User Guide

Vaisala viewLinc Enterprise Server version 5.2

VAISALA

Table of contents

List of tables

1. About this document

1.1 Version information

This document provides information for installing, configuring, and operating the Vaisala viewLinc Enterprise Server software. This document is intended for both viewLinc administrators and users.

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

.

Table 1   Document versions (English)

Document code	Date	Description
M212933EN-A	February 2024	This version, updated for viewLinc 5.2. For a list of updates and changes, see What's new (page 14).
M212315EN-C	February 2021	Previous version (for viewLinc 5.1). Added information on shutting down and starting up viewLinc services manually. Minor corrections and updates.
M212315EN-B	October 2020	Previous version (for viewLinc 5.1). REST API and Finnish language support added, authentication security and user account control enhancements, clarified purchased certificate requirements, minor corrections and updates.
M212315EN-A	October 2019	First version (for viewLinc 5.1).

You can view previous versions of a document by using the toggle in the top bar of the Vaisala documentation portal.

1.2 Related manuals

Table 2   Related manuals

Document code	Name
M212965EN	*Vaisala viewLinc Monitoring System Setup Guide*
B212751EN	*Vaisala viewLinc Enterprise Server Software Datasheet*
M211700EN	*Vaisala vNet PoE Network Interface User Guide*

Document code	Name
M211821EN	*Vaisala VaiNet Access Point AP10 Quick Guide*
M211822EN	*Vaisala VaiNet Wireless Data Logger RFL100 Quick Guide*
M211860EN	*Vaisala VaiNet Access Point AP10 User Guide*
M211861EN	*Vaisala VaiNet Wireless Data Logger RFL100 User Guide*
M212325EN	*Vaisala OPC UA Server User Guide*

1.3 Documentation conventions

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

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

Note highlights important information on using the product.

CAUTION! Caution warns you of a potential hazard. If you do not read and follow instructions carefully at this point, the product could be damaged or important data could be lost.

Tip gives information for using the product more efficiently.

1.4 Trademarks

Vaisala® is a registered trademark of Vaisala Oyj.

Android™ is a trademark of Google LLC.

Apple® and iPhone® are trademarks of Apple Inc., registered in the U.S. and other countries.

Google Chrome™ is a trademark of Google Inc.

Microsoft®, Windows®, Excel®, and Microsoft Edge® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other product or company names that may be mentioned in this publication are trade names, trademarks, or registered trademarks of their respective owners.

1.5 Training

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

For customers with active support plans, see www.vaisala.com/viewLinc-eLearning.

To learn more about Vaisala Services, contact Vaisala Technical Support at helpdesk@vaisala.com.

2. Product overview

2.1 Vaisala viewLinc Enterprise Server software

Vaisala viewLinc Enterprise Server is the software used to support all combinations of the Vaisala viewLinc Monitoring System. It features triple-redundant data retention ensuring that data is immune to power outages, network interruptions, and human error.

Use viewLinc to monitor device readings locally on a PC, across a network using a supported Internet browser, or from mobile devices like the iPhone or Google Android.

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

Intended use

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

The intended use of viewLinc is to monitor environmental conditions. Typical applications include monitoring manufacturing/storage conditions of pharmaceuticals, medical devices, or biologicals to ensure their quality, efficacy, and safety. It is not intended to be used as a control system or to monitor conditions wherein human health and safety are immediately at risk.

2.1.1 What's new

Vaisala viewLinc 5.2 provides you and your team with new integrated feature functionality to expand your network monitoring and reporting capabilities.

Table 3   New viewLinc 5.2 features

Feature	Description
Active Directory	You can simplify user authentication in viewLinc by using Microsoft Azure Active Directory to manage identity and access management for your organization.
Korean language support	The user interface language can be set to Korean. The Tours tutorial content is also available in Korean.
OAuth 2.0	viewLinc now supports using OAuth 2.0 authorization framework to help you enable email authentication for your users.

To increase the number of monitored devices on your system, an additional viewLinc license may be required. To see the remaining available device room see **Help** > **About**.

Table 4   Key features of viewLinc

Feature	Description
In-product support	Additional interactive tours to help both new and seasoned users.
User guidance at your fingertips	User-focused design ensures more intuitive software interaction.
Flexible alarm notifications	Send visual, audible, email, SMS or voice alarm notifications when conditions you are monitoring are out of compliance or if there is a network communication problem.
Controlled access	Manage access to monitored areas, system configuration or alarm acknowledgment functions according to a user's group.
Multi-language support	Send reports and notifications to your team members around the world in one of nine languages (EN, FR, DE, ES, KO, PT, SV, FI, JA, ZH).

Table 5   Key changes for viewLinc 5.2

Feature	Description
New historical data alarm types	Historical data is delayed
	The delayed historical data alarm indicates that the device is still communicating with the viewLinc server, but it will take some time before the system processes the previously generated data and catches up with the real-time data.
	Historical data is unrecoverable
	The unrecoverable historical data alarm indicates that the system didn't receive or was unable to process all of the historical data because it is missing or doesn't exist. The system now considers the data as unrecoverable.
	These new alarm types replace the Missing historical data alarm.

Feature	Description
New provisional threshold alarm	In rare cases in which the system is receiving real-time data but has delayed historical data that indicates a potential alarm condition, the system generates a provisional alarm. This alarm only occurs for RFL100 loggers and if a threshold alarm delay is set.
	After the system receives the missing data, the provisional alarm will either: • disappear because the excursion was temporary, and conditions have returned to acceptable levels, or • become a true threshold alarm because subsequent data confirmed that the excursion is persisting.
	Provisional alarms are intended as proactive warnings to viewLinc users. Instead of waiting for confirmation of an alarm condition, which could be delayed by a communication problem, users can take action to immediately to check their physical setup for issues.
Communication security enhancements	SSL certificate improvements • Additional file types supported.
	Starting in viewLinc 5.2, additional digital certificate file formats are supported for generating the SSL certificate and key during the installation or upgrade of viewLinc Enterprise Server. Previously, viewLinc only allowed CRT and KEY files, but now you can also use Distinguished Encoding Rules (DER) files and Personal Information Exchange (PFX) file types. • Secure host checking
	viewLinc now performs a secure host check for all new installations and upgrades. For new users, this means the install wizard will prompt you to provide a list of all the URLs and aliases that your users will access the viewLinc server from. For upgrade users, the upgrade wizard will list the allowed URLs and aliases in your existing certificate file and ask you to confirm the list.
	TLS 1.3 viewLinc 5.2 uses the faster and more secure TLS 1.3 for its security protocol.

More information

2.1.1.1 What's new in viewLinc 5.2 for upgrade users

Table 6   Important changes for upgrade users from 5.1 or earlier

Feature/Change	Description
Removed support for point-of-sale (POS) devices	viewLinc no long supports use of POS devices as display terminals. Use a computing device such as a laptop, or a web browser on a mobile device to administer or monitor viewLinc.
Secure host checking	viewLinc performs a secure host check for all new installations and upgrades. For new users, this means the install wizard will prompt you to provide a list of all the URLs and aliases that your users will access the viewLinc server from. For upgrade users, the upgrade wizard will list the allowed URLs and aliases in your existing certificate file and ask you to confirm the list. In both cases, users will only be able to connect to the viewLinc web server using the names provided in the certificate, even if they were able to connect in earlier versions of viewLinc.

2.1.1.2 Watch a tour

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

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

Available tours can be found in **Help > Tours**.

> Tours are available based on your assigned access Rights.

2.1.2 Device connection options

Your viewLinc Enterprise Server can support a combination of device connections and setup configurations.
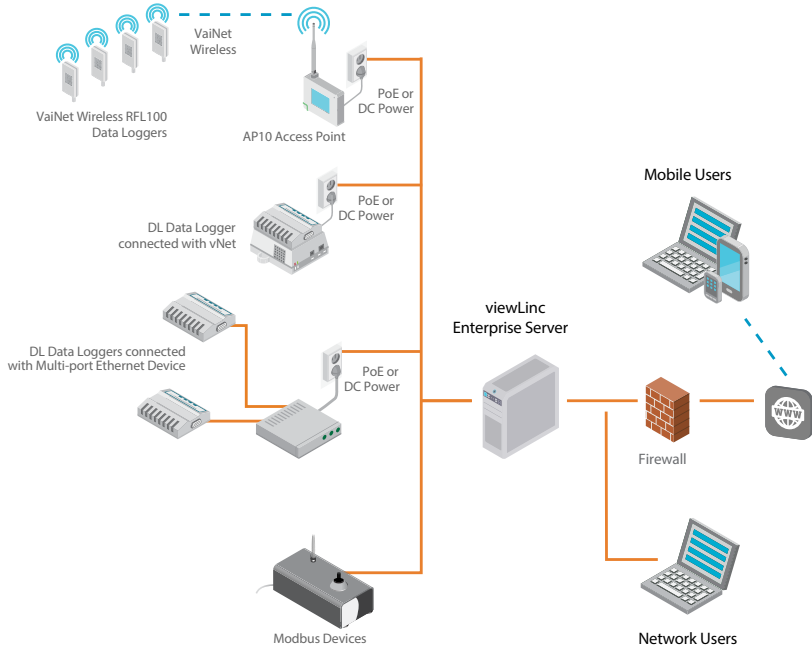
2.1.2.1 Ways to connect hardware

How you connect devices to your network is a very important administrative decision. It is possible to use a mix of the following connection methods depending on your system requirements.

> For specific installation and configuration information, see the device user guide.

2.1.2.2 Using wireless devices

VaiNet RFL100 Series

RFL100 series data loggers connect using Vaisala VaiNet protocol. To use VaiNet data loggers in your network, you require an AP10 access point. Refer to the RFL100 and AP10 device documentation for complete setup and configuration instructions.

VaiNet Data Logger   **Access Point**   **viewLinc Enterprise Server**

VaiNet Wireless

PoE or DC Power
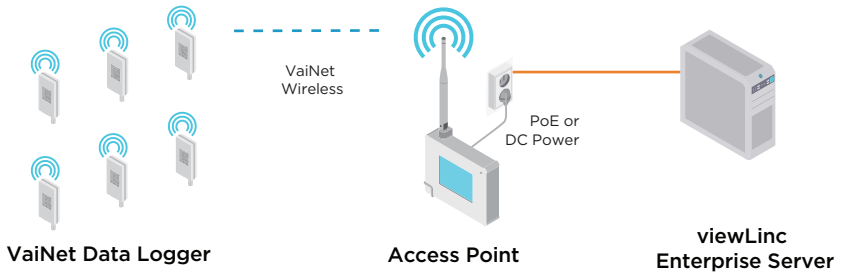
> ℹ️ Connected and configured RFL100 devices are automatically recognized by viewLinc.

HMT140 Series

HMT140 series data loggers connect using Wi-Fi protocol. To add HMT140 series data loggers to your network, you will need an HMT140 configuration cable and HMT140 Utility software (shipped with the device). Refer to the HMT140 device documentation for complete setup and configuration instructions.

Wi-Fi Data Logger HMT140 Series   **Wi-Fi Router**   **viewLinc Enterprise Server**
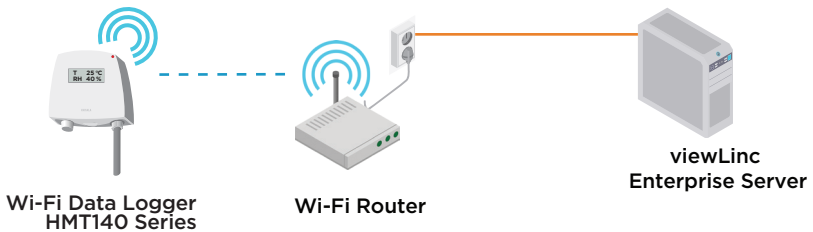
> ℹ️ Connected and configured HMT140 devices are automatically recognized by viewLinc.

More information

‣ Adding access point hosts (page 48)
‣ Accepting wireless devices (page 49)

2.1.2.3 Using vNet devices

vNet Power-over-Ethernet devices are 802.3af compliant and work with both end-point and mid-span systems. viewLinc Aware automatically detects and configures DL series data loggers connected with vNet devices (requires vNet device drivers provided with vNet devices). For information about connecting Vaisala data loggers to your network using vNet devices, see the *Vaisala vNet PoE Network Interface User's Guide* (M2117000) available at the Vaisala Product documentation portal.
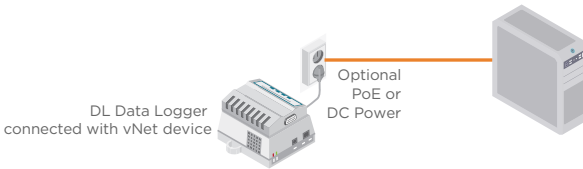
> If you are installing vNet devices on the same subnet as viewLinc, device drivers are installed automatically when you enable viewLinc Aware functionality.

More information

‣ Discovering networked devices (page 49)

2.1.2.4 Using single or multi-port ethernet device connectors

You can connect Vaisala DL series data loggers and Modbus devices to your viewLinc network using single- or multi-port Ethernet connection devices (such as Digi or Moxa devices).

When you set up viewLinc for the first time, viewLinc automatically detects and configures Ethernet-connected DL data loggers; Modbus devices must be added manually. DL data loggers can also be added with the Discover Devices function, or use the Add New Device procedure. For complete network installation instructions, refer to your Ethernet product documentation
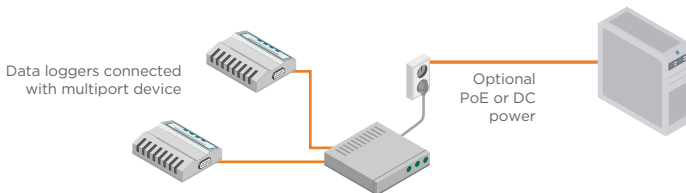
> Obtain a reserved (recommended) or static IP address for your Ethernet device from your IT department, unless your networking policy requires you to reserve IP addresses using DHCP.

More information

‣ Discovering networked devices (page 49)
‣ Modbus device addition (page 220)
‣ Adding devices manually (page 50)

2.1.2.5 Using USB ports

Connect Vaisala DL series data loggers or Modbus RTU devices directly to viewLinc Device Host servers using a Vaisala USB-to-logger cable connected to a USB port.
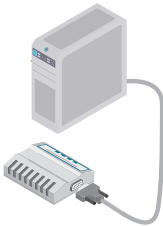
DL Data Loggers
connected with USB
or Serial Cables

1. Install USB drivers on each server used to connect devices.

2. Connect the Vaisala device to a Vaisala USB-to-logger cable.

3. Connect the Vaisala USB-to-logger cable to your viewLinc Device Host (ensure the computer is attached to your network). You only need to install drivers once on each machine to which devices are connected.

Repeat these steps for all devices. USB-connected devices are recognized automatically in viewLinc, or can be discovered manually.

More information

‣ Discovering networked devices (page 49)
‣ Adding devices manually (page 50)

2.1.2.6 Using serial ports

Connect Vaisala DL series data loggers or Modbus RTU devices directly to viewLinc Device Host servers using a Vaisala serial-to-logger cable connected to a serial COM port.
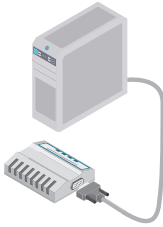
DL Data Loggers
connected with USB
or Serial Cables

1. Connect the Vaisala device to a Vaisala serial-to-logger cable.

2. Connect the Vaisala serial-to-logger cable to your viewLinc Device Host server (ensure the computer is attached to your network).

Repeat these steps for all devices. Serial-connected devices are recognized automatically in viewLinc, or can be discovered manually.

More information

‣ Discovering networked devices (page 49)
‣ Adding devices manually (page 50)

3. How does viewLinc work?

3.1 How does viewLinc Enterprise Server work?

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

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

3.1.1 System components

The Vaisala viewLinc Monitoring System comprises both software and hardware components, and can be configured to use one or more optional features:

- **Software**: viewLinc Enterprise Server (for data monitoring), and device drivers (if required to connect your devices to a network).
- **Hardware**: Vaisala data loggers, VaiNet access points, HMT140 Wi-Fi data loggers, one or more PCs with a supported Internet browser, and, depending on how you connect the devices to your PC, various cables, Vaisala vNet or Digi network devices.

3.1.2 Security requirements

viewLinc Enterprise Server software requires a secure end-to-end HTTPS connection to encrypt and protect data transmitted to logged in users. Certificate and security key files (stored on the Enterprise Server and in some cases on a client PC) are used to make the connection secure. During viewLinc installation you can choose to automatically generate a viewLinc-signed certificate or upload existing certificate files (viewLinc-signed or CA-signed/trusted).

> Refer to your company's security policy to determine whether you can use generated certificates or require trusted certificates.
> For frequently asked questions about security certificates, see Security certificate management tips (page 232).

> If you use purchased certificates instead of viewLinc-signed certificates, see the information in Purchased certificate requirements (page 24).

	viewLinc-signed Certificates	Trusted Certificates
When to use	For companies with network access limited to a few PCs.	For companies with remote network access needs.
How to install	Automatically created during viewLinc ES installation.	Certificate request sent to a certificate signing authority for paid validation.
Validity	Valid for up to 10 years.	Valid for 2 years.
Cost	Free.	Cost varies/annual renewal fee.
Action required	A network administrator can automatically distribute the certificate to network PCs. The certificate must be installed individually on non-network PCs.	Install the trusted certificate on viewLinc ES.
User experience	Until the certificate is installed on a user's PC, a warning message displays after user enters viewLinc address. ⚠ Not secure | ~~https~~:// User must acknowledge the warning to access viewLinc.	When user tries to access viewLinc from a network or remote PC, no warning appears.

If you require a trusted certificate but do not have one yet, during installation choose to automatically generate certificate files. You can replace the generated files with trusted certificates at a later time.

More information

‣ Security certificate management tips (page 232)

3.1.3 Purchased certificate requirements

When installing viewLinc, you can choose to automatically generate a viewLinc-signed certificate, or upload existing certificate files (viewLinc-signed or CA-signed/trusted).

If you use a purchased certificate, the certificate **must not have a passphrase**. Using a certificate with a passphrase will result in the connection being rejected.

3.1.4 Hardware requirements

Your Vaisala viewLinc monitoring system requires a minimum of one data logger to monitor data, and can support any combination of the following hardware components (number of data loggers permitted is based on your viewLinc and/or Modbus license key):

• One or more Vaisala DL data loggers, RFL100-series data loggers and VaiNet access points, HMT140-series wireless data loggers, or Vaisala or third-party Modbus-enabled devices.

- Optional hardware requirements:
    - Additional servers to manage devices at multiple locations (running viewLinc Device Host software or OPC UA Server software).
    - Remote display terminals to provide monitoring opportunities in areas without PCs.
    - Vaisala cables for connecting data loggers and setting up HMT140-series data loggers.
    - vNet or multi-port Ethernet interface devices for connecting Vaisala DL data loggers using an Ethernet connection.
    - Patlite signal towers to issue visual and/or audible notifications.

3.1.5 Server requirements

Table 7   Server requirements

Property	Description/value
Availability	Dedicated server (a virtual server is recommended) available 24 hours a day, 7 days a week
Server management	Connected to an uninterruptible power supply (UPS)
	A tested backup solution with support for open file backup
	Synchronizes time with a Network Time Protocol (NTP) server
Operating system	Windows Server® 2022
	Windows Server® 2022 Datacenter Edition
	Windows Server® 2019
	Windows Server® 2019 Datacenter Edition
	Windows Server® 2016
	Windows Server® 2016 Datacenter Edition
	Windows Server® 2012 R2 (64-bit)
	Windows® 10 Enterprise (64-bit)
	Windows® 11 Pro
Application disk space	350 MB
Database disk space [1]	200 KB/data point [2]/day
Network traffic [3]	Approx. 100 KB/minute/device
Web interface protocol [4]	TLS 1.3
Security certificate for web interface	Authorized TLS certificate and key [5]
Email encoding	RFC 2047

Property	Description/value
Secure email protocol	TLS 1.3

1) *Not applicable to Device Host installation.*
2) *Data points are device channels monitoring and recording data.*
3) *Depends on number of devices, system configuration and type of communication devices used.*
4) *viewLinc 5.2 includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. http://www.openssl.org/*
5) *viewLinc-signed certificate and key can be generated during installation.*

> A supported Internet browser is only required on the viewLinc Enterprise Server computer if you plan to use it to run viewLinc.

Table 8   Device host server requirements

Property	Description/value
Availability	24 hours a day, 7 days a week
Operating System	Windows Server® 2019
	Windows Server® 2016
	Windows Server® 2012 R2 (64-bit)
	Windows® 10 (64-bit)
Disk space	2 GB
Internet browser	Google Chrome™
	Microsoft® Edge™

Table 9   Requirements based on system size

System size in measurement points	1 ... 20	21 ... 400	400+
Dedicated or shared server	Either	Either	Dedicated
CPU	1.6 GHz dual core	1.6 GHz dual core	3.2 GHz quad core
RAM	8 GB	12 GB	16 GB
Disk space increase/year	1.5 GB/year for 20 data points	15 GB/year for 200 data points	75 GB/year for 1000 data points
Continuous free disk space for reports [1]	2 GB	4 GB	10 GB

1) *1 month duration with 1 minute scan/sample*

Table 10   Client requirements

Property	Description/value
Internet browser	Google Chrome™ Microsoft® Edge™
Computer clients	Any network computer with a supported Internet browser, a minimum 2.4 GHz CPU, and 4 GB of RAM.
Display and tablet clients	Touchscreen or mouse-operated panel with a supported Internet browser. Must be connected to the same network as viewLinc Enterprise Server.

Table 11   Network ports

Default	Type	Used by
80	TCP	Signal towers
389	TCP	Active Directory (less secure)
443	TCP	viewLinc web interface
502	TCP	Modbus TCP-enabled devices
636	TCP	Active Directory (secure connection)
771	TCP	vNet and multi-port Ethernet devices
950	TCP	Moxa serial-to-Wi-Fi devices
9065	UDP	viewLinc Aware service for vNet discovery
12500	TCP	Twilio web services
12600	TCP/UDP	AP10 and viewLinc device host
55000	TCP	Vaisala OPC UA Server

3.1.6 Installed system size

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

Table 12   Server Requirements Based on System Size

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

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

> ℹ️ To increase the number of monitored devices on your network, make sure you have a license to support all the devices you need (see **Help > About**).

3.1.7 End-user PC and remote display requirements

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

- 2.4 GHz
- 4 GB RAM
- Google Chrome™ or Microsoft Edge®

3.1.8 Default application file locations

It is recommended that you use the default installation folders for data file storage, as other folders may have unique security restrictions placed on them (restrictions vary between operating systems).

Table 13   Default Installation Folders

Installed Files	Default Path
Program files	`C:\Program Files\Vaisala\Vaisala viewLinc`
Data files	`C:\Users\Public\Public Documents\Vaisala\Vaisala viewLinc`

3.1.9 Web API and REST API programming interfaces

The optional Web API license enables the use of an API interface to connect to viewLinc Enterprise Server Software without using the viewLinc ES user interface. The API interface can be accessed by any client application capable of sending and receiving HTTP requests and responses.

The viewLinc Web API license (includes REST API) is provided in a package that includes reference documentation and instructions for both the Web API and REST API interfaces.

4. Setup and installation

4.1 Setup and installation

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

4.2 Setup roadmap

1 Setup checklist

2 Install viewLinc Enterprise Server

3 Install devices

Install access points

Install data loggers

Install other devices

Discover and accept devices

4 Configure viewLinc Enterprise Server

Create zones and locations

Add groups and users

Define alarm templates

Set system preferences

5 Test system

✓ Setup complete
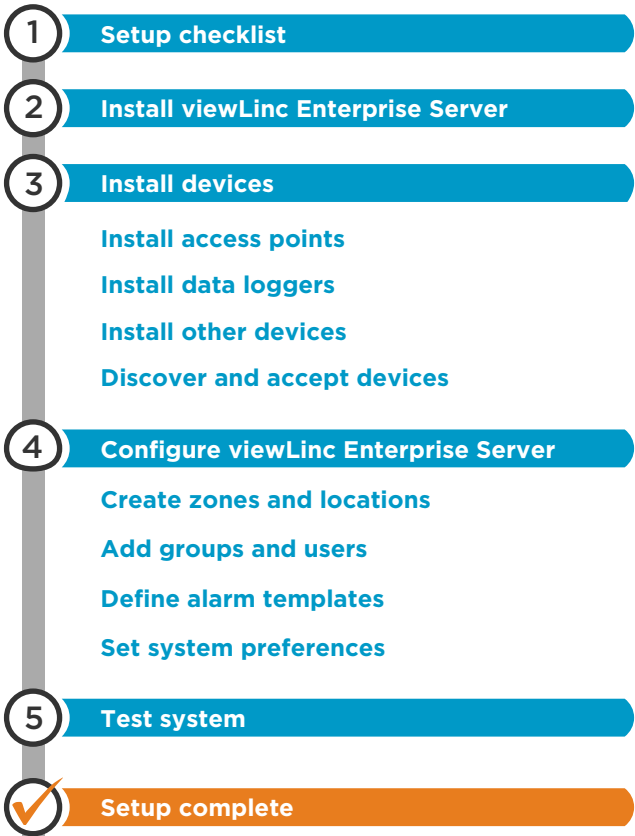
> If you require assistance with the setup of your system, the Vaisala Technical Support team is ready to assist you, free of charge [1] at helpdesk@vaisala.com.

4.3 Setup checklist

viewLinc Enterprise Server
☐ A system administrator is available to help me with network and server configuration.
☐ A dedicated network server is allocated to run viewLinc Enterprise Server 24x7. I know its IP address and hostname, and it meets minimum installation requirements.
☐ The server's network connection is to a secure network, and the network type has been appropriately set on the server (**Private** or **Domain**, not **Public**).
☐ I know the address of the Network Time Protocol (NTP) server in the network.
☐ My laptop or workstation meets minimum client requirements.
☐ I know where the program files and viewLinc database should be stored. A backup system is in place to make sure the files are recoverable in case of server failure.
☐ I have the required security certificate and key files, or have the information needed to generate a security certificate and key during installation. Users will only be able to connect to the viewLinc web server from the list of URLs and aliases specified in the certificate file, so ensure you provide a complete list.
☐ If I'm using Active Directory to manage users, I have already created a viewLinc Organizational Unit and a user with limited permissions to manage viewLinc.
☐ I have the license keys and access to the viewLinc image via: • the USB drive that contains the viewLinc setup files, or • a download link provided after the product was purchased.

Devices
☐ I have a plan that lists device serial numbers, mounting and installation information.
☐ IP addresses are allocated for my data loggers' network connections (DHCP address reservations or static IPs).
☐ Planned locations of wired devices are within 180 cm (6 feet) distance of power outlets.
☐ I know if drilling or door access is required for probes (for example, freezer installation).
☐ For upgrade users, I have verified that my existing devices are running compatible firmware.

---

1) *Software product purchase entitles you to basic support, which is limited to hardware and software installation assistance. Comprehensive support is available through the purchase of a support plan.*

Network
☐ Ethernet network drops with RJ45 jacks are installed and tested at each location where a wired network connection is needed.
☐ A Power over Ethernet (PoE) injector or switch provides operating power at network drops where a PoE powered device will be installed.
☐ (Optional) I have set up my Azure environment for OAuth 2.0 Authentication and have the following information: • a valid company email address to receive notifications from viewLinc, • Client ID, • Tenant ID, and • Secret.
☐ (Optional) I have installed a supported modem for SMS notifications.
☐ (Optional) I have an account set up with a voice/SMS web notification service provider (Twilio), and an internet-accessible port available.

Optional license keys		
I have the license key(s) required to enable one or more of the following features:		
☐ Voice web service	☐	Vaisala OPC UA Server
☐ SMS web service	☐	Web API and REST API
☐ Modbus devices (non-Vaisala)		

4.4 Installation

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

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

Refer to the Device Host and Enterprise Server requirements for different installation sizes, to determine if your system is better suited to one or both software installations.

> **i** During viewLinc Enterprise Server software installation you are required to either upload your company's existing security certificate and key files, or generate viewLinc-signed files.

More information

- Hardware requirements (page 24)
- Server requirements (page 25)
- Installed system size (page 27)
- Security requirements (page 23)

4.4.1 Installing viewLinc Enterprise Server software

If you have a previous version of viewLinc software installed, see Installing viewLinc - Upgrade an existing server (page 34) or Installing viewLinc - Upgrade on a new server (page 36).

▶ 1. Ensure you have completed the Setup Checklist and have recorded the serial number from your viewLinc USB.

2. On the dedicated viewLinc Enterprise Server, insert the viewLinc USB and run `viewLincInstall.exe`, if it does not start automatically.

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

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

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

4. Start the installation wizard.

5. Enter your license key.

6. Select the installation package. All viewLinc monitoring systems require Vaisala viewLinc Enterprise Server. If your system will support a large installation with several devices, rerun the install wizard to install viewLinc Device Host software on additional dedicated servers.

7. Accept the Vaisala General License Conditions and BerkleyDB License Agreement.

8. Accept the default installation path for the viewLinc software, or specify a new destination folder (location must have at least 2 GB of free disk space).

9. Accept the default installation path for viewLinc data, or specify a new destination folder (location must have at least 10 GB of free disk space).

10. Choose your certificate and security key files:

   Upload a purchased certificate and key (trusted)
   Choose this option if you already have the files and they are available on your network.

   Generate a certificate and key (viewLinc-signed)
   Enter your site and company details. If you plan to use a trusted certificate, the Hostname must be a fully qualified domain name, such as `viewLincESname.yourcompanyname.com`. Users will only be able to connect to the viewLinc webserver using the URLs or aliases provided in the certificate, so ensure that the list is complete.
   The installation wizard automatically generates a viewLinc-signed certificate and key file. These files are installed on the server the first time the admin user logs into viewLinc. You can replace the generated files with trusted files at any time.

   > For frequently asked questions about security certificates, see Security certificate management tips (page 232).

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

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

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

More information

‣ Hardware requirements (page 24)
‣ Security certificate management tips (page 232)

4.4.2 Installing viewLinc on a Device Host server

You can also set up additional computers as Device Hosts. This option allows for greater flexibility when managing devices, reduces the bandwidth required to communicate from server to device, and reduces the chance of network interference.

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

1. Insert the viewLinc USB and run **viewLincInstall.exe**.

2. Select the installation language.

3. Start the installation wizard.

4. Accept the Vaisala and BerkleyDB license agreements.

5. Enter the license key number, found on the USB package.

6. Choose a destination for the viewLinc program files.

7. Select **Device Host**.

8. Select **Install**.

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

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

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

More information

‣

4.4.3 Installing viewLinc - Upgrade an existing server

To ensure a successful upgrade of your viewLinc software on an existing server, make sure your system meets the viewLinc system requirements, and review the new features and functional changes introduced in viewLinc. See .

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

▶ 1. Ensure you have completed the Setup Checklist and have recorded the license key that is included with the viewLinc USB drive.

2. Verify that the current installation of viewLinc is version 3.6.1 or higher.

3. Back up your current application data directory .

   • viewLinc 3.6x default directory: `...\Program files\Veriteq Instruments \viewLinc\`
   • viewLinc 4.x default directory: `...\Public Documents\Vaisala\Vaisala Veriteq viewLinc\` (exclude the `\debug` folder and any files named `log \watchdog*.*`
   • viewLinc 5.1 default directory: `...C:\Program Files\Vaisala\Vaisala viewLinc\...` (exclude the `\debug` folder and any files named `log \watchdog*.*`

4. If your backup application does not support open database backup, stop viewLinc Watchdog and viewLinc Enterprise Server services:

    a. On your Windows server, select **> Start > Control Panel > Administrative Tools > Services** (this path may vary depending on your Windows version and settings).

    b. Right-click on the service (viewLinc Enterprise Server, viewLinc Watchdog), then select **Stop**.

5. On the existing viewLinc server, open the `viewLinc.cfg` file (found in the `\config` subfolder) and set the level entry to debug (in the `[logging]` section), `level = debug`.

> ⚠️ **CAUTION!** Modifying the `.cfg` file should only be performed by qualified system administrators.

6. On the existing viewLinc server, insert the viewLinc USB drive and run `viewLincInstall.exe`, if it does not run automatically.

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

8. Accept the Vaisala and BerkleyDB license agreements.

9. Enter the viewLinc license key.

10. Select your security certificate and key files. You can choose to keep the currently installed certificate and key files, upload new certificate and key files, or automatically generate viewLinc-signed certificate and key files. To learn more about security and certificate files, see Security certificate management tips (page 232).

> ℹ️ Users will only be able to connect to the viewLinc webserver using the URLs or aliases provided in the certificate, so ensure that the list is complete.

11. Review the install settings and click **Install**.

12. Click **Finish**.

13. Wait 20 minutes to an hour for viewLinc to upgrade the database. viewLinc will not be available during this time. There will be a gap in the Events log reflecting the duration of the upgrade.

14. If your network includes viewLinc Device Hosts, run the install wizard to install viewLinc Device Host software on each device host server.

15. On the viewLinc Enterprise Server, double-click the desktop icon to start viewLinc in a supported browser. It may take a few minutes to start. If a security warning appears, click OK to proceed. For more information about certificates see Security requirements (page 23).

16. Log in with your administrator credentials, such as `admin/admin`.

17. Open **Sites Manager** to verify your Location data is available.

18. In **System Preferences** on the **General** tab, set **System log** to **Basic**.

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

More information

‣ Hardware requirements (page 24)
‣ What's new in viewLinc 5.2 for upgrade users (page 17)
‣ Installation tips (page 232)
‣ Security certificate management tips (page 232)

4.4.4 Installing viewLinc - Upgrade on a new server

If you are upgrading viewLinc on an existing server, see Installing viewLinc - Upgrade an existing server (page 34).

1. Ensure you have completed the Setup Checklist and have recorded the license key that is included with the viewLinc USB drive.

2. Verify that the current installation of viewLinc is version 3.6.1 or higher.

3. Make a copy of the application data directory on the old server and store it in a secure network location.

   - viewLinc 3.6x default directory: `...\Program files\Veriteq Instruments \viewLinc\`
   - viewLinc 4.x default directory: `...\Public Documents\Vaisala\Vaisala Veriteq viewLinc\` (exclude the `\debug` folder and any files named `log \watchdog*.*`
   - viewLinc 5.1 default directory: `C:\Program Files\Vaisala\Vaisala viewLinc\...` (exclude the `\debug` folder and any files named `log \watchdog*.*`

4. On the new viewLinc server, insert the viewLinc USB drive and run `viewLincInstall.exe`.

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

6. Accept the Vaisala and BerkleyDB license agreements.

7. Enter the viewLinc license key.

8. Select your security certificate and key files. You can choose to keep the currently installed certificate and key files, upload new certificate and key files, or automatically generate new certificate and key files. To learn more about security and certificate files, see Security certificate management tips (page 232).

9. Review the install settings and click **Install**.

10. Click **Finish**.

11. If your network includes viewLinc Device Hosts, run the install wizard to install viewLinc Device Host software on each device host server.

12. On the new viewLinc Enterprise Server, double-click the desktop icon to start viewLinc in a supported browser. It may take a few minutes to start. If a security warning appears, click OK to proceed.

