 - conventions used in this
 - document 4
 - copying reports 149
 - creating
 - alarm templates 54
 - aliases for Devices and Channels 28
 - dashboards 83
 - Email & SMS templates 53
 - Groups 43
 - multi-threshold templates 60
 - preconfigured comments 62
 - reports 140
 - single-threshold template 59
 - system reports 148
 - transfer schedules 151
 - trends 92
 - Views 87
 - Zones 71
 - custom
 - Email & SMS templates 53
- D**
- Dashboards 71, 83, 90
 - adding images 84
 - adding Locations 85
 - deleting 86
 - deleting data points 86
 - modifying data display 85
 - preferences 85
 - reading Location data 84
 - data points
 - deleting on a dashboard 86

-
- data transfers
 - immediate transfer 153
 - scheduled transfer 151
 - data trends
 - graphing 91
 - deactivating
 - Groups 44
 - reports 149
 - Threshold Alarms 83
 - transfer schedules 154
 - Users 47
 - deactivating/reactivating
 - Locations 77
 - Deadband 60
 - default application file locations 9
 - default reports 138
 - definition file for Devices 176
 - deleting
 - dashboard data points 86
 - dashboard image 86
 - Locations 77
 - preconfigured comments 62
 - reports 149
 - Zones 75, 77
 - Device Configuration Alarms
 - defined 119
 - Device Host, about 6
 - Device Properties pane, about 71
 - Device status column 67
 - Device Validation Alarms 119
 - devices
 - properties, viewing 98
 - Devices
 - adding
 - 300 Series Transmitters 36
 - HMT140 Wi-Fi Data Loggers 36
 - Locations to Zones 72
 - multiple 176
 - Upload Definitions file (for multiple devices) 37
 - calibration properties 109
 - configuring 18
 - connecting 11
 - creating Zones and Locations 73
 - definitions file 176
 - Digi 10
 - discovering 35
 - editing properties 99
 - installing 5, 10
 - naming 28
 - specified by security key 31
 - transfer schedules 151
 - Digi Devices
 - installation of viewLinc with 14
 - installing 10
 - moving location of 180
 - RealPort driver installation 15
 - troubleshooting 177, 180
 - disabling
 - auto refresh 121
 - Communication Alarms 107
 - Threshold Alarms 82
 - transfer schedules 155
 - disconnect after scan 100
 - discovering 35
 - Digi Devices 15
 - Vaisala Veriteq Devices 35
 - display preferences 28
 - displaying data on a POS display terminal 85
 - documentation, conventions 4
 - drivers
 - RealPort 15
 - USB cable 16
- E**
- e-learning 4
 - editing
 - alarm templates 58
 - communication alarms 107
 - Device aliases 99

- Device and Channel
 - properties 99
- Email & SMS templates 53
- Locations 78
- Logger alarms 108
- threshold settings 81
- transfer schedules 154
- User accounts 47
- Zones and Locations 76
- Email
 - Administrator address 50
 - templates
 - macros 53
- Email notification 120
 - in alarms 56
 - setting up 49
 - settings 49
- Email or SMS message
 - acknowledging an alarm 125
- Email/SMS template
 - defined 52
- enable/disable
 - viewLinc Aware Service 32
- Enterprise Server, about 6
- erasing
 - dashboard 86
- Event Log Report Status 132
- event logs
 - adding comments to 133
 - adding custom events 134
 - exporting 135
 - printing 135
 - saving 135
 - viewing 132
- Event Validation alarms
 - about 118
- Events 131, 136
 - adding comments 133
- Excel reports 142, 144

- F**
- file locations
 - application default 9
- files
 - backing up 177
- finding
 - Access Control permissions 42
 - linked Location 75
- firewall 176
- G**
- General Parameters
 - templates 54
- generating and emailing reports
 - system 148
- getting help 24
- getting started 1
- graphing a trend 91
- Groups
 - creating 43
 - deactivating or reactivating 44
 - setting up 42
- H**
- hardware requirements 7
- Help 24
- hiding columns 68
- HMP110 103
- HMT140
 - sampling in viewLinc 185
- HMT140 Wi-Fi Data Loggers
 - adding 36
 - installing 11, 17
 - max blocks per beacon 101
 - timeout 101
 - transmit period 101
- host, installing 21
- Hosts
 - adding 37
- HTTPS
 - disabling 179
 - enabling 179

