

IQ/OQ

Software Installation/Operational Qualification Protocol
Vaisala viewLinc Enterprise Server Software Version 5.2

Document #:

M212958EN-B

Date Prepared:

May 3, 2024

Prepared by:

Paul Daniel
Sr. GxP Regulatory Expert

Reviewed by:

Steven Bell
Product Manager

Protocol Pre-approval

This Protocol has been reviewed and approved by the following individuals and is ready for execution. Signing this Protocol indicates that the contents of this document have been reviewed, all test procedures are appropriate, and the acceptance criteria are applicable for the intended purpose of this Protocol. The following responsible functional areas have approved this Installation/Operational Qualification Protocol for the Vaisala viewLinc Monitoring System software:

Approved By:

Information Technology

Date

Operations

Date

Quality Assurance

Date

Disclaimers and Prerequisites

- This Protocol is a ready-to-use template. It may be executed with no changes. The Protocol may be edited to match the needs of a particular customer. Care must be taken in editing to avoid making material changes to the test procedures. Test discrepancies may occur if the test procedures are altered.
- Prior to execution of this Protocol, the following conditions must be met:
- All devices (data loggers and transmitters) use for testing have been attached to the system via a USB cable, Ethernet cable, Ethernet Adaptor, Wi-Fi, or VaiNet connection.
- All cables being used that require drivers have been properly installed on the viewLinc Enterprise Server.
- All Ethernet Adaptors (vNet/Digi/Moxa) being used have been set up with IP addresses and correct network information and have had the appropriate drivers installed on the viewLinc Enterprise Server.
- All computers used as Enterprise Server, Host Device Servers, or clients, in the Vaisala viewLinc Monitoring System, must meet the applicable minimum requirements as specified in the *viewLinc User Guide*.
- Prior to approval and execution of this Protocol, refer to vaisala.com/viewLinc-Errata to review known issues related to viewLinc software or viewLinc protocol documentation.
- Administrative access to the desktop of the viewLinc Enterprise Server is required to complete some sections of this Protocol.
- A minimum of two connected data loggers with temperature channels are recommended to execute this Protocol. A single device may be used, provided that two temperature channels are available on the data logger.
- Unless otherwise specified, the procedures in this Protocol assume that devices on the system are synchronized and use a sample interval of five (5) minutes or less. Test discrepancies may occur if longer sample intervals are used.
- The data connection between test data loggers and the viewLinc Enterprise Server must not become disconnected during testing (unless otherwise specified within the test procedure).
- DL-series data loggers used in this Protocol must not be linked to vLog audit trails, as discrepancies relating to Logger and Channel description modifications may occur.
- Events may not be written to the Event Log immediately. If an expected event does not appear in the log, wait a few minutes then advance the end time of the log and refresh the event list.
- When representations of data appear in this Protocol, text surrounded by <angled brackets> will be replaced by data specific to your installation.
- The procedures in this Protocol may not leave the system in an ideal configuration for your particular application, especially in the case of an upgrade from a previous version. Review and restoration of the system configuration, settings, and templates is highly recommended following validation.

Vaisala

Email: helpdesk@vaisala.com

Web: www.vaisala.com/en/lifescience

© 2024 Vaisala. All rights reserved. Product and company names listed in this document are trademarks or trade names of their respective companies.


Table of Contents

1. Purpose	6
1.1 Installation Qualification	6
1.2 Operational Qualification	6
2. Responsibilities	6
2.1 Vendor Responsibilities	6
2.2 User Responsibilities	6
3. System Description	6
4. Objective	7
5. Validation Approach	7
5.1 Validation Package Overview	7
5.2 Basic Risk Assessment	7
5.3 Installation Qualification (IQ)	8
5.4 Operational Qualification (OQ)	8
5.5 Performance Qualification (PQ) Considerations	8
5.6 Other Considerations	9
6. Documentation Procedures	9
6.1 Good Documentation Practices	9
6.2 Execution Guidance	10
7. Installation Qualification	12
7.1 Test Plan	12
7.2 Vaisala Software Verification	13
7.3 Vaisala Documentation Verification	15
7.4 Customer Quality System Documentation Verification	16
7.5 Server Hardware Requirements Verification	18
7.6 Software Installation Verification	21
7.7 Email Configuration Verification	24
7.8 SMS Configuration Verification	27
7.9 Voice Notification Configuration Verification	29
8. IQ Final Approval	31
9. Operational Qualification	32
9.1 Test Plan	32
9.2 Event Log and Audit Trail Verification	36