13. Log in with viewLinc 5.2 administrator credentials, `admin/viewL!ncAdm1n`.

14. In **System Preferences** on the **General** tab, set **System log** to **Detailed**.

15. On the viewLinc Enterprise Server, stop all viewLinc services (select **Start > Control Panel > Administrative Tools > Services**. This path may vary depending on your Windows version and settings); right-click on each service, then select Stop).

16. From the stored network location, copy the backup `\db` and `\log` folders and replace the `\db` and `\log` folders in:`C:\Users\Public Documents\Vaisala\Vaisala viewLinc\`.

17. On the viewLinc Enterprise Server, restart viewLinc services, then wait 20 minutes to an hour for viewLinc to upgrade the database. viewLinc will not be available during this time. Do not stop or restart services during this period. There will be a gap in the Events log reflecting the duration of the upgrade.

18. Open **Sites Manager** to verify your Location data is available.

19. In **System Preferences** on the **General** tab, set **System log** to **Basic**.

More information

‣ Security certificate management tips (page 232)

4.5 Install devices

See device-specific documentation for detailed instructions.

If you are upgrading an existing system without adding new devices, you can skip this section.

Create a device installation plan to keep track of data logger serial numbers and installation locations.

4.5.1 Install access points

Set up your **VaiNet access points** so that:

- They are able to connect to the Ethernet network
- They have the IP address or hostname of at least one NTP server they can access
- Their VaiNet channel number is set
- They have the IP address or hostname of viewLinc Enterprise Server
- They are in installation mode so that they can connect new VaiNet data loggers to the system

If you have new **WLAN access points**, configure their network and wireless settings.

If your installation has more than 8 access points, assign a unique segment ID and channel ID combination for each access point. For guidance in designing and installing a large system, see Guidelines for large VaiNet systems Technical Note.

When your wireless access points are set up, install them at their planned locations.

4.5.2 Install data loggers and transmitters

Set up your **data loggers** and **transmitters** so that they are ready for installation.

If you have **Vaisala vNet PoE Data Logger Interfaces** for your wired data loggers, follow vNet documentation to connect and configure them.

Mount the data loggers and transmitters at their planned locations.

You can install many other types of devices to a viewLinc Monitoring System. See *viewLinc User Guide* for instructions on how to make use of these devices:
- viewLinc device hosts for connecting devices on a remote location
- Measurement devices with Modbus RTU or Modbus TCP/IP output
- Signal towers for visual and audible alarm status recognition
- Remote display terminals for viewing data

4.6 Log in to viewLinc

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

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

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

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

> To save your display language setting, ensure that your browser is not set to automatically delete cookies upon exit. To set a default language for reports and notifications that are sent to you, set your preferred language in your user profile.

3. Type your username and password.

   • The first time the viewLinc system administrator logs in, type the default administrator username and password, `admin/viewL!ncAdm1n`.

   > For security purposes, it is important to change the default admin user password as soon as possible.

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

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

More information

‣ Adding users (page 78)
‣ Groups and users (page 205)

4.7 Discover and accept devices

New devices (3)

You must explicitly accept or add data loggers to the system before their data can be collected and used.

1. Open the viewLinc Enterprise Server user interface by double-clicking the desktop icon
   , or by entering the server's IP address and port in a web browser's address field.

2. Log in to viewLinc Enterprise Server as the default administrator user (username, `admin`, password, `viewL!ncAdm1n`).

   > It is recommended that you change the default administrator password immediately after logging in to ensure site security. Remember to record the new password in a safe location.

3. If this is the first time logging in as the admin user, a brief setup tour starts automatically. Complete the tour to familiarize yourself with system setup.

4. When viewLinc detects new devices, **New Devices** text appears at the top of the screen. Click it to open the **New Devices** window.

5. Compare the list of new devices to your device installation plan to verify that all your devices have been found. In the **Accept** column, select each device you want to add.

6. Select **Save** to register the selected devices with your viewLinc Enterprise Server.

7. Open the **Sites Manager** window and select the **Hosts and Devices** tab. On the **Hosts and Devices** tree, verify that all of your devices are now listed.

   > • If none of your devices are listed, check that network traffic to ports used by viewLinc (for example, 12600, 771, and 6767) is not blocked by a firewall.
   > • If some devices are missing, make sure they are configured, powered on, and connected to the network. Refer to the device-specific documentation for troubleshooting assistance.
   > • If the automatic discovery is not finding all of the devices, refer to the *viewLinc User Guide* for instructions on how to add or discover devices manually.

4.8 Configuring viewLinc Enterprise Server

After installing, accepting or adding devices, you are ready to configure the viewLinc Enterprise Server to meet site-specific monitoring needs. Several interactive tours are available from the viewLinc desktop **Help > Tours** menu:

1. viewLinc Enterprise Server configuration
   - Create Zones and Locations
   - Add groups and users
   - Add and apply alarm templates
   - Set system preferences

> Use the *Planning Worksheet* to define:
> - Names for your monitored sites (Zones and Locations)
> - Users, their assigned groups, rights and permissions
> - Alarm thresholds required for different Locations
> - Alarm notification delivery methods (email/SMS/command/voice), and notification escalation paths

2. Optional setup tasks
   - Assign permissions to groups
   - Set up schedules for alarms and notification periods, and report generation
   - Create predefined comments
   - Define views
   - Add signal towers or remote displays
   - Set up voice and/or SMS web services
   - Connect to Vaisala OPC UA Server
3. Optional installation verification tasks:
   - System test
   - Validate system

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

4.8.1 viewLinc Enterprise Server planning worksheet

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

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

Zones and Locations (Sites Manager)	
☐	Create Zones to organize areas with many Locations (optional).
	1.
	2.

Groups and Users	
☐	Name your groups, and identify the rights to be assigned to each group.
	Group name/rights:
	Group name/rights:
☐	List your users and the group(s) to which they will be assigned.
☐	Users in the default Administrators group (all rights):
☐	Users in the default Everyone group (Manage Events right):
☐	Users in _____ group:
☐	Users in _____ group:
☐	(Optional) For Vaisala OPC UA Server, name of dedicated user and a dedicated group:

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

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

Alarm Notification Settings (Alarm Templates)	
	2nd notice sent via:
	Repeat?
	Frequency:

	(Optional) Voice call tree:
	1. Username:
	   _____
	2. Username:
	   _____
	3. Username:
	   _____
	4. Username:
	   _____

General Settings (System Preferences)	
☐	Select remote alarm acknowledgment method(s): email, SMS (web service or modem), and/or voice call acknowledgments. Requires set up of settings for enabled acknowledgement method(s).
☐	Enable and then create schedules if Location monitoring/alarm acknowledgement is required for certain time periods, or if different groups will receive different alarm notifications.
☐	Enable audible alarming for browsers. User profiles must be set to allow audible alarms when they are logged in.
☐	Define display of temperature units and value for MKT.
☐	Determine whether to use device and channel descriptions in viewLinc , or create longer descriptions (aliases) in viewLinc.
☐	Select the default calibration duration (default 12 months). Reminder notifications are sent based on this value.
☐	Determine DL data logger lock settings (automatic or disabled) to add another layer of security.
☐	Enable and then create pre-configured comments for your users to add when responding to alarm conditions.
☐	If you are using vNets, save connection time with viewLinc Aware functionality.
☐	For multilingual companies, determine the language to use for system notifications.

Email Settings (System Preferences)	
☐	Required: Your IT network manager's email address to receive all system alarm email notifications.
☐	An available email address that will be used to send viewLinc notifications.

Email Settings (System Preferences)
☐ SMTP server address, port number, account username, and password.
☐ POP3 server address, port number, account username, and password (optional).

(Optional) SMS Settings (System Preferences)
☐ Select method of SMS delivery, via modem or with a web service (Twilio).
☐ If using an SMS Modem: • Configure modem to network • Specify modem settings: port/baud rate/SIM card PIN number (if required)
☐ If using an SMS web service: • Set up Twilio account • Specify account settings: account SID, authentication token, phone number, and viewLinc URL

(Optional) Voice Settings (System Preferences)
☐ Set up Twilio account (www.twilio.com)
☐ Specify web service account settings (received from Twilio): • account SID • authentication token • phone number • viewLinc URL

System Alarms (System Preferences)
☐ Mobile number and email address for your designated IT network manager.
☐ Additional information for system-generated validation alarms: priority, delay, message, comments.

4.9 System test

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

- Verify notification functionality (email/SMS/voice).
- Ensure all devices are calibrated.
- Generate a Location History report to verify that linked Locations are reporting data.
- Review the **Events** window to verify that changes to the system generate an event in viewLinc.

If you are running viewLinc in a GxP environment, you may require validation testing.

More information

- ‣ Device calibration (page 224)
- ‣ Tracking events (page 172)
- ‣ Creating Location History reports (page 189)

4.10 Validate your system

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

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

5. Device management

5.1 Device management
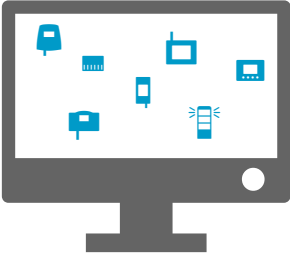
Data is collected from Vaisala monitoring devices connected directly to your network - wired or wireless data loggers and transmitters. Additional devices may be connected to your network, such as Vaisala or non-Vaisala Modbus-enabled environmental monitoring equipment, or signal towers.

> ℹ️ Your viewLinc license defines the number of monitoring devices (data loggers/ transmitters/Vaisala Modbus devices) that can be added. An additional Modbus license is required to add non-Vaisala Modbus devices. See ❓**> > About** to view your current licensed options.

Different types of devices are added to viewLinc in a variety of methods:

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

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

5.2 Managing hosts and devices

Vaisala devices (data loggers, transmitters, device hosts, access point hosts) are either identified by viewLinc automatically, or added to your system using viewLinc Device Discovery or viewLinc Aware functions. Data loggers and transmitters can also be added manually using a configuration file.

Once devices are connected to your viewLinc Enterprise Server, they are listed in **Sites Manager** window, on the **Hosts and Devices** tab.

Users who are part of the default Administrator group, or are part of a group assigned Manage Devices right, use the **Sites Manager** window to complete host and device administrative and maintenance activities.

5.3 Device hosts

For larger viewLinc system installations, viewLinc Enterprise Server provides the option of adding multiple servers to act as device hosts. Connecting groups of devices to device hosts provides you with greater control over specific devices (group management for devices connected to a single host), and ensures greater network stability. AP10 access points are the device hosts which manage your RFL100-series data loggers. Additional third-party access points can be added to support groups of HMT140 data loggers.

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

This setup allows you to:
- Manage devices more effectively. You may find it easier to pause alarming on all devices connected to a host, rather than trying to pause alarming on specific devices.
- Ensure even distribution of network traffic. Device hosts help manage the flow of device data to the Vaisala viewLinc Enterprise Server.

5.3.1 Adding device hosts

🔒 **Manage Devices**

Add additional servers as device hosts to help manage groups of devices.

> ℹ️ Make sure your viewLinc license will support the addition of new devices. For license details. see ❓**> > About**.

1. On the viewLinc Enterprise Server, open **Sites Manager** and select the **Hosts and Devices** tab.
2. In the **Hosts and Devices** tree, select **Configure > Add Host**.
3. Type the hostname or IP address.

4. Select **Save**.

   The viewLinc Enterprise Server automatically discovers the new host and all devices connected to it. Discovery of all devices on the new host may take a few seconds to several minutes to complete. You can continue with other activities during the discovery process. You are notified when the process is complete.

5. Select **Yes** when prompted to refresh.

More information

‣ Installing viewLinc on a Device Host server (page 33)

5.3.2 Adding access point hosts

🔒 **Manage Devices**

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

1. Make sure the access point is configured and connected to your network (refer to the *AP10 User Guide* for instructions).

2. In **Sites Manager** select the **Hosts and Devices** tab and then select **Refresh**.

3. If the new access point does not appear automatically in the **Hosts and Devices** tree, add the AP manually.

   a. Select **Configure > Add Host**.

   b. Type the hostname or IP address.

   c. Select **Save**.

   d. Select **Yes** if prompted to refresh viewLinc.

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

More information

‣ Accepting wireless devices (page 49)

5.4 Ways to add devices

As your network monitoring needs increase, it's easy to expand your monitoring capabilities with the addition of new devices.

Depending on the type of devices you are adding to the viewLinc network, the following options are available to you:

• Automatic detection of new RFL100-series or HMT140-series devices (**Accept Devices**).

- Automatic detection of new DL devices connected via vNet, USB or multi-port Ethernet device (**Discover Devices**).
- Manual addition, when you want to add several devices of various types at one time or Modbus devices.

> **i** A license key is required for the addition of third-party Modbus devices, and IT Administrator support.

More information

‣ Accepting wireless devices (page 49)

5.4.1 Discovering networked devices

🔒 **Manage Devices**

Use the **Discover Devices** feature to identify DL data loggers using USB or serial connection cable, or a non-Vaisala single or multi-port Ethernet device connector. Device discovery can also be used if any DL devices connected using vNet devices are not detected by the **viewLinc Aware** function. Wireless devices (RFL100 series data loggers or HMT140 series transmitters) are detected automatically.

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

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

5.4.2 Accepting wireless devices

🔒 **Manage Devices**

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

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

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

▶ 1. Open **Sites Manager**.

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

> **i** If the **New Devices** prompt does not appear, you can add the device manually.

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

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

4. Select **Accept**.

5. Select **Save**.

6. Open **Sites Manager** to verify that all accepted devices are available in viewLinc:

   a. Select the **Hosts and Devices** tab.

   b. Locate new devices on the **Hosts and Devices** tree.

5.4.3 Adding devices manually

🔒 **Manage Devices**

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

- Discovering DL devices is taking too long.
- Wireless devices are not being recognized automatically.
- You want to add a variety of device types at one time.

> **i** Before adding new devices, make sure your viewLinc license has room available to support the number of new devices you want to add. To view your current device license status, see **?** **> > About**.

More information

‣ Modbus device addition (page 220)

5.4.3.1 Adding Vaisala DL Data Loggers

🔒 **Manage Devices**

▶ 1. In **Sites Manager** select the **Hosts and Devices** tab.

2. On the **Hosts and Devices** tree select the Vaisala viewLinc Enterprise Server or a device host, then select **Configure > Add Device > DL Data Logger**.

3. In the **Add Device** window, in the **Port** field, type the COM Port number (to view available COM port numbers, go to the Windows start menu and open Device Manager).

4. Select **Save**.

5.4.3.2 Adding HMT140 Series Data Loggers

🔒 **Manage Devices**

▶ 1. Ensure no users are logged on to the HMT140 you want to add.

2. In **Sites Manager** select the **Hosts and Devices** tab.

3. On the **Hosts and Devices** tree select the Vaisala viewLinc Enterprise Server or a device host, then select **Configure > Add Device**.

4. In the **Add Device** window, in the **Device Class** field, select **HMT140**.

5. Complete the following:

   Timeout
   To ensure continuous monitoring, do not change (default 30 seconds).

   Serial number
   Type the HMT140 serial number.

   UDP port
   Can be modified if required.

   Max blocks per beacon
   Accept the default number of data blocks (64) transferred between viewLinc and the device to maximize network efficiency, or modify as required (256 max).

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

6. Select **Save**.

5.4.4 Adding multiple device types

🔒 **Manage Devices**

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

▶ 1. Create a *.txt* definitions file that identifies the device class and device properties.

2. In **Sites Manager** select the **Hosts and Devices** tab.

3. On the **Hosts and Devices** tree, select a host, then select **Configure > Add Device > Upload Definitions File**.

4. In the **Add New Device** window, in the **Device Class** row, browse to select the correct file.

5. Select **Save**.

5.5 Configure hosts and devices

After devices are connected to your network and visible in viewLinc (**Sites Manager > Hosts and Devices**), you are ready to configure your devices to work with your viewLinc monitoring system.

Configuration activities you can complete in viewLinc for most devices include:

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

> If you were using DL data loggers prior to installing viewLinc 5.2, you may have set them up on your system with vLog software. You can continue to use vLog or use viewLinc for new configuration activities.

More information

- Editing host properties (page 55)
- Editing device properties (page 56)
- Editing channel properties (page 59)
- Locking or unlocking DL data loggers (page 227)

5.5.1 Viewing host and device properties

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

Table 14   Device Properties - columns

Properties	
Description	System Preference in use - description or alias.
Description in Device	Description preconfigured in device or modified in viewLinc.
Device Alias	Long description configured in viewLinc.
Device ID	ID assigned by viewLinc when device was added.
Device Status	Connection status with viewLinc.

Properties	
Serial Number	Serial number associated with the device.
Probe Serial Number	Displays the serial number of the probe if one is connected to the channel.
Probe Hardware Model	The model of the changeable probe (for example, 'HMP115'). Shown if the connected probe supports providing this data to viewLinc.
Probe Hardware Revision	The hardware revision number of the changeable probe (for example, '1.1'). Shown if the connected probe supports providing this data to viewLinc.
Probe Firmware Version	The firmware version number of the changeable probe (for example, '2.1'). Shown if the connected probe supports providing this data to viewLinc.
Clock Battery Level	An icon showing the status of the realtime clock battery. The status can be either normal: ▮▮▮▮ or low: ▯. Shown if the connected device supports providing this data to viewLinc.
Sample Interval	Interval between samples taken from device.
Log Capacity	Estimated time remaining for data collection.
Device Address	Address of device recognized in viewLinc.
Device IP Address	The IP address of the device.
MAC Address	MAC address of the channel's device, if available.
Security Status	Only DL data loggers will display as Not secure. If a DL data logger indicates Tampered.
Next Calibration Date	Displays next calibration date, if one is set in the device.
Calibrated By	Company which completed most recent calibration service. SP data logger calibration information can only be found on the calibration certificate shipped with the device.
Channels	Number of available channels for the selected device.
Device Alarming	Indicates whether device alarming is paused.
Hardware Model	Hardware model information for the channel's device.
Hardware Revision	Latest hardware revision number for the channel's device.
Firmware Version	Latest revision number of the firmware in the channel's device.
Transmit Period	Time between each transmission.
Battery Level	Estimated battery life remaining.
RSSI (Signal Strength)	For wireless devices, displays the device signal strength (dBm)
Signal Quality	For wireless devices, displays current signal quality, 📶

Properties	
SNR	Signal to Noise ratio for wireless devices (dB).
Lock Status	DL data loggers are either locked to viewLinc (Locked) and cannot be modified outside of viewLinc, are locked to vLog or another instance of viewLinc (Remote Lock), or are not yet locked to any software (Unlocked).
Realtime Only	Yes indicates that the data logger only sends real-time data to viewLinc. It does not store data history.
Communication Alarm Template	Name of alarm template in use for channel's device.
Configuration Alarm Template	Name of alarm template in use for channel's device.
Validation Alarm Template	Name of alarm template in use for channel's device
Calibration Alarm Template	Name of alarm template in use for channel's device.
Channel Index	Index number that the channel has assigned on its device.
Channel Description	System Preference in use - description or alias.
Channel Description in Device	Description provided with the device. Refer to the Location name.
Channel Alias	Displays the alias, if one has been created in viewLinc.
Channel Alarming	Indicates whether device alarming is paused
Channel ID	Unique channel identifier.
Device Units	Units measured (such as RH, C, mA, mV).
Editable	Indicates whether the device has properties that can be modified in viewLinc.
Location	Displays the Location name linked to the channel (if linked).

Table 15   Host Properties - columns

Properties	
Hostname	Displays the host name for the selected device or channel.
Resolved Name	For administrative purposes.
Description	System Preference in use - description or alias.
Status	Connection status with viewLinc.
Host IP Address	Host IP address.
Host Type	Indicates whether the selected host is the Vaisala viewLinc machine.
Number of Devices	The number of devices connected to the host.

Properties	
Version	viewLinc version running on the host.
Status	Indicates whether the host is currently connected to the viewLinc monitoring system.
viewLinc Aware	Indicates whether the viewLinc Aware Service is enabled on the host.
Host Alarming	Indicates that host alarms are currently enabled.
Installation Mode	If host is a VaiNet access point, indicates whether status is enabled or disabled.
VaiNet Channel	Indicates the channel being used for the VaiNet access point, if applicable.
Host ID	Unique host identifier.

5.5.2 Editing host properties

🔒 **Manage Devices**

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

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

1. In **Sites Manager** select the **Hosts and Devices** tab.

2. On the **Hosts and Devices** tree, select a host.

3. Select **Configure > Edit Properties**.

4. In the **Edit Host Properties** window, edit available properties for viewLinc Enterprise Server host (go to step 5 for Access Point host properties).

   Alternate viewLinc server name
   If the viewLinc ES is behind a firewall, add a server name to ensure that device hosts are recognized, even if the IP address of the viewLinc ES changes.

   viewLinc Enterprise Server port
   This is the port that device hosts use when connecting to the viewLinc ES (refer to your IT port policy to determine if it needs to change).

   viewLinc Aware
   Disable this function if you have another viewLinc ES or device host running on the same subnet (to ensure vNets connect to the correct viewLinc ES or device host).

   viewLinc system ID (64-bits)
   The auto-generated system ID is used by devices to recognize the viewLinc ES. If you need to change this number, contact Vaisala Technical Support for assistance.

5. In the **Edit Host Properties** window, edit available properties for an Access Point host.

> **Description**
> Add a description (up to 64 alpha-numeric characters) to help identify this host. On the **Hosts and Devices** tree the host name appears in addition to the description. For example, `My Host (AP10-X###)`.

> **Installation mode**
> Enable this function to pair new RFL data loggers with the access point.

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

> **VaiNet channel (1-8)**
> If your viewLinc system supports several access points on the same wireless frequency, each access point requires a unique channel number to ensure uninterrupted wireless communication.

> **AP display**
> Set the panel display on or off.

> **AP display brightness**
> Select the panel display brightness level.

> **AP LED**
> Set the device signal light on or off.

> **AP LED brightness**
> Select the device signal light brightness level.

6. Save your changes.

5.5.3 Editing device properties

🔒 **Manage Devices**

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

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

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

1. In **Sites Manager** select the **Hosts and Devices** tab.

2. On the **Hosts and Devices** tree, select the device you want to edit.

3. Select **Configure > Edit Properties**.

4. Edit RFL data logger properties in the **Edit Device Properties** window:

    Device alias
    Optional. Type a longer, more detailed device description (up to 64 alpha-numeric ASCII characters, less if using UNICODE characters). The alias is displayed in viewLinc and in reports instead of the description, if the option to use aliases is set up in **System Preferences**.

    Device description
    Type a short device description (up to 16 alpha-numeric characters) to help identify this device. On the **Hosts and Devices** tree the device description appears in addition to the product-supplied name. For example, `My Device (van10-X###)`.

    RFL LED
    Set the device signal light on or off.

    RFL display panel
    Set the device panel display on or off.

    RFL units
    Display metric or standard units.

5. Edit DL data logger properties in the **Edit Device Properties** window:

Device alias

Optional. Type a longer, more detailed device description (up to 64 alpha-numeric ASCII characters, less if using UNICODE characters). The alias is displayed in viewLinc and in reports instead of the description, if the option to use aliases is set up in **System Preferences**.

Device description

Type a short device description (up to 16 alpha-numeric characters) to help identify this device. On the **Hosts and Devices** tree the device description appears in addition to the product-supplied name. For example, `My Device (van10-X###)`.

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

COM Port

Modify if a new COM Port is required.

Sample interval

Select the frequency of data sample collection. Depending on the sample interval selected, the **Log Capacity** field will update the estimated log time available before overwriting historical data on the device (all data history continues to be stored in viewLinc).

Sample warm up time

Set the time required to prepare for collection of data (option available if function supported by the data logger).

Channel [#]

Allow a channel to start collecting data (Enabled), or prevent a channel from collecting data (Disabled).

6. Edit HMT140 data logger properties in the **Edit Device Properties** window:

Device alias

Optional. Type a longer, more detailed device description (up to 64 alpha-numeric ASCII characters, less if using UNICODE characters). The alias is displayed in viewLinc and in reports instead of the description, if the option to use aliases is set up in **System Preferences**.

Device description

Type a short device description (up to 16 alpha-numeric characters) to help identify this device. On the **Hosts and Devices** tree the device description appears in addition to the product-supplied name. For example, `My Device (van10-X###)`.

Timeout (s)

Specify the number of seconds to wait for data before canceling a transmission.

UDP port

Auto-generated, can be modified if required.

Password

Type the device password, if this device is password-protected. The password is not saved.

Max blocks per beacon

Set the maximum size permitted for historical data retrieval. Entering a lower number helps to conserve battery life.

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

Retry count

Specify the number of times data transmission is attempted by the device if it fails to receive an acknowledgement.

Transmit period (min)

Set the frequency of data transmissions, in minutes.

Sample interval (min)

Set the frequency that data samples are saved to the device, in minutes.

7. Save your changes.

More information

‣ Editing device or probe calibration properties (page 225)
‣ Editing channel calibration properties (page 224)

5.5.4 Editing channel properties

🔒 **Manage Devices**

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

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

1. In **Sites Manager** select the **Hosts and Devices** tab.

2. On the **Hosts and Devices** tree, select a device channel to edit.

3. Select **Manage > Edit Properties**.

4. In the **Edit Channel Properties** window, modify the fields as required.

   Channel alias
   Optional. Type a longer, more detailed channel description (up to 64 alphanumeric ASCII characters, less if using UNICODE characters). The alias is displayed in viewLinc and in reports instead of the description, if the option to use channel aliases is set up in **System Preferences**.

   Channel description
   (DL and HMT140 series data loggers) Type a short channel description (up to 16 alpha-numeric characters) to help identify this channel in the **Hosts and Devices** tree. For example, `Temperature`.

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

5. To edit **Vaisala DL data loggers** with specific channel types:

   Voltage or current channel properties:
       First/Second input value
       To convert data input, set the first and second input range scaling values.

       First/Second output value
       To convert data output, set the first and second output range scaling values.

       Output units
       Specify the type of units to display converted input values in viewLinc.

   Boolean channel properties:
       Value when closed
       Set the value to display in viewLinc.

       Output units
       Editable when the channel is not linked to a Location. Specify the channel units to display in viewLinc.

6. To edit **Vaisala HMT140 Series Wi-Fi Data Loggers** using probes:

HMP110 probe properties:

Password

If passwords are enabled on an HMT140 device (using the HMT140 Utility software) type the password to ensure changes to HMT140 properties are updated on the device.

Decimal Places

Set the number of decimal places to display on the device.

High/Low Alarm Value

High and low range alarm values that initiate a data transmission. l High/Low Alarm Time: High and low alarm time specifies the number of seconds the probe is in alarm state before transmitting a beacon. The default setting, 255, disables the transmission.

Presentation Scale/Offset

Editable based on channel type. Refer to the *Vaisala HMT140 Wi-Fi Data Logger User's Guide*.

Engineering Scale/Offset

Editable based on channel type. Refer to the *Vaisala HMT140 Wi-Fi Data Logger User's Guide*.

Calibration Scale/Offset

The primary calibration scaling (x = Scale* V + Offset). If the calibration scale or offset are modified, device calibration dates appear. Before you can save the new calibration scale or offset values, update the device calibration settings.

7. Save your changes.

More information

‣ Editing device or probe calibration properties (page 225)
‣ Editing channel calibration properties (page 224)

6. Sites management

6.1 Sites management

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

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

6.2 Zones and Locations

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

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

By identifying Locations in Zones you can also:

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

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

6.3 Create Zones and Locations

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

viewLinc provides you with one top-level Zone automatically, viewLinc. It can be renamed at any time, perhaps with your company name, or the name of one of the buildings you monitor. Additional Zones and sub-zones can be set up to help identify monitored floors, rooms, warehouses, cooling or warming facilities). You can easily create Locations from device channels and add them to Zones.

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

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

6.3.1 Creating Zones

Manage Sites

Create Zones to help organize groups of Locations.

1. In **Sites Manager** on the **Zones and Locations** tree, select the top-level folder. You can also select an existing Zone to create a sub-zone.

2. Select **Manage > Create Zone**, or right-click a Zone folder and select **Create Zone**.

3. On the **Create Zone** window, type a unique name for the Zone, then specify:

    Dashboard icon
    Select an icon you want used to represent the type of Zone when displaying on the dashboard.

    Description
    For additional clarification, you can type a description of this Zone (optional).

4. Select **Create**.

5. Select **Save**, or **Undo** to cancel.

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

6.3.2 Creating Locations

🔒 **Manage Sites**

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

> Use your mouse to drag a device channel from the Hosts and Devices tree to a Zone, automatically creating a new linked Location.

▶ 1. In **Sites Manager** navigate the **Zones and Locations** tree to select a Zone or Location.

2. Select **Manage > Create Location**, or right-click a Zone folder and select **Create Location**.

3. On the **Create Location** window, type a name for the Location.

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

4. Add Location properties:

   Measurement type
   Select the value being measured. If the type is Temperature, select the preferred temperature unit to display in browser windows (°C or °F, or the system default, set in the **System Preferences** window).

   Decimal places
   Specify the number of decimal places to display. Any threshold alarm settings are rounded to a Location's decimal place before comparison. Consider the following example:
   - Threshold alarm: 22.37500 ℃
   - Data logger reading: 22.35124 ℃

   If Decimal Places = 1, an alarm may be triggered because both the threshold alarm and the logger sample are rounded up to 22.4 ℃.
   If Decimal Places = 2, an alarm is not triggered because the threshold alarm is rounded to 22.38 ℃ and the logger sample value is rounded to 22.35 ℃.

   Description
   For additional clarification, you can type a description of this Location (optional).

5. Select **Create**.

6. Select **Save**, or **Undo** to cancel.

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

More information

‣ Creating linked Locations automatically (page 66)

6.4 Link device channels to Locations

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

> Only device channels linked to Locations can generate alarms.

▶ Workstation 1

  💧 Humidity ——————— linked

  🌡 *Temperature* ——————— unlinked

When data monitoring for a specific area is no longer required, you can easily unlink a device channel and link it to a different Location.

> For audit trail security, you cannot delete a Location that was linked to a device channel; however, unused Locations can be unlinked and hidden from view.

More information

‣ Unlinking or relinking Locations and channels (page 210)
‣ Deactivating Locations (page 213)

6.4.1 Linking channels to Locations

🔒 **Manage Sites**

Before you can start monitoring conditions with viewLinc , device channels must be linked to viewLinc Locations.

> **Full Control** permission is required for all Locations being linked.

▶ 1. In **Sites Manager** on the **Zones and Locations** tree, select an unlinked Location (displayed in *italicized* text).

2. Select the **Hosts and Devices** tab.

3. In the **Hosts and Devices** tree, select an unlinked channel (displayed in *italicized* text) with a matching measurement type.

4. Select **Configure > Link Channel**

5. In the **Link Channel to Location** window, choose when you want this new Location to start monitoring data.

   Start now
   Data is recorded starting from the next available sample time.

   Start from earliest available link time
   Include all channel data history recorded by the device. This option is useful if the channel has been in use but unlinked for a period of time.
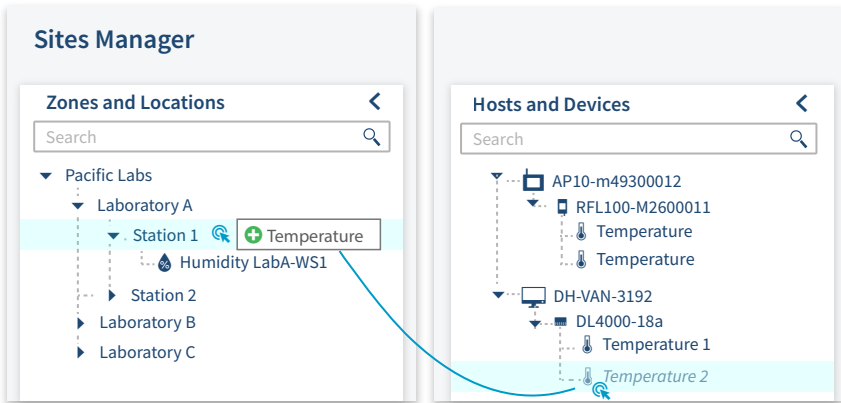
   Start from a specified time
   Set a specific time to start recording data history. You may want to use this option to delay the start of recorded history.

6. Select **Link**.

7. Select **Save**.

6.4.2 Creating linked Locations automatically

🔒 **Manage Sites**

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

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

1. In **Sites Manager** select the **Hosts and Devices** tab.

2. In the **Hosts and Devices** tree, select the new device.

3. Select an unlinked device channel, then drag it over to the Zone where the new Location will be created. The icon changes to 🟢 when the position is valid.

4. In the **Link Channel to Location** window, choose when you want this new Location to start monitoring data:

   Start now
   Data is recorded starting from the next available sample time.

   Start from earliest available link time
   Include all channel data history recorded by the device. This option is useful if the channel has been in use but unlinked for a period of time.

   Start from a specified time
   Set a specific time to start recording data history. You may want to use this option when you want to delay the start of recorded history.

5. Select **Link**.

6. To define a unique Location name, select the new Location and right-click to select **Edit Properties**.

7. Select **Update**, then select **Save**.

6.4.3 Viewing channel link history

🔒 **Manage Devices**

> You must have **View** permission to see specific **Zones and Locations** in **Sites Manager**.

1. In **Sites Manager**, navigate the **Zones and Locations** tree to select a linked Location.

2. On the **Location Properties** tab select the Location on the grid.

3. Select the channel history tool bar button, 🕐.

4. Review historical details the **Linked Channel History** window:

   Link Start
   > Unlimited indicates this channel has remained linked and has continuously monitored data at the linked Location since the channel started monitoring data.

   Link End
   > Unlimited indicates this channel is still linked to the Location and is monitoring data continuously.
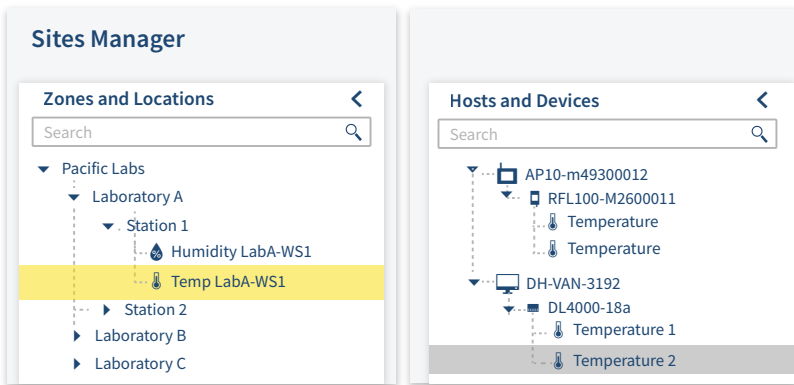
More information

‣ Applying group permission to Zones (page 136)

6.4.4 Finding a channel's linked Location from Sites Manager

🔒 **Manage Sites**

▶ 1. In **Sites Manager**, select the **Hosts and Devices** tab.

2. Navigate to a channel in the **Hosts and Devices** tree.

3. Select **Configure > Find Linked Location** or right-click and select **Find Linked Location**. A yellow highlight bar appears temporarily in the Zones and Locations tree to indicate the linked Location.