-
- I**
- ICMP Ping Host 71
 - icons
 - alarm status 67
 - images
 - dashboard 84
 - Inactive alarms
 - acknowledging 123-124
 - inheriting
 - Access Control 79
 - installing 11
 - Digi RealPort driver 15
 - host 21
 - viewLine 10, 22
 - vNet Devices 12
 - wireless Devices 11
 - Wireless Devices 17
 - Internet browsers
 - supported 1
 - Internet Explorer
 - versions supported 8
 - items on the dashboard
 - display options 85
- L**
- language option 34
 - link history
 - viewing 76
 - linking
 - Channels 74
 - Locations 74
 - list of Access Control
 - permissions 42
 - Location Alarms tab
 - acknowledging an alarm 123
 - Location data
 - dashboards 84
 - location of
 - application files 9
 - Locations
 - about 65
 - adding to a dashboard 85
 - adding to Zones 72
 - alarm notification schedules 48
 - alarm templates, editing 58
 - alarms
 - templates 54
 - assigning access 79
 - changing unit preference 104
 - creating a trend 92
 - deactivate/reactivate 77
 - editing 78
 - finding linked Channel 75
 - finding linked Zone 89
 - linking Channels 72, 74
 - moving 73
 - organizing 70
 - pop-up trends 95
 - remove/delete 77
 - renaming 76
 - setting up 69
 - Threshold Alarm schedule,
 - selecting 79
 - unlinking/relinking
 - Channels 74-75
 - viewing your data 65
 - Locations window 65
 - columns 67
 - navigation pane 66
 - Options menu 66
 - Search 66
 - tab definitions 67
 - using 88
 - Loggers
 - alarms
 - adding email
 - notifications 56
 - adding pop-up
 - notification 55
 - editing 108
 - aliases 99
 - attaching to vNet Devices 12

-
- Channel descriptions 102
 - descriptions 99
 - setting up 11
 - transfers 153
 - schedules 151
 - troubleshooting 184
 - logging in 22
 - problems with 182
 - viewLinc mobile 161
 - M**
 - macros
 - using in Email & SMS templates 53
 - magnifying glass 89
 - maintenance
 - restarting or stopping
 - viewLinc 64
 - manually adding Devices 35
 - measurement units
 - temperature 30
 - messages
 - Email & SMS templates 53
 - Microsoft Excel
 - viewLinc event logs and 135
 - min/max statistics
 - in trends 93
 - MKT activation energy
 - setting value 29
 - mobile devices
 - supported 157
 - Mobile display 157, 162
 - about 161
 - logging in 161
 - pause or resume alarming 164
 - monitoring
 - Alarms 90
 - Channels 65
 - moving
 - Locations 73
 - Locations or Zones 77
 - multi-threshold templates
 - creating 60
 - multiple alarm notifications 54
 - N**
 - navigation tree
 - Locations window 66
 - network communications
 - testing 71
 - network traffic
 - distributing with Remote Hosts 37
 - notification
 - Email & SMS settings 49
 - Email setup 49
 - run a command 120
 - SMS setup 51
 - notification of alarm
 - email 120
 - pop-up display 120
 - O**
 - organizing Locations & Zones 70
 - orientation
 - Alarms window 121
 - viewLinc desktop 65
 - output quantities 69
 - P**
 - passwords
 - editing 47
 - reconfirmation after session
 - expiry 31
 - pausing alarms 126, 164
 - Device Channels 127
 - Device Host 127
 - single Location 126
 - single Zone 126
 - PC requirements 9
 - PDF reports 142, 144
 - permanently deleting reports 149
 - Permissions
 - defined 40
 - inherited 79

User 22
 pop-up notification 120
 Pop-up Trend
 acknowledging an alarm 125
 navigation 95
 viewing 94
 POP3 51
 POS 157
 setting up display options 85
 preconfigured comments
 creating 62
 deleting 62
 in alarm template 63
 preferences
 temperature units 30
 units 32
 printing alarm reports 128
 private
 Threshold Alarm (custom) 60