9.3	User Creation and Password Verification.....	39
9.4	Group Creation and Assignment Verification.....	43
9.5	Password Complexity Verification.....	46
9.6	Password Change Verification.....	48
9.7	Failed Login Lockout Verification.....	50
9.8	Security Preferences Verification.....	53
9.9	Security Rights Verification.....	57
9.10	Access Permissions Verification.....	63
9.11	Notification and Threshold Template Verification.....	71
9.12	Email Alarm Notification Verification.....	76
9.13	SMS Alarm Notification Verification.....	83
9.14	Voice Message Alarm Notification Verification.....	89
9.15	Low Threshold Alarm Verification.....	96
9.16	High Threshold Alarm Verification.....	102
9.17	Multi-Threshold Verification.....	108
9.18	RFL100-Series Local Threshold Verification.....	114
9.19	HMT140-Series Local Threshold Verification.....	119
9.20	Notification Escalation Verification.....	125
9.21	User Schedule Verification.....	132
9.22	Threshold Schedule Verification.....	138
9.23	Alarm Pause Verification.....	142
9.24	Communication Alarm Verification.....	146
9.25	Device Historical Data Alarm Verification.....	151
9.26	Configuration Alarm Verification.....	156
9.27	Host Communication Alarm Verification.....	161
9.28	Data Presentation Verification.....	166
9.29	Calculation Verification.....	169
9.30	Time Zone Verification.....	176
9.31	System Watchdog Verification.....	180
10.	OQ Final Approval	184
11.	Signature ID Form.....	185
12.	IQ/OQ Protocol Final Approval	186
13.	Revision History.....	187

1. Purpose

The purpose of this Installation / Operational Qualification (IQ/OQ) Protocol is to provide assurance that the Vaisala viewLinc Monitoring System has been set up properly, is fully functional, and operates with a high degree of integrity, security, and reliability.

-  This document is provided in Microsoft Word document format for customization, and as a secure PDF for use without changes. Both documents are located on the provided USB drive.

1.1 Installation Qualification

The Installation Qualification (IQ) portion of the Protocol was written, executed, and approved to ensure that the system, composed of both hardware and software elements, has been installed correctly at the point of use, per the manufacturer's specifications. The IQ will capture the hardware baseline of the system, including relevant configuration information. The IQ will also verify the presence of the basic Quality System elements necessary to support system operation in a GxP environment.

1.2 Operational Qualification

The Operational Qualification (OQ) section of the Protocol was written, executed, and approved to ensure that each component of the system operates as intended, per the manufacturer's specifications.

2. Responsibilities

The responsibilities listed below apply only to the creation and execution of this validation Protocol. If the user chooses to contract out any of the activities associated with the listed responsibilities, sole responsibility will continue to rest with the user.

2.1 Vendor Responsibilities

Vaisala is responsible for the following:

- IQ/OQ Protocol template creation

2.2 User Responsibilities

User (_____) is responsible for the following:

- Equipment maintenance
- Ensuring calibrated status of unit(s)
- Protocol pre-approval
- Protocol execution and reporting of results
- Protocol execution deviations, assessment, and corrective measures
- Protocol and report review
- Protocol and report approval

3. System Description

The Vaisala viewLinc Monitoring System is a server-based, real-time environmental monitoring, alarming, reporting, and data collection system. The system consists of discrete, self-contained, microprocessor-based data collection devices (data loggers and transmitters) and a PC-compatible software reporting system for monitoring and recording temperature and relative humidity in regulated environments.

Additional types of data input may be monitored by the system with the appropriate Vaisala sensors.

The system is comprised of Vaisala viewLinc Enterprise Server 5.2 software; a Microsoft Windows® based PC or server; client PCs with an approved web browser; Vaisala data loggers and transmitters; and connectivity cabling.

The Vaisala viewLinc Monitoring System consists of Server and Client components. For the purposes of the Protocol, a Server is the computer on which the viewLinc software is installed. The Server component is the core of the Vaisala viewLinc Monitoring System. It controls the central database, web server, system configuration, alarming, and other functions. The Clients are standard web browsers (such as Microsoft Internet Explorer) operating on workstations on the LAN, which connect to the Server in order to view real-time conditions at the points being monitored, or to make configuration changes.

The Vaisala viewLinc Monitoring System supports the use of a variety of Vaisala devices, including Vaisala DL data loggers, Vaisala VaiNet data loggers, Vaisala HMT140-series data loggers, and Vaisala 300 series transmitters. (The qualification of these items is addressed in a separate hardware protocol, Document #M212957, Hardware IQ for the Vaisala viewLinc Monitoring System.)