Sites Manager

Zones and Locations	Hosts and Devices
Search	Search
▼ Pacific Labs	▼ AP10-m49300012
▼ Laboratory A	▼ RFL100-M2600011
▼ Station 1	Temperature
Humidity LabA-WS1	Temperature
Temp LabA-WS1	▼ DH-VAN-3192
▶ Station 2	▼ DL4000-18a
▶ Laboratory B	Temperature 1
▶ Laboratory C	Temperature 2

6.4.5 Finding a Location's linked channel from Sites Manager

🔒 **Manage Sites**

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

▶ 1. In **Sites Manager** select the **Hosts and Devices** tab.

2. Navigate to a Location in the **Zones and Locations** tree.

3. Select **Configure** or right-click and select **Find Linked Channel**. A yellow highlight bar appears temporarily in the **Hosts and Devices** tree to indicate the linked channel.

6.4.6 Finding a Location's linked channel from Sites

▶ 1. In **Sites** navigate to a Zone in the **Zones and Locations** tree.

2. On the **Status** tab select a Location.

3. Select the **Find in Tree** toolbar button, or right-click on the Location and select **Find in Tree**. A yellow highlight bar appears temporarily in the Zones and Locations tree to indicate the corresponding Location.

6.5 Dashboards

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

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

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

6.5.1 Building dashboards

🔒 **Manage Sites**

Upload a dashboard image file from any desktop or network location, in *.png* or *.jpg* format.

You can add a dashboard image to a Zone or a Location, or to a view (a view you created or are permitted to edit).

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

6.5.1.1 Adding dashboard image

🔒 **Manage Sites** or **Manage Views**

▶ 1. In **Sites Manager** on the **Zones and Locations** tree, select a Zone or a Location (or in **Views Manager** on the **Views** tree, select a view).

2. Select the **Dashboard** tab, then select **Add Dashboard Image**.

3. Browse to find an image, then select **Add**. The image automatically resizes to fit the screen. If it is necessary to resize the image, adjust the borders with your mouse, starting from the bottom right corner.

4. Select **Save**.

6.5.1.2 Adding Zones and Location data points

🔒 **Manage Sites** or **Manage Views**

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

▶ 1. In **Sites Manager** on the **Zones and Locations** tree, or in **Views Manager** on the **Views** tree, select a Zone or Location you want to display on the dashboard.

2. Click and drag the Zone or Location to the dashboard. When you drag the Zone or Location, an icon appears to indicate when it can be added to the dashboard, 🟢.

- • When a sub-zone is added to the dashboard, it displays with its assigned dashboard icon, or, if one was not assigned, the default folder icon. Double-click the icon to view Location data.
- • When a Location is added to the dashboard, it displays the current numeric data reading, with the icon color indicating current condition severity (as set in the threshold alarm template).

3. Select **Save**.

6.5.2 Changing dashboard display settings

🔒 **Manage Sites** or **Manage Views**

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

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

6.5.2.1 Changing the dashboard image

🔒 **Manage Sites** or **Manage Views**

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

▶ 1. In **Sites Manager** on the **Zones and Locations** tree, select the Zone or Location you want to modify (or in **Views Manager** select a view).

2. Select the **Dashboard** tab, then select **Add Dashboard Image**, 🖼️.

3. Type the file location or use the **Browse...** button to navigate to the image you wish to use, then select **Add**.

4. Save your changes.

6.5.2.2 Changing font size for all Zones

🔒 **Manage Sites** or **Manage Views**

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

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

▶ 1. In **Sites Manager** on the **Zones and Locations** tree, select a Zone.

2. On the **Dashboard** tab, select **Settings > Dashboard Zone Settings**.

3. In the **Dashboard Zone Settings** window, select the font size in the **Value** column.

4. Save your changes.

6.5.2.3 Changing font size for individual Zones

🔒 **Manage Sites** or **Manage Views**

1. In **Sites Manager** on the **Dashboard** tab, right-click on a Zone and select **Edit Display Settings**.

2. In the **Edit Zone Display Settings** window, choose a font size from the drop-down list, or select **Set to Default** to change it to use dashboard preferences.

3. Save your changes.

6.5.2.4 Changing preferences for all Locations

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

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

1. In **Sites Manager** on the **Zones and Locations** tree, select a Zone with Locations set on a dashboard.

2. On the **Dashboard** tab, select the **Settings > Dashboard Location Settings**.

3. In the **Dashboard Location Settings** window, select a property to modify. Select a row in the **Value** column to see available options.

4. Save your changes.

6.5.2.5 Changing preferences for individual Locations

To set Location preferences for an individual Dashboard Location:

1. In **Sites Manager** on the **Dashboard** tab, right-click on a Location to modify, and select **Edit Display Preferences**.

2. In the **Edit Location Display Preferences** window, select a property to modify. Select a row in the **Value** column to see available options.

3. Save your changes.

6.5.2.6 Changing description display options for all Locations

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

1. In **Sites Manager** on the **Dashboard** tab, select **Settings > Dashboard Location Settings**.

2. In the **Dashboard Location Settings** window, modify the description display options:

    Description
    Choose to display the Location description (as specified in Location Properties) above, below, or beside the data reading.

    Description format
    Description format

3. Save your changes

6.5.2.7 Changing description display options for individual Locations

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

▶ 1. In **Sites Manager** on the **Dashboard** tab, right-click on a Location to modify, and select **Edit Display Settings**.

2. In the **Edit Location Display Settings** window, modify the description display options

   Description
   Choose to display the Location description (as specified in Location Properties) above, below, or beside the data reading.

   Description format
   Display only the Location description or Location and Zone descriptions.

   Set to Default
   Select to accept all globally-set dashboard preferences.

3. Save your changes.

6.5.2.8 Setting up dashboard for wall-mounted monitors

▶ 1. In **Sites Manager** on the **Dashboard** tab, select **Settings**.

2. Choose to display Location data in 1-, 2-, 3-, or 4-columns of tiles. A greater number of Locations may require a greater number of columns. Test each option to determine which display option suits your needs most effectively.

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

3. Save your changes.

6.5.3 Deleting dashboard images or data points

Manage Sites or **Manage Views**

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

> Users belonging to groups with **Manage Sites** right and **Full Control** permission can modify dashboards in **Sites Manager**. Users belonging to groups with **Manage Views** right and **Full Control** permission can modify dashboards in **Views Manager**.
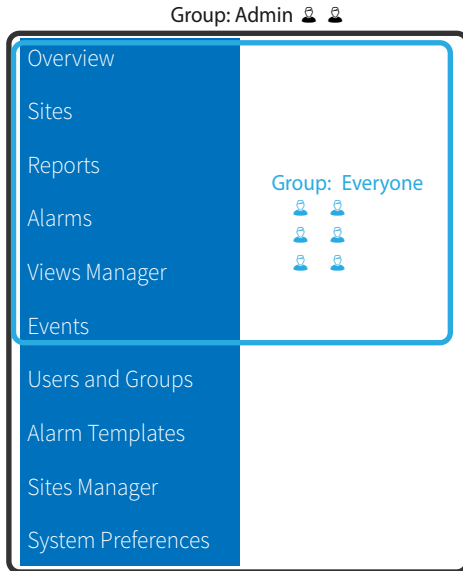
6.5.3.1 Delete a single dashboard's data point

▶ 1. In **Sites Manager** on the **Zones and Locations** tree (or in **Views Manager** on the **Views** tree), select the Zone or Location dashboard you want to modify.

2. On the **Dashboard** tab, right-click a dashboard data point then select **Delete**.

3. At the prompt, select **Delete**.

4. Save the change, or select **Undo** to cancel.

6.5.3.2 Deleting dashboard images or all dashboard data points

▶ 1. In **Sites Manager** on the **Zones and Locations** tree (or in **Views Manager** on the **Views** tree), select the dashboard you want to delete.

2. On the **Dashboard** tab select **Clear Dashboard**.

3. Choose to delete either the Zones and Locations or the dashboard image, or both, then select **Clear**.

4. Save the change, or select **Undo** to cancel.

7. Groups and users

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

Group: Admin 👤 👤

Overview	
Sites	
Reports	Group: Everyone
Alarms	👤 👤
Views Manager	👤 👤
Events	👤 👤
Users and Groups	
Alarm Templates	
Sites Manager	
System Preferences	

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

- 👥 **Administrators**: A user added to the viewLinc **Administrators** group has all rights assigned. They can access all windows and perform any function within viewLinc .
- 👥 **Everyone**: All new users are automatically assigned to the **Everyone** group. This group has access to the **Overview**, **Sites**, **Reports**, **Alarms**, **Views Manager**, and **Events** windows. The Zones and Locations users are permitted to view and/or modify within a window are set with permission levels.

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

> ℹ️ To learn more watch these tours: **Rights and Permissions**, **Add a Group**, and **Add a User**, available on the **Help** menu.

More information

‣ Applying group permission to Zones (page 136)

7.1 Rights

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

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

> ℹ️ Once removed, legacy user rights cannot be reapplied.

> ℹ️ Users assigned to the viewLinc **Administrators** group are automatically granted these additional system-level functions:
> • Undo remote-lock on DL data loggers
> • Restart viewLinc
> • Test network communications
> • Acknowledge all inactive alarms
> • Acknowledge system alarms
> • Correct security status
> • Pause host alarms
> • Add users to the **Administrators** group
> • Edit user profiles of **Administrators** group members

Table 16   Rights Definitions

Name	Access to	Description
🔒 **Manage Alarm Templates**	**Alarm Templates**	Add or edit alarm templates (threshold alarms, device alarms, notifications, email and SMS content, schedules).

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

> ℹ️ Group rights are refined by permissions. While rights allow groups to complete specific tasks in viewLinc windows, permissions control the Zones and/or Locations a group can view, configure or manage.

More information

‣ Permissions (page 134)

7.2 Adding groups

🔒 **Manage System**

Assigning users to groups helps define which areas of viewLinc you want specific users to access.

▶ 1. In the **Users and Groups** window, select the **Groups** tab, then select **Add**.

2. In the **Add Group** window on the **Properties** tab, type a name for the group. You can use the **Description** field to describe the rights you will assign to the group, or the primary job function of the group.

3. Select the **Rights** tab, then select the rights you want to assign to the group

> **i** If you are creating a group for use with Vaisala OPC UA Server, no rights are required. The group does require **View** permission to access data in Zones and/or Locations.

4. To add users to this group, select the **Members** tab then select users to add the group.

5. Select **Save**.

7.3 Adding users

Manage System

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

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

1. In the **Users and Groups** window select the **Users** tab.

2. To avoid adding a duplicate user account, check that the user does not already exist

   a. In the **Search** field, type the username or full name, then select the search icon $\mathcal{Q}$.

   b. Select the ✖ to clear the field and display the full list of users.

3. Select **Add**.

4. On the **Properties** tab, add user details:

   User name and **Full name**
   Type a username to use on the login page, and a full name, for internal reference (your company may use abbreviated names for login credentials). If this user will log in with Windows authentication, type their Windows username then select Windows as the Authentication method.

   Email, **Mobile number**
   Add the user's contact details to receive reports and alarm notifications, and send alarm acknowledgements. Type 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).

5. If schedules functionality is enabled, choose a schedule from the **Send alarm notifications** field to define when to send alarm notifications to this user:

   Always
   > This user will receive notifications at any time of day or night.

   According to schedule
   > If this user is a member of a group set up to receive alarm notifications, select the schedule which defines when this user should receive notifications.

   Never
   > This user will not receive alarm notifications, even if they are assigned to a group set up to receive alarm notifications.

6. Specify notification details:

   viewLinc PIN
   > Enter a unique 4 to 5 digit number between 1000 and 99999. This number is required when the user acknowledges an email or SMS alarm notification on their mobile device.

   Preferred language
   > Choose the language to use when user generates a report or viewLinc sends this user reports and alarm notifications. If no language selected, the system default language is used. Users can select any language.

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

   Audible alarm notification
   > Choose to enable audible alarms on the user's device (desktop PC) when logged in to viewLinc. Audible alarms must be enabled in **System Preferences**.

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

7. If you want to use the REST API programming interface (included in the Web API license), create an authentication token to access viewLinc with your REST API application.

   a. Select **Create** to generate a token.

   b. Copy the generated token to your REST API application.

   c. To remove the token you generated from use, select **Revoke**. All requests made using the revoked token will be rejected.

   > ℹ️ The REST API token can only be changed by the user that created the token. This also applies to administrator users: they cannot create or revoke the REST API tokens of other users.

   The **Last used** field shows the latest time when the token was used to access viewLinc.

8. Choose the method of **Authentication**:

   viewLinc
   Select this option to add a unique viewLinc password, then type a password in the **Password** and **Confirm new password** fields.

   > 💡 Note the password complexity requirements: minimum length 8 characters, containing at least 1 upper case letter, 1 lower case letter, 1 digit, and 1 special character.

   Windows
   Select this option to allow user to log into viewLinc with their current Windows password. Check that the Windows user name is added in the **User name** field (see the previous step), and then specify the **Domain**.

   > 💡 You can require that users re-confirm their identity (re-enter their username and password) whenever a change is made in viewLinc, or after a set number of minutes. For instructions, see Setting authentication requirements (page 117).

80

9.

> The authentication preference settings in this step are required only if you chose **viewLinc** authentication in step 8. If you chose **Windows** authentication, move to step 10.

Set authentication preferences and account locking status for this user:

a. **Password never expires**: the default setting is **Expires according to system preferences** (password expires according to the time limit set in **System Preferences**). If you want to switch password expiry off, select **Never expires**. This may be required, for example, for uninterrupted access through automatic systems such as API or OPC.

b. **Must change password on next login**: select **Yes** or **No**.

c. **Account locked**: select either **Locked** or **Unlocked**. If a user that uses viewLinc authentication has been locked out due to too many failed login attempts, an administrator can unlock the account with this selection.

> If you are creating a dedicated user for Vaisala OPC UA Server, prevent access interruptions by setting the **Must change password on next login** selection as **No**, and the **Password never expires** selection as **Never expires**.

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

> If you are creating a dedicated user for Vaisala OPC UA Server, add this user to the dedicated Vaisala OPC UA Server group.

11. Select **Save**.

More information

‣ Setting authentication requirements (page 117)
‣ Locking and unlocking user accounts (page 205)

7.3.1 Configuring Azure to set up OAuth authentication

To enable OAuth2 implementation, perform this task to create the service settings for viewLinc Enterprise Server in Azure for your Microsoft 365 account.

1. Navigate to the **Azure Active Directory**.

2. Create the application as follows:

    a. Under the **Add** drop-down, select **App Registration**. Name the new application `viewlinc-es`.

    b. Select the supported account types associated with your organization. The default will be Single tenant.

    > **i** Do not add a Redirect URI.

    c. Select **Register** to complete the registration.

3. Create a client secret as follows:

    a. Under **Manage**, select **Certificates & secrets**.

    b. Select **New client secret** and add a description.

    > **i** Your secret will have an expiry date. Set a reminder to renew your secret for when it expires. Once your secret expires viewLinc email notifications will stop working.

    c. Copy your Secret Value after you have created it.

    > **i** Your secret will only be visible right after you create it. You may want to save it to a notepad as you will need to enter it when you configure viewLinc in the subsequent task.

4. Add API permissions as follows:

   a. Under **Manage**, select **API permissions**.

   b. Select **Add a permission** and select **Microsoft Graph**.

   c. Select **Application permissions**, then search for and add **Mail.ReadWrite** and **Mail.Send**.

   > ℹ️ Write access is required to mark emails as read.

   > ℹ️ Because this step allows application permission to access all mailboxes in your organization, you should limit application access to a specific mailbox only. Consult the following topic for instructions on how to create that mailbox and an appropriate application access policy: https://learn.microsoft.com/en-us/graph/auth-limit-mailbox-access

   d. Ensure you select **Grant admin consent**, found next to **Add a permission**, for the selected permissions. Select **Yes**.

7.3.2 Configuring viewLinc to set up OAuth authentication

Ensure you have completed the steps described in Configuring Azure to set up OAuth authentication (page 81).

Perform this task to configure email settings in viewLinc to enable an OAuth2 implementation.

1. In **System Preferences**, select the **Email Settings** tab.

2. In the **Authentication type** drop-down menu, select Microsoft 365.

3. In the **Sent from system email** area, type a valid sent from address (email notifications from viewLinc are sent from this address, so the email address must exist within your company), then complete the following:

   Client ID
   > Type the **Client ID** from your Azure app **Overview** page.

   Tenant ID
   > Type the **Tenant ID** from your Azure app **Overview** page.

   Secret
   > Type the **Secret** you created in your Azure app **Certificates & secrets** page.

4. Select **Send Test Email** to verify the test email is sent successfully.

5. Select **Save**.

8. Alarm templates

8.1 Alarm templates

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

Create **threshold alarm templates** to specify the conditions that should trigger an alarm, then apply the template to one or more Locations.

Default **device alarm templates** are provided and assigned to each new device connected to your viewLinc system. They specify how and when you want to be notified of device status. The default templates can be modified, or you can create new device alarm templates.

Create **alarm notification templates** to define who should be notified in the event of a threshold or device alarm, the information that should be distributed in email, SMS, or voice messages, or whether to initiate a command to activate visual or auditory alarms, and whether the notified individual must acknowledge an alarm. Alarm notification templates are applied to Locations using threshold alarm templates.

Default **email, SMS and voice templates** are provided. They contain standard information issued from viewLinc about different alarm conditions in your network. The default content can be modified. Note that SMS functionality requires a supported modem, and voice/SMS services via web require a Twilio account.

(Optional) Create **schedules** to define when Location thresholds should be monitored, and when you want alarm notifications sent. You can set up a day schedule and an evening schedule to send notifications to different teams, or set schedules to prevent users on holiday from receiving alarms. Schedules functionality must be enabled.

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

More information

‣ Setting up voice or SMS web services (page 150)
‣ Enabling or disabling schedules (page 116)

8.1.1 Types of alarms

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

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

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

Table 17   Alarm Descriptions

Alarm type	Description
System	Event log validation alarms indicate whether changes have been made to the event log from outside the viewLinc system.
	Database validation alarms indicate database corruption or configuration changes made to the historical database originating outside viewLinc.
	System alarm settings are configured in **System Preferences**.
Threshold	Threshold alarms indicate excessive condition changes in a monitored environment.
	Threshold alarm settings are defined in threshold alarm templates and are then applied to Locations.
	Provisional alarms are threshold-specific alarms that occur if the system is receiving real-time data but has delayed historical data that indicates a potential alarm condition.
Device	Device calibration alarms indicate upcoming calibration service requirements.
	Device communication alarms indicate a communication error between a host computer, access point or viewLinc Enterprise Server, and its connected devices.
	Device configuration alarms indicate interruptions collecting device data.
	Device validation alarms indicate corruption in the device memory.
	Historical data alarms notify you that historical data has either fallen behind or is unrecoverable.
	Host communication alarms occur when a device host or access point loses connection with the viewLinc Enterprise Server.
	Host configuration alarms indicate synchronization errors between a device host or access point and the viewLinc Enterprise Server.
	Device and host alarm settings are defined in templates.

8.1.2 System alarms

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

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

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

You can modify the content of system alarm email and SMS messages.

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

8.1.3 Threshold alarms

Thresholds define the accepted condition limits required to preserve the quality of your inventory or production environment. Threshold condition limits are saved as threshold alarm templates, and can be applied to one or more Locations. If condition limits are exceeded, viewLinc can activate an alarm, and, optionally, send one or more alarm notifications.

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

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

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

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

Example

If you have a monitored area that should remain between 10°C and 12°C, you could set up one or all of these levels:
- Low threshold set at 10.5 °C to warn when the temperature is close to the Low-Low threshold.
- Low-Low threshold set at 10 °C lasting for more than 1 minute to trigger specific alarm settings for the breach of the lower threshold.
- High threshold set at 11.5 °C to warn when the temperature is close to the High-High threshold.

- High-High threshold set at 12 °C lasting for more than 5 minutes to trigger specific alarm settings when upper threshold exceeded.
- Rate of Change set to 0.25 °C/min to warn when temperature increases or decreases rapidly.

Provisional threshold alarms

In rare cases in which the system is receiving real-time data but has delayed historical data that indicates a potential alarm condition, the system generates a provisional alarm. This alarm only occurs for RFL100 loggers and if a threshold alarm delay is set.

After the system receives the missing data, the provisional alarm will either:
- disappear because the excursion was temporary, and conditions have returned to acceptable levels, or
- become a true threshold alarm because subsequent data confirmed that the excursion is persisting.

Provisional alarms are intended as proactive warnings to viewLinc users. Instead of waiting for confirmation of an alarm condition, which could be delayed by a communication problem, users can take action to immediately to check their physical setup for issues.

More information

‣ Creating threshold alarm templates (page 87)
‣ Alarm notifications (page 101)

8.1.3.1 Creating threshold alarm templates

🔒 **Manage Alarm Templates**

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

▶ 1. In the **Alarm Templates** window select the **Threshold Alarms** tab.

2. Select **Add > Add Threshold Alarm Template**. To copy settings from an existing template, select the template, then **Add > Copy Selected Threshold Alarm Template**.

3. In the **Add Threshold Alarm Template** window, add a unique name for the new template and then set the template details:

Measurement type
Select the type of measurement monitored at selected Location(s).

Unit
Choose the units you want used to record the measurement type.

Alarm off margin
Specify an active alarm range. If an alarm condition fluctuates within the active alarm range, the alarm does not turn off. For example, if the high threshold is 10 °C, and the alarm off margin is 1 °C, the alarm will not turn off until the temperature falls to or below 9 °C.

Permissions
Select the groups authorized to modify or apply this template to Locations.

Description
(optional) Provide more details about the threshold template settings.

4. Enable one or more threshold levels:

Select
Select the threshold levels you want to activate.

Level
Five threshold levels are available, but you only set values for the levels that are selected.

Threshold
Set a numerical value manually or with the up/down arrows.

> The device's properties and not the alarm template (which always uses 5 zeroes) determine the number of decimal places used in determining when the threshold is reached.

Priority
Set the response priority for the threshold value. Priority value provides users a visual clue about the severity of conditions in the **Alarms** window.

Report Category
This setting defines whether alarms triggered by the threshold level appear on reports as Alarms or Warnings. You can set report options to include or exclude these categories, depending on your reporting requirements.

Alarm Delay
Set a delay if you want to prevent a threshold alarm from triggering immediately after threshold is exceeded. You may want to set a delay if you want an alarm triggered only if the condition persists beyond a delay period.

5. Select **Save**.

8.1.3.2 Applying threshold alarm templates to locations

🔒 **Manage Alarm Templates**

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

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

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

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

2. Select **Manage > Add Threshold Alarms**. Complete the fields in the **Add Threshold Alarm** window:

Location
Verify that you are adding a threshold alarm template to the correct Location(s). If you selected a Zone, the threshold alarm template is applied to all Locations in the Zone.

Status
Set status to **Enabled** to actively monitor thresholds on selected Location(s). If you do not want the threshold alarm settings activated on this Location until a later time (you may have more configuring to do), set as **Disabled**.

Send to device
Choose whether to send threshold level information to an RFL100-series or HMT140-series data logger. Select the threshold levels to display using the checkboxes in the **Alarm on Device** column. Only two levels can display on an HMT140 device (1 high and 1 low).

Device password
If the selected Location is linked to an HMT140 device with password functionality enabled, type the password to apply threshold settings.

Measurement type
Select the type of conditions being measured at this Location.

Threshold alarm template
Select an available threshold alarm template. The threshold template details appear in the grid.

3. For each alarm level, update threshold alarm settings:

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

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

Alarm Notification Template
Select an alarm notification template to use if this threshold is exceeded. Alarm notification templates define who is notified and when.

Message or Comment
All threshold alarm notifications use content specified in viewLinc's default notification content templates. Use this field to insert custom text in place of the [AlarmMessage] and [Comment] macros embedded in the content templates. For example, you may want to add a description of an action required to resolve a common issue, "This pump tends to cause this alarm, make sure to reset it before acknowledging."

4. Select **Save**.

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

More information

8.1.3.3 Editing threshold alarm templates

 Manage Alarm Templates

Adjust threshold levels for all Locations using the same threshold alarm template.

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

1. In **Alarm Templates** select the **Threshold Alarms** tab.

2. Select the template you want to modify, then select **Edit**.

3. Select **View Locations** to verify that changes can be applied to all Locations currently using the template.

4. Modify the editable settings.

5. Select **Save**.

8.1.3.4 Editing location threshold alarm settings

🔒 **Manage Alarm Templates**

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

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

1. In **Sites Manager** in the **Zones and Locations** tree, select the Zone or Location you want to modify (**CTRL**+click to select multiple Zones and Locations).

2. Select the **Threshold Alarm Settings** tab, and then select one or more threshold alarm rows .

3. Select **Edit threshold alarm settings**.

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

4. Select **Save**.

8.1.3.5 Deactivating threshold alarms

🔒 **Manage Alarm Templates**

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

To prevent a Location from using applied threshold alarm settings temporarily (useful if you need to store more than six threshold alarm settings with a Location), simply disable a threshold alarm setting.

1. In **Sites Manager** select a Location in the **Zones and Locations** tree.

2. On the **Threshold Alarm Settings** tab, select the threshold you want to deactivate.

3. Select **Deactivate**.

4. At the prompt, select **Deactivate**

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

More information

‣ Enabling or disabling threshold alarm settings (page 215)

8.1.3.6 Reactivating threshold alarms

🔒 **Manage Alarm Templates**

You can reactivate a deactivated threshold alarm settings on the Location at any time.

1. In **Sites Manager** select a Location in the **Zones and Locations** tree.

2. On the **Threshold Alarm Settings** tab select **View > Include Deactivated Threshold Settings**.

3. From the list of threshold alarm templates that appear, highlight the threshold you want to reactivate, then select **Activate**.

4. At the prompt, select **Activate**.

8.1.4 Device and host alarms

Communication between devices and the viewLinc Enterprise Server is essential for continuous monitoring of conditions. To ensure you are notified of any issues that require attention, configure the default host and device alarm templates according to your company's notification requirements.

In **Sites Manager**, the **Device Alarms** tab displays a list of the device alarm templates applied to your devices. You can modify the default device alarm templates, or create new device alarm templates in the **Alarm Templates** window.

8.1.4.1 Types of device and host alarms

Device alarm templates are automatically applied to each monitoring device connected to the viewLinc Enterprise Server (data loggers and transmitters). Host alarm templates are applied to hosts (Device Host computers and access points).

Device alarm templates contain default (and modifiable) settings which define:

• Alarm priority
• Alarm notification delay
• Acknowledgment requirements
• Group authorized to modify device alarm settings

You can modify the default device and host alarm templates. You can also create new alarm templates with unique settings for specific Locations.

Device or host communication alarms (`Default Communication Alarm`)

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

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

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

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

> If a device host computer or access point host goes offline, the system generates a host communication alarm only. Connected devices do not generate device communication alarms.

Device or host configuration alarms (`Default Device/ Host Configuration Alarm`)

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

- An internal device error is preventing data history from recording.
- viewLinc detects a device's stop mode is not set to Wrap when full (DL data loggers).
- viewLinc cannot retrieve historical samples because a device is configured with a delayed data recording start (DL data loggers).
- viewLinc detects a device that is locked to another system.
- A device may have a disabled channel that is linked to Location.
- There is a problem with the HMT140, causing it to send too many transmissions which may drain the battery.

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

Device validation alarms (`Default Device Validation Alarm`)

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

Device
calibration
alarms (`Default`
`Device`
`Calibration`
`Alarm`)

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

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

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

Historical data alarms
(`Default Historical`
`Data Alarm`)

An historical data alarm is a notification send when there is communication between the host and device(s), but the historical data has either fallen behind or is unrecoverable.

8.1.4.2 Editing host communication alarm settings

🔒 **Manage Alarm Templates**

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

▶ 1. In **Sites Manager** select the **Hosts and Devices** tab.

2. On the **Hosts and Devices** tree select one or more hosts.

3. Select **Configure > Host Communication Alarm Settings**.
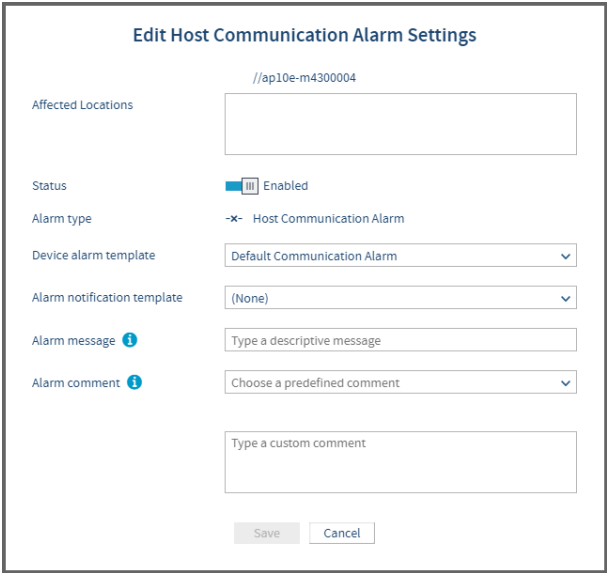
4. Set properties:

Status
Host communication alarms can only be generated when status is enabled.

Device alarm template
Accept the default template, **Default Communication Alarm**, or select a custom template from the drop-down list. Template selection applies to all selected hosts.

Alarm notification template
Select a custom template from the drop-down list. Notifications are not sent if no alarm notification selected (alarms are always indicated on the **Location Alarms** tab in **Sites** or **Overview**, or in the **Alarms** window).

Alarm message
(Optional) Add a descriptive message to include in alarm notifications. This text is used in place of the [AlarmMessage] macro in the related default email templates, or can be added to a custom email/SMS/voice template.

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

5. Save your changes.

More information

‣ Editing device alarm templates (page 100)

8.1.4.3 Editing host configuration alarm settings

🔒 **Manage Alarm Templates**

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

1. In **Sites Manager** select the **Hosts and Devices** tab.

2. On the **Hosts and Devices** tree select one or more hosts.

3. Select **Configure > Host Configuration Alarm Settings**.

4. Set properties:

   Status
   Host configuration alarms can only be generated when status is enabled.

   Device alarm template
   Accept the default device alarm template, Default Host Configuration Alarm, or select a custom template from the drop-down list. Template selection applies to all selected hosts.

   Alarm notification template
   Select a template from the drop-down list. Notifications are not sent if no alarm notification selected (alarms are always indicated on the **Location Alarms** tab in **Sites** or **Overview**, or in the **Alarms** window).

   Alarm message
   (Optional) Add a descriptive message to include in alarm notifications. This text is used in place of the [AlarmMessage] macro in the related default email templates, or can be added to a custom email/SMS/voice template.

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

5. Save your changes.

More information
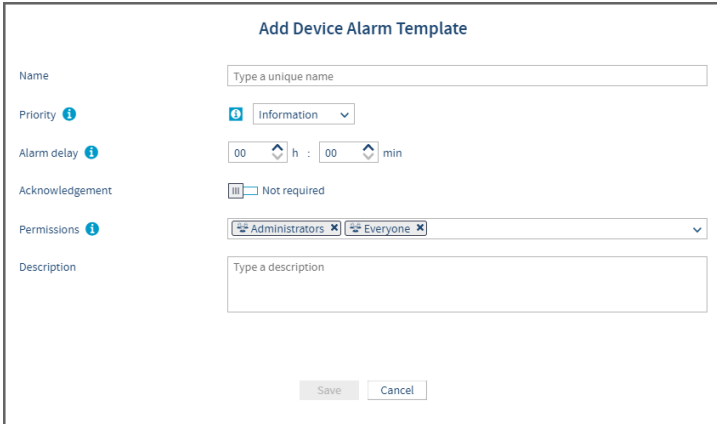
‣ Editing device alarm templates (page 100)

8.1.4.4 Creating device alarm templates

🔒 **Manage Alarm Templates**

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

▶ 1. In **Alarm Templates** select the **Device Alarms** tab.

2. Select **Add > Add Device Alarm Template**. To copy settings, select an existing template, then select **Add > Copy Selected Device Alarm Template**.

3. In the **Add Device Alarm Template** window, type a unique name for the new template and then set the template properties:

Priority
The priority level is used as a visual indication of issue severity, to help you determine how quickly to respond to the issue.

Alarm delay
When viewLinc identifies a device alarm condition, the delay is the time period starting from the moment an issue is detected and when the device alarm is triggered. It is recommended that you set the delay according to the priority.

Acknowledgement
Indicate whether user acknowledgement of this device alarm is required. When an alarm is acknowledged, the action is tracked in the event log.

Permissions
Select the groups permitted to modify or apply this template. The group requires **Configure Alarms** permission to apply the template to Locations.

Description
(Optional) Provide more details about the device alarm template.

4. Select **Save**.

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

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

More information

‣ Types of device and host alarms (page 92)

8.1.4.5 Applying device alarm templates

🔒 **Manage Alarm Templates**

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

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

1. In **Sites Manager** navigate the **Zones and Locations** tree to select a Zone or a Location.

2. Select the **Device Alarm Settings** tab.

3. Select the row for each device alarm type you want to modify, then select 🖊 **Edit** (or use the right-click menu). Sort the **Alarm Type** column in ascending or descending order to select a group of the same device alarm types.

4. On the **Edit Device Alarm Settings** window, verify you have selected the correct Location(s).

5. Edit device alarm settings:

Status
Device alarms are only generated when status is enabled.

Device alarm template
Select the template to use for the alarm type. If multiple templates are in use, it is recommended not to change the current template selections.

Alarm notification template
Select an available alarm notification template to use for device alarms at selected Location. If multiple templates are in use, it is recommended not to change the current template selections.

Alarm message or **Alarm comment**
All device alarm notifications use content specified in viewLinc's default notification templates. Use these fields to insert custom text in place of the [AlarmMessage] and [Comment] macros embedded in the content templates.

6. Select **Save**.

More information

‣ Notification content (page 110)

8.1.4.6 Editing device alarm templates

🔒 **Manage Alarm Templates**

Modify device alarm template settings for all Locations using a default viewLinc device alarm template.

▶ 1. In **Alarm Templates** select the **Device Alarms** tab.

2. Select the template you want to modify, then select **Edit**.

3. Select **View Locations** to verify that changes can be applied to all Locations currently using the template.

4. Modify editable settings.

5. Select **Save**.

8.1.4.7 Editing location device alarm settings

🔒 **Manage Alarm Templates**

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

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

▶ 1. In **Sites Manager** in the **Zones and Locations** tree, select the Zone or Location you want to modify (**CTRL**+click to select multiple Zones and Locations).

2. Select the **Device Alarm Settings** tab, and then select one or more device alarm rows in the grid.

3. Select ✎ **Edit device alarm settings**, then adjust settings in the **Edit Device Alarm Settings** window:

Affected Locations
Verify that all Locations linked to this device can be updated with new device alarm settings. If a device has multiple Locations linked to its channels, make sure that new alarm template settings are applicable to all affected Locations.

Status
If the status is disabled, viewLinc will not initiate the specified device alarm or device notifications.

Device alarm template
Select a device alarm template or accept the default option provided. Device alarm templates set the priority level for the device alarm condition, when it is issued, and if it needs to be acknowledged. If multiple device alarms selected, it is recommended not to change the current template selections.