R

Rate of Change (ROC) 59
 reactivating
 Groups 44
 Threshold Alarms 83
 Users 47
 reading
 graphs
 in pop-up trend view 95
 threshold values 95
 reboot 64
 receiving alarm notification 122
 refresh
 Alarms window 121
 relinking/unlinking Channels 75
 Remote display 157
 acknowledge an alarm 165
 assign Access Control per-
 mission 159
 changing View 160
 creating a View 159
 requirements 158

 setting up 159
 views 86
 removing
 Locations 77
 Reports 137
 adding signature or comments
 box 143, 147
 alarm history 138
 alarm reporting 128
 cloning/copying 149
 color 146
 colors 185
 creating 138, 140
 deactivating/reactivating 149
 deleting 149
 Excel 142, 144
 exporting 129
 generating 138
 on-demand 150
 PDF 142, 144
 saving a trend 94
 System 148
 types 137-138
 requirements
 remote display 158
 viewLinc setup 7
 restarting viewLinc 64
 Rights
 about 38
 assigning to Users 39
 definitions 39
 ROC (Rate of Change) 59

S

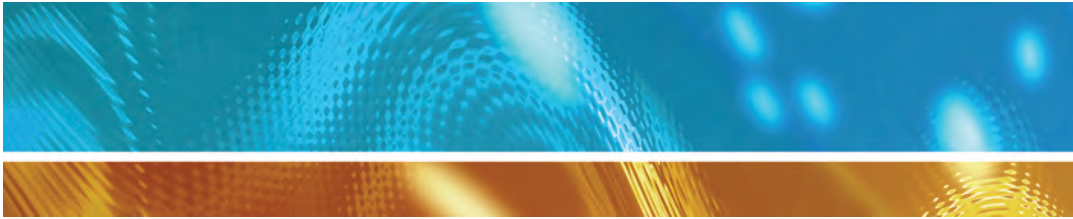
sample rate
 300 Series Transmitters 100
 scaling
 trend values 93
 scheduled data transfer
 deactivating 154
 disabling 155
 editing 154

-
- scheduling 151
 - schedules 33
 - creating 48
 - Search 66
 - filters 89
 - for a User 45
 - syntax 89
 - secure SMTP 51
 - security
 - levels 22
 - security key
 - entering 31
 - Security Key files 175
 - serial ports 11
 - installation of viewLinc
 - with 17, 22
 - server requirements 7
 - services 6
 - session expiry 31
 - setting up 27
 - calibration properties 110
 - discovering Devices 35
 - Email & SMS notification
 - Email & SMS
 - notification 49
 - Locations and Zones 69
 - remote display 157, 159
 - Road Map 24
 - schedules 48
 - system preferences 27
 - Threshold Alarms
 - Threshold Alarms 58
 - showing deactivated items 77
 - Threshold Alarms 83
 - showing inherited access permission 79
 - signatures
 - adding to Reports 143, 147
 - SIM Card PIN 51
 - single threshold alarm template 59
-
- SMS
 - message templates 53
 - notification settings 49
 - setting up 51
 - SIM Card PIN 51
 - templates
 - macros 53
 - sorting columns 68
 - stopping viewLinc 64
 - subnets
 - troubleshooting 181
 - support information 24
 - supported browsers 8
 - System alarms
 - defined 119
 - system preferences 27
 - Access Control 38
 - alarm acknowledgement 30
 - aliases 28
 - comments 29
 - MKT activation energy 29
 - security key 31
 - session expiry 31
 - temperature units 30
 - unit descriptions 32
 - viewLinc Aware Service 32
 - system requirements 7
 - system settings 27
 - temperature units 30
 - T**
 - technical support log 31
 - temperature
 - setting measurement units 30
 - templates
 - alarm 52
 - Alarm 53
 - Email or SMS variables 62
 - Email/SMS 52
 - General Parameters 54
 - multi-threshold 60
 - preconfigured comments 63