The Vaisala viewLinc Monitoring System also includes user-based security and unique file identifiers for data integrity. The Vaisala viewLinc Monitoring System allows the end user to set alarm thresholds and notifies the end user through multiple formats (email, SMS, etc.), when an alarm condition is triggered, acknowledged, or when a data logger communication problem exists. The software has built-in trending functions, and can generate Location data, alarm history, and system configuration reports.

4. Objective

The objective of this Protocol is to qualify the installation and operation of the Vaisala viewLinc Monitoring System at

This Protocol will verify the proper installation, correct functionality and operation of the Vaisala viewLinc Monitoring System according to manufacturer's specifications and the requirements of

5. Validation Approach

5.1 Validation Package Overview

5.1.1 There are multiple protocols available to support qualification of Vaisala viewLinc Monitoring System. All customers will use the two protocols below:

- Software IQ/OQ for Vaisala viewLinc Enterprise Server Software, Document #M212958
- Hardware IQ for Vaisala viewLinc System, Document #M212957

5.1.2 The following protocols are recommended only if the customer is using specific software functions, additional hardware, or additional software with their Vaisala viewLinc Monitoring System.

- Output Device IQ/OQ for Vaisala viewLinc System, Document #M213008
- Software IQ for Vaisala OPC UA Server Software, Document #M212323

5.2 Basic Risk Assessment

5.2.1 Basic risk assessment philosophy requires that the focus of a validation effort be on the functions most likely to fail, or those functions with the greatest consequence of a failure.

5.2.2 All viewLinc system elements are considered reliable and were extensively tested in development. However, configured functions in any system are considered to be more likely to malfunction than non-configured elements.

- 5.2.3 There are two basic business processes in viewLinc with critical impact on the quality of products in controlled storage: 1) the collection of the environmental data itself, and 2) any alarm functions to identify problems, either with the data collected, or with the data collection process itself. Therefore, testing in this IQOQ Protocol will focus on the two highest risk activities performed by the system (Data Collection and Alarming) with an emphasis on configurable functions. Peripheral lower risk functions will be included in the testing where they impact the operation of these two critical areas.
- 5.2.4 All functions not related to Data Collection and Alarming are considered low risk and may not be tested in this IQOQ Protocol. These low-risk functions have been thoroughly tested by Vaisala in Unit and Module testing during development and do not require additional testing in the installed environment.

5.3 Installation Qualification (IQ)

- 5.3.1 The IQ will verify the presence of the minimum Quality System elements considered necessary for basic system operation. This will be done by verifying the presence of vendor system documentation and supporting customer documentation (such as network diagrams and SOPs) which is not supplied by Vaisala. Furthermore, this verification is not definitive of all customer documentation that is appropriate or that should be present, such as a Monitoring SOP or a Calibration Program; such documentation items are considered to be customer responsibilities and are not supplied by Vaisala.
- 5.3.2 The IQ will document the baseline server hardware required for the Vaisala viewLinc Enterprise Server Software, and the configuration of these items to function on the customer network. This will include the Enterprise Server itself and any server-based device hosts. It does not document the baseline configuration of the Local Area Network, or LAN, which may be comprised of additional network equipment, such as switches, routers, and servers. It is assumed that the qualification of the network, including the server used for the viewLinc application, has either been performed under the auspices of another test document, or that such testing has been deemed unnecessary by the user for this application.
- 5.3.3 The IQ will document the correct installation of the viewLinc software and record critical installation parameters.
- 5.3.4 The IQ will not document the baseline sensor and transmitter hardware (data loggers, transmitters, Ethernet Adaptors, and access points) associated with the Vaisala viewLinc Monitoring System, and the configuration of these items to function on the customer network. The qualification of these items is addressed in Document#M212957, Hardware IQ for the Vaisala viewLinc Monitoring System.