Alarm notification template
Select an alarm notification template or accept the default option provided. Alarm notification templates specify who is notified, when and how. If multiple device alarms selected, it is recommended not to change the current template selections.

Alarm message
(Optional) Add a descriptive message to include in notification messages. This text is used in place of the [AlarmMessage] macro in the related default email templates, or can be added to a custom email/SMS/voice template.

Alarm comment
(Optional) Select from the list of available predefined comments, or type a custom comment to include in notification messages. This text is used in place of the [Comments] macro in the related default email templates, or can be added to a custom email/SMS/voice template.

4. Select **Save**.

8.1.5 Alarm notifications

An integral feature of the Vaisala viewLinc Monitoring System is the ability to configure multiple alarming functions to ensure that you are notified as soon as conditions exceed set parameters. Alarm events are immediately visible on a user's desktop or a remote display, and viewLinc can also be configured to initiate audible browser alarms, deliver email, send SMS messages (via modem or web service provider), or issue voice calls to individuals on a call tree.

> ℹ Activation of web-enabled SMS and voice messaging services requires purchase of feature license keys and a service provider account.

Alarm notification templates define:
- When to send an alarm notification.
- Who should receive a notification.
- How the notification is delivered (email, SMS, voice call).

- If a visual external alarm command is initiated.
- If a notification delay is required after an alarm is triggered, and if the notification will repeat at timed intervals to the same or different recipient(s).

The content of an alarm notification is defined by the messaging template associated with the alarm.

> **i** Audible browser alarms are enabled in **System Preferences** on the **General** tab, and the user receiving an alarm must have their PC set up to receive audible alarms.

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

Example

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

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

More information

‣ System preferences (page 113)
‣ Notification content (page 110)

8.1.5.1 Web service for SMS and voice notifications

Web-enabled voice and SMS notifications allows web delivery of voice or SMS alarm notifications. Message recipients are able to acknowledge web-delivered voice and SMS alarm notifications remotely with their mobile device and assigned PIN. Additionally, you can set up voice call trees to ensure there is a response from someone on your team.

① 📞 → 🧑❌
② 📞 → 🧑❌
③ 📞 → 🧑✅
④ 📞   🧑
⑤ 📞   🧑

For more information see Setting up voice or SMS web services (page 150).

8.1.5.2 Creating alarm notification templates

🔒 **Manage Alarm Templates**

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

> ℹ️ Command notifications do not initiate for system alarms.

The content generated for alarm notifications is provided in over 40 default email/SMS/voice templates. Message content can also be customized to send specific information to select groups.

▶ 1. In **Alarm Templates**, select the **Alarm Notifications** tab.

2. Select **Add > Add Alarm Notification Template**. To copy settings, select an existing template, then select **Add > Copy Selected Alarm Notification Template**.

Permissions

Select the groups authorized to modify or apply this template to Locations.

Description

(optional) Provide more details about the alarm notification template.

3. In the **Notification Escalation Path** area, select **Add** to choose an alarm notification format.
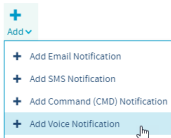
4. To create an email or SMS notification, complete the fields in the **Email Notification Settings** pane:

Name

Type a unique name for each notification. You may want to indicate whether it is an initial or follow-up notification, or identify the group it goes to.

Notification delay

Specify a delay in hours and/or minutes from when an alarm is triggered and you want an alarm notification message sent. Alarm activation delays can also be added to threshold alarms.

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

Send to

Select a user or select a group containing all the users you want notified. All users in the group will receive an alarm notification message (the content varies based on the type of alarm).

Send recurring notifications

Turn this option on to send the a repeat notification at set intervals while the alarm condition exists, or after a specific number of notification messages are sent.

When the alarm is acknowledged

Specify whether to stop or continue sending notifications after an alarm is acknowledged, and whether to send an acknowledgment notification message and/or an alarm off notification message.

5. To create a voice notification, complete the fields in the **Voice Notification Settings** pane:

Name

Type a unique name for this notification. You may want to indicate whether it is an initial or follow-up notification, or identify the users it goes to.

Notification delay

Specify a delay in hours and/or minutes from when an alarm is triggered and you want an alarm notification message sent. Alarm activation delays can also be added to threshold alarms.

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

Call order list

To add recipients to a call list, select **Edit call list**. Select a group which contains the user(s) you want to add. Next, select users in the order you want them called; you can reset the order with the Order arrows (right column). You can choose more groups to select additional users. Save the list.

> Only users with mobile phone numbers assigned in viewLinc display on the list.

Send recurring notifications

Turn this option on to send a repeat voice call at set intervals (every 15 minutes to 24 hours) while the alarm condition exists, or after all call tree notifications are sent. Each user who receives a call has the option to acknowledge the notification and stop the call tree or, if the system preference for voice acknowledgment is not enabled, to confirm receipt of the call, or to verify that the alarm is no longer active (all options require the user to have a mobile phone number and PIN recognized in viewLinc).

When the alarm is acknowledged

> Specify whether to stop or continue calling recipients after an alarm is acknowledged, and whether to send an acknowledgment notification message and/or an alarm off notification message.

6. To create a command notification, complete the following fields in the **Command Notification Settings** window:

   Name
   > Type a unique name to describe the command.

   Notification delay
   > Specify a delay in hours and/or minutes from when an alarm is triggered and you want the command to run. Alarm activation delays can also be added to threshold alarms.

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

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

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

   Run recurring commands
   > Choose to send the same or different command at repeating intervals while the condition still exists; specify whether you want the commands to stop running after the alarm is acknowledged, or after a specific number of commands are run.

   When the alarm is acknowledged
   > Choose to continue or block recurring commands.

   Run command when alarm acknowledged/when alarm turns off
   > Choose a different command to run when an alarm is acknowledged or when the alarm turns off.

7. Select **Save**. You can now apply this alarm notification template to one or more Locations (**Sites Manager > Manage**), or assign it for use with system alarms (**System Preferences > System Alarms**).

More information

8.1.5.3 Applying alarm notification templates

🔒 **Manage Alarm Templates**

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

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

8.1.5.3.1 Applying an alarm notification template to a location threshold alarm

▶ 1. In **Sites Manager** on the **Zones and Locations** tree, select a Location.

2. Select the **Threshold Alarm Settings** tab.

3. Select a threshold alarm settings row on the grid, then select ✎**Edit Threshold Alarm Settings**. If no templates are available, you must add a threshold template to the Location (**Manage > Add Threshold Alarms**).

4. On the **Edit Threshold Alarm Settings** window, select an enabled threshold level.

Level	Threshold	Alarm Delay		Acknowledgement	Alarm on Device	Alarm Notification Template	Message or Comment
		h	min				
⬆ HighHigh	⚠ > 60.0 %RH	0	0	Required	☐	Default Threshold... ✎	(None) ✎
▲ High	⚠ > 55.0 %RH	0	0	Required	☐	Defau Default Threshold Notifications	

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

6. Select **Save**.

8.1.5.3.2 Applying an alarm notification template to multiple location threshold alarms

▶ 1. In **Sites Manager** navigate the **Zones and Locations** tree to select a Zone or several Locations (**CTRL** + click).

2. On the **Threshold Alarm Settings** tab, select one or more threshold setting rows.

3. Select ✎**Edit threshold alarm settings**.

4. On the **Edit Threshold Alarm Settings** window in the **Alarm notification template** column, select a template for one or more enabled threshold levels.

5. Select **Save**.

8.1.5.3.3 Applying an alarm notification template to a location device alarm

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

8.1.5.3.4 Applying an alarm notification template to multiple location device alarms

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

8.1.5.3.5 Applying alarm notification templates for system alarms

1. In **System Preferences** select the **System Alarms** tab.

2. Select an alarm notification template for Database Validation Alarms and/or Event Log Validation alarms.

3. Select **Save**.

8.1.5.4 Editing alarm notification templates

🔒 **Manage Alarm Templates**

Before making changes to an alarm notification template, check which Locations and system alarms are using the template.

▶ 1. In **Alarm Templates** select the **Alarm Notifications** tab.

2. Select the template you want to modify, then select ✏️**Edit**.

3. Modify the editable settings.

4. Select **Save**.

8.1.6 Notification content

Location threshold, device and system alarm notifications contain default message content to inform your team about alarm conditions occurring on your network.

viewLinc provides more than 40 default message templates, in all supported languages. Message templates are provided for all stages of the notification cycle: initial notification of an alarm condition, recurring notifications, notification that an alarm condition is no longer present, and notification of an acknowledged alarm.

💡 To view and edit messages in other languages, log into viewLinc using the required language.

ℹ️ Additional alarm messages and/or comments can be included in the content of standard threshold, device, and system alarm notifications.

More information

‣ Applying threshold alarm templates to locations (page 89)
‣ Editing location device alarm settings (page 100)

8.1.6.1 Creating custom message content

🔒 **Manage Alarm Templates**

You can modify email, SMS and voice message content issued from viewLinc. Type specific text or add a macro to insert system-generated content, such as a timestamp or a predefined alarm comment. For a complete of list of macro definitions, see Predefined settings (page 236).

> When adding macros to SMS or voice messages, make sure the expected content will not generate unnecessarily long messages.

1. In **Alarm Templates** select the **Notification Content** tab.

2. Select a template to modify, then select **Edit**. In the window, default content is displayed but it cannot be modified.

3. To modify email message content:

   a. Select the **Email Message** tab, then select **Custom Email Content**.

   b. Add new content in the active custom text areas, **Email subject**, **Email text**.

   c. To insert system-generated content, such as a timestamp or a predefined alarm comment, move the cursor where you want to add the content, then select an option from the **Add [macro]** dropdown. For a complete of list of macro definitions, see Table 28 (page 237).

4. To modify SMS message content:

   a. Select the **SMS Message** tab, then select **Custom SMS Content**.

   b. Add new content in the **SMS text** field. Note: SMS modem messages are limited to 70 characters in length; SMS web service messages are split after 160 characters. SMS modem message length can increase if your network supports longer SMS messages.

5. If your system is licensed for voice web service and you have selected a template with a voice message option:

   a. Select the **Voice Message** tab, then select **Custom Voice content**.

   b. Add new content in the Voice text field. Note: Make sure to write a message that is understandable as a spoken message. Make use of colons, commas and periods to create pauses in the verbal message and insert applicable macros.

6. Save your changes.

If you have a voice notification that uses macros, such as: **"This is a repeat notification for a communication alarm recorded on [AlarmTimestamp]. On Device Host: [DeviceHostName]"**, and the notification is sent at 13:54 for hostname VANHOST-AP10E-1001, your recipient will hear the macro information read out as: **"This is a repeat notification for a communication alarm recorded on UTC-7 thirteen fifty-four on v-a-n-h-o-s-t-dash-a-p-one-zero-e-dash-one-zero-zero-one."**

If a zone or location name is included in a message, Twilio will read out the names if they are identified as proper nouns; otherwise, the letters will be read out. To help Twilio recite zone or location names clearly, add a space between characters and letters. For example,

Zone A = **"zone a"**

ZoneA = **"z-o-n-e-a"**

More information

- Applying threshold alarm templates to locations (page 89)
- Editing location device alarm settings (page 100)

9. System preferences

9.1 System preferences

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

9.1.1 Modifying general system settings

> The **General** tab of the **System Preferences** also includes the **Add License** option. By adding new license keys, you can increase the number of supported devices or add new licensed features. For more information on adding license keys, see Entering a new license key (page 117).

Manage System

1. Set default units and values. These values are used wherever units display (trend graphs, reports). These values can be modified for specific Locations.

   Default temperature units
   By default, all devices monitoring temperature display in Celsius.
   To learn more, see Setting temperature measurement units (page 129)

   Default value for MKT activation energy
   Set the MKT value according to your GxP requirements.
   To learn more, see Setting Mean Kinetic Temperature (MKT) activation energy value (page 129).

2. Specify device options:

Device description
Choose to display the device alias (a longer description) in viewLinc.
To learn more, see Setting device or channel alias preferences (page 130).

Channel description
Choose to display the channel alias (a longer description) in viewLinc.
To learn more, see Setting device or channel alias preferences (page 130).

Default calibration duration
Set default data logger and probe calibration cycle length in months.
To learn more, see Setting system-wide default calibration duration (page 130).

Automatically lock DL data loggers
Enable auto-locking to ensure all newly connected DL data loggers can only be
modified by viewLinc.
To learn more, see Locking or unlocking DL data loggers (page 227).

DL data logger timebase synchronization
When the logger timebase synchronization feature is enabled, the time clock in a
logger is continuously compared with the viewLinc clock and adjusted, if required.
To learn more, see Enabling or disabling timebase synchronization (page 131).

viewLinc Aware functionality
Enable viewLinc Aware to ensure faster setup for vNet devices.
To learn more, see Enabling or disabling viewLinc Aware (page 131).

3. In **System Preferences** on the **General** tab, set **General** options:

System language

Set the default system language for reports and notifications. You can also enable additional languages to allow users to set preferred language output for reports, notifications and their viewLinc desktop display.

To learn more, see Setting the system language (page 118).

Email alarm acknowledgement, **SMS alarm acknowledgement**, **Voice alarm acknowledgement**

Allow users to acknowledge alarms by responding to notifications sent via email, SMS, or voice call.

To learn more, see Allowing remote acknowledgement (page 122).

Scheduling

Enable this option to control when users receive notifications, and when Location alarming should be active. After enabling this option, create schedules.

To learn more, see Creating schedules (page 139).

Audible alarm notification

Enable audible alarm notification in a browser, then set up each user's account profile to receive audible alarming.

To learn more, see Enabling or disabling audible alarms (page 123).

Audible alarm sound

Choose the sound for audible browser alarms. Select the ▶ to start/stop a sound test.

Provisional threshold alarms

By default, the system has provisional threshold alarms enabled.

4. Set security options:

Comments on changes
Indicate whether comments are required when users acknowledge alarms or modify the system.
To learn more, see Adding predefined comments (page 132).

Confirm identity on changes
Require user authentication when making system changes.
To learn more, see Setting authentication requirements (page 117).

Maximum failed login attempts
Set the number of times a user can enter incorrect login information before the user account is locked. For administrator instructions on locking and unlocking users, see Locking and unlocking user accounts (page 205).

> **i** Account locking by viewLinc due to too many login attempts only applies to users using viewLinc authentication, not users that use Windows authentication.

Maximum password age
Set the maximum time a login password can be used before the user must change the password.

Minimum time for password reuse
Set the minimum time before a password that has been used earlier can be set as the login password again.

5. Adjust technical support log settings (optional).

System log
Record different amounts of system activity.

Device driver log
Record different amounts of device activity.

Log maximum age
Specify how long to store technical support files. Once the limit is reached, old log files are deleted.
To learn more, see Changing technical support log settings (page 118).

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

6. Save your changes.

9.1.2 Enabling or disabling schedules

🔒 **Manage System**

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

▶ 1. In **System Preferences** on the **General** tab, select the **Scheduling Functionality** row.

   2. Enable or disable scheduling.

   3. Save your changes.

More information

   ‣ Schedules (page 138)

9.1.3 Entering a new license key

🔒 Manage System

The viewLinc license key entered during installation specifies how many devices can be managed by viewLinc, it does not monitor how many users can access the system (unlimited). Add new license keys to increase the number of devices you can monitor with viewLinc, or to enable additional licensed features (to support third-party Modbus devices, integration with OPC UA Server, Voice web services, SMS web services, and/or Web API).

> ℹ Your current license information is displayed in the **About** window (**Help > About**).

▶ 1. In **System Preferences**, select the **General** tab.

   2. Select **Add License** and enter the new viewLinc or feature license key number (or copy and paste).

   3. Select **Add**.

9.1.4 Setting authentication requirements

🔒 **Manage System**

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

▶ 1. In **System Preferences** select the **General** tab.

2. Select **Confirm identity on changes**, then choose an authentication option:

   Never
   > Logged-in users are not required to confirm their identity when making changes.

   Always
   > Logged-in users are required to enter their password each time they try to make a change.

   After 1 - 30 minutes/**After 1 hour**
   > Logged-in users are required to re-enter their password if the selected time period has passed since their last authenticated change.

3. Select **Save**.

9.1.5 Changing technical support log settings

🔒 **Manage System**

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

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

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

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

9.1.6 Setting the system language

🔒 **Manage System**

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

Enable support for additional languages on the **System Preferences > Languages** tab, and then set the user language preference on each user's profile.

Important notes about system language setting and user language preference:
• Quick reports: When a user generates a Quick Report, the content is generated according to the user's logged-in language, even if it is different from their language preference.

- Scheduled reports: Sent to recipients according to their language preference.
  - If no user language preference is specified, report content is generated in the report language.
  - If no user language preference or report language is specified, the content is generated according to the default system language.
- User-generated reports: Report content is generated in the system language.

Languages supported:

- Chinese (Simplified - ZH)
- English (EN)
- Finnish (FI)
- French (FR)
- German (DE)
- Italian (IT)
- Japanese (JA)
- Korean (KO)
- Portuguese (Brazilian - PT)
- Spanish (International - ES)
- Swedish (SV)

▶ 1. In **System Preferences** select the **General** tab.

2. In the **System language** row, select the system language.

3. Select **Save**.

9.1.6.1 Making additional languages available

▶ 1. In **System Preferences** select the **Languages** tab.

2. Enable the language choices you want displayed when users log in.

3. Select **Save**.

9.1.7 Authenticating users with Active Directory

🔒 **Manage System**

You can simplify user authentication for your viewLinc deployment by setting up Active Directory Link.

Before you start this task, you should have already set up Active Directory (AD) with an organizational unit (OU), groups, and users. You should also create a specific Active Directory user with limited permissions whose user principal name (UPN) you will provide to allow viewLinc to access your AD server.

▶ 1. In **System Preferences** select the **Active Directory Link** tab.

2. Provide the appropriate details for the Active Directory connection:

Host name
> Specifies the active directory host or the domain name; must be fully qualified if the connection type (the next field) is Secured or Kerberos.

Connection type
> - **Unsecured**: Specifies unencrypted communication to the Active Directory. Username and password are required.
>   Not recommended.
> - **Secured**: Specifies TLS-protected communication to the Active Directory. Username and password are required.
> - **Kerberos**: Specifies Kerberos security to the Active Directory. Username and password are not required. If omitted, the username and password applied to the service will be used; if provided, the service will impersonate the user.

Port number
> Specifies the TCP port to connect on. For Unsecured connection types, 389 is the default; for Secured or Kerberos connection types, the default is 686.

User principal name
> Specifies the username used for authentication to the Active Directory. Must be in UPN format: *username@AD-domain*

User password
> Specifies the password for the UPN provided for Active Directory authentication. Required for Unsecured or Secured connection type.

Server domain DN
> Specifies the distinguished name of the Active Directory server name, in the following format: dc=test,dc=local

Organization unit DN
> Specifies the distinguished name of the organizational unit, in the following format: ou=*viewLinc*, dc=*test*,dc=*local*

Synchronize every
> Specifies how often to synchronize identity data from Active Directory to your viewLinc server. If you do not specify a regular interval, you should manually click the **Sync now** button after changes to the Active Directory.

User authentication method
> Specifies the authentication for users:
> - **Domain**: Use Windows server authentication. User must have login privileges on the viewLinc server.
> - **Active Directory**: Use Active Directory server authentication. User doesn't require login privileges on the viewLinc server.

3. Provide the relevant details for the user property mapping:

Mobile
> Name of the Windows property used to fetch the user's mobile number.

Email
> Name of the Windows property used to fetch the user's email address.

viewLinc PIN
> User's PIN for acknowledging alarms.

> This property doesn't exist by default, so you must create it in the Active Directory, if desired.

Preferred language
> Name of the Windows property used to fetch the user's preferred language.

> This property doesn't exist by default, so you must create it in the Active Directory, if desired.

Send alarm notification
> Name of the Windows property used to fetch the user's alarm notification setting.

> This property doesn't exist by default, so you must create it in the Active Directory, if desired.

Audible alarm notification
> Name of the Windows property used to fetch the user's audible alarm setting.

> This property doesn't exist by default, so you must create it in the Active Directory, if desired.

4. Click the **Test connection** button to ensure that the details provided are correct.

9.2 Alarm templates

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

> Create **threshold alarm templates** to specify the conditions that should trigger an alarm, then apply the template to one or more Locations.

Default **device alarm templates** are provided and assigned to each new device connected to your viewLinc system. They specify how and when you want to be notified of device status. The default templates can be modified, or you can create new device alarm templates.

Create **alarm notification templates** to define who should be notified in the event of a threshold or device alarm, the information that should be distributed in email, SMS, or voice messages, or whether to initiate a command to activate visual or auditory alarms, and whether the notified individual must acknowledge an alarm. Alarm notification templates are applied to Locations using threshold alarm templates.

Default **email, SMS and voice templates** are provided. They contain standard information issued from viewLinc about different alarm conditions in your network. The default content can be modified. Note that SMS functionality requires a supported modem, and voice/SMS services via web require a Twilio account.

(Optional) Create **schedules** to define when Location thresholds should be monitored, and when you want alarm notifications sent. You can set up a day schedule and an evening schedule to send notifications to different teams, or set schedules to prevent users on holiday from receiving alarms. Schedules functionality must be enabled.

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

More information

‣ Setting up voice or SMS web services (page 150)
‣ Enabling or disabling schedules (page 116)

9.2.1 Allowing remote acknowledgement

Manage System

viewLinc must be configured to allow users to acknowledge alarm notifications remotely, via email, SMS, or voice call.

> Each user who is permitted to acknowledge SMS alarm notifications remotely must include a mobile number and unique PIN on their user account profile.

▶ 1. In **System Preferences** on the **General** tab, enable the acknowledgement option(s) you want:

> **Email alarm acknowledgement**
> To allow email acknowledgement, make sure your email server is set up to receive email acknowledgements.

> **SMS alarm acknowledgement**
> To allow SMS acknowledgement, make sure each user has a mobile phone number and unique PIN entered in their user account profile. Also make sure your SMS modem is set up to receive SMS acknowledgements, or you have set up an SMS web service account and SMS web settings configured.

> **Voice alarm acknowledgement**
> Acknowledgment by voice call requires a voice web service account and voice settings configured.

2. Select **Save**.

9.2.2 Enabling or disabling audible alarms

🔒 **Manage System**

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

• To hear an audible alarm, the user must be logged into viewLinc on their computer and have audible alarms enabled on their user profile.
• To turn off an active audible alarm, the user can click the alarm icon.

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

▶ 1. In **System Preferences** select the **General** tab.

2. On the **Audible alarm notification** row, select **Enabled** or **Disabled**.

3. If audible alarms are enabled, use the **Audible alarm sound** row to select a sound. Select the ▶ to start/stop a sound test.

4. Select **Save**.

9.2.3 Configuring email/SMS/voice preferences

Alarm notifications are issued via email, via SMS modem or SMS web service, and/or via voice web service (web services require purchase of a Twilio account). An IT administrator can help define the notification connection settings for the issuing and receiving server(s).

9.2.3.1 Configuring email settings

🔒 **Manage System**

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

1. In **System Preferences** select the **Email Settings** tab.

2. In the **Outgoing Server** area, type a valid send from address (email notifications from viewLinc are sent from this address, so the email address must exist within your company), then complete the following:

   SMTP server
   Type the mail server address. For example, `smtp.company.com`.

   Port
   Type the outgoing mail server port number (between 1-65535, default is 25). Your IT network administrator has this information.

   SMTP authentication
   Select if your outgoing mail server requires authentication, and then type the username or email address, and password required to send email.

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

3. Select **Send Test Email** to verify the test email is sent successfully.

4. In the **Incoming Server** area, configure the required mail server settings for your connection type:

   Connection type: **POP3**
   POP3 server
   Type the incoming POP3 mail server name (for example, `pop.company.com`).

   Port
   Type the incoming mail server port number (default is 110).

   User name and **Password**
   Type the username (or address) and password for a valid POP3 account, required to receive email.

   Connection type: **IMAP**
   IMAP server
   Type the incoming IMAP mail server name (for example, imap.company.com).

   Port
   Type the incoming IMAP mail server port number (default is 143).

   User name and **Password**
   Type the username (or address) and password for a valid IMAP account, required to receive email.

5. Select **Save**.

9.2.3.2 Configuring SMS settings

🔒 **Manage System**

If you want viewLinc to send alarm notifications and receive acknowledgements via SMS, you can choose to set up and configure an SMS modem, or configure viewLinc to use an SMS web service. Activation of the SMS web service requires a feature license, an account with a service provider, and an internet-accessible port. For more information, see Setting up voice or SMS web services (page 150)

1. In **System Preferences** select the **SMS Settings** tab.

2. To configure an SMS modem, select **SMS modem** and then complete the SMS modem settings:

> **SMS COM port**
> Type your SMS modem COM port number. If you are setting up an SMS web service, this port must allow access to the internet.

> **Baud rate**
> Select the rate which is best supported by your modem.

> **SIM Card PIN number**
> Type the PIN number required to receive incoming messages.

> ℹ️ SMS modem messages are limited to 70 characters in length. Message length can increase if your network supports longer SMS messages.

3. To configure the Twilio SMS web service, select the **SMS sender** option, **Web service**, and enter your Twilio account details:

> **Account SID**
> Type the security identifier number provided by your SMS service provider. The SID is used to identify your account like a username.

> Authentication token
> Type the token number provided by your SMS service provider. The token identifies your account like a password.

> Phone number
> Type the country code followed by the full phone number provided by the web service provider.

> viewLinc URL
> Type the viewLinc Enterprise Server hostname or IP address used to access viewLinc through the Internet

> ℹ️ SMS web messages are limited to 160 characters in length. If a message contains more characters, it is separated and sent as an additional message.

4. To complete SMS configuration, select the **Test** button.

   a. Type a recognized viewLinc user's mobile phone number to receive the test message. If the SMS test message is not sent (it may take a minute before delivery), adjust the settings until the test message is sent successfully.

   b. If you are testing an SMS web service configuration, on the receiving mobile phone, type a reply to the message, `test`. This action will verify that viewLinc can receive SMS acknowledgements sent via the web service.

5. **Save** the settings.

9.2.3.3 Configuring voice call web service

🔒 **Manage System**

Before you start, make sure you have added the voice call feature license, you have your Twilio account details available, and a valid internet-accessible URL is available. For more information, see Setting up voice or SMS web services (page 150).

▶ 1. In **System Preferences** select the **Voice Settings** tab.

2. Add your Twilio voice account settings:

   Account SID
   Type the security identification number provided by your voice messaging service provider. The SID is used to identify your account (like a username).

   Authentication token
   Type the token number provided by your voice messaging service provider. The token allows messages to be sent from your Twilio account (like a password).

   Phone number
   Add your Twilio phone number. This number is used to send notifications to your users.

   viewLinc URL
   Type the viewLinc Enterprise Server hostname or IP address used to access viewLinc through the Internet.

3. Send a test message:

   a. Type a recognized viewLinc user's mobile phone number to receive the test message. Note that calls cannot be sent if viewLinc is not accessible through the Internet.

   b. If the voice test message is not delivered (it may take a minute before delivery), adjust the settings until the test message is sent successfully.

4. **Save** the settings.

9.2.4 Setting system alarm preferences

🔒 **Manage System**

System alarms are generated automatically to indicate general system issues, database history integrity, and event log tampering. They are always high priority, are issued immediately, and always require acknowledgement. Acknowledgement of system alarms can be performed in viewLinc or remotely via email/SMS/voice.

> To issue voice call notifications for system database or event log validation alarms, create an alarm notification template that includes a voice call tree.

1. In **System Preferences** select the **System Alarms** tab.

2. In the **IT Network Manager** area, type the mobile number and email address you want to receive viewLinc system notifications. You can also choose whether to send copies of system alarm notifications to members of the **Administrators** group.

3. In the **Database Validation Alarm** area, the **Priority**, **Alarm delay** and **Acknowledgement** options cannot be modified. You can modify the following options:

    Alarm notification template
    Choose an alarm notification template to use with the system alarm notification. The alarm notification template defines whether a notification is issued, in what format, how soon after the alarm is triggered the notification is sent, and how often it is repeated.

    > Commands are not initiated for system alarms.

    Alarm message
    Alarm message text replaces the **[AlarmMessage]** macro in database validation alarm notifications, email messages only.

    Alarm comment
    Choose to include a predefined comment (if available), or type a custom comment. Comments text replaces the **[Comments]** macro in database validation alarm notifications, email messages only.

4. In the **Event Log Validation Alarm** area, the **Priority**, **Alarm delay** and **Acknowledgement** options cannot be modified. You can modify the following options:

Alarm notification template
Choose an alarm notification template to use with the system alarm message. The alarm notification template defines whether an email, SMS or command notification is issued, how soon after the alarm is triggered the notification is sent, and how often it is repeated.

Alarm message
Alarm message text replaces the **[AlarmMessage]** macro in event log validation alarm notifications, email messages only.

Alarm comment
Choose to include a predefined comment (if available), or type a custom comment. Comments text the **[Comments]** macro in event log validation notifications, email messages only.

5. Select **Save**.

9.3 Display and unit preferences

9.3.1 Setting measurement unit display preferences

🔒 **Manage System**

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

1. In **System Preferences** select the **Units** tab.

2. Select a unit type row, then select **Edit**.

3. Update the unit properties:

Name
For non-viewLinc default unit types, you can modify the name of the unit type.

Device Units
Type a maximum of 6 CAPITAL letters per unit of measurement. Use a comma (,) to separate unit types.

Display Text
Type the format to display for each unit. For example, if a temperature unit is C, you may want to display Celsius.

Min
Set the minimum value permitted for this unit.

Max
Set the maximum value permitted for this unit.

4. To add new device units, select **Add**. In the **New Unit** window make sure you type the unit properties as they are set in your device.

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

5. Select **Save**.

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

9.3.2 Setting temperature measurement units

🔒 **Manage System**

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

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

> You can set measurement units on individual device channels.

1. In **System Preferences**, on the **General** tab, select the **Default temperature units** row.

2. Set the value.

3. Select **Save**.

9.3.3 Setting Mean Kinetic Temperature (MKT) activation energy value

🔒 **Manage System**

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

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

1. In **System Preferences** on the **General** tab, select the **Default value for MKT activation energy** row.

2. Set the value.

3. Select **Save**.

9.4 Device preferences

9.4.1 Setting device or channel alias preferences

🔒 **Manage System**

Vaisala devices have descriptions stored inside them that have a maximum length of 16 alpha-numeric characters. These descriptions can be defined and modified using viewLinc or device configuration software (vLog or HMT140 Utility).

For easier reference, you can configure viewLinc to display a longer, more informative description for a device or a channel, up to 64 alpha-numeric characters. This longer description is called an alias. **Events**, **Alarms**, **Reports** windows, and email messages all use the selected description for channels and devices.

▶ 1. In **System Preferences** on the **General** tab, select the **Channel description** or **Device description** row.

2. Set to **Use [ ] alias**.

3. Select **Save**.

9.4.2 Setting system-wide default calibration duration

🔒 **Manage System**

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

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

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

▶ 1. In **System Preferences** select the row, **Default calibration duration**.

2. Choose a time period in months.

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

3. Select **Save**.

9.4.3 Enabling or disabling timebase synchronization

🔒 **Manage System**

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

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

> Enable DL data logger timebase synchronization only on one viewLinc Enterprise Server. Timebase synchronization only corrects time drift up to 15 minutes. If the drift is greater than 15 minutes, clear data logger history.

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

9.4.4 Enabling or disabling viewLinc Aware

🔒 **Manage System**

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

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

▶ 1. In **System Preferences** select the **General** tab.
2. Select the **viewLinc Aware functionality** row, then select **Enabled** or **Disabled**.

3. Select **Save**.

New devices are automatically discovered in viewLinc within five minutes. If the autodiscovery process is taking too long, you can force discovery.

9.5 Comment preferences

9.5.1 Setting comments preferences

🔒 **Manage System**

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

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

▶ 1. In **System Preferences** select the **General** tab.

2. In the **Comments on changes** row, select an option:

Not required
Users will not be prompted to enter a comment when system changes are made.

Optional
The comments window will appear for system changes, and users have the option to enter a comment or select a predefined comment.

Required
The comments window will appear and users must enter a comment or select a predefined comment.

Only predefined comments required
The comments window will appear with a list of available predefined comments. This option requires predefined comments to be available.

3. Select **Save**.

9.5.2 Adding predefined comments

🔒 **Manage System**

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

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

▶ 1. In **System Preferences** select the **Comments** tab.

2. Select **Add**.

3. Type a new comment (up to 300 characters).

4. Select **Save**.

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

You can add predefined comments to:

- System alarms
- Location threshold alarm settings
- Alarm acknowledgements
- Events

10. Additional setup tasks

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

- Add group permissions to Zones and Locations. Permissions are used to control the groups which can view, configure or manage different viewLinc Zones and associated Locations.
- Create schedules to define active periods for alarming and notifications. Schedules can ensure users who are not on shift do not receive notifications, or prevent unnecessary alarming during maintenance periods.
- Build views to help users more easily identify Locations of importance. For larger installations, views can help organize different categories of Locations.
- Connect a signal tower for wide-area visual and/or audible alarming.
- Set up a remote display to broadcast live conditions on a large monitor in a warehouse.
- Set up a Twilio account and configure viewLinc to support web-enabled voice and/or SMS message services.
- Configure viewLinc to connect with Vaisala OPC UA Server.

10.1 Permissions

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

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

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

Important Notes about Permissions

- Permissions granted to a Zone apply to all sub-zones and Locations (inherited).
- An individual user's permission is based on the highest group permission available for the Zone.
- If you upgraded from version 4.3.x or earlier version of viewLinc, permissions assigned to users are preserved; however, if you remove a user's permission it cannot be reapplied.

> Before assigning permissions to groups, make sure each group has the rights required to complete tasks associated with the Zone or Location.

Example

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

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

Laboratory A	Inherit from ☐	Acknowledge Alarms ☑	View ☑	Inheritable ☑
▸ Workstation 1				
💧 Humidity				
🌡 Temperature				
▸ Workstation 2				

▸ Warehouse X	Inherit from ☐	Acknowledge Alarms ☐	View ☑	Inheritable ☑
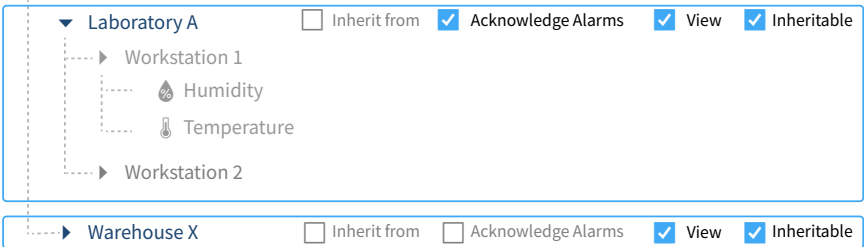
More information

- Rights (page 76)

10.1.1 Permission levels

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

Table 18   Permission Levels

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

10.1.2 Applying group permission to Zones

🔒 **Manage Sites**

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

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

10.1.2.1 Adding permissions

🔒 **Manage Sites**

1. In **Sites Manager** navigate the **Zones and Locations** tree to select a Zone or sub-zone.

2. To check currently applied permissions, select the **Permissions** tab and open the **Permissions Viewer**.

3. Select **Manage > Edit Permissions**.

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

4. Add permissions in the **Edit Permissions** window:

- To apply the same group permissions for the selected Zone to all sub-zones and Locations, select the group then select **Inherit from**.
- To change the group permission level, de-select **Inherit from** then choose a permission level in the **Permissions** columns.
- To ensure a group has a permission level passed on to all current and future sub-zones and Locations in the selected Zone, ensure the **Inheritable** option is selected.