- threshold 52
 - using macros 53
- Threshold Alarms
 - about 118
 - adding email notifications 56
 - adding pop-up notifications 55
 - deactivating/reactivating 83
 - disabling temporarily 82
 - multi-threshold templates 60
 - multiple notifications 58
 - pausing 126
 - private (custom) 60
 - ROC 59
 - schedules 48
 - setting 79
 - templates 54, 58-59
 - templates, editing 58
 - type 60
 - value 60
- Threshold status column 67
- Threshold templates
 - defined 52
- Threshold values, reading 95
- Thresholds
 - applying 80
 - editing 81
- timeout period 31
 - 300 Series Transmitters 100
 - HMT140 Wi-Fi Data
 - Loggers 101
- Timestamp column 67
- touchscreen display 157
- training 4
- transfer schedules
 - creating 151
 - deactivating 154
 - disabling 155
 - editing 154
- transferring data
 - about 151
 - immediately 151, 153
 - schedules 151
- transmit period
 - HMT140 Wi-Fi Data
 - Loggers 101
- Transmitters
 - adding 36
 - output quantities 69
 - setting up 11
 - supported 167
- Trend tab
 - functions 91
- trends
 - building 91
 - creating 92
 - modifying 93
 - save as a report 94
 - viewing min/max statistics 93
- troubleshooting 167, 188
 - subnets 181
- types of alarms 118
 - Threshold Alarm 60
- types of reports 137-138
- U
- unit descriptions 32
- unit preferences 32
 - locations 104
- unlinking/relinking Channels 75
- upgrading from earlier version 20, 167, 170
- USB ports
 - connecting Devices 11
- User accounts
 - editing 47
 - logging in 22
- Users
 - adding 45
 - assigning Rights 39
 - deactivating 47
 - passwords 47
 - reactivating 47
 - searching for 45

-
- security levels 22
 - setting timeout period 31
 - setting up access to a
 - Location 79
 - setting up viewLinc access 38
 - views 86
 - using
 - color for reports 143
 - Locations window 88
 - V**
 - Vaisala Veriteq Devices
 - adding manually 35
 - Validation alarms 118
 - values
 - MKT activation energy 29
 - Threshold Alarm
 - ROC 59
 - Threshold Alarm 60
 - variables (macros)
 - using in Email or SMS templates 62
 - Veriteq Loggers
 - setting up 11
 - viewing
 - active alarms 96
 - COM ports 179
 - device properties 98
 - event comments 134
 - event logs 132
 - pop-up trends 94, 163
 - trends
 - navigation 92
 - viewing device properties 98
 - viewLinc
 - Access Control 38
 - backing up 177
 - browsers supported by 8
 - components 6
 - connecting Devices 11
 - default application folder 9
 - desktop orientation 65
 - Device Host, about 6
 - end-user PC requirements 9
 - Enterprise Server, about 6
 - features 1
 - installation
 - with Digi devices 14
 - with serial ports 17, 22
 - with USB 11, 16
 - with vNet Devices 12
 - installation options 10
 - installing 22
 - wireless Devices 11
 - installing Devices
 - with serial ports 11
 - logging in 22
 - Mobile
 - about 161
 - acknowledging alarms 164
 - logging in 161
 - mobile display 157
 - Mobile display 162
 - remote display 157
 - remots host requirements 7
 - restarting 64
 - Rights 38
 - security options 31
 - server requirements 7
 - services 6
 - setting up Devices 11
 - setting up Groups 42
 - SMTP 51
 - supported Internet browsers 1
 - supported transmitters 167
 - system requirements 7
 - upgrading from earlier
 - version 20, 167, 170
 - User Rights and
 - Permissions 38
 - viewLinc Aware Service 32
 - Views 86
 - about 65

- access control 88
- creating 87
- for remote display
 - terminal 159
- remote display
 - changing 160
- vNet Devices
 - attaching Loggers 12
 - installing 10, 12
 - moving location of 180
 - troubleshooting 177, 180
 - viewLinc Aware Service 32
- W**
- wireless devices
 - connecting 11
- Y**
- yellow highlight bar, not appearing 89
- Z**
- Zones
 - about 65
 - adding Locations 71-72
 - assigning access 79
 - deleting 77
 - editing 73
 - renaming 76
 - setting up 69, 71
 - steps before deleting 75
 - viewing data 65
 - viewing trends 96



www.vaisala.com