5.4 Operational Qualification (OQ)

- 5.4.1 The OQ portion of the IQOQ Protocol documents the correct operation of Vaisala viewLinc software relative to the manufacturer's specifications, with specific attention to the configurable aspects of the software, and to those software operations requiring interaction with the server Operating System, and the network environment. The tests in this Protocol simply verify that the devices under test respond as expected to outputs from the Vaisala viewLinc Monitoring System.
- 5.4.2 A risk-based approach, following the rationale presented in section 5.1, will focus OQ testing on the two highest risk areas of the system: Data Collection and Alarming.
- 5.4.3 The correct run-time configuration of the data collection process will be verified in the IQ activities described above. System security, where pertinent to the process and configuration of data collection, will be verified in the OQ. Furthermore, the data reporting process and the accuracy of the associated statistics will be verified.
- 5.4.4 The alarming functions of the software will be tested at arbitrary configured values to demonstrate functionality in the operating environment. This will include both system alarms (which may indicate conditions that would compromise accurate and gap-free data collection) as well as threshold alarms (which may indicate out-of-limit conditions).

5.5 Performance Qualification (PQ) Considerations

- 5.5.1 The OQ portion of the IQOQ Protocol does not verify the functionality of any specific configuration that may be adopted for use of the system. It is assumed that if qualification of a specific configuration is required, a Performance Qualification (PQ) will be performed in addition to this IQOQ document. Such

PQ testing is considered to be outside the scope of this document.

5.6 Other Considerations

- 5.6.1 The Protocol is written with the expectation that the tester is familiar with the operation of the viewLinc system. For additional detail to assist in any test steps, refer to the relevant section of the viewLinc User Guide, viewLinc online Help, or viewLinc embedded Tours.
- 5.6.2 A 'black box' approach to testing is utilized within the IQOQ Protocol to demonstrate the consistent and reliable function of the various configurable features in viewLinc.
- 5.6.3 From the perspective of the viewLinc system, any single input is identical to any other input whether it is derived from a channel from a Vaisala DL data logger, a Vaisala HMT140-series data logger, Vaisala VaiNet data logger, or a Vaisala 300 series transmitter. Every input is simply a digital data stream. As a result, it is only necessary to test each function on a single input to have confidence the function will operate correctly for all inputs.
- 5.6.4 Vaisala HMT140-series data loggers and Vaisala VaiNet data loggers are unique among Vaisala devices compatible with viewLinc, as they can store high and low thresholds locally in the data logger memory. This capability ensures local alarming in the event of disconnection of these wireless devices, which could prevent the generation of an alarm from the viewLinc Server. In this Protocol, the ability to adjust the local thresholds will be verified, and the resulting local alarm will be verified for a single HMT140-series data logger (if applicable) and a VaiNet data logger (if applicable). However, since these devices are slaved to the viewLinc Enterprise Server, it is only considered necessary to test the viewLinc Enterprise Server functions in this IQOQ. Specific testing of local thresholds for each individual data logger is considered to be performance testing appropriate for a PQ, and therefore out of scope of this IQOQ.
- 5.6.5 Two connected data loggers with temperature channels are recommended to complete the testing described in this Protocol. A single data logger may be used, provided it has a minimum of two temperature channels. The temperature channels must be configured to display Celsius. As viewLinc treats all inputs as identical and equivalent digital data streams, separate OQ testing of individual device types or measurement parameters is not considered necessary. Any additional viewLinc data loggers will have been demonstrated as equivalent in Document #M212957, Hardware IQ for the Vaisala viewLinc Monitoring System.
- 5.6.6 In this Protocol, **bold text** is used to refer to items and text that are visible on the viewLinc interface, such as Location Names, User Names, Report Names, Template Names, etc.
- 5.6.7 The computer used to access the viewLinc system for execution of this Protocol must have specific software installed. Refer to the *viewLinc User Guide* for a comprehensive list of compatible software. The following software is required:
 - A viewLinc compatible web browser.
 - A spreadsheet application, such as Microsoft Excel, capable of opening .tsv files.
 - A PDF reader application, such as Adobe Reader, capable of opening .pdf files.
- 5.6.8 viewLinc can only be accessed by a compatible web browser, all of which utilize SSL (including TLS) as the standard security technology for establishing an encrypted link between a web server and a browser. A valid SSL Certificate will be required for your viewLinc web server to be accessed by a client web browser without generating a security warning from the browser. It is assumed that customer will have existing policies and practices in place to guide the creation and maintenance of SSL certificates. In addition, it is assumed that any qualification of this standard SSL functionality on the customer network has either been performed under the auspices of another test document, or that such testing has been deemed unnecessary by the user for this application.

6. Documentation Procedures

6.1 Good Documentation Practices

- 6.1.1 Data generated during the execution of this Protocol will be collected and recorded on the datasheets provided.