5. Select **Save**.

More information

‣ Using permissions viewer (page 138)

10.1.2.2 Editing permissions

🔒 **Manage Sites**

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

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

1. In **Sites Manager** on the **Zones and Locations** tree, select a Zone.

2. Select **Manage > Edit Permissions**.

3. In the **Edit Permissions** window, de-select the group's **Inherit from** checkbox, then choose a new permission level in the **Permissions** columns. If all permission levels are de-selected, sub-zones are not visible (on the **Permissions** tab the column grid displays **Hide** in the **Permission** column).

4. Select **Save**.

10.1.2.3 Deleting permissions

🔒 **Manage Sites**

Before permissions can be deleted, inherited permissions must be removed.

> ⚠️ **CAUTION!** Deleting group permission may disable the group's permission levels applied to subzones.

1. In **Sites Manager** on the **Zones and Locations** tree, select a Zone.

2. Select **Manage > Edit Permissions**.

3. In the **Edit Permissions** window, select the group.

4. Select **Delete**. If the **Delete** button is not active, you first need to disable inherited permissions.

5. Select **Save**.

More information

‣ Editing permissions (page 137)

10.1.3 Using permissions viewer

🔒 **Manage Sites**

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

1. In **Sites Manager** select a Zone on the **Zones and Locations** tree.

2. Select the **Permissions** tab. The highest available permission level assigned to groups or upgraded users appears in the **Permission** column. If no group permissions are available on a Zone, the group permission level is **Hide**.

3. To view all permissions for a specific group or user, select the **Permissions Viewer** button.

4. In the **Permissions Viewer** window, choose to **Show groups** or **Show users**.

5. Select a group or user to view all assigned permissions.

More information

‣ Editing permissions (page 137)

10.2 Schedules

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

💡 You can temporarily turn off all threshold alarming and prevent notifications from being sent, perhaps during a system maintenance period.

More information

‣ Pausing threshold alarming (page 169)

10.2.1 Creating schedules

🔒 **Manage System**

Schedules define a specific period of time when a user can receive alarm notifications, or to restrict the time frame when threshold alarms can be triggered for a Location.

ℹ️ Before you can apply schedules to users or Locations, make sure scheduling functionality is enabled.

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

Add Schedule

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

Schedule	▬⚫▐Ⅲ▌ Enabled
Name	Type a unique name
Time zone	▾
	Server time zone: (UTC-07:00) Mountain Time (US & Canada)
Start date	2019-01-18 📅
Repeat schedule every	7 days
	To add a standard weekday schedule, Monday to Friday, type 7 days and do not type a time period for Saturday or Sunday.

Define active time periods

Day	Day of the Week	Date	Time Periods
1	Friday	2019-01-18	
2	Saturday	2019-01-19	
3	Sunday	2019-01-20	
4	Monday	2019-01-21	
5	Tuesday	2019-01-22	
6	Wednesday	2019-01-23	
7	Thursday	2019-01-24	

Type multiple time periods separated by a comma. For all day alarm monitoring type 00:00-24:00. For no monitoring leave blank.

Save   Cancel

2. On the **Add Schedule** window define the schedule settings:

   Schedule
   You can create a schedule before setting it to **Enabled**. Once the schedule is applied to users or Locations, you can quickly enable or disable it here. If a schedule is disabled, thresholds are always monitored and notifications always sent for threshold excursions.

   Name
   Type a unique name for the schedule.

   Time zone
   Select the time zone you want the schedule to use. If your company monitors conditions in multiple time zones, you may want to create schedules for each time zone.

   Start date
   Choose a start date by typing in the text box or choosing a date from the calendar. This date defines the day of the week to start the schedule.

   Repeat schedule every
   To set the schedule for a standard work week that repeats every 7 days, type **7** and do not create an active time period for non-work days. For a continuous week (no days off), type **9**. The maximum value is 99 days.

   Define active time periods
   Specify the time period for each day in the cycle, in 24-hour time. Use the following format (xx:xx is the start time and yy:yy is the end time):

   ```
   xx:xx-yy:yy
   ```

   This time period specifies when threshold alarming is active and alarm notifications will be issued.

3. Select **Save**.

You can now apply this schedule to Locations and/or users.

More information

‣ Enabling or disabling schedules (page 116)
‣ Adding user schedules (page 141)

10.2.2 Setting threshold alarm schedules

🔒 **Manage Sites**

Apply a schedule to a Zone or a Location to define when threshold excursions should trigger an alarm notification. Schedules are created in the **Alarm Templates** window.

Before applying a schedule to a Location, make sure you have enabled the scheduling function in **System Preferences** and created a schedule in **Alarm Templates**.

Configure Alarms permission is required to the selected Locations or Zones.

1. In **Sites Manager** in the **Zones and Locations** tree, select a Location.

2. Select **Manage > Set Threshold Alarm Schedule**.

3. In the **Set Threshold Alarm Schedule** window, select **According to schedule** and select a schedule from the dropdown list.

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

4. Select **Save**.

More information

10.2.3 Adding user schedules

🔒 **Manage System**

Apply a schedule to a user to define when they should receive alarm notifications. Schedules are created in the **Alarm Templates** window.

Before adding a schedule, make sure you have enabled the scheduling function in **System Preferences** and created a schedule in **Alarm Templates**.

1. In the **Users and Groups** window select the **Edit** toolbar button.

2. On the **Edit User** window in the **Send alarm notifications**:

Always
Select to indicate that this user should always receive an alarm notification 24x7. This is the default setting.

According to schedule
Select and then choose a schedule from the dropdown list.

Never
Select to make sure this user never receives alarm notifications. This is a useful option when a user is away on holiday.

3. Select **Save**.

More information

‣ Enabling or disabling schedules (page 116)
‣ Creating schedules (page 139)

10.3 Views

Views are an easy way for users to monitor important Locations, or group Location data according to job function.
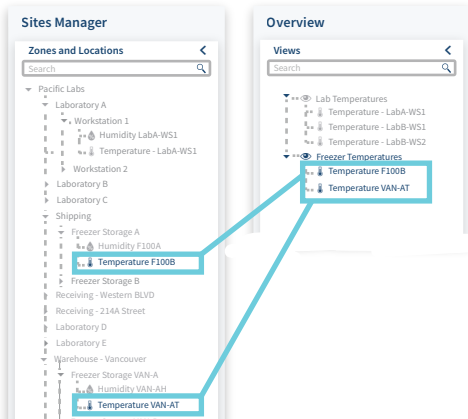
Views can be set up to display Location status on a new dashboard image, or to display a trend graph for select Locations (useful when presenting a view on a remote display terminal). Create new views in **Views Manager** and access them in the **Overview** window.

10.3.1 Your views

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

Use views to:

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

10.3.2 Creating views

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

▸   1. In **Views Manager** select **Add** > **Add View**.

2. In the **Add View** window, type a name for the view.

3. Select **Add > Add Locations**.

4. Select Locations you want to include in the view:

- Select all Locations in a Zone (select the Zone checkbox), or select individual Locations in one or more Zones.
- Only the Locations within a selected Zone are included in a view. You can organize Locations within a view using folders.

5. Select **Add**.

6. Save the **View**.

If you are a member of a group with **Manage Views** right, you can also share your view.

More information

‣   Sharing views (page 144)

10.3.3 Organizing Locations in a view

▸   1. In **Views Manager** on the **Views** tree, select a saved view.

2. Select **Add > Add Folder**.

The menu is not active if there are unsaved changes in the tree.

3. In the **Add Folder** window, type a name for the folder.

4. Select an icon to display on a dashboard.

5. Select **Add**.

6. On the **Views** tree, drag Locations into the new folder.

10.3.4 Sharing views

🔒 **Manage Views**

Allow other users to access a view you create. When a user logs in, new shared views display automatically in the **Overview** window. Sharing views is an easy way to customize a remote display.

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

1. In **Views Manager** in the **Views** tree select a view.

2. On the **Permissions** tab select **Add**. The **Add Permissions** window appears.

3. Select one or more groups and then select the permission level you wish to give:

   View
   > Allow group to see this view in their **Overview** window.

   Full Control
   > Allow group to modify the view in **Views Manager**, or share the view with others.

4. Select **Save**.

More information

- Creating views for remote display (page 145)

10.3.5 Setting a default view

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

1. In **Overview** on the **Views** tree, select a view.

2. Select **Options > Set as Default View**. A star icon ⭐ appears on your default view.

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

Each user can specify a different default view.

10.3.6 Creating views for remote display

🔒 **Manage System**, **Manage Views**

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

▶ 1. Create a new view which includes the Zones and/or Locations you want to see on the display terminal.

2. Create a new group with **Acknowledge Alarms** permission for the Zones and/or Locations in the view.

3. Share the view with the group.

4. Make sure that there is at least one user in the group. This user account will be used to log in to the remote display. You can create a remote display-only user and add the user to the new group.

5. Set up the view as the user's default view.

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

More information

‣ Setting a default view (page 144)

10.4 Signal towers

Integrate your viewLinc system with a Patlite signal tower to ensure wide area visual and audible alarm status recognition (templates for supported Patlite model included in viewLinc). You can use a signal tower to indicate threshold, device or system alarm severity to a widespread audience. Several configuration options are built into viewLinc and include:
  • Choose the type(s) of alarms you want to trigger signal tower alarming.
  • Select colors to reflect priority status.
  • Modify color formats to accommodate tower position (ceiling-, wall- or floor-mounted).
  • Choose a sound pattern or turn sound off.

To learn more about your light tower color scheme and sound options, refer to the documentation provided with the device.

10.4.1 Adding signal towers

🔒 **Manage Devices**

Connect a signal tower to your network to deliver visual and/or audible notification of an alarm state to a wide area.

▶ 1. Connect the signal tower to your network according to the manufacturer's directions.

2. In **Sites Manager** on the **Signal Towers** tab, select **Add**.

3. Complete the general configuration options:

    a. **Description**: Type a unique description of the signal tower.

    b. **Model**: Select the model number.

    c. **IP address**: Type the numerical IP address assigned to the tower.

    d. **Port number**: Choose a unique and available port number. The default port number for signal towers is 80.

4. In **Alarm Settings**, select the alarm types you want to trigger signal tower alarmings.

> Use a signal tower to indicate the most critical alarm types, such as threshold and communication alarms.

5. In **Light Settings**, select how to display visual alarms. Only the highest priority alarm condition will display at one time.

   • **All segments**: Use all available color bands to display highest priority alarm (for example, all bands will be red for a High priority alarm)
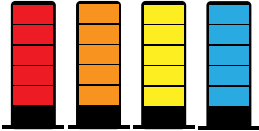
   • **Priority position**: Use two color bands to display a specific priority alarm, lowest priority at the bottom, highest priority at the top of the tower. If there is a High priority alarm, the top two bands display red; if there is only a Medium priority alarm, the two middle bands display orange; if there is only a Low priority alarm, the two bottom bands display yellow.
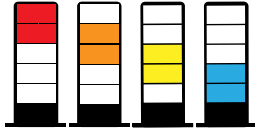
   • **Priority position - inverted**: It is important to consider the installed position of the signal tower - if it is hanging from the ceiling, the position of alarm colors may need to be top to bottom.

   > Priority position bands can help those who are color-blind identify alarm priority.

6. Configure the sound settings:

   • **Sound/When alarms are acknowledged**: Choose to enable tower sound, and whether to stop or continue tower sound signal after an alarm is acknowledged. By default, tower sound turns off only after all alarms are no longer present.
   • **Alarm priorities**:
     Select all of the alarm priorities that you want to initiate alarm sound on the signal tower. High alarms will always trigger an alarm sound when the sound setting is enabled.
   • **Duration**: Choose the length of time you want the alarm sound to be active, either a continuous loop of the selected sound pattern, or only activate sound for 5 seconds. After 5 seconds the sound will stop, but if the alarm condition still exists during the next system scan, the sound repeats for another 5 seconds.
   • **Sound pattern**: Select a sound pattern. To test the sounds, visit www.patlite.com.

7. **Test** the connection and configuration settings. If the **Test** button remains disabled, check that the IP address and port settings are configured correctly.

> ℹ️ Warn your team before testing signal tower performance.

8. To save the new signal tower settings, click **Add**.

9. To connect the signal tower to specific Zones and/or Locations:

    a. On the Signal towers tab select a signal tower, then click the link icon, 🔗 .

    b. Select the Zones and/or Locations you want to display alarms on the signal tower.

10. Click OK to save the link settings. The linked Locations appear in the Locations column on the Signal Towers grid.

> ℹ️ If the signal tower is configured to indicate threshold alarms, make sure that the selected Zones and/or Locations have threshold alarm templates applied.

10.5 viewLinc access through a remote display or mobile device

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

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

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

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

10.5.1 Remote display requirements

Before setting up a remote display terminal, ensure the following:
- The display hardware meets viewLinc System Requirements.
- The display can connect to a wired keyboard, or has a touchscreen keypad.

- A remote display view is available to the logged in user.

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

More information

‣ Hardware requirements (page 24)
‣ Creating views for remote display (page 145)

10.5.2 Setting up a remote display

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

1. Set up a remote display view.

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. This ensures the browser launches automatically when a user logs in.

4. Disable Windows updates to prevent popups on the display screen.

5. Launch the terminal browser and set the default home page to your viewLinc address, followed by */display* (for example, *http://viewLinc.com/display*).

6. Set the remote terminal browser to work in full screen mode (press **F11**).

7. Log in to the viewLinc remote display application with the remote user account name and password. The user's default view opens automatically. These settings are remembered until a user logs out from the display application.

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

More information

‣ Creating views for remote display (page 145)

10.5.3 Using viewLinc Mobile

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

▶ 1. Open a supported Internet browser on your mobile device.

2. Type your viewLinc IP address followed by */mobile*. For example, *##.###.##.##/mobile*.
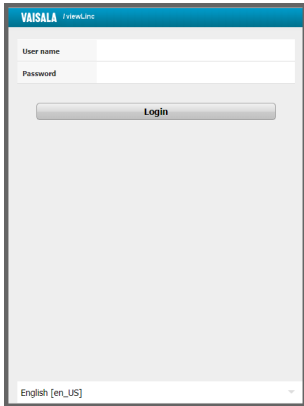
3. Select the language you want to display. When changing to a language other than English, the page automatically refreshes to display the new language.

4. Log in with your viewLinc user name and password.

5. Tap **Login**.

More information

‣ Viewing data with viewLinc Mobile (page 200)

10.6 Setting up voice or SMS web services

viewLinc Enterprise Server supports voice and/or SMS text messaging via the web service provider, Twilio. With a Twilio account and a network port set up to access the Internet, viewLinc can send default or custom voice calls and/or SMS message notifications to your users, in all supported languages. Your viewLinc users can also acknowledge voice calls and SMS messages received from the web service using their mobile device and PIN.

> ℹ SMS message delivery is also possible using a modem.

• All voice call/SMS notifications are sent from a single phone number assigned by Twilio.
• Notifications are sent to the phone numbers assigned to your viewLinc users.

- Voice calls or SMS notifications sent to international numbers require additional permissions (see International Voice Dialing Geographic Permissions in Twilio documentation).

> Contact a Twilio account representative to make sure the voice and/or web services you require are available in your region.

When and how voice or SMS messages are delivered is determined by the alarm notification template assigned to a Location, a device, or to system alarms.

Voice calling trees

Multiple users can be called sequentially on a call tree; the order is specified by the corresponding alarm notification template which includes a voice call tree. When a voice notification is triggered by an alarm event, a call initiates and delivers the message to each designated recipient, first to last.

Setup steps

1. Purchase a Vaisala Voice Web Service or Vaisala SMS Web Service feature license (contact www.vaisala.com/contact-us).
2. Add the feature license to viewLinc Enterprise Server.
3. Sign up for a free trial Twilio account (www.twilio.com) to obtain a phone number and configuration information required to enable the voice calling and/or SMS web service feature in viewLinc. Once you determine your messaging volume needs, simply convert your trial account to a paid subscription.
4. Configure voice and/or SMS web services in viewLinc. Contact your IT administrator to ensure your network has an Internet-accessible port available (incoming TCP port 12500).
5. Create an alarm notification template which includes one or more voice call or SMS web service notification recipients.

More information

‣ Entering a new license key (page 117)
‣ Creating alarm notification templates (page 103)

10.7 Vaisala OPC UA Server

Vaisala OPC UA Server is built on an industry standard tool preconfigured to bring real-time and historical data from viewLinc into your existing systems, such as data historians, manufacturing execution, reporting, or building automation systems. By installing the stand-alone Vaisala OPC UA Server software, you can leverage your viewLinc data without extensive validation or complex programming.

Before installing Vaisala OPC UA Server software, the following setup steps must be completed in viewLinc:

Table 19   Connecting to Vaisala OPC UA Server

Setup Requirements	
☐	Vaisala OPC UA Server license key added to viewLinc. The same license key is entered during Vaisala OPC UA Server installation.
☐	A dedicated group and user configured in viewLinc. The dedicated group must have View permission to access the required Zone and/or Location data. The user account is used only to transfer data to the Vaisala OPC UA Server so that activity between viewLinc and the Vaisala OPC UA Server can be traced clearly in the Events log.
☐	viewLinc hostname identified, or IP address (a recognized certificate hostname is required if your network requires certificate authentication).
☐	viewLinc port number identified (default is 443).
☐	Vaisala OPC UA server port number identified (default is 55000).

1)   *Your security policy determines whether you are required to use strict or relaxed certificate authentication. If you choose strict security (recommended), you must install trusted security certificate and key files. If you prefer to use relaxed security, you can have the wizard generate VOPC UA Server-signed certificate and key files during installation.*

If you would like to purchase a license for Vaisala OPC UA Server, please contact your local sales representative:

www.vaisala.com/contact

More information

- ‣ Entering a new license key (page 117)
- ‣ Groups and users (page 75)
- ‣ Security requirements (page 23)

11. Daily tasks

11.1 Daily tasks

To help you become more familiar with the viewLinc workspace, it is recommended that you watch the tour, Using viewLinc, which is available under the ❓ (Help) menu.

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

11.2 Desktop orientation

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

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

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

> The **Zones and Locations** tree can be expanded or collapsed to reduce visual clutter, and can be further customized into views. Views can be set up to contain only the Locations that are most important to you.

More information

‣ Your views (page 143)

11.2.1 Sites window

All viewLinc users have access to the **Sites** window, which is used to observe current conditions and acknowledge alarms. The Locations you see listed in the **Zones and Locations** tree are defined by your group permissions. Permissions are assigned by your viewLinc administrator (see Permissions (page 134)).

> If there is a Location that is not currently visible in the **Zones and Locations** tree, contact your viewLinc administrator to adjust your permissions.

The **Sites** window contains various options and control buttons to help you display data in a way that is meaningful to you.

11.2.2 Icons

Table 20   Home Screen Icons

Icon	Description
💓	Amount of time that has passed since receiving the last data transmission from any device. When view is regularly updating, icon is green. When view has not been able to update, icon is red.
🔔	Number of alarms currently active, on Locations user is permitted to view. Click to open the **Alarms** window and acknowledge alarms.
🔊	An audible alarm is active. Click to cancel the sound and open the **Alarms** window.
❓	Open online Help or watch a tour.

Icon	Description
👤	Log out or open the **Users and Groups** window to edit your personal details. Requires **Manage System** right.
UTC+7	Time zones in viewLinc are expressed in terms of an offset from UTC (Coordinated Universal Time). UTC is the time standard used to synchronize the clocks of computers over the internet.

Table 21   Window Icons

Icon	Description
🔄	Refresh - View the most current system modifications or data updates.
🗂	Find in Tree - Highlight the selected Location in the Zones and Locations navigation tree.
📝	Quick Reports - Generate an Alarm-, Location History-, or System report for the selected Zone or Location.
🌡	Measurement type: Temperature
💧	Measurement type: Humidity
◇	Measurement type: Other
10 01	Measurement type: Boolean
🌡 *Lab A*	An unlinked channel or Location displays in gray, italicized text.
~~🌡Lab A~~	A deactivated Location displays in red, strike-out text.
📱	Vaisala device icon: RFL100-series data logger
▦	Vaisala device icon: DL data logger
🔲	Vaisala device icon: HMT140-series data logger
🖳	Vaisala or third-party Modbus device
⬓	Host icon: Access point
🖥	Host icon: Device Host server
🗄	viewLinc Enterprise Server (ES)
📴	Alarming paused
👥	Group
🎚	Calibration alarm
-✕-	Communication alarm

Icon	Description
⚙	Configuration alarm
⚠	Validation alarm

11.2.3 Searching for Zones and Locations

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

Full search

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

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

Search tips

- To search for a Location containing the word 'South', type **South** (viewLinc searches for Zones or Locations containing the word South, or combination phrases, such as South-West or Fridge: South Corner).
- To search for a Zone starting with the term, 'Room', type: **Room***.
- To search for a Zone starting with the term, 'Room', and all Locations starting with the term, 'Temp', type: **Room*/Temp***.
- To search for a term with a single character difference, such as 'temperature' or 'température', type: **temp?rature**.

11.2.4 Working with columns

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

11.2.4.1 Sorting column content

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

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

  2. On the menu that appears, select **Sort Ascending** or **Sort Descending** (you can also click on any column header to sort all the rows alphabetically in ascending or descending order).

11.2.4.2 Changing column order

Use your mouse to move columns further left or right.

▶ 1. Open a window with movable columns: **Overview**, **Sites**, **Alarms**, **Views Manager**, **Events**, **Users** and **Groups**, and **Sites Manager**.

  2. Select a column header name and click and hold to drag it right or left.

3. Release the column and drop it when the green drop indicator arrows appear:
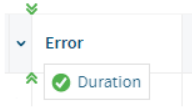
> ℹ️ If the drop indicator does not appear, the column is in a fixed position and cannot be moved.

11.2.4.3 Showing or hiding columns

▶ 1. Hover your mouse over a column heading, then click the down arrow, ∨.
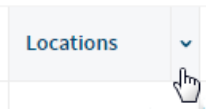
2. On the menu that appears, select **Columns**, then select columns to display or deselect columns to hide.
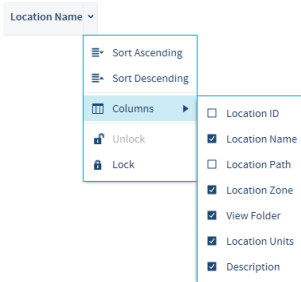
3. Click outside the column list, or press **ESC** to close the list.

11.3 Monitoring conditions

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

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

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

> All active alarm types, including system alarms, display in the **Alarms** window. Alarms display only for the Locations or Zones you have permission to view.

More information

- Types of alarms (page 84)

11.3.1 Identifying active alarms

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

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

Active and inactive Alarms

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

Alarm Acknowledgement

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

11.3.2 Using the Status tab

To review the severity levels of active threshold and device alarms, select the **Status** tab in the **Sites** or **Overview**

Table 22   Status tab columns

Column	Definition
State	Current threshold condition (this column cannot be removed)
Type	Value being measured (this column cannot be removed)
Threshold Status	Summary of all active threshold alarms
Device Status	Connection status with viewLinc
Value	Current measured value
Timestamp	Time of most recent recorded value
Threshold Summary	Description of threshold measurement criteria
Location ID	System-generated ID for reference purposes.
Location Path	Folder
Location Description	User-defined description
Device ID	System-generated ID for reference purposes.
Device Serial Number	Device-specific serial number
Device Address	Device Host location
Device Description	User-defined description
Sample Interval	Device-configured sample timing
Battery Level	Estimated remaining battery life
Signal Quality	Wireless reception quality
Channel ID	Device-configured channel ID
Channel Number	Device-configured channel number recording data for this Location
Channel Description	User-defined channel description

11.3.3 Threshold alarms

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

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

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

11.3.4 Responding to alarms

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

> 💡 If you are set up to receive audible alarms on your desktop, click the active alarm sound icon to turn off, 🔊.

You may receive an alarm notification in a variety of ways, depending on how the system administrator has configured your system:

- **Email/SMS/Voice**: Receive notifications when an alarm condition is present, once or repeatedly, according to the alarm notification template assigned to a Location or a device.
- **Command**: An application may activate an external device or emit an audible alarm. For example, when an alarm condition occurs a command could activate a light or buzzer, or a have a computer page or phone a particular number.
- **Signal tower**: Your system may include a signal tower to indicate an alarm condition across a wide area with light or sound.

More information

11.3.5 Viewing conditions on dashboards

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

Table 23   Dashboard alarm status

No alarm condition detected	Green	💧 49.1 %RH
High priority alarm	Red icon, or	💧 43.5 %RH
	with red background	🌡 21.7 °C
Medium priority Alarm	Orange	🌡 21.5 °C

| Low priority alarm | Yellow | 🌡 **21.7 °C** |
| Information priority alarm | Blue | 🌡 **22.0 °C** |

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

More information

‣ Changing dashboard display settings (page 71)

11.3.6 Viewing dashboard location trends

▶ 1. In the **Sites** window or the **Overview** window, select a Zone or Location using a dashboard image.

2. On the **Dashboard** tab, select a current data reading.

3. Select the 〰 **View Trend** toolbar button (or right-click on the data reading and select **View Trend**). In the open Trend window, you can modify the trend start and end times, and the graph contents.

11.3.7 Finding linked Locations

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

▶ 1. In **Sites** select a Zone or Location which is using a dashboard image (or in **Views Manager** on the **Views** tree, select a view).

2. On the **Dashboard** tab, select a current data reading.

3. Select the ⊨ **Find in Tree** toolbar button (or right-click on the dashboard data reading). A yellow highlight bar appears temporarily in the **Zones and Locations** tree (or **Views** tree) to indicate the corresponding Location.

11.3.8 Printing current alarm data

In the **Alarms**, **Sites** or **Overview** window, you can print current alarm data directly to your printer.

▶ 1. To print:

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

11.3.9 Exporting current alarm data

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

▶ 1. To export active data in the **Alarms** window, select 📊 **Export to Excel**.

A list of all active alarms export to a `.tsv` format file in a spreadsheet program (default spreadsheet software is set on user PC).

2. To export active data in the **Sites** window:

   a. On the **Zones and Locations** tree, select one or more Locations or Zones with currently active alarm conditions.

   b. On the **Location Alarms** tab select 📊 **Export to Excel**. A list of all active alarms export to a `.tsv` format file in a spreadsheet program.

3. To export active data in the **Overview** window:

   a. On the **Views** tree, select one or more views containing Locations with currently active alarm conditions.

   b. On the **Location Alarms** tab select 📊 **Export to Excel**. A list of all active alarms export to a `.tsv` format file in a spreadsheet program.

4. The file download (`.tsv`) appears in the status bar at the bottom of the display window. Double-click the file icon to open the `activealarms.tsv` file in the spreadsheet program of your choice.

5. At the prompt, select **Save** (the file is saved to your default downloads folder) or **Open**.

   If Windows does not recognize the file format, select Excel from your Programs folder to view the file and make changes.

More information

‣ Creating alarm reports (page 195)

11.4 Receiving alarm notifications

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

✉ or 🗩	Receive an email or SMS notification (SMS from web service provider or modem)
🔔	See a visual indicator in viewLinc
🔊	Hear an audible area alarm (browser or signal tower)
📳	See a visual area alarm (signal tower)
📞	Receive a voice call

You can respond to any alarm by acknowledging the alarm in viewLinc (Overview, Sites, or Alarms window). If your system is set up to accept acknowledgments remotely, you can use a mobile device to reply to an email, SMS or voice notification using a recognized phone number and PIN.

11.4.1 Acknowledging alarms

An acknowledgement indicates to the viewLinc system and others that users from specified groups have recognized the alarm condition. The system records the details provided during acknowledgement about the steps taken to correct the alarm condition, as well as any comments, as an event in the **Events** window.

If you work remotely, you can acknowledge alarms from your mobile device.

> ℹ Only viewLinc users with Acknowledge Alarms permission (or higher) for the Locations where an alarm is occurring can acknowledge alarms.

More information

‣ Acknowledging an alarm with viewLinc Mobile (page 203)

11.4.1.1 Acknowledging alarm notifications

To allow users to acknowledge alarm notifications received by email, SMS, or voice call, your viewLinc system must allow remote acknowledgement and users must have an assigned phone number and PIN.

▶   1. Open or answer the alarm notification.

  • Email notifications are sent from the viewLinc server administrator account (for
    example, viewLinc.boulder@companyemail.com).
  • SMS notifications are sent from an SMS modem number or SMS web service provider
    number.
  • Voice call notifications are sent from the designated web service provider number.

  2. To acknowledge an email alarm notification, send a reply which includes the default
     subject line (with ticket number), and type your PIN in the body of the message.

To: viewLincadmin@mycompany.com
Subject: RE: [Ticket 1234] viewLinc - Threshold Alarm on Location 'East Lab', Zone 'Boston'

4545

----Original Message----
From: viewLincadmin@mycompany.com
Sent: Feburary 01-17 2:56 pm
Subject: [Ticket 1234] viewLinc - Threshold Alarm on Location 'East Lab', Zone 'Boston'

There has been a threshold alarm on 2017-02-01 14:55:00 on Location 'East Lab', Zone 'Boston'.

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

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

[1234] Threshold Alarm
East Lab Zone Boston
                                2:56PM

          3:08 PM   1234 4545
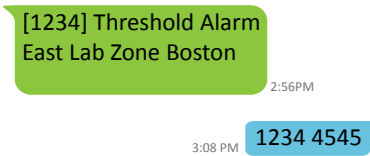
> ℹ   Only SMS replies sent from your recognized phone number and PIN will
>   acknowledge an alarm.

4. To acknowledge a voice call notification, follow the prompts:

- Press 1 to repeat the message.
- Press 2 to acknowledge the alarm and enter your PIN (this option is available if voice acknowledgement is enabled in System Preferences).

> **i** Once a voice call alarm notification is acknowledged, call tree notifications stop.

- Press 3 to confirm receipt of an alarm and enter your PIN (this option is available if voice acknowledgment is not enabled in **System Preferences**, or the alarm was already acknowledged using a different method, or if the alarm condition is no longer present).

> **i** Alarm acknowledgement in viewLinc does not prevent voice notifications from being sent.

> **💡** If you enter an incorrect PIN, or enter your PIN using an unrecognized phone number, you must log into viewLinc to acknowledge the alarm.

11.4.1.2 Acknowledging alarms within the viewLinc UI (Sites or Overview windows)

▶ 1. In the **Sites** or **Overview** window select the **Location Alarms** tab.

2. Review the list of all active alarms (**Status** column).

3. Use the **Acknowledgement** column to identify alarms that require acknowledgement. To acknowledge multiple alarms, press the **CTRL** or **SHIFT** keys while you select multiple alarms.

4. Select **Acknowledge** (or right-click and select Acknowledge).

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

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

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

11.4.1.3 Acknowledging alarms within the viewLinc UI (Alarms window)

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

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

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

11.4.1.4 Acknowledging system alarms

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

> ℹ️ You must be a member of the viewLinc **Administrators** group to use the acknowledge all system alarms function.

1. In the **Alarms** window on the alarms grid, right-click on a system alarm and select **Acknowledge**.

2. In the **Acknowledge Alarms** window indicate any action taken, select a predefined comment, if available, or type any additional comments about why you are acknowledging an inactive alarm.

3. Select **Acknowledge**.

11.4.1.5 Acknowledging all system alarms

1. In the **Alarms** window select **Acknowledge > Acknowledge All System Alarms**. Multiple Location selection is not required.

2. In the **Acknowledge Alarms** window indicate any action taken, select a predefined comment, if available, or type any additional comments about why you are acknowledging inactive alarms.

3. Select **Acknowledge**.

11.4.2 Acknowledging inactive alarms

Some companies' standard operating procedures may require that users acknowledge inactive alarms. Inactive alarms indicate that an alarm was triggered, but the alarm condition is no longer present.

To acknowledge inactive threshold or device alarms, you can use the **Alarms**, **Sites**, or **Overview** windows.

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

11.4.2.1 Acknowledging an inactive alarm in the Alarms window

1. In the **Alarms** window on the alarms grid, right-click on an inactive alarm and select **Acknowledge**.

2. In the **Acknowledge Alarms** window, indicate any action taken, select a predefined comment, if available, or enter any additional comments about why you are acknowledging an inactive alarm.

3. Select **Acknowledge**.

11.4.2.2 Acknowledging all inactive alarms in the Alarms window

1. In the **Alarms** window select **Acknowledge > Acknowledge All Inactive Alarms**. Multiple Location selection is not required.

2. In the **Acknowledge Alarms** window indicate any action taken, select a predefined comment, if available, or type any additional comments about why you are acknowledging inactive alarms.

3. Select **Acknowledge**.

11.4.2.3 Acknowledging an inactive alarm in the Sites window

1. In the **Sites** window on the **Zones and Locations** tree, select a Zone.

2. On the **Location Alarms** tab in the alarms grid, right-click on an inactive alarm and select **Acknowledge**.

3. In the **Acknowledge Alarms** window, indicate any action taken, select a predefined comment, if available, or type any additional comments about why you are acknowledging an inactive alarm.

4. Select **Acknowledge**.

11.4.2.4 Acknowledging an inactive alarm in the Overview window

1. In the **Overview** window on the **Views** tree, select a view.

2. On the **Location Alarms** tab in the alarms grid, right-click on an inactive alarm and select **Acknowledge**.

3. In the **Acknowledge Alarms** window, indicate any action taken, select a predefined comment, if available, or type any additional comments about why you are acknowledging an inactive alarm.

4. Select **Acknowledge**.

11.4.3 Responding to audible alarms

If your system generates audible alarms, they are only received by users logged in to viewLinc with the audible alarm preference enabled in their user profile. The user's PC must have volume turned on.

When an audible alarm is turned off, it is not recognized in viewLinc as an acknowledgement of the alarm. Audible alarm activation and cancellation are not tracked in the events log.

1. To cancel an active audible alarm, select the red audible alarm icon at the top of the viewLinc screen, ◀)).

2. To cancel an active audible alarm and acknowledge the alarm:

    a. Select the red audible alarm icon at the top of the viewLinc screen, ◀)). The icon changes to an alarm icon, 🔔.

    b. Select the alarm icon to open the **Alarms** window.

    c. Locate the alarm in the alarms table and then select **Acknowledge > Acknowledge Alarm**.

3. Complete the **Acknowledge Alarms** window.

More information

‣

11.5 Pausing alarms

To avoid receiving unnecessary threshold or device alarm notifications when moving devices, or if a known situation will result in conditions exceeding set thresholds, you can pause threshold alarming on one or more Locations, or device alarming on a single device or all devices connected to a host. Data collection continues during a pause period at all linked Locations.

The key difference between a paused alarm and a disabled alarm is that disabled threshold or device alarms remain disabled until a user manually re-enables them. Paused alarms reactivate automatically after 24 hours, if not resumed manually before that time.

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

11.5.1 Pausing threshold alarming

Pause threshold alarming to avoid triggering unnecessary threshold alarms. For example, if you are moving monitored inventory out of one facility and moving it to another, or are bringing in additional inventory and the activity will impact device readings.

When you pause threshold alarming, viewLinc continues to monitor your Location, but ignores all threshold levels. Data continues to be logged on your devices, and device alarming is still active.

You can pause threshold alarms on one or more Locations in the **Sites** window, or pause all threshold alarms for Locations assigned to a view in the **Overview** window. If you work remotely, alarms can be paused from a mobile device.

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

More information

- Pausing or resuming alarming with viewLinc Mobile (page 202)

11.5.1.1 Pausing threshold alarming on a Location

▶ 1. In **Sites** on the **Zones and Locations** tree select one or more Locations or Zones (**CTRL** +click).

   2. Select **Options > Pause Threshold Alarms** (or right-click to select **Pause Threshold Alarms**).

3. In the **Pause Threshold Alarms** window, specify:

      Duration
          Select the length of time you want alarming paused (1 ... 24 hours).

      Add comments
          If required, add a reason for pausing threshold alarms using a predefined comment (if available), or type your own notes in the text box.

4. Select **OK**.

     The active alarms list on the **Location Alarms** tab refreshes automatically.

11.5.1.2 Pausing threshold alarming in a view

1. In the **Overview** window on the **Views** tree, select one or more views (**CTRL**+click).

2. Select **Options > Pause Threshold Alarms** (or right-click to select **Pause Threshold Alarms**).

3. In the **Pause Threshold Alarms** window, specify:

      Duration
          Select the length of time you want alarming paused (1 ... 24 hours).

      Add comments
          If required, add a reason for pausing threshold alarms using a predefined comment (if available), or type your own notes in the text box.

4. Select **OK**.

     The active alarms list on the **Location Alarms** tab refreshes automatically.

11.5.2 Pausing device or host alarming

Pause device or host alarming to avoid unnecessary alarms (for example, if you are renovating a controlled space and need to shut down power temporarily). When you pause alarming, viewLinc continues to monitor your Location(s), but ignores all device and host communication interruptions.

Pausing device or host alarms does not interrupt data collection for any linked Locations. You can pause alarms on one or more Locations in the **Sites** window, or pause all Locations assigned to a view in the **Overview** window.

If you work remotely, alarms can be paused from a mobile device.

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

More information

‣ Pausing or resuming alarming with viewLinc Mobile (page 202)

11.5.2.1 Pausing device alarming on a single location

▶ 1. In the **Sites** window on the **Zones and Locations** tree, select a Location.

2. Select **Options > Pause Device Alarms** (or right-click to select **Pause Device Alarms**).

3. In the **Pause Device Alarms** window, ensure you have selected the correct data logger channel, then select **Yes** to continue.

   Duration
   Select the length of time you want alarming paused (1 … 24 hours).

   Add comments
   If required, add a reason for pausing threshold alarms using a predefined comment (if available), or type your own notes in the text box.

4. Select **OK**.

11.5.2.2 Pausing Device Alarming on Multiple Locations

▶ 1. In the **Sites** window on the **Zones and Locations** tree, select multiple Locations or Zones (**CTRL**+click), then select **Options > Pause Device Alarms** (or right-click to select **Pause Device Alarms**).

2. In the **Pause Device Alarms** window, ensure you have selected the correct data logger channel, then select **Yes** to continue.

   Duration
   Select the length of time you want alarming paused (1 … 24 hours).

   Add comments
   If required, add a reason for pausing threshold alarms using a predefined comment (if available), or type your own notes in the text box.

3. Select **OK**.

11.5.2.3 Pausing Device Alarming in a View

▶ 1. In the **Overview** window on the **Views** tree, select one or more views (**CTRL**+click).

2. Select **Options > Pause Device Alarms** (or right-click to select **Pause Device Alarms**).

3. In the **Pause Device Alarms** window, select **Yes** to continue.

   Duration
   Select the length of time you want alarming paused (1 … 24 hours).

   Add comments
   If required, add a reason for pausing threshold alarms using a predefined comment (if available), or type your own notes in the text box.

4. Select **OK**.

11.5.2.4 Pausing Host Alarming

▶ 1. In the **Sites** window on the **Zones and Locations** tree, use your mouse to select a Location then select **Options > Pause Host Alarms** (or right-click to select **Pause Host Alarms**).

2. In the **Pause Host Alarms** window, select **Yes** to continue.

> **Duration**
>> Select the length of time you want alarming paused (1 ... 24 hours).
>
> **Add comments**
>> If required, add a reason for pausing threshold alarms using a predefined comment (if available), or type your own notes in the text box.

3. Select **OK**.

11.5.3 Resuming threshold, device, or host alarming

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

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

1. In the **Sites** window on the **Zones and Locations** tree, select the Location or Zone which currently has alarming paused. Or, in the **Overview** window on the **Views** tree, select a view which currently has alarming paused.

2. Select **Options > Resume Threshold Alarms**, **Resume Device Alarms**, or **Resume Host Alarms** (or right-click to select **Resume Threshold Alarms**, **Resume Device Alarms**, or **Resume Host Alarms**).

11.6 Tracking events

Use the **Events** window to analyze events and determine when and where particular problems occurred, or to diagnose a situation that requires troubleshooting. All viewLinc system activity is treated as an event, and all events are tracked in the events log. Data tracked as an event is different from monitored data logged in a device. Here are some key differences:

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

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

11.6.1 Viewing events

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

To ensure no tampering has been recorded, check that the Event Log Status in the top right corner of the **Events** window displays status as valid.

1. Open the **Events** window.

2. To view events during a specific period, select **Edit Duration**.

3. Specify the time frame.

Edit Duration					
○ Show events for	1 day	ending at	2017-04-28	11:00	
○ Show events from	2017-04-27	10:59	to	2017-04-28	11:00
	Save	Cancel			

Show events for/ending at
Choose a time frame with an end date.

Show events from/to
Type a specific date and time, or use the calendar buttons to make your selection.

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

5. Select from the available filters.

Category
Select one or more types of events to include in the export.

Locations
Select the Zones and/or Locations to include.

Groups and **Users**
Show events recorded by selected groups or users.

6. Select **Apply Filters**. To reset filters, select **Clear**.

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

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

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

11.6.2 Adding comments to events

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

▶ 1. In the **Events** window, select an event, then select **Add Comment**.

2. In the **Add Comment** window, select from the list of predefined comments (if available), or type your own comment.

3. Select **Save**.

11.6.3 Viewing comments to events

▶ 1. In the **Events** window, select a row containing an event (a comment icon ⬭ appears in the **Comments** column).

2. Double-click the event row.

3. In the **Event Details** window, comments appear on the last line of the grid.

Comments also appear in the Event Log Report.

11.6.4 Adding custom events

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

▶ 1. In the **Events** window, select **Add Custom Event**.

2. Fill in the custom event message and details, then select **Save**.

   Event message
   Type a short description that will display in the Events window Message column.

   Details
   Type a full description of the custom event (required). This information is included when printing the Event Log report.

3. Save the new event. It appears at the top of the events grid.

11.6.5 Printing 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.

▶ 1. In the **Events** window, specify parameters for the report:

   a. To choose a preset or custom timeframe select **Edit Duration**:

   Show events for/ending at
   Choose a timeframe with end date.

   Show events from/to
   Set a specific date and time period, or use the calendar buttons to make your selection.

   b. To refine the report contents, select **Show Advanced Filters**:

   Category
   Check the types of events to include in the report.

   Locations
   Show events occurring at one or more selected Zones and/or Locations.

   Groups/Users
   Show events recorded by selected groups or users.

2. Select **Apply Filters**. To reset filters, select **Clear**.

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

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

11.6.6 Exporting event logs

You can also export the record details to a spreadsheet (using *.tsv* format), for custom reporting.

▶   1. In the **Events** window, specify parameters for the report:

   a. To choose a preset or custom timeframe select **Edit Duration**:

   Show events for/ending at
   Choose a timeframe with end date.

   Show events from/to
   Set a specific date and time period, or use the calendar buttons to make your
   selection.

   b. To refine the report contents, select **Show Advanced Filters**:

   Category
   Check the types of events to include in the report.

   Locations
   Show events occurring at one or more selected Zones and/or Locations.

   Groups/Users
   Show events recorded by selected groups or users.

2. Select **Apply Filters**. To reset filters, select **Clear**.

3. Select **Export**.

4. To open the file, specify the spreadsheet program to use for `.tsv` files. Exported `.tsv`
   files open in read-only mode.

11.7 Creating trends

To better understand condition fluctuations at your Locations, create a trend. Trends display
current or historical data readings for one or more Locations in a graphical format.
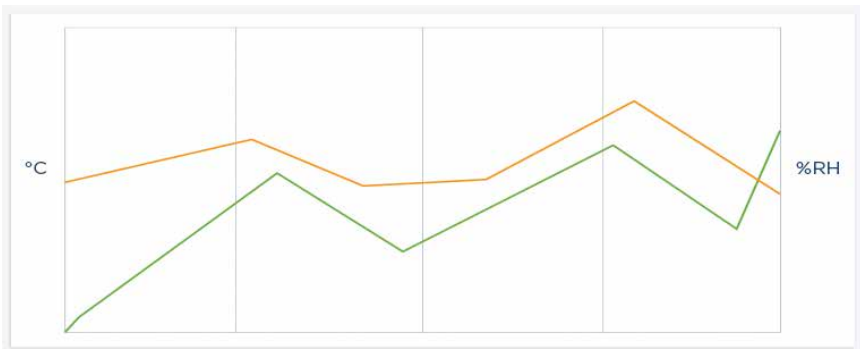
Table 25   Key Elements in a trend graph

Item	Description
Graph area	A graphical representation of Location data history.
Left and right Y-axis measurement scales	Shows the range of data displayed in the graph. You can modify the scale minimum and maximum values.
X-axis time scale (bottom)	Shows the reporting time frame. Use the forward and back arrows below the graph to adjust the reporting timeframe.
Location lines	Indicate path of historical measurement readings based on a specific date or time frame. Move your mouse and hover over a specific point to show the specific X- and Y-axis values.
Threshold lines	Color-coded line (based on threshold setting) to show historical threshold values. Move your mouse and hover over a specific point to show the specific X- and Y-axis values.
Locations / Group Statistics	View Location details in separate rows, or group statistics for all Locations.

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

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

More information

‣ Trend navigation (page 179)

11.7.1 Building trends

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

> You can build trends in the **Sites** or **Views Manager** windows.

▶ 1. In the **Sites Manager** window, navigate the **Zones and Locations** tree and select a Location you want added to the trend, or in **Views Manager** on the **Views** tree, select a view that contains the Location(s) you want to view as a trend.

2. Select the **Trend** tab.

3. Use your mouse to drag the selected Location or view to the **Trend** pane. You can continue to build upon and modify your trend at any time by simply dragging more Locations onto the graph (up to 16 Locations, up to 4 measurement units).

4. To modify the trend start date, select **Edit Trend**:

   Show trend for [time] ending at [date/time]
   Trends only display data logged up to the current time. You can select a set trend time period up to 1 month prior to the current date/time.

   Show trend from [date/time] to [date/time]
   If you want to see more historical data, select a specific time period to show (you cannot select a future date).

   Include real-time samples
   When checked, this option includes more frequent real-time samples alongside with the logged device data (based on the device sample rate).

   Show data markers
   When checked, this option adds small markers on the trend graph, indicating exactly when the readings took place.

   Vertical Axis Scale
   For each measurement value, you can set the minimum or maximum range you want included in the trend, or choose Auto to include all values.

> 💡 When you create a trend in **Sites** or **Views Manager** window, you can save the trend as a view and share it with team members, or save the graph as a Location history report for future reference.

More information

‣ Saving trends (page 182)

11.7.2 Trend functions

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

Refresh ⟳
Retrieve most recent data readings from server. If **Updates on** is enabled, the trend graph automatically retrieves data readings every minute.

Open trend in new window 📉 (**Overview** window)
Opens the trend in a new window.

Save As (**Sites** window)

Save the current trend graph as a single page Location history report or as a view. To save as a report requires **Manage Reports** right. To save as a view requires **Manage Views** right.

Edit Trend

Modify the trend start or end date, set the time duration, select line properties, and specify axis scale values.

Clear Trend (**Sites** window)

Clear all Location data lines from the trend graph, or clear lines and reset trend graph settings to default.

> Use the Locations grid below the trend graph to remove individual Location lines.
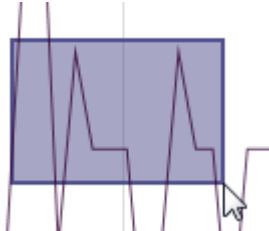
Updates on/off

Update real-time data readings, to a maximum trend duration of 7 days.

11.7.3 Trend navigation

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

Icon	Description
▶ ◀	Adjust the trend time frame by increments of 1/4. For example, if you are viewing 6 hours of data, the frame moves forward or back 1.5 hours; if you are viewing 1 month of data, the frame moves forward or back 1 week. The frame can only move forward up to the current time.
◀◀ ▶▶	Adjust the trend time frame by a full increment. For example, if you are viewing 6 hours of data, the frame moves forward or back 6 hours; if you are viewing 1 month of data, the frame moves forward or back 1 month. The frame can only move forward up to the current time.
▶⏸	Show the most recent data (up to current date/time).
▭⏸	Select this option to continuously update the trend with most current readings (this option has the same effect as pressing the ▶⏸ button).

Icon	Description
	To see close-up trend details, click and drag across a trend line. Drag right to zoom in/drag left to zoom out.

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

11.7.4 Modifying trends

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

> Trends modified in the **Sites** or **Views Manager** windows can be saved and shared with others.

More information

- Saving trends (page 182)

11.7.4.1 Showing or hiding selected Locations

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

11.7.4.2 Viewing trend max-min statistics

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

11.7.4.3 Changing trend duration/data/scale

▶ 1. Select **Edit Trend**.

2. To modify trend duration:

   a. Select a preset time range. Graph will display data for the selected time range, prior to the specified end time (default is 6 hours ending at current time).

   b. Select a time period based on specific calendar dates.

3. To modify line properties (by default these options are not selected):

   Include real-time samples
   Update Location trend lines to include both data collected in viewLinc based on viewLinc scan rate, and data reported by a device based on device sample rate.

   Show data markers
   Add points on Location trend lines to indicate when a data sample was recorded.

4. Define the vertical axis scale min/max graph range:

   For each measurement type included in a graph, you can set the minimum and/or maximum value automatically based on actual readings, or set specific min/max values to include in the graph (by default, the min/max settings are automatically generated).

   > If you reduce the sample rate, samples for data stored prior to upgrading to viewLinc Enterprise Server 5.2 will appear to have gaps in the trend line.

11.7.4.4 Clearing trends in the Sites window

▶ 1. To remove all Location graph lines select **Clear Trend > Delete all Lines**.

   Trend settings remain intact.

2. To remove all graph lines and return to the default trend settings, select **Clear Trend > Reset to Defaults**.

11.7.4.5 Refreshing trend data

▶   1. To refresh trend data:

Show most current data ▶▋ or **Updates on**
>   Select to refresh the graph with most recent data collected by the viewLinc
>   Enterprise Server.

Refresh ↻
>   Select to force retrieval of the most recent data collected by the viewLinc Enterprise
>   Server. If **Updates on** is enabled, the trend graph automatically retrieves real-time
>   data readings every minute.

Updates on/off
>   Select to update trend with real-time data readings, up to a maximum trend
>   duration of 7 days. If the trend duration is set for more than 7 days, the **Updates on**
>   setting is automatically disabled.

11.7.5 Saving trends

🔒 **Manage Views**, **Manage Reports**

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

11.7.5.1 Saving a trend as a view

▶   1. In the **Sites** window, create a trend.

2. Select **Save As > View**.

3. Type a name to identify the view, then select **Save**.

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

11.7.5.2 Saving a trend as a report

▶   1. In the **Sites** window or **Views Manager**, create a trend.

2. Select **Save As > Location History Report**.

3. Type a name to identify the report, then select **Save**.

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

11.8 Viewing Quick Trends

To quickly view Location data in a trend graph use the **View Trend** toolbar button, ▨, available in **Sites**, **Sites Manager** and **Overview** windows.

You can view multiple, individual Location trends at once by opening multiple trend view windows.

More information

‣ Alarm notifications (page 101)
‣ Creating trends (page 176)

11.8.1 Viewing Quick Trends in the Sites window

▶ 1. In the **Sites** window on the **Zones and Locations** tree, select a Zone.

2. On the **Status** tab select a Location, then select the **View Trend** toolbar button (or right-click to select **View Trend**).

3. In the open **Trend** window, you can modify the trend start and end times, and the graph contents.

11.8.2 Viewing Quick Trends in the Sites Manager window

▶ 1. In the **Sites Manager** window on the **Zones and Locations** tree, select a Zone.

2. On the **Location Properties** tab select a Location, then select the **View Trend** toolbar button (or right-click to select **View Trend**).

3. In the open **Trend** window you can modify the trend start and end times, and the graph contents.

11.8.3 Viewing Quick Trends in the Overview window

▶ 1. In the **Overview** window on the **Views** tree, select a view.

2. On the **Status** tab select one or more Locations, then select the **View Trend** toolbar button (or right-click to select **View Trend**).

3. In the open **Trend** window, you can modify the trend start and end times, and the graph contents.

11.9 Reporting

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

• Review data readings for specific monitored areas over selected time periods.

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

11.9.1 Types of reports

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

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

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

More information

11.9.2 Generating reports

All available reports are listed in the **Reports** window. The reports available are either default viewLinc reports, reports you have created, or reports that others have shared with you.

Reports are templates, waiting to be populated with generated data. Once a report is generated, open the **Downloads** tab to find out when the report is ready to print (a generated .pdf file) or export to a spreadsheet (a generated $.tsv$ file).

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

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

▶ 1. In **Reports** select a report, then select ⌐ **Generate**.

2. Choose a report option:

   PDF (.pdf)
   Choose this option to generate the report according to PDF settings specified in the Scheduled Generation parameters. This option is available for Alarm and Location History reports.

   Excel (.tsv)
   Generate the report in *.tsv* format.

   Email
   Generate and send report to predetermined list of users or groups, as a *.pdf* attachment (system reports are only *.xls* attachments). Once generated, the report is sent according to the report's scheduled generation parameters.

   > Automatically generated and emailed report content is generated according to the recipient's language preference.
   > - If no language preference is specified for the recipient, the content is generated in the language specified for the report (language can be specified for reports that are automatically generated and saved).
   > - If no language is specified for the recipient or the report, the content is generated in the system default language (**System Preferences**).

3. On the **Downloads** tab, the most recently generated report appears at the top of the list. Once report generation is complete, open or save the report by clicking the link in the **Progress** column.

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

More information

‣ Generating Quick Reports (page 186)
‣ Viewing report downloads (page 186)

11.9.3 Sharing Quick Reports

🔒 **Manage Reports**

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

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

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

▶ 1. In the **Reports** window, select a report, then select **Edit**.

2. In the **Available as quick report field**, select **Yes**.

3. Save the change.

11.9.4 Generating Quick Reports

A quick report is a report made available to others to generate easily from the **Sites** or **Overview** windows. The structure of the report adheres to the structure defined by the report owner, but the content of the report (data) is limited to the Zones and Locations the user is permitted to view.

If you have **Manage Reports** right, you can make a report available to others as a quick report.

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

▶ 1. In the **Sites** window or **Overview** window, select one or more Locations or Zones.

2. Select **Options > Quick Reports**, choose a report type (Alarm, Location History, or System), then select an available quick report.

3. To create a .pdf output of the report, select **Generate Report (*.pdf)**.

4. To create a report you can manipulate in a spreadsheet, select **Generate for Excel (*.tsv)**.

5. To send the report to another user, select **Generate and Email Report**:

    a. Choose the report format.

    b. Type the email address of the recipient, and any additional viewLinc users or groups to whom you want the report sent.

    c. Optional: Modify the **Subject** and **Body** fields for the email message.

    d. Select **Send**.

6. To find out when the report is ready to download and print, open **Reports > Downloads**.

More information

‣ Sharing Quick Reports (page 185)

11.9.5 Viewing report downloads

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

▶ 1. In the **Reports** window, select the **Downloads** tab.

2. To check the report status, locate your report in the list:

> **Generated By**
>> Identifies the person who initiated the report generation (username), or if it was automatically generated (System).
>
> **Generated As**
>> Indicates whether the report owner generated the report (report includes all source data), or, if another user generated it as a quick report (report only includes data for the Locations user has permission to view).
>
> **Generated**
>> When report content was generated, seen as the user's local time.
>
> **Available For**
>> Indicates remaining time the generated report will be available to download and print. Manually generated and scheduled reports remain available for 24 hours.

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

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

> If the report is taking too long to generate, you can click **Cancel** to remove the report from the queue. If a scheduled report is canceled, viewLinc notifies recipients via email.

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

11.9.6 Deactivating reports

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

▶   1. In the **Reports** window, select a report.

2. Select **Deactivate**.

11.9.7 Activating reports

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

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

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

11.9.8 Generating alarm reports

Default viewLinc alarm reports—Last 8 hours, Last day, Last week—can be generated by all users from the **Sites** or **Overview** windows. Additional custom alarm reports are available from these windows if they are set up as Quick Reports.

1. In the **Sites** window on the **Zones and Locations** tree, select a Zone or a Location. Hold the **CTRL** key to select multiple Zones/Locations.

2. Select **Options > Quick Reports > Alarm Reports**, then select the report type and the output format: .pdf (standard presentation format), .tsv (modifiable format with a spreadsheet program), or send the report as an email attachment (.pdf).

3. To generate and send the report to an email recipient:

   a. Type the email address of the recipient, and any additional viewLinc users or groups to whom you want the report sent.

   b. Optional: Modify the **Subject** and **Body** fields for the email message.

   c. Select **Send**.

4. To find out when the report is ready to download and print, or when it was sent, open **Reports > Downloads**.

More information

‣ Printing current alarm data (page 162)
‣ Exporting current alarm data (page 162)
‣ Creating custom reports (page 188)

11.10 Creating custom reports

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

You can also specify:

• A user or group authorized to modify the report
• The time zone to use when generating data
• The groups who can receive the report by email

- A schedule to generate the report automatically
- Availability as a quick report

You require **Manage Reports** right to create or modify reports.

11.10.1 Creating Location History reports

Manage Reports

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

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

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

2. Complete the **General** tab.

Name
> Type a unique name for the new report.

Report owner
> Your viewLinc username appears automatically as the report owner. If you have **Manage Reports** right, you can select a different or additional user as owner of this report.

Range type
> Specify the period of time you want the report to include. A fixed date sets duration according to specific dates, or choose a period in hours/days/weeks/months.

Duration of report
> Specify the time period you want included in the report. If you want to include only the last 8 hours of data, type **8** and then choose **hours** from the drop-down list.

Time zone
> Change this value if the reporting time zone is not the same as the server time zone.

PDF font
> If you want to generate a report that uses Chinese, Japanese, or Korean characters, select the language. Otherwise, leave as **No Asian Characters** to reduce the generated file size.

Available as quick report
> Allow users to generate this report from the **Sites** and **Overview** windows. Quick reports generate data for the user's selected Location(s) or view(s).

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

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

Generate and email
Generate and then send the report directly to specific viewLinc users and groups.

Generate and save
Generate and then save the report to a specific file location.
  Save To
  Specify an accessible network server or restricted file location where you want the report saved.

  Language
  Saved reports are automatically generated in the system default language unless a report language is specified.

Start generating
Set the data generation start date and time.

Generate report every
Set the start date and time you want the report generated.

Report format
Specify whether you want the report generated hourly, daily, weekly, or monthly.

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

Title page
> Include content overview.

Trend graph
> Generate a graphical display of the report data. You can choose to include separate graphs for each Location, compile all Location data on a single graph (the default option, limited to a maximum of 16 Locations), or choose to group measurement units together on the same graph (up to 4 measurement types per graph). If you choose to include a statistics summary, a statistics summary table is included in the report. Choose samples in the **Include in statistics tables** section.

Report summary table
> This option can be deselected independent of the statistics summary table.

Interval statistics table
> Select a timeframe measured in days/hours, or on a calendar month. If the **General** tab setting for the **Duration of report** is set on a weekly interval and you want to daily interval statistics, specify `1 day, 0 hours`. Choose **Show graph** to include an additional graphical representation of the statistics. Choose samples in the **Include in statistics tables** section.

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

Historical sample statistics tables

Include statistics calculated by Location (ordered according to measurement type). Choose samples in the section, Include in statistics tables.

Group statistics table

Generate one statistics table for all Locations with the same measurement type. For example, the maximum temperature of all the temperature recording Locations included in the report. Choose samples in the **Include in statistics tables** section.

Real-time samples and/or **Historical samples**

If you choose to include historical samples, select a set data period (every 5, 15, 30, or 60 minutes) and indicate whether the last sample reflects the closest reading to the period interval timestamp. This option is useful when reporting Locations have different sample rates.

Include in statistics tables

Select the historical sample data to include in all statistics tables.

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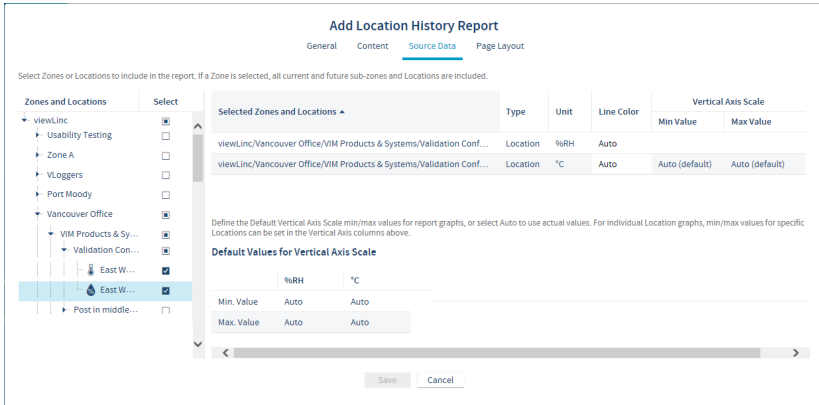
Zones and Locations

> To select all Locations in a Zone, select the checkbox corresponding to the Zone name. When a Zone is selected, all current and future Locations are automatically included in the report. To select or deselect a specific Location in a Zone, expand the Zone.

Line Color

> Specify a color to identify Locations (color not available for Zones). Auto chooses the next available color (see How does viewLinc select colors for reports?).

Vertical Axis Scale Min/Max Values

> If trend graphs will be generated (Content tab, Trend graph - One Location per graph) each Location graph can have specific min/max values, or accept the default values.

Default Values for Vertical Axis Scale

> Choose the minimum and maximum values to define the upper and lower limits for the graph measurement range.

6. Modify report output display options on the **Page Layout** tab:

Paper
Choose the report page size and orientation.

Page Header/Page Footer
For header or footer options, choose to display on all pages, on the first page only, on the last page only, or on the first and last page.

Left header, **Center header** or **Right header**
To define the content of your header or footer, type text in the **Left header**, **Center header** or **Right header** fields. You can also use the **Footer** field to include a Signature box or Comments box.

Image
To include an image instead of text in **Left header**, select **Image**, then choose a `.jpg` image file from the drop-down (for previously used images) or upload a new `.jpg` image file using **Upload new** button.

7. Save the new report.

More information

‣

11.10.2 Creating alarm reports

🔒 **Manage Reports**

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

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

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

2. Complete the **General** tab:

Name
Type a unique name for the new report.

Report owner
Your viewLinc username appears automatically as the report owner. If you have **Manage Reports** right, you can select a different or additional user as owner of this report.

Range type
Specify the period of time you want the report to include. A fixed date sets duration according to specific dates, or choose a period in hours/days/weeks/months.

Duration of report
Specify the time period you want included in the report. If you want to include only the last 8 hours of data, type **8** and then choose **hours** from the drop-down list.

Time zone
Change this value if reporting time zone is not the same as the server time zone.

PDF font
If you want to generate a report that uses Chinese, Japanese, or Korean characters, select the language. Otherwise, leave as **No Asian Characters** to reduce the generated file size.

Available as quick report
Allow users to generate this report from the **Sites** and **Overview** windows. Quick reports generate data for the user's selected Location(s) or view(s).

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

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

Generate and email
> Generate and then send the report directly to specific viewLinc users and groups.

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

Start generating
> Set the data generation start date and time.

Generate report every
> Set the start date and time you want the report generated.

Report format
> Specify whether you want the report generated hourly, daily, weekly, or monthly.

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

Include content
> Include a summary of all active, activated, deactivated and acknowledged alarms by Location.

Report detail level
> Choose to group all alarm details in shortened form or expand the length of the report to include all alarm details. Depending on the number of alarms, this can increase the size and time required to generate the report significantly.

Alarm content
> Choose to report on specific types of device alarms.

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

Zones and Locations
> To select all Locations in a Zone, select the checkbox corresponding to the Zone name. When a Zone is selected, all current and future Locations are automatically included in the report. To select or deselect a specific Location in a Zone, expand the Zone.

6. Modify report output display options on the **Page Layout** tab:

Paper
Choose the report page size and orientation.

Page Header/Page Footer
For header or footer options, choose to display on all pages, on the first page only, on the last page only, or on the first and last page.

Left header, **Center header** or **Right header**
To define the content of your header or footer, type text in the **Left header**, **Center header** or **Right header** fields. You can also use the Footer field to include a Signature box or Comments boxes.

Image
To include an image instead of text in **Left header**, select **Image**, then choose a .jpg image file from the drop-down (for previously used images) or upload a new .jpg image file using **Upload new** button.

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

7. Save the new report.

More information

‣ Generating reports (page 184)

11.10.3 Creating system reports

🔒 **Manage Reports**

⚙ System reports provide an overall snapshot of select system information.

1. In **Reports**, select **Add > System Report**.

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

2. Complete the **General** tab:

> **Name**
>> Type a unique name for the new report.
>
> **Report owner**
>> Your viewLinc username appears automatically as the report owner. If you have **Manage Reports** right, you can select a different or additional user as owner of this report.
>
> **Time zone**
>> Change this value if the reporting time zone is not the same as the server time zone.
>
> **PDF font**
>> If you want to generate a report that uses Chinese, Japanese, or Korean characters, select the language. Otherwise, leave as **No Asian Characters** to reduce the generated file size.
>
> **Available as quick report**
>> Allow users to generate this report from the **Sites** and **Overview** windows. Quick reports generate data for the user's selected Location(s) or view(s).

3. Complete the **Automatic Generation** section:

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

> **Generate and email**
>> Generate and then send the report directly to specific viewLinc users and groups.
>
> **Generate and save**
>> Generate and then save the report to a specific file location.
>>> **Save To**
>>>> Specify an accessible network server or restricted file location where you want the report saved.
>>>
>>> **Language**
>>>> Saved reports are automatically generated in the system default language unless a report language is specified.
>
> **Start generating**
>> Set the data generation start date and time.
>
> **Generate report every**
>> Set the start date and time you want the report generated.

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

> **Server**
>> Include viewLinc Enterprise Server configuration details.
>
> **System Preferences**
>> Include the currently selected viewLinc system preferences.
>
> **Alarm templates**
>> Include details for selected templates (active and deactivated).
>
> **Users and groups**
>> Include all users and/or groups, and their assigned permissions to Locations. The report shows the highest available permission for each Location, listed alphabetically by user or group.
>
> **Sites**
>> Include Location details about current threshold and device alarm templates, and permission levels granted to users/groups for each Location (active and deactivated).

> The report lists highest available permission for the user or group, listed alphabetically by Location.

> **Devices**
>> Include a list of all linked system hosts, data loggers and transmitters (active and deactivated).

5. Save the new report.

More information

11.11 Viewing data with viewLinc Mobile

Several viewLinc functions are accessible via mobile device. To log in, open a device browser and type the IP address/mobile (*##.###.##.##/mobile*). The initial screen that appears after you log in is the **Sites** window navigation tree. Tap the name of a Zone to reveal the Locations below it. Select a Location and then tap the **Options** button to view available options:

> **Refresh**
>> Update display to show most recently collected data.
>
> **Pop-up Trend**
>> Display selected Location data in trend graph.
>
> **Pause/Resume Threshold Alarming**
>> Pauses threshold alarming temporarily on all Locations in the selected Zone for 1 hour.

Ways to display mobile data

Sites view: Display trends, change trend graph settings, pause threshold alarming. When a Zone is selected, the view expands to display sub-zones and Locations.
- To go up a folder, tap the previous screen button (do not use your device Back button, it closes the active tab and ends the browsing session).

Table view: Displays detailed Location information for whichever Location was selected from the Sites view. Pause threshold, host or device alarming.
- To view Location information, select the Location, then double-tap to view details. Click ✕ to return to the previous screen.
- To go up a folder, tap the **Sites** button (do not use your device Back button, it closes the active tab and ends the browsing session).

Alarm view: Displays alarm information for whichever Location was selected from the Locations pane view (or all Location alarms, if none selected).
- To view alarm information, select the Location, then double-tap to view details. Click ✕ to view the previous screen.
- To go up a folder, tap the **Sites** button (do not use your device Back button, it closes the active tab and ends the browsing session).

Only Locations that have active alarms display on the mobile device. For example, if you are at the system level when you press the alarm grid, it displays all active alarms in the system, if any.

11.11.1 Opening a pop-up trend

Before you can view pop-up trends on a mobile device, ensure the device browser is not set to block pop-ups. Refer to your device-specific user guide for more information.

▶ 1. Tap the **Sites** button, then navigate to a specific Location.

2. Tap **Options > Pop-up Trend**. The pop-up trend window appears in a new browser tab.
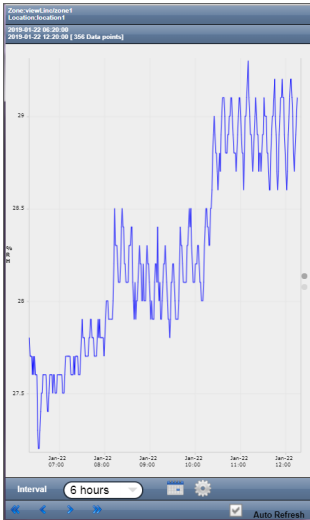
Interval

Trends display up to 1 month of data logged up to the current date.
-   Tap the calendar button to set the end date.
-   Tap the settings icon to include real-time samples or threshold lines on the graph.

Auto Refresh

Select this option to update the trend with real-time data readings. Only available for trends set to a maximum duration of 7 days.

Use the arrows to scroll the trend forward and back.

More information

‣ Trend navigation (page 179)

11.11.2 Pausing or resuming alarming with viewLinc Mobile

You can pause or resume alarms on a mobile device for the Locations you have permission to view on your desktop display.