- 6.1.2 Actual results will be recorded at the time of observation. The Protocol is designed to either accept handwritten data entry, or handwritten indication of a YES or NO answer. In all cases, a NO answer will be considered to indicate a failed step.
- 6.1.3 During the execution, the executor's initials and date will be provided at the time of completion for each activity.
- 6.1.4 Handwritten data is to be neatly printed using a black or blue ball point pen. Corrections are to be crossed out with a single line, initialed, and dated. If the reason for the correction is not obvious, an explanation for the correction will be included.
- 6.1.5 Charts, printouts, notes, etc. generated during the execution will be dated, signed, and attached to the completed Protocol document.
- 6.1.6 All test sections will be reviewed and signed by appropriate _____ personnel to verify document completeness.
- 6.1.7 Throughout this document, the use of "N/A" and "U/A" shall be interpreted as "not applicable" and "unavailable", respectively. A written explanation must be provided whenever "N/A" or "U/A" is used, except where "N/A" is used as the result of explicit test instructions.
- When instructed to mark a test step as "N/A", line out the entire row, mark "N/A" and add your Initial and Date.
 - When instructed to mark a test section as "N/A", line out the entire test table on each relevant page, mark "N/A" and add your Initial and Date. Add a comment explaining the reason for not executing the test section.
- 6.1.8 Pages may be photocopied as needed in order to complete additional testing or perform testing required to resolve deviations/discrepancies. Additional pages must be numbered appropriately to identify them as extra pages and to identify the order in which they appear. Identification shall be applied using alphabetical characters next to the page number and a numeric group annotation to the right of the page number as it appears in the header. For example, if three (3) additional copies of page seven (7) of a forty-one (41) page document are required, the page numbering shall be annotated to read as follows: "Page 7A of 41, Additional page 1 of 3" for the first additional page, "Page 7B of 41, Additional page 2 of 3" for the second additional page, and so on.
- 6.1.9 Throughout this document, it is necessary to attach additional documents, such as Event Logs, reports, etc. All attachments should be clearly labeled with the following information on the first page: Document Number (for example, M212958EN-A), reference section and step (for example, Section 9.6, Step 12), total number of pages (for example, 6 pages), and the Date/Initial of the test executor.
- 6.1.10 Protocol Definitions:
- A discrepancy is defined as a difference between the expected results and the actual results.
 - An exception is defined as a difference between the approved Protocol procedure and the procedure followed in testing.
 - A deviation is defined as a discrepancy or exception that prevents meeting the acceptance criteria.
- 6.1.11 Discrepancies, exceptions, and deviations to approved Protocols may occur. It is the responsibility of the customer qualification group to document each deviation, exception, or discrepancy and to provide an explanation of the circumstances that led to said deviation, exception, or discrepancy. They should be documented in the space provided in each test section or utilize the relevant user SOP for Deviation Reporting (if applicable). Deviations, exceptions, and discrepancies must be approved by the Quality Assurance group according to current customer standard operating procedures, prior to any further execution of the Protocol test section in which the deviation occurred.

6.2 Execution Guidance

- 6.2.1 The IQ Test Sections of this document should be completed prior to beginning the OQ Test Sections. However, the following IQ test sections do not need to be completed prior to initiating OQ testing:
- Vaisala Documentation
 - Customer Quality System Documentation

- IQ Final Approval

- 6.2.2 There is a Hardware IQ protocol (Document #M212957) for the Vaisala viewLinc Monitoring System hardware. It is recommended that the Hardware IQ protocol be executed prior to beginning the OQ test Sections of this document. However, there is no logistical requirement that these documents be executed in order and the OQ Sections of this document may be executed prior to execution of the Hardware IQ.
- 6.2.3 The Test Steps outlined in Test Procedures must be performed in sequence within a given Test Section. It is recommended that the Test Sections be performed in sequence. If necessary, the Test Sections within the OQ may be performed out of sequence; however, Test Sections 9.2, 9.3, and 9.4 must be performed in sequence, and are prerequisites for all later test sections.
- 6.2.4 Certain OQ Test Procedures require a specific test configuration that may require the user to perform data entry and/or verify a configuration. In these instances, the test procedure will refer to the Configuration Table located at the end of each test section, after the Comments and Acceptance Criteria. Only relevant configuration parameters will be included in the Configuration Tables. If a parameter is not included, it may be left at the default value.
- 6.2.5 Certain OQ Test Procedures involve timestamp comparisons between timestamps recorded by the tester (using the viewLinc onscreen clock in HH:MM format), timestamps recorded by the viewLinc system on reports and event logs (using timestamps in HH:MM:SS format with date), and timestamps for events recorded by outside systems (such as external email providers). When such timestamps are compared, they will not be identical due to different source clocks and inherent sources of network lag. Therefore, it is not required that timestamp comparisons be identical. However, timestamps must correspond in terms of order of operations, and small time differences will be considered acceptable as follows:
- Comparison between viewLinc timestamps are considered acceptable with a lag of no more than 2 minutes.
 - Comparison between viewLinc timestamps and external timestamps are considered acceptable with a lag of no more than 5 minutes. Additional lag should be investigated to determine the actual time difference between the source clocks.
- 6.2.6 Certain OQ Test Procedures involve verification that test steps and resulting system actions are accurately captured in the Event Log. In these instances, it is not necessary that the Event Log text match the test description. Event Log entries must convey the following:
- General event description
 - Event occurred without error
 - Event timestamp
 - Identity of the correct user (if applicable)
 - Data before/after change (if applicable)