1. Open   **Table** view.

2. Select the Location you want to pause or resume alarming, then select **Options**.

3. To pause alarming, tap **Pause Threshold Alarming**, **Pause Host Alarming**, or **Pause Device Alarming**.
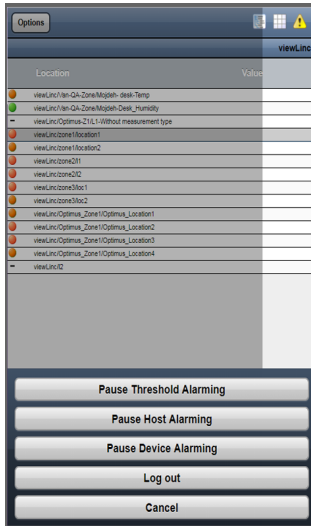
- Once alarming is paused, it remains paused for one (1) hour.
- To resume alarming within the hour, repeat these steps and select **Resume Threshold Alarming**, **Resume Host Alarming** or **Resume Device Alarming**.

More information

‣ Pausing alarms (page 169)

11.11.3 Acknowledging an alarm with viewLinc Mobile

If you are authorized to acknowledge alarms for the Locations you can view, you are authorized to acknowledge those alarms remotely.

▶ 1. Open ⚠ **Alarms** view.

2. Select the alarm you want to acknowledge.

3. Tap **Options > Acknowledge**. At the prompt, type the action taken, select a predefined comment (if required) and add extra comments (optional).

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

More information

‣ Acknowledging alarms (page 163)

11.11.4 Viewing data on a remote display

Several viewLinc functions are available on a remote display.

> **i** If the display terminal does not have touch-screen capability, a connected keyboard is required.

▶ 1. Open the Internet browser on the display terminal.

2. Type your viewLinc IP address followed by /display (for example, `##.###.##.##/display`).

3. Select the language you want to display. When changing to a language other than English, the page automatically refreshes to display the new language.

4. Log in as the remote display user. The content displayed is defined by the default view for the signed in user. These settings are remembered until the user logs out.

5. Select display options:

   • Open the **Dashboard** tab to display a graphic of monitored Locations in the view (dashboards for views are set up in **Views Manager**).
   • Open the **Trend** tab and select a view. The graph automatically loads data for all Locations in the view.
   • To view multiple Location trends on a single monitor, open multiple browser windows. In each browser window, log in to viewLinc as a different user, each with a different default view.

> If a browser reboots unexpectedly, viewLinc automatically relaunches the browser and logs in as the last user. The browser opens the user's default view with the last open tab displayed.

11.11.5 Changing a display terminal view

To change the view displayed on a display terminal, you can either select a different view assigned to the user currently logged in, or log in as a new user with different views available.

▶ 1. To select a different view:

   a. On the viewLinc remote display, expand the **Views** pane.

   b. In the **Views** tree, select another available view. The display updates automatically.

2. To log in as a new user:

   a. On the viewLinc remote display, select **User > Logout**, then select **Yes**.

   b. At the viewLinc log in prompt, type the new username and password.

   c. Expand the **Views** pane to select an available view.

12. Administrator tasks

12.1 Administrator Tasks

After the viewLinc system is set up and system monitoring is active, ongoing system maintenance tasks can be performed by members of the Administrators group, or users assigned the required rights.

12.2 Groups and users

As your team grows or responsibilities change, you can quickly adjust user profiles and group properties.

More information

12.2.1 Editing user or group details

🔒 **Manage System**

▶ 1. In the **Users and Groups** window, select the user or group you want to edit, then select **Edit** (or right-click and select **Edit**).

2. Edit settings as needed.
   • Only members of the **Administrators** group can modify a user's group assignments.
   • Only viewLinc passwords can be modified.

3. Select **Save**.

More information

12.2.2 Locking and unlocking user accounts

🔒 **Manage System**

▶ 1. In the **Users and Groups** window, select the user you want to edit, then select **Edit** (or right-click and select **Edit**).

2. Use the **Account locked** selection to either set the user as **Locked** or **Unlocked**.

3. Select **Save**.

   - When a user account is set as **Locked**, the user is immediately logged out of viewLinc with a security notification.
   - Administrators can unlock any user accounts, and also lock other administrator user accounts.

   > If an administrator is locked out due to too many failed login attempts, restarting the server will reset the login attempt count.

12.2.3 Deactivating users

Manage System

Users cannot be deleted from the viewLinc database; however, you can use the deactivate function to ensure users who have moved to other positions or left the company are no longer included in group alarm notifications and/or group report distribution (this is easier than removing groups from individual alarm templates or reports).

1. In the **Users and Groups** window select the **Users** tab.
2. Select the user you want to deactivate. If your user list is long, use the **Search** tool to locate a user, or click the top column header to sort names in alphabetical order.
3. Select ✖ **Deactivate**.
4. To confirm, select **Deactivate**.

   The user row is automatically hidden.

   > To show all deactivated users, select **View > Include Deactivated Users**.

12.2.4 Reactivating users

Manage System

1. In the **Users and Groups** window select the **Users** tab.
2. Select **View > Include Deactivated Users**.
3. Select a deactivated user row (greyed out text row).
4. Select **Activate**.

   The user row reappears in the table.

12.2.5 Deactivating groups

🔒 **Manage System**

Groups cannot be deleted from the viewLinc database; however, you can use the deactivate function to ensure that the group is no longer used for alarm notifications or group report distribution (this is easier than removing the group from multiple alarm notification templates and/or reports).

> ℹ️ All users in a group must be deactivated before a group can be deactivated.

▶ 1. In the **Users and Groups** window select the **Groups** tab.

2. Select the group you wish to deactivate.

3. Select ✖ **Deactivate**.

4. To confirm, select **Deactivate**.

   The group row is automatically hidden.

> 💡 To show all deactivated groups, select **View > Include Deactivated Groups**.

12.2.6 Reactivating groups

🔒 **Manage System**

▶ 1. In the **Users and Groups** window select the **Groups** tab.

2. Select **View > Include Deactivated Groups**.

3. Select a deactivated group row (greyed out text row).

4. Select **Activate**.

   The group row reappears in the table.

12.3 Zones and Locations

Modification to Zones and Locations is performed in the **Sites Manager** window. Common administrator activities include changing a Zone or Location name, unlinking and moving a Location to a different zone, applying different permissions, creating schedules, and/or applying different threshold templates.

> ℹ️ **Full Control** permission is required to make changes to Zones or Locations.

12.3.1 Editing Zone display properties

🔒 **Manage System**

▶ 1. In **Sites Manager** on the **Zones and Locations** tree, select the Zone you want to edit.

2. Right-click to select **Edit Properties** or select **Manage > Edit Properties**.

3. In the **Edit Zone** window, modify the information viewLinc uses to display the Zone: name, dashboard folder icon, description.

4. Save the changes.

12.3.2 Editing Location display properties

🔒 **Manage System**

▶ 1. In **Sites Manager** on the **Zones and Locations** tree, select the Location you want to edit.

2. Right-click to select **Edit Properties** or select **Manage > Edit Properties**.

3. In the **Edit Location** window, modify the information viewLinc uses to display the Location: name, description, units and decimal places. These settings control the way the Location appears throughout viewLinc. If you enter a smaller number of decimal places than your device reads, viewLinc automatically rounds the data it receives from the device to the nearest decimal point.

4. Save the changes.

12.3.3 Viewing Location properties

In the **Sites Manager** window use the **Location Properties** tab for at-a-glance review of important Location details. Access to the **Sites Manager** window requires **Manage Sites** right.

Icon	Description
〰️	**View Trend**: View a Location's historical data as a trend in a new browser window.
🗂	**Find in Tree**: Highlight the selected Location in the **Zones and Locations** navigation tree.
🕘	**Show Linked Channel History**: Find out how long a specific device channel has been linked to a selected Location, when the link first began, and for how long it has been linked.

Table 26   Location properties columns

Column	Contains
Type	The Location Type icon. This column cannot be moved.
Zone	Full path of the parent Zone.
Location	Location name as displayed in the navigation tree.

Column	Contains
Location ID	Number assigned by viewLinc to a new Location. It can never be changed. Used to avoid confusion if more than one Location is given the same name.
Description	User-entered device description.
Device Description	Name of a device, as defined by a user.
Device Serial Number	Device serial number automatically stored in viewLinc .
Channel Description	Description provided by a user.
Device ID	A number assigned to a new device, generated by viewLinc , and can never be changed. Used to avoid confusion if more than one device is given the same name.
Channel ID	A number assigned to a new channel, created by viewLinc , and can never be changed. Used to avoid confusion if more than one channel is given the same name.
Channel Index	Channel number assigned to the linked Location.
Location Units	Unit display format set in viewLinc , often modified for reporting purposes (for example, American sites may want to see readings in standard measurement units, Fahrenheit, while Canadian operations may prefer them in metric, Celsius).
Preferred Units	Unit display option (such as C or F), for the specific Location (units can be set differently for different Locations).
Device Units	Data logger or transmitter units, such as C, DEGC, TDC, set by Vaisala. These can be changed in viewLinc to display in a more meaningful way (Location or Preferred Units).
Measurement Type	The value being measured (temperature, humidity, Boolean, pressure).
Decimal Places	System-defined preference for this Location. Any threshold alarm settings are rounded to a Location's decimal place before comparison. Consider the following example: • Threshold alarm: 22.37500 ℃ • Data logger reading: 22.35124 ℃ If Decimal Places = 1, an alarm may be triggered because both the threshold alarm and the logger sample are rounded up to 22.4 ℃. If Decimal Places = 2, an alarm is not triggered because the threshold alarm is rounded to 22.38 ℃ and the logger sample value is rounded to 22.35 ℃.
Device Address	System folder path to this Location.
Link Start	Date the Location started recording data (Unlimited indicates this Location has remained linked to the current channel since it started monitoring data).
Link End	Date the Location stopped recording data (Unlimited indicates the Location is still linked to the current channel, and continuously recording data).
Permission	The permission a user has been granted for this Location.

Column	Contains
Threshold Alarm Schedule	The name of the threshold alarm schedule set for this Location, if one has been assigned.

More information

‣ Icons (page 154)

12.3.4 Renaming Locations or Zones

🔒 **Manage Sites**

Renaming Zones edits the Zone name only; it does not change the Locations assigned within it.

1. In **Sites Manager** on the **Zones and Locations** navigation tree, select the Location or Zone you want to rename.

2. On the **Manage** menu, select **Edit Properties**, or right-click and select **Edit Properties**.

3. Type a new unique name, then select **Update**.

4. Select **Save** or **Undo** to cancel the change.

12.3.5 Unlinking or relinking Locations and channels

🔒 **Manage Sites**

As your company's monitoring needs change, perhaps due to a change in monitored spaces or a facility move, you may want to link a device channel to a different viewLinc Location. This is an easy change with viewLinc's unlink/relink function.

> ℹ️ **Full Control** permission is required for all Zones where Locations are being linked or unlinked.

Channels can be unlinked individually, or you can unlink all channels within a Zone at one time. This option saves you time when you want to deactivate a Zone that is no longer being monitored. For some organizations, the list of Locations and Zones is lengthy, and the first step is to identify the Location to which a channel is linked.

12.3.5.1 Unlinking a Location from a channel

When a device channel is unlinked from a viewLinc Location, data history is retained in the Location History report.

1. In **Sites Manager** navigate the **Zones and Locations** tree to the linked Location.

2. Select **Manage > Unlink Channel** (or right-click and select **Unlink Channel**).

3. Select **Unlink**. The device channel is now available to link to another Location.

4. Select **Save**.

12.3.5.2 Unlinking all Locations in a Zone

> These steps are required if you want to delete a Zone.

1. In **Sites Manager**, navigate the **Zones and Locations** tree to find the Zone with the Locations you want to unlink.

2. Select **Manage** > **Unlink Channels** (or right-click and select **Unlink Channels**).

3. Select **Unlink** to confirm the change.

4. Select **Save**.

More information

‣ Removing Zones and Locations (page 213)

12.3.5.3 Linking a previously linked channel to a new Location

1. In **Sites Manager** select the **Hosts and Devices** tab.

2. In the **Zones and Locations** tree, navigate to a new, unlinked Location.

3. In the **Hosts and Devices** tree select an unlinked channel (the channel may have been linked before, but is now in the unlinked state, displaying italicized text).

4. Select **Configure > Link Channel**.

5. In the **Link Channel to Location** window, choose when you want this new Location to start monitoring data:

   Start now
   Data is recorded at this Location starting from the next available sample recorded on the channel.

   Start from earliest available link time [ ]
   New channel data starts recording to the Location based on last time the channel was linked.

   Start from a specified time
   Set the time to start recording data history.

6. Select **Link**.

7. Select **Save**.

12.3.5.4 Linking a new channel to a previously linked Location

1. In **Sites Manager** select the **Hosts and Devices** tab.

2. In the **Zones and Locations** tree, navigate to an unlinked Location (the Location may have been linked previously to another channel, but is currently in the unlinked state, displaying italicized text).

3. In the **Hosts and Devices** tree select the unlinked channel.

4. Select **Configure > Link Channel**.

5. In the **Link Channel to Location** window, choose when you want this new Location to start monitoring data:

   Start now
   Data is recorded at this Location starting from the next channel reading.

   Start from earliest available link time [ ]
   New channel data starts recording to the Location based on last time the Location was linked.

   Start from a specified time
   Set a specific time to start recording data history.

6. Select **Link**.

7. Select **Save**.

12.3.5.5 Linking previously linked channel to a previously linked Location

1. In **Sites Manager** select the **Hosts and Devices** tab.

2. In the **Zones and Locations** tree, navigate to an existing, unlinked Location.

3. In the **Hosts and Devices** tree, select an existing, unlinked channel.

4. Select **Configure > Link Channel**.

5. In the **Link Channel to Location** window, choose when you want this Location to start monitoring data:

   Start now
   Data is recorded at this Location starting from the next available sample time.

   Start from earliest available link time [ ]
   This option automatically selects the most recently linked time, the Location or the channel linkage. This prevents data duplication and invalid alarms.

   Start from a specified time
   Set a specific time to start recording data history.

6. Select **Link**.

7. Select **Save**.

> ℹ️ Location data and alarm history is preserved when unlinking/relinking devices.

12.3.6 Moving Locations

🔒 Manage Sites

viewLinc recognizes devices regardless of their assigned Zone, which allows you to move devices and channels from one Zone to another, without losing data history. For example, if you need to move a monitored refrigeration unit to another physical location, in viewLinc, simply move the device Location data point to a different refrigeration Zone. Full Control permission for the Location is required.

▶ 1. In **Sites Manager** make sure you have a destination Zone created for the Location.

2. On the **Zones and Locations** tree, select the Location you want to move.

3. To move the Location with your mouse, in the **Zones and Locations** tree select a Location and drag it to the new Zone.

> ℹ️ If the new Location has the same name as another Location in the Zone, at the prompt modify the Location name.

4. To move the Location manually, in the **Zones and Locations** tree select a Location:

   a. Select **Manage > Cut** (or right-click and select **Cut**).

   b. Select the Zone where the Location will be moved and then select **Manage > Paste**.

5. Select **Save**, or **Undo** to cancel the move.

12.3.7 Removing Zones and Locations

As your company grows, or monitoring needs change, you may find that you no longer need a Zone or Location displayed on your desktop. To ensure complete audit trail records, Locations can be deleted only if they have never been linked to a channel to collect data. Any Locations that cannot be deleted can still be prevented from appearing on the viewLinc desktop, with the deactivate function.

- **Deactivate**: The Location is hidden from view (Zones and Locations tree) and can be reactivated at a later time.
- **Delete**: The Zone or Location can no longer be used. This option is a good way to remove the visual clutter associated with deactivated Zones or Locations.

> ℹ️ You cannot delete the top-level Zone or a Zone with Locations that have been used to collect data. Zone deletion is only available when all child Locations are deleted or moved to another Zone.

12.3.7.1 Deactivating Locations

🔒 **Manage Sites**

When you no longer want to record data or monitor a Location, deactivate the Location so it is no longer visible on the **Zones and Locations** tree. All previously recorded history is saved.

▶ 1. In **Sites Manager** on the **Zones and Locations** tree, select a Location to deactivate.

   2. Select **Manage > Deactivate** (or right-click and select **Deactivate**).

   3. At the prompt, select **Deactivate**. The Location is hidden from view.

   4. Select **Save**, or **Undo** to cancel the change.

> 💡 To show or hide all deactivated Zones or Locations, select **More > Include Deactivated Locations**.

12.3.7.2 Reactivating Locations

🔒 **Manage Sites**

Only deactivated Locations which were never linked to a device channel may be reactivated.

▶ 1. In **Sites Manager** on the **Zones and Locations** tree, select **More > Include Deactivated Locations**.

   2. Select the deactivated Location (appears as red strikeout text ~~Lab A~~), then select **Manage > Activate** (or right-click to select **Activate**).

   3. At the prompt, confirm activation.

   4. Select **Save**.

12.3.7.3 Hiding or showing deactivated Locations

🔒 **Manage Sites**

When you deactivate a Location, it is hidden from view in the **Zones and Locations** tree. You can make them visible again in **Sites Manager**.

▶ 1. In **Sites Manager**, select or deselect **More > Include Deactivated Locations**.

12.3.7.4 Deleting Locations

🔒 **Manage Sites**

Unlinked Locations which have never been linked to a device channel can be deleted. Once deleted, they are no longer available in the **Zones and Locations** tree.

If a Location has been linked to a device channel, the Location can only be deactivated. Deactivated Locations are hidden from view and can be reactivated.

▶ 1. In **Sites Manager** select an unlinked Location.

   2. Select **Manage > Delete** (or right-click to select **Delete**). If the option to delete is not available, the selected Location was previously linked to a channel and cannot be deleted, only deactivated.

3. Select **Save**.

More information

‣ Deactivating Locations (page 213)

12.3.7.5 Deleting Zones

🔒 **Manage Sites**

Zones can only be deleted if all child Locations are deleted.

▶ 1. In **Sites Manager** select an empty Zone to delete. To verify that the Zone does not contain any hidden deactivated Locations, select **More > Include Deactivated Locations**.

> 💡 If the Zone you want to delete contains any deactivated Locations, you can drag them to another unused Zone.

2. Select **Manage > Delete** (or right-click and select **Delete**).
3. Select **Save**.

12.4 Enabling or disabling alarming

To prevent unnecessary alarming during system maintenance periods, which may take more than 24 hours, disable device alarms.

- Disable or enable device alarming
- Disable or enable threshold alarm settings
- Disable or enable threshold alarm template level (affects all Locations using the template)

To disable alarming on devices for a temporary period of up to 24 hours, you can pause the alarm.

To stop device alarming and data logging until further notice or even permanently, you must deactivate a device or host.

More information

‣ Pausing alarms (page 169)
‣ Deactivating hosts or devices (page 218)

12.4.1 Enabling or disabling threshold alarm settings

🔒 **Manage Sites**

Disabling threshold alarm settings is useful when you want to temporarily prevent threshold alarming on one or several Locations. You can also disable individual levels in a threshold alarm template. You must have at least **Configure Alarms** permission for selected Location(s).

Disabled threshold alarm settings remain visible on your viewLinc screen and can be enabled at any time.

> When you no longer want threshold settings used, use the deactivate option (threshold alarm settings cannot be deleted). Deactivated threshold alarms are hidden from view, but can be reactivated at any time.

▶ 1. In **Sites Manager** navigate to a Location in the **Zones and Locations** tree.

2. On the **Threshold Alarm Settings** tab, select one or more rows (**CTRL**+click to select multiple), then select ✎ **Edit threshold alarm settings** (or use the right-click menu).

3. On the **Edit Threshold Alarm Settings** window, enable or disable the **Status** setting.

4. Select **Save**.

More information

‣ Deactivating threshold alarms (page 91)
‣ Enabling or disabling threshold alarm template levels (page 216)

12.4.2 Enabling or disabling threshold alarm template levels

🔒 **Manage Alarm Templates**

When creating a threshold alarm template, you may not want to enable all levels. You may want to apply the threshold alarm template to several Locations, then enable specific levels at different times.

> Enabling or disabling a threshold alarm template level affects all Locations using the template.

▶ 1. In **Alarm Templates** select the **Threshold Alarms** tab.

2. Select the threshold alarm template you want to modify, then select ✎ **Edit**.

3. On the thresholds grid in the **Enabled** column, enable or disable threshold levels. At least one threshold level must remain enabled.

4. Select **Save**.

12.4.3 Enabling or disabling a device alarm assigned to a Location

🔒 **Manage Sites**, **Manage Alarm Templates**

To prevent unnecessary alarming during system maintenance periods, which may take more than 24 hours, disable device alarms. You can also disable all alarming on a device for a temporary period, up to 24 hours.

Alternatively, to stop all device alarming and data logging until further notice or even permanently, you can deactivate a device or host.

1. In **Sites Manager** select a Location in the **Zones and Locations** tree.

2. On the **Device Alarm Settings** tab select the device alarm type you want to enable or disable. You must have at least **Configure Alarms** permission for the selected Location.

3. Select ✎ **Edit** device alarm settings.

4. In the **Edit Device Alarm Settings** window set the **Status** option to **Enabled** or **Disabled**.

5. Select **Save**.

More information

‣ Pausing alarms (page 169)
‣ Deactivating hosts or devices (page 218)

12.4.4 Enabling or disabling multiple device alarms

🔒 **Manage Sites**

1. In **Sites Manager** select one or more Zones or Locations in the **Zones and Locations** tree (**CTRL**+click). You must have at least **Configure Alarms** permission for selected Location(s).

2. On the **Device Alarm Settings** tab, select the alarm types you want to enable or disable.

3. Select ✎ **Edit device alarm settings**.

4. In the **Edit Device Alarm Settings** window select the status option: **Enabled** or **Disabled**, or, if multiple alarm types are selected, leave the default option selected, (**Mixed - leave unchanged**).

5. Select **Save**.

12.4.5 Enabling or disabling host alarming

🔒 **Manage Devices**

Disable host alarms to prevent continuous alarming during maintenance periods.

1. In **Sites Manager** on the **Hosts and Devices** tree, select a host.

2. Select **Configure > Host Communication Alarm Settings** or **Configure > Host Configuration Alarm Settings**.

3. Set the **Status** option to **Enabled** or **Disabled**.

4. Select **Save**.

12.5 Device maintenance

Users who are part of the default **Administrators** group, or are part of a group assigned
Manage Devices right, use the **Sites Manager** window to manage and maintain hosts and
devices.

More information

‣ Configure hosts and devices (page 52)

12.5.1 Device removal

🔒 **Manage Devices**

Before you remove a device from your network, or transfer it to a new monitoring area on the
same network, the device must be deactivated. A deactivated device stops logging data and
disables all device and threshold alarming.

You may want to remove a device when:

• a device requires maintenance (such as recalibration)
• a device is no longer required

🛈 When a device is swapped it is automatically deactivated.

More information

‣ Deactivating hosts or devices (page 218)
‣ Releasing RFL data loggers (page 219)
‣ Swapping devices (page 226)

12.5.1.1 Deactivating hosts or devices

🔒 **Manage Devices**

You can deactivate a single device or all devices connected to a host. This action will stop all
alarming and all data collection until you reactivate the device or host.

1. In **Sites Manager** select the **Hosts and Devices** tab.

2. On the **Hosts and Devices** tree, select the host or device you want to deactivate.

3. Select **Configure > Deactivate** (or right-click and select **Deactivate**).

4. A message appears, asking that you confirm deactivation of the host or device. Select
   Deactivate.

The host/device is no longer visible on the **Hosts and Devices** tree, but the network
connection is still intact, allowing you to reactivate the host/device at a later time.

Deactivated devices are not included in the total number of licensed devices.

12.5.1.2 Reactivating hosts or devices

Manage Devices

1. In **Sites Manager** select the **Hosts and Devices** tab.
2. On the **Hosts and Devices** tree, select **More > Include Deactivated Devices**.
3. Select the deactivated host/device (indicated by red strikeout text ~~Lab A~~), then select **Configure > Activate** (or right-click and select **Activate**).

12.5.1.3 Hiding or showing deactivated hosts or devices

Manage Devices

1. In **Sites Manager** select the **Hosts and Devices** tab.
2. On the **Hosts and Devices** tree select **More**, then check or uncheck the option, **Include Deactivated Devices**.

12.5.1.4 Releasing RFL data loggers

Manage Devices

Before moving or removing RFL data loggers on your network, they must be released from their access point to prevent unnecessary alarming.

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

1. In **Sites Manager** select the **Hosts and Devices** tab.
2. Select one or more RFL data loggers in the **Hosts and Devices** tree.
3. Select **Configure > Release Device from Access Point**.

After releasing an RFL data logger, it can be accepted later by the same or by another access point host.

4. At the prompt, select **Release**.

12.5.2 Modbus device addition
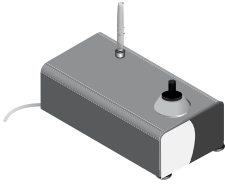
You can configure viewLinc Enterprise Server to retrieve data from both Vaisala and non-Vaisala Modbus-enabled measurement devices containing a maximum of 8 channels per device. You can connect Vaisala Modbus devices to a viewLinc device host as part of your standard viewLinc license, while third-party/non-Vaisala Modbus devices require the purchase and addition of a Modbus license.

> To see the current number of licensed Modbus devices or available viewLinc device spaces, see ❓ **> About**.

Several of Vaisala's measurement devices and other manufacturer's devices use the Modbus communications protocol. The associated device documentation provides important details you will need to configure a Modbus TCP or Modbus RTU device in viewLinc.

Connecting Modbus devices

Modbus RTU devices may be connected to your network with a Digi or other Ethernet device, or with a serial cable to connect directly to a viewLinc Device Host. Modbus TCP devices are connected directly to your network with a network cable.

> Connecting Modbus devices to your network requires advanced networking expertise. Refer to your Modbus device documentation to complete the installation steps, including installation of required Digi or Ethernet device drivers on the host server, and verification of network connectivity.

Input and Holding Registers

Modbus devices contain input and holding registers that read and write data using 16-bit or 32-bit wide integers. The data structure used by the Modbus device manufacturer defines the way you will need to configure viewLinc.
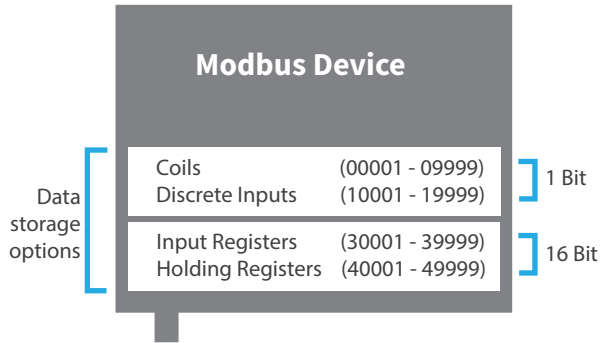
The first step is to refer to your Modbus device documentation to determine whether the register format is based on an address (decimal or hexadecimal) or a number. If your device uses the wider 32-bit format, the data format may be higher byte/word first or lower byte/word first.

Register types	Register number ranges	Data format options
Coil	00001-09999	Boolean / Boolean Inverted
Discrete Input	10001-19999	Boolean / Boolean Inverted
Input Register	30001-39999	• 16-bit Integer / Unsigned Integer • 16-bit Boolean / Boolean Inverted
Holding Register	40001-49999	• 32-bit Integer, Little-endian / Little-endian, word swapped • 32-bit Integer Big-endian / Big-endian word swapped • 32-bit Unsigned Integer, Little-endian / Little-endian, word swapped • 32-bit Unsigned Integer Big-endian / Big-endian word swapped • 32-bit Float Little-endian / Little-endian word swapped • 32-bit Float Big-endian / Big-endian word swapped • 32-bit Boolean / Boolean Inverted

Additional Modbus reference information about mapping registers can be found online, such as www.modbus.org.

> Since Modbus device documentation is not standardized, it may provide configuration information in a variety of ways. To learn more about Modbus, useful online resources include: www.modbus.org, and "Add a Modbus device" , available from the Tours menu.

12.5.2.1 Configure Modbus device connections

Refer to your Modbus device documentation to collect required register configuration details.

🔒 **Manage Devices**

> Before completing this configuration task, make sure the Modbus device is connected to your network and, if installing third-party/non-Vaisala Modbus devices, make sure the Modbus license key has been added. If you are adding a Modbus RTU device, make sure you have the COM port number assigned (Go to Windows Start menu to open **Device Manager > Ports > Communications Port**). If you are adding a Modbus TCP device, refer to the device manual to determine Port number and IP address.

> If you are using a Digi device connection, install the Digi device drivers on the host server.

1. In **Sites Manager** select the **Hosts and Devices** tab.

2. In the **Hosts and Devices** tree select a viewLinc Device Host server, then select **Configure > Add Device > > Vaisala Modbus Device** or, if licensed, **Non-Vaisala Modbus Device**

3. If you are adding a Vaisala Modbus device or have added a similar non-Vaisala Modbus device and saved the device configuration details as a template, select **Template...** and select the template you want to use.

4. In the **Add Modbus Device** window type a device **Description** (do not use < or >), **Model** (do not use dashes, --), then add a unique **Serial number** (alpha numeric only).

5. To modify calibration details or to set up calibration reminder notifications, select **Edit calibration data...**:

   Calibration date:
   The original calibration date for the measurement probe, set by the factory and cannot be modified.

   Calibrated by:
   The name of the person or company who performed the calibration service.

   Next calibration date:
   Type a new date to automatically have viewLinc generate a calibration notification to remind you when calibration service is needed.

6. Add communication settings:

    Modbus TCP: Type the Modbus device IP address, port number (default 502), and unit ID. This must be a unique combination. **Modbus RTU Serial**: Type the COM port number the Modbus device is connected to, the device's Slave ID, the serial bit rate (default 9600), parity and stop bits, as specified in the Modbus device documentation.

7. Add viewLinc channel details:

    Measurement type / **Unit**:
    Choose from the available viewLinc measurement type and unit options.

8. Add Modbus register details:

    Format:
    Choose a format option based on the register number or address (defined in the Modbus device documentation).

    Register type
    - **Coil** or **Discrete input**: Type the number or a decimal address.
    - **Input register** or **Holding register**: Type the decimal address and then choose byte format.

    Number or **Address**:
    Depending on the format selected, add the required number or address in decimal or hexadecimal format.

    > After details are saved, when you select a different option in the Format field, the entered details automatically convert to the selected format.

9. Define scaling parameters (optional). You can use the **Scale** field to add a multiplier value, and the **Offset** field to add a positive or negative number, to calculate a recognized or expected **Current value**. Some integer registers need a scaling adjustment to make sure the value read from the register corresponds with the actual value it is communicating. For example, if a register stores a value of 2406, it requires a scaling factor of 100:1 to display as an actual temperature of 24.06 ºC.

10. Click the test icon, to test the connection. If an expected value appears in the row, the configuration is complete. If the value is not displayed, is incorrect, or the warning icon remains in view, , review and adjust the configuration and/or scaling settings entered for the device. Re-test as required.

    Modbus documentation may indicate a specific order that data will be sent; however, viewLinc may expect receive it in another syntax. If the combination of register format and address selection is not correct, the device value will be significantly different than expected. You may need to enter register details in a variety of formats and test until the correct device value displays.

11. Save the channel detail row and start a new row for an additional device channel. To delete an extra row, click 'X'.

12. When you are finished entering details and the **Add device** button is enabled, select **Save** or **Save as template...** to save the details as a reusable template.

More information

‣ Ways to connect hardware (page 18)
‣ Entering a new license key (page 117)

12.5.2.2 Editing Modbus device settings

🔒 Manage Devices

▶ 1. In **Sites Manager** select the **Hosts and Devices** tab.

2. In the **Hosts and Devices** tree select the Modbus device, then select **Configure > Edit Properties** (or right-click to view the options menu).

3. **Save** changes.

12.5.3 Device calibration

Calibration ensures that data recorded by the measurement equipment (data loggers, transmitters, probes) is reliable and accurate.

For example, most people are used to adjusting their watches to the correct time. Working standards (clocks) are visible and almost everywhere, and making a comparison–calibration–is easy. If the time on the watch differs from the trusted reference, make an adjustment. The measured data (the time) shown on the trusted reference (the clock) can be can be relied upon as a reference point.

Use viewLinc to update your device, probe and channel calibration values. To make sure your devices are calibrated on schedule, set up viewLinc calibration reminders for your devices and their probes.

> ℹ️ Refer to the https://docs.vaisala.com/r/M211060EN-L/en-US for information about calibrating HMP110 Humidity/Temperature probes.

12.5.3.1 Editing channel calibration properties

🔒 **Manage Devices**

Channel calibration settings are the reference values used for testing measurement accuracy on Vaisala data loggers

> ℹ️ Ensure that the initial calibration values have been downloaded from the device to viewLinc (automatically discovered when device detected by viewLinc).

▶ 1. In **Sites Manager** select the **Hosts and Devices** tab.

2. In the **Hosts and Devices** tree, select a data logger channel to edit.

3. Select **Configure > Edit Properties**.

4. In the **Edit Channel Properties** window, edit the properties, **Calibration scale** and **Calibration offset** using information provided by Vaisala or collected from on-site calibration testing.

5. If you are changing calibration settings on an HMT140 device, you are prompted to reset the device calibration settings.

6. Select **OK**.

More information

‣   Editing channel properties (page 59)

12.5.3.2 Editing device or probe calibration properties

🔒 **Manage Devices**

When you set calibration dates for devices and their probes, viewLinc automatically issues calibration reminder notifications at 3 months and 1 month before to the due date, and again on the due date.

You can set the properties for calibration notifications (priority, delay, acknowledgment) in a device calibration alarm template, and add a notification message, such as who to contact to initiate the calibration service.

💡   Calibration duration can be set for all devices in **System Preferences** by selecting the value column beside the option, **Default calibration duration**; however, the calibration duration set on a data logger or a probe overrides the system preference.

ℹ️   Calibration information on some devices is set automatically and cannot be modified.

▶   1. In **Sites Manager** select the **Hosts and Devices** tab.

2. In the **Hosts and Devices** tree, select a device.

3. Select **Configure > Edit Properties**.

4. In the **Edit Device Properties** window, calibration fields are available for the device and any attached probes. Add calibration details:

Calibration date
Type the last calibration date, unless preset by Vaisala Calibration Services.

Calibrated by
Type the name of person who last calibrated the device, unless preset by Vaisala Calibration Services.

Next calibration date
Type the date for next calibration. If no date entered, the system automatically sets the date to one year after last calibration date.

5. Select **OK**.

More information

‣ Editing channel properties (page 59)

12.5.3.3 Off-site calibration

To maintain the high accuracy measurement of the viewLinc system, Vaisala offers calibrations and complete functional testing in our own ISO 17025 accredited lab, which meets the standards of ISO/IEC 17025 & ANSI/NCSL Z540-1-1994.

Calibration services include:

- Verification of specifications against the original calibration
- Battery check and replacement if necessary
- Update firmware if necessary

12.5.3.4 On-site calibration

When sending devices in for recalibration is impractical, Vaisala's on-site calibration team is ready to assist. On-site calibration includes a NIST-traceable certificate and reminders of recalibration due dates.

To reduce the costs of calibration Vaisala offers optional 3 or 5-year pre-paid plans that not only provide protection from price increases, but also offer significant savings on calibration costs. For convenience, rental devices are available.

12.5.4 Swapping devices

🔒 **Manage Devices**

The swap device function allows you to exchange a device that is currently linked to a Location, while retaining the threshold and device alarm settings which are currently applied to the Location. A swap may be required for maintenance purposes, such as calibration of the device or probe, an update of the data logger firmware, or to change to a wireless device.

When a device is swapped, 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.

Any device linked to a Location can be swapped without interruption to threshold monitoring or causing a device alarm.

> Only a device with the same settings may be swapped (for example, a device with 3 channels cannot be swapped for a device with 2 channels, and the channels must record the same type of data).

1. Make sure the replacement device is:

    • connected to your network
    • on the same host as the device to be swapped
    • has the same sample rate
    • has the same channel indexes and measurement types

2. In **Sites Manager** select the **Hosts and Devices** tab.

3. On the **Hosts and Devices** tree, select the device to be swapped.

4. Select **Configure > Swap This Device With**.

> Only compatible and available replacement devices are displayed.

5. In the **Swap Device** window, select the replacement device.

    Show device currently connected to port
    If you are swapping a DL logger and the new device is already connected, enable this option to help locate a specific device.

    Link start time
    Select Start now to associate all channel data starting from this point forward with the linked Location.

    Start from last channel sample recorded at Location
    This option automatically starts from the most recently linked time. This option prevents data duplication and invalid alarms.

> To ensure gap-free data, if the data logger was offline while still connected to viewLinc , viewLinc will not try to restore the data history during the offline period.

6. Select **OK**.

12.5.5 Locking or unlocking DL data loggers

If your viewLinc monitoring system includes DL data loggers, viewLinc can be set to prevent other software (such as other installations of viewLinc or vLog) from being used to make changes to DL data loggers.

Lock DL data loggers to ensure other software cannot be used to:

- Modify data logger or channel description
- Enable or disable a channel
- Set sample interval
- Clear data logger
- Set channel scaling
- Change warmup time

DL data loggers that are linked to vLog or Spectrum software prior to being connected to viewLinc are remote locked. You can unlink data loggers in vLog (refer to your vLog user guide for instructions), or undo the remote lock in viewLinc.

12.5.5.1 Locking a DL data logger to viewLinc

🔒 **Manage Devices**

▶ 1. In **Sites Manager** select the **Hosts and Devices** tab.

2. On the **Hosts and Devices** tree, select one or multiple DL data loggers (**CTRL**+click).

3. Select **Configure > Lock Device**.

4. Select **Save**.

12.5.5.2 Unlocking a DL data logger from viewLinc

🔒 **Manage Devices**

ℹ️   DL data loggers with a preexisting link to other software, a remote lock, can only be unlocked by a member of the **Administrators** group.

▶ 1. In **Sites Manager** select the **Hosts and Devices** tab.

2. On the **Hosts and Devices** tree, select one or multiple DL data loggers (**CTRL**+click).

3. Select **Configure > Unlock Device**.

4. Select **Unlock**.

12.5.6 Clearing historical samples in DL data loggers

🔒 **Manage Devices**

If your system includes DL data loggers, use the clear history function to:

- Remove collected data on a DL data logger prior to sending it out for calibration or repair.
- Remove data collected on the DL data logger during calibration (you can also choose to ignore the interim data when you relink the device channel to a Location in viewLinc).

- Set DL data logger sampling to **Wrap When Full** (the required device setting for continuous data collection in viewLinc).

> Editing DL data logger properties (sample interval, sample warmup time, enable/disable channels, calibration settings) automatically clears data history.

- If you use older models of Vaisala DL data loggers (with gray case) which do not support timebase synchronization, clearing history automatically synchronizes the data logger clock with the viewLinc clock to correct any time drift.

> Over time, the clock time in a data logger begins to differ from the clock time in viewLinc; this is called time drift. Some time drift is expected over long data monitoring periods and is corrected through synchronization. Synchronized timing ensures more accurate data collection results.

> If your DL data loggers are already set to **Wrap When Full** (by a calibration team or using vLog), clearing of historical samples is not required.

1. In **Sites Manager** select the **Hosts and Devices** tab.
2. On the **Hosts and Devices** tree, select one or more DL data loggers (**CTRL**+click).
3. Select **Configure > Clear Historical Samples**.
4. At the warning prompt, select **Clear**.
5. At the confirmation prompt, select **OK**.

12.5.7 Clearing tampered security status

> Only a member of the default viewLinc **Administrators** group can perform this task.

If a DL data logger security status indicates tampered (in **Sites Manager** on the **Hosts and Devices** tab, **Properties** table, **Security Status** column), it is advised that a member of the **Administrators** group investigate the issue to determine the cause. For assistance, contact Vaisala Technical Support. Once the issue is identified and/or corrected (according to your company security policy) you can complete the following steps to reset the security status.

> Change to the security status does not interrupt continuous monitoring.

▶ 1. In **Sites Manager** select the **Hosts and Devices** tab.

2. On the **Hosts and Devices** tree, select one or multiple DL data loggers (**CTRL**+click) you want to edit.

3. Select **Configure > Correct Security Status**.

4. At the warning prompt, select **Yes**.

5. At the completion prompt, select **OK**.

12.5.8 Restarting viewLinc device hosts or access points

🔒 **Manage Devices**

You can restart a device host or an access point host to return it to factory settings. Restarting a device host or access point does not interrupt data collection on connected devices.

A system or host restart is recorded in the Event Log.

▶ 1. In **Sites Manager** select the **Hosts and Devices** tab.

2. On the **Hosts and Devices** tree, select a device host or access point, then select **Configure > Restart** [**Device Host**/**Access Point**]. A system-wide message alerts all logged in users that viewLinc is about to restart.

12.6 Testing network communications

ℹ Only a member of the default viewLinc **Administrators** group can perform this task.

If you are receiving communication alarms, you may want to verify the stability of network communications.

▶ 1. In **Sites Manager** select the **Hosts and Devices** tab.

2. On the **Hosts and Devices** tree, select a host.

3. Select **Configure > Ping Host**. This may take up to a minute, depending on network traffic.

4. The **Ping Results** window indicates whether any communication failures were detected. Select **OK** to close the window.

12.7 Restarting viewLinc Enterprise Server

ℹ Only a member of the default viewLinc **Administrators** group can perform this task.

Occasionally, you may want to take viewLinc offline, or complete a reboot of your system (this does not affect the data collection). You can choose to restart or stop viewLinc temporarily.

▶ 1. In **Sites Manager** select the **Hosts and Devices** tab.

2. On the **Hosts and Devices** tree, select the viewLinc Enterprise Server, then select **Configure > Restart viewLinc Enterprise Server**.

3. Select **Yes** to confirm restart. An event message is generated and an email is sent to the IT Network Manager (specified in **System Preferences > System Alarms**).

12.8 Shutting down and starting up viewLinc services manually

If you need to shut down or start up viewLinc services manually, always follow the order specified below to ensure data integrity and avoid operating issues.

▶ 1. To **shut down** viewLinc services manually, shut down the services in this order:

1. Watchdog
2. Web Server
3. Enterprise Server
4. DB Service
All remaining services can be shut down in any order.

2. To **start up** viewLinc services manually, start the services in this order:

1. DB Service
2. Enterprise Server
3. Web Server
All remaining services can be started in any order.

13. Frequently Asked Questions

13.1 Installation tips

How does viewLinc upgrade data for use in viewLinc 5.2?

viewLinc automatically detects and converts your data. This is done transparently when you install viewLinc.

Upgrading from v3.6.1 to 5.2:

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, new permissions are applied, according to the following procedure:
   a. All users are assigned to the group **Everyone**.
   b. The group **Everyone** is assigned **View** permission to the top-level Zone, without inheriting **View** permission to the Locations in the top-level Zone.
   c. Users have their historical permission level automatically assigned to Zones.
   d. If previously granted permission to a channel, users have their historical permission level automatically assigned to the linked Location.
   e. Users are assigned to groups according to their historical permissions.
   f. Users with **Full Control** permission are automatically added to the default **Administrators** group.
4. Thresholds configured on active channels are applied to linked Locations.
5. Reports are upgraded to retrieve data from the new Locations/Zones.

For more about upgrade changes, see What's new in viewLinc 5.2 for upgrade users (page 17).

How do I configure a firewall for viewLinc?

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.

13.2 Security certificate management tips

Why am I receiving a certificate error? Will it go away?

⚠ Not secure | https://

viewLinc requires certificate and security key files to establish a secure connection between network PCs and the viewLinc Enterprise Server. The files encrypt data and authenticate the viewLinc Web Server. If your system uses an automatically generated (viewLinc-signed) security certificate, users may see this error each time they log in, but it does not prevent user from logging in. To prevent the warning from appearing, set each user's browser to trust the certificate (for example, open Chrome and go to **Settings > Advanced > Privacy and Security > Manage Certificates**). Alternatively, purchase a trusted certificate from a Certificate Authority (CA). Updating the viewLinc-signed certificate with a trusted certificate automatically prevents certificate errors from appearing.

How do I install a certificate on local PCs?

1. On each client PC, copy the certificate file (`viewLinc-CA.crt`) to any desktop location, then right-click on the file to select **Install Certificate**.

> For systems with many users, it may be more efficient to automate the installation of security certificates on client PCs. Contact your local IT group to determine whether distribution of certificates via Group Policy is an option.

2. In the **Certificate Import Wizard Welcome** screen, select **Local Machine**.
3. On the **Certificate Store** screen select **Place all**, click **Browse**, and then select **Trusted Root Certification Authorities**. If you receive an unknown publisher warning, click **OK**.
4. Click **Finish**, then **Yes**.

> Users who are currently logged in to viewLinc must log out and then log in again to establish a secure browser session.

My security certificate has expired. Will viewLinc still run? How do I renew it?

If your certificate expires, you will start to receive a certificate warning in your browser, but viewLinc will continue to run. Use the certificate signing utility included on the viewLinc USB drive (`SignCSR.exe`) to generate a new viewLinc-signed certificate.

How do I purchase a trusted certificate?

Trusted certificates can be purchased from a Certificate Authority (CA). You will use a viewLinc-generated certificate request file (.csr) to purchase the trusted certificate.

1. If you generated viewLinc-signed certificate files during initial installation, go to step 5.
2. If you did not generate viewLinc-signed certificate files during initial installation, copy the certificate request software, `CreateCSR.exe` from the viewLinc installation USB drive to `C:\Users\Public\Documents\Vaisala\Vaisala\viewLinc\config\keys` folder.

3. Drag your existing key file, `viewLinc-yy-mm-dd.key`, and drop it onto `CreateCSR.exe`.

4. Answer the questions. This process generates a certificate request file (.csr).

5. In your *….\config\keys* folder locate the generated certificate request file (`viewLinc-yyyy-mm-dd.csr`). The date in the filename reflects the date it was created.

6. Complete the purchasing steps required by your selected certificate signing authority.

7. When you receive the trusted certificate:
    • If the trusted certificate is received as a file, save the file as `viewLinc-yyyy-mm-dd.crt`.
    • If the trusted certificate is received as text, copy all the lines between `--------BEGIN CERTIFICATE---------` and `--------END CERTIFICATE--------`, and save as `viewLinc-yyyy-mm-dd.crt`.

8. Replace the existing `viewLinc-yyyy-mm-dd.crt` file with the new trusted file in the viewLinc `config\keys` folder.

9. Open Windows Services Manager.

10. Restart the viewLinc Web Server service.
    Users who are currently logged in to viewLinc must log out and then log in again to establish a secure browser session.

Why am I unable to connect to viewLinc using my purchased certificate?

The properties of the purchased certificate may be incompatible with viewLinc. Review the information in Purchased certificate requirements (page 24). Alternatively, consider using a viewLinc-signed certificate.

How do I update my security certificate and key files?

viewLinc stores certificate and key files in the viewLinc installation directory. You can update the files at any time:

1. Copy new files to the viewLinc Enterprise Server data directory (`<data folder>\config\keys\`).

2. If the filenames are different from the original filenames, update the viewLinc.cfg file (`<data folder>\config\viewLinc.cfg`):

```
[web]
privatekeyfile = <newname>.key
certificatefile = <newname>.crt
```

3. Restart viewLinc Web Server (see Restarting viewLinc Enterprise Server (page 230)).

13.3 Managing data

What happens with the sampling in viewLinc when I attach a USB cable to a device for configuration etc.?

If a USB cable is attached to a device (for example, the HMT140), the sampling is interrupted. When the USB cable is removed, sampling resumes. The sample timestamps start when the cable is removed, and are not an integral number of sample rate seconds since the previous sample. This should not affect operation. If the USB cable is attached for a long time, greater than twice the transmit rate, configuration alarms occur indicating a delay in the historical data. They will clear once the sampling resumes.

My upload keeps failing when using a file to upload logger info. How do I upload successfully?

Check that you have separated your parameters with tabs, not spaces, commas, and so on. Only parameters entered as tab-separated lines (*.tsv* format) work.

13.4 Managing devices

How do I create a definitions file to add multiple device types at one time?

Create a *.txt* definitions file that identifies the device class and device properties (separating each field with a tab):

Table 27   Definitions File Fields

Device Type	Properties to Define
DL	Define the COM Port number to which a device is connected, for example: vcom com_port=101 vcom com_port=102 vcom com_port=103
HMT140	Define the serial number: hmt140 serial_number

How do I add IP addresses for Vaisala devices using Ethernet devices (such as Digi, Moxa, or vNet devices)?

You don't. However you do assign IP addresses to your Vaisala devices. Because viewLinc communicates using COM ports, attaching Vaisala devices to the network using Ethernet/IP addresses requires the use of vNets or other Ethernet interface devices. Ethernet interface devices create virtual COM ports that allow Vaisala devices to communicate with viewLinc using Ethernet.

We recommend that you do not use dynamic IP addresses for your Vaisala devices; instead, use a reserved or static IP address (obtained from your IT department). IP addresses are assigned to Ethernet interface devices during driver configuration. To learn more about using vNet devices, see www.vaisala.com/products. To learn more about Digi devices, see www.digi.com.

13.5 Predefined settings

How does viewLinc select colors for reports?

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:

1	Black (0, 0, 0)
2	Red (255, 0, 0)
3	Green (0, 128, 0)
4	Orange (255, 165, 0)
5	Blue (0, 0, 255)
6	Yellow (255, 255, 0)
7	Purple (128, 0, 128)
8	Brown (150, 75, 0)
9	Grey (128, 128, 128)
10	Maroon (128, 0, 0)
11	Lime (0, 255, 0)
12	Tomato (255, 99, 71)
13	Azure (30, 127, 255)
14	Amber (255, 204, 0)
15	Byzantium (112, 41, 99)
16	Bronze (205, 127, 50)

17	Silver (192, 192, 192)
18	Crimson (220, 20, 60)
19	Emerald (80, 200, 120)
20	Coral (255, 127, 80)
21	DeepSkyblue (0, 191, 255)
22	Ecru (205, 178, 128)
23	Eggplant (97, 64, 81)
24	Buff (240, 220, 130)

What content variables can I add to a notification template?

Auto-generated content can be added to an email, SMS or voice template using macros. Not all macros are available in all notification templates.

Table 28   Notification Macros

Macro	Description
Available to use with all custom notification templates	
[AlarmMessage]	Include the custom alarm message, if specified for the corresponding alarm template (threshold, device or system). If no alarm message available, no content is generated for the macro. You can add alarm messages to: • Threshold alarm settings (**Sites Manager > Threshold Alarm Settings**. • Device alarm settings **Sites Manager > Device Alarm Settings**. • System Event Log and Database Validation alarms **System Preferences > System Alarms**.
[Comments]	Include the predefined or custom comment, if specified for the corresponding alarm template (threshold, device, or system). If no comment available, no content is generated for the macro. Predefined comments are created in **System Preferences > Comments**. You can add custom or predefined comments to: • Threshold alarm settings (**Sites Manager > Threshold Alarm Settings**). • Device alarm settings (**Sites Manager > Device Alarm Settings**). • System Event Log and Database Validation alarms (**System Preferences > System Alarms**).
[Date]	Date of alarm.

Macro	Description
[Server]	Time of alarm event.
Alarm-related Messages	
[AlarmObject]	Description of where alarm was triggered, from a channel, a data logger or host.
[AlarmType]	Type of alarm, Communication or Threshold.
[AlarmTimestamp]	Time alarm occurred.
[AlarmDeactivationTimestamp]	Time alarm turned off.
Alarm Acknowledgement Messages	
[Acknowledger]	Person who acknowledged the alarm.
[AcknowledgerAction]	What was done in response to the alarm.
[AcknowledgerComments]	Comment entered by person acknowledging the alarm.
[AcknowledgeTimestamp]	Time alarm was acknowledged.
[AlarmID]	Alarm ticket ID (used for remote acknowledgements).
Threshold Alarms	
[AlarmValue]	Location value when alarm occurred.
[MinAlarmValue]	Minimum Location alarm value during alarm period.
[MaxAlarmValue]	Maximum Location alarm value during alarm period.
[CalibrationUrl]	Calibration Services website address.
[LocationValue]	Location alarm value when email issued.
[ThresholdCondition]	Summary of the threshold condition.
[LocationTimestamp]	Device Communication Alarms
[DeviceChannelsSummary]	Brief description of all data logger channels associated with the alarm event.
[LocationSummary]	List of data logger channels in alarm state.
Host Communication Alarms	
[DeviceHostDevicesSummary]	Brief description of all data loggers on a host, associated with the alarm event.
[DeviceChannelsSummary]	Brief description of all data logger channels associated with the alarm event.

13.6 Troubleshooting tips

Why can't I log in to viewLinc using the correct username and password?

Ensure the viewLinc Enterprise Server service is running: If viewLinc is not running, a blue screen and status message appears on your desktop display. If the viewLinc Web service is not running, you will see a browser error message. In Windows Control Panel, choose **Administrative Tools** | **Services**, then find "viewLinc Enterprise Server" on the list and right-click to select **Start**.

> Has your domain name changed? If you are using Windows authentication, ensure your domain name matches your current log in password.

I have entered incorrect login credentials too many times and the account is now locked. How can I unlock the account?

Contact an administrator: administrator users can both unlock and lock user accounts in the **Users and Groups** window. For more information on administrator options related to account locking, see Locking and unlocking user accounts (page 205).

Why can't I see any Zones and Locations?

viewLinc Zones and Locations are only visible if a group has been granted permission to view them. viewLinc Administrators set up group permissions on Zones. Permission to a Zone is required before you can access Zones and Locations in **Sites Manager**, **Sites**, **Alarms** or **Events** windows.

Why can't I access all viewLinc navigation pane windows?

viewLinc Administrators set up group rights to functional areas of viewLinc. If you require additional rights to access another viewLinc window, contact your Administrator.

Why am I receiving a device configuration alarm indicating a low battery alarm when I know the batteries are new?

If you are using an older model DL data logger, some low battery alarms are triggered even when the battery is not the issue. Look up the event corresponding to the device configuration alarm in the **Events** window, and review the event details. For more assistance, contact Vaisala Technical Support.

I'm receiving communication alarms in viewLinc. I think my network device or Vaisala device has stopped responding. What do I do?

1. Make sure your data loggers and transmitters are plugged in and/or batteries are full.
2. Make sure your network devices are connected to a power supply and the power supply is plugged in. On a Digi or vNet network device, the power light on the front of the device should be solid red.
3. Ensure each device is connected to and communicating with the network. Try to connect with the device (see Testing network communications (page 230)).
4. If there is communication between the device and the network, check that the Vaisala-supplied cable is connected properly. If the light is solid red, there is a problem with the network device or device cable. Make sure your device has been configured to use RealPort (see http://www.vaisala.com/en/lifescience). If this still doesn't fix the problem, go to step 6.
5. If the light is working correctly but you are still receiving communication alarms, open Windows Device Manager on the viewLinc computer and ensure the device is still installed:
   a. From the Windows Control Panel select **System and Security > Administrative Tools > Computer Management > Device Manager**.
   b. Under the Multiport serial adapter category in Device Manager, look for duplicate drivers using the same COM port.
6. If the light on the cable is not working properly, open vLog and determine if the cable can communicate with the Vaisala device. If there is a problem with the device communicating with the vLog graphing application, it is likely the device or device cable is not functioning properly. Try connecting the device to a new vNet or Digi networking device, or to a computer using USB, and see if you can connect to it from vLog.

How can I stop alarming while we reconfigure a storage area?

Table 29   Tips for Managing Alarms

What do you want to do?	Function	Description
Stop Location threshold alarming temporarily.	Pause/Resume	You can pause Location threshold alarming for up to 14 days (threshold alarming resumes automatically after 14 days). To pause Location threshold alarming for a longer period, disable the threshold alarm template (affects all Locations using the template).
		Go to **Sites > Zones and Locations > Options** and select the alarm type you want to pause (**Pause [Alarm Type] Alarms**).

What do you want to do?	Function	Description
Stop device alarming temporarily.	Pause/Resume	Stop device alarming for up to 14 days (device alarming resumes automatically after 14 days). Affects the device and all device channels (and linked Locations). Go to **Sites > Zones and Locations > Options** and select the alarm type you want to pause (**Pause [Alarm Type] Alarms**).
Stop host alarming temporarily.	Pause/Resume	Stop host alarming temporarily up to 14 days (host alarming resumes automatically after 14 days). Affects the host, all devices connected to the host, and all device channels (and linked Locations). Go to **Sites > Zones and Locations > Options** and select the alarm type you want to pause (**Pause [Alarm Type] Alarms**).
Stop all threshold alarming at a specific Location or Zone.	Disable/Enable	Stop all threshold alarming for the selected Location or Zone. Go to **Sites Manager > Threshold Alarm Settings** and select a Location or Zone. Select a threshold alarm template listed for the Location or Zone, **Edit** (or double-click) and set the **Status** selection to **Disabled**.
Stop all threshold alarming at several Locations.	Disable/Enable	Stop threshold alarming at all Locations using the selected threshold alarm template. Go to **Sites Manager > Threshold Alarm Settings** and sort the alarm template list as needed. Select multiple alarm templates with CTRL+click or Shift+click, then **Edit** and set the **Status** selection to **Disabled**.
Ignore one or more threshold levels, at several Locations.	Disable/Enable	Prevent a threshold level from being recognized by all Locations using the template. Go to **Alarm Templates > Threshold Alarms**, select an alarm and then **Edit**, and then deselect threshold levels as needed.
Delete a threshold alarm template.	Threshold alarm templates cannot be deleted. They can be deactivated or disabled at the Locations where they are applied.	

What do you want to do?	Function	Description
	Deactivate/Activate	Deactivated threshold alarm settings are hidden from view, and do not monitor Locations. Threshold data is not included in reports while settings are deactivated. Go to **Sites Manager > Threshold Alarm Settings** and see the instructions in Deactivating threshold alarms (page 91) and Reactivating threshold alarms (page 92).
	Disable/Enable	Disabled threshold settings remain with the Location, but are not used for monitoring or reporting. Go to **Sites Manager > Threshold Alarm Settings** and sort the alarm list as needed. Select multiple alarms with CTRL+click or Shift+click, then **Edit** and set the **Status** selection to **Disabled**.
Delete a Location.	Delete	Current or previously linked Locations cannot be deleted, only hidden from view (for audit trail purposes). Only Locations which have never been linked (used to record data) can be deleted. Go to **Sites Manager > Zones and Locations**, select a location from the list, and then **Manage > Delete**.
	Deactivate/Activate	Go to **Sites Manager > Zones and Locations**, select a location from the list, and then **Manage > Deactivate**; reactivate with **Activate**.
Delete a device or host.	Deactivate/Activate	Device continues to record data in viewLinc, but hidden from display in viewLinc UI (you cannot delete devices for audit trail purposes). Go to **Sites Manager > Hosts and Devices**, select a device or host from the list, and then **Configure > Deactivate**; reactivate with **Activate**.

Vaisala OPC UA Server Service not running

Check your Group Security Policy settings to make sure your user account has the necessary permission to run software on the installation server.

By default, both viewLinc Enterprise Server and Vaisala OPC UA Server software are installed as Windows services. These services are only permitted to run on the LOCAL SYSTEM user account, the Windows default account which has full control on the system. If your computer system is configured with custom security settings, the viewLinc/Vaisala OPC UA services may need additional configuration to run.

1. Go to the Windows **Start** menu and open or type `Services`.
2. Locate the **Vaisala OPC UA Server Service** and open the **Properties** window.
3. On the **Log on** tab select **This account**, then enter an authorized username and password. The user must have read and execute permission on all installed program files sub folders, inheritable Full Control access on all sub folders, and network access rights to allow it to connect to other systems.

13.6.1 How to respond to alarms

Table 30   Tips for responding to alarms

Alarm message	How to respond
Configuration Alarm message: Unable to receive packet from COM port (`Unable to receive packet from COM port`)	If you are using a Digi device, there may be a physical device issue. Try swapping equipment to test the following: • Port on the Digi leading to the data logger • CAT5 cable running to the data logger • CAT5 to serial adapter used to connect the cable to the data logger
Communication Alarm message: Unable to receive packet from COM port (some bytes missing) (`Unable to receive packet from COM port(some bytes missing)`).	If you are using a vNet device, viewLinc may not detect a data logger attached to it. Check for loose connections, or remove the data logger from the vNet and inspect for broken or bent PINS. If the issue continues, try swapping the data logger or vNet to determine which piece is not functioning.
Configuration Alarm message: Sensor failure (`Sensor failure`).	HMT140 or RFL100 data loggers: If your device is using an HMP110 probe, it could indicate damage to the probe or the device. We would recommend first powering down the device, then disconnecting the probe to inspect for damage. If the problem continues after reconnecting the probe, try swapping with another functioning probe (to see if the problem follows the probe, or stays with the device).
Database Validation Alarm message Database validation failed (`Database validation failed`).	If an external application has corrupted any viewLinc files, or has broken the digital locks on the files, viewLinc will attempt to correct the corruption and trigger this alarm. Severe enough corruption could cause viewLinc not to start up, and you should restore the system from a known working and tested backup. Possible software suspects include anti-virus, security or backup applications. Contact your IT team to identify processes that preceded the alarm.
Configuration Alarm message: Data sample inconsistency (`Data sample inconsistency`).	Discrepancy between real-time and historical samples on a device. Check cables, low batteries, or malfunctioning data logger. Make sure that timebase synchronization is enabled (**System Preferences**), or clear the device (**Sites Manager > Hosts and Devices**).

Alarm message	How to respond
Historical Data Alarm message: Delayed historical data (`Historical data is delayed`).	The delayed historical data alarm indicates that the device is still communicating with the viewLinc server, but it will take some time before the system processes the previously generated data and catches up with the real-time data. RFL100 data logger: This is a normal alarm when first setting up RFL devices, and could last 24 hours or more. If it continues beyond that, this could indicate a wireless issue with the RFL connecting to the AP10. Try moving the RFL100 closer to the AP10. HMT140 data logger: The wireless connectivity may be weak or there is congestion on your network. If the alarm persists, try using the HMT140 Utility software to identify the problem when the device is in an alarm state.
Historical Data Alarm message: Unrecoverable historical data (`Historical data is unrecoverable`).	The unrecoverable historical data alarm indicates that the system didn't receive or was unable to process all of the historical data because it is missing or doesn't exist. The system now considers the data as unrecoverable.
Failure to generate a report or report generation aborted	Review the number of reports in the queue. Very large reports or excess report generation may slow down performance. Refer to the *viewLinc Datasheet* for system performance specifications.
System running slow	Check for unacknowledged alarms. Removing the acknowledgment requirement can stop the build-up of alarm notifications from re-occurring.
Provisional alarm message: (`Provisional: Threshold Alarm`).	After the system receives the missing data, the provisional alarm will either: • disappear because the excursion was temporary, and conditions have returned to acceptable levels, or • become a true threshold alarm because subsequent data confirmed that the excursion is persisting. Provisional alarms are intended as proactive warnings to viewLinc users. Instead of waiting for confirmation of an alarm condition, which could be delayed by a communication problem, users can take action to immediately to check their physical setup for issues.

Glossary

access point (AP)
A host device that enables communication between wired and wireless parts of a network. Access points typically use specific network standards. Also known as a gateway. Required to connect RFL100-series data loggers to viewLinc.

Acknowledge Alarms permission
A permission level which allows a group to view Locations and acknowledge Location alarms.

acknowledgement
User response to an alarm event.

Administrators group
Members of the Administrator's Group have all rights, plus extra system-level rights which allow them to: undo Remote-lock on DL data loggers; restart viewLinc; test network communications; acknowledge inactive alarms; acknowledge system alarms; correct security status; add users to the Administrator group; edit user profiles of Administrators group members

alarm condition
Environmental state which initiates an alarm event.

alarm event
A record of an alarm condition.

alarm notification template
Defines who is notified, when and how. Can be applied to a Location using a threshold template, or a device using a device alarm template.

Alarm off margin
Also known as deadband. An active alarm will not turn off if conditions fluctuate within set margin.

Alarms window
Window used to monitor active alarms.

Alarm Templates window
Window used to create threshold, device, and notification alarm templates; Define content for email and SMS alarm messages; Create schedules.

ANSI characters
Keyboard characters for all supported European languages. See https:// www.w3schools.com.

audit trail
continuous record of all changes made to a device or the viewLinc system. The viewLinc audit trail is recorded in the Event Log.

calibration

    The process of checking and correcting the reading of any instrument giving measurements.

channel

    A device data transmission path. A device may have more than one channel available.

child

    Location which resides within a Zone, or a sub-zone that resides within a Zone.

Communication alarm

    Notification that there is a problem with the transfer of data.

Configuration alarm

    Notification of an internal system error.

Configure Alarms permission

    A permission level which allows a group to view Locations, acknowledge Location alarms, and add or modify Location threshold alarms.

continuous monitoring

    Unbroken record of environmental surveillance.

dashboard

    An image file that provides a visual reference to a physical space being monitored.

deadband

    Alarm off margin. An active alarm will not turn off if conditions fluctuate within the set margin.

device

    Data collection hardware connected to your network (data loggers, transmitters).

device hosts

    Additional servers running viewLinc device host software. Allows for easier management of connected devices and greater network stability.

drift

    When data logger time gradually deviates from viewLinc server time.

Enterprise Server

    Required Vaisala viewLinc monitoring system software.

Events window

    Window used to record all system activities. Functions include: add comments about events, generate reports on specific event periods.

excursion

    When Location conditions exceed or deviate outside specified threshold limits.

Full Control permission

    A permission level which allows a group to view Locations, acknowledge Location alarms, configure Location threshold alarms, and modify or delete Zones and Locations.

inherit
> To automatically grant a permission level assigned to a top-level folder to its sub-zones or Locations.

IQOQ
> Installation Qualification / Operation Qualification protocol document used for system validation.

IT network manager
> The person responsible for maintaining your network, including connected software and hardware.

Location
> A viewLinc data collection point, such as a freezer or storage shelf, connected to a device channel that is part of the Vaisala viewLinc Monitoring System.

Location alarm
> Notification that a threshold level has been exceeded or communication problem has occurred at point of data collection.

macros
> Predefined text strings you can add to custom email, SMS and voice alarm notification message templates.

Manage Alarm Templates
> A right assigned to a group to allow configuration of alarm templates (for threshold alarms, device alarms, alarm notifications, and notification content).

Manage Devices
> A right assigned to a group to allow addition or removal of devices, configure and edit device settings.

Manage Events
> A right assigned to a group to allow addition of custom events, add comments to events, print and export event details.

Manage Reports
> A right assigned to a group to allow addition and configuration of reports created by others (all users can add, edit and delete their own reports).

Manage Sites
> A right assigned to a group to allow addition or modification of Zones and Locations, add threshold alarms, permissions, and schedules.

Manage System
> A right assigned to a group to allow configuration of all system preferences, add users and groups, add schedules and predefined comments.

Manage Views
> A right assigned to a group to create new views, add or rename Zones, define access permissions for Zones, add dashboard images, share and manage trends.

MKT Activation Energy
Mean Kinetic Temperature

Overview window
Window used to display user-defined and shared views, specific collections of Zones and Locations. Set a default view to open automatically at login, generate view-specific reports and trends.

parent
Zone which includes sub-zones or Locations

permission
An access level which allows groups to view, configure or manage specific Locations and Zones.

PIN
Personal Identification Number

PoE
Power over Ethernet. Allows one cable to provide both data and electrical power to devices such as wireless access points. Benefits of PoE include longer cable lengths and elimination of the need for nearby power outlets.

real-time data
viewLinc collects real-time data from devices more frequently than a device's set sample rate (usually in 10 second intervals).

report owner
Individual who created a report.

Reports window
Generate and create reports; download user-generated and shared reports.

RFL
VaiNet wireless data logger.

rights
Rights allow group access to viewLinc windows and additional window functions. All users have Manage Views right, which allows access to the basic functions in Overview, Sites, Reports, Alarms, Views Manager, and Events windows. Permissions must be granted for groups to see and perform functions on Zones and Locations in these windows.

ROC
Rate of Change. Measures the amount of variation within one (1) minute. For example, you may want to know how quickly the temperature in a refrigerator rises when the door is opened.

sample
One (1) recorded and time-stamped data logger measurement.

sampling rate
Frequency of samples recorded over time.

sites

Term used to refer to a collection of Zones and Locations.

Sites Manager window

Window used to manage Zones, Locations, devices, and hosts. Functions include: Manage hosts and devices, create Zones and Locations, configure permissions, set Location threshold and notification settings, load dashboard images.

Sites window

Windows used to display Zones and Locations a group is permitted to view. Functions include: pause alarming, generate quick reports, monitor conditions on the dashboard, build trends.

System alarm

Notification when viewLinc detects changes made outside standard viewLinc operation (such as possible database tampering).

System Preferences window

Define global settings, such as: system language, enable remote acknowledgement, set up audible alarming, enable use of schedules, set device default settings, enable comments.

threshold

A level that when exceeded, initiates a threshold alarm.

Threshold alarm

Notification that a threshold level has been exceeded.

TLS (SSL)

Transport Layer Security (formerly Secure Sockets Layer). Communications protocol used to secure communications between network servers and web browsers.

VaiNet devices

Vaisala wireless communication devices that use LoRa technology.

Validation alarm

Notification when a problem with data collection is detected.

view

User- or group-specific collection of Locations. Created in Views Manager, available in the Overview window.

View permission

A permission level which allows a group to view Locations, acknowledge Location alarms, configure Location threshold alarms, and modify or delete Zones and Locations.

vLog

Configuration software shipped with DL data loggers (prior to viewLinc 5).

Wrap when full

This setting ensures a device will continue to record data, overwriting the earliest recorded data with new history when it reaches capacity. No interruption in data recording.

Zone

A collection of Locations being monitored. Zones can be divided into sub-zones.

Index

Z

Zones

Warranty

For standard warranty terms and conditions, see www.vaisala.com/warranty.
Please observe that any such warranty may not be valid in case of damage due to normal wear and tear, exceptional operating conditions, negligent handling or installation, or unauthorized modifications. Please see the applicable supply contract or Conditions of Sale for details of the warranty for each product.

Technical support

Contact Vaisala technical support at helpdesk@vaisala.com. Provide at least the following supporting information as applicable:
- Product name, model, and serial number
- Software/Firmware version
- Name and location of the installation site
- Name and contact information of a technical person who can provide further information on the problem

For more information, see www.vaisala.com/support.

Recycling

Recycle all applicable material according to local regulations.

VAISALA