7. Installation Qualification

7.1 Test Plan

Testing will be performed to verify that the installation of the Vaisala viewLinc Monitoring System is in conformance with manufacturer's specifications and customer requirements. The test plan consists of these eight (8) sections:

7.1.1 Vaisala Software Verification

System software is considered a basic requirement for proper maintenance of a GxP computerized system. This test section will verify that the necessary system software is available and securely stored.

7.1.2 Vaisala Documentation Verification

Vendor documentation is considered a basic requirement for proper maintenance of a GxP computerized system. This test section will verify that the necessary Vaisala documentation for the viewLinc software is available and securely stored.

7.1.3 Customer Quality System Documentation Verification

Customer Quality System documentation is considered a basic requirement for proper operation of a GxP computerized system. This test section will verify that the Quality System documentation to support the viewLinc system is available and securely stored.

7.1.4 Server Hardware Requirements and Configuration Verification

The viewLinc server must meet the recommended hardware requirements to ensure satisfactory performance. This test section will verify that the viewLinc server meets the recommended hardware requirements for the viewLinc Enterprise Server software.

7.1.5 Software Installation Verification

The viewLinc software must be correctly installed to allow for proper system operation. Capturing the installation variables also allows for easier system recovery and provides a baseline for future change control. This test section will capture the software installation variables.

7.1.6 Email Configuration Verification

Email is the primary means by which the viewLinc system communicates with users when they are not actively logged into viewLinc. The capability to successfully send an email is dependent on multiple network parameters outside the viewLinc system. This test section will verify that email parameters in viewLinc have been configured to interact correctly with the host network to allow emails from the viewLinc system to be sent.

7.1.7 SMS Configuration Verification

SMS (Short Message Service) is an additional method by which the viewLinc system communicates with users when they are not actively logged into viewLinc. The capability to send an SMS is dependent on the presence of either an installed SMS modem with an active service plan, or an active account plan with a web service SMS provider. This test section will verify that SMS parameters in viewLinc have been configured correctly to allow SMS messages to be sent by the viewLinc system.

7.1.8 Voice Notification Configuration Verification

Telephone voice messages are an additional method by which the viewLinc system communicates with users when they are not actively logged into viewLinc. The capability to successfully send a telephone voice message is dependent on an active service provider account plan. This test section will verify that the parameters in viewLinc have been configured to allow telephone messages to be sent from the viewLinc system.

9. Operational Qualification

9.1 Test Plan

Testing will be performed to verify that the operation of the Vaisala viewLinc Monitoring System is in conformance with manufacturer's specifications and customer requirements. The Acceptance Criteria for all sections are derived from Vaisala recommendations. The test plan will consist of thirty (30) areas of functionality defined below:

9.1.1 Event Log and Audit Trail Verification

viewLinc 5.2 has an Event Log in which it records events occurring in the system. The Event Log is also an Annex 11 / Part 11 compliant Audit Trail to record changes to electronic records in the viewLinc application. This test will verify that the Event Log accurately and effectively records instances of record creation, modification, and deletion.

9.1.2 User Creation and Password Verification

viewLinc 5.2 utilizes user accounts to control access to viewLinc. Each user must be created and assigned various rights and permissions to control what actions the user can perform, and what areas may be accessed by the user. This test will verify that users can be created in viewLinc, and that the created users may access the viewLinc application to maintain an individual user profile.

9.1.3 Group Creation and Assignment Verification

viewLinc 5.2 utilizes Groups to simplify management of user accounts and access to viewLinc. Each group must be created and assigned various rights and permissions to control what actions the member users can perform, and what areas may be accessed by the member users. This test will verify that groups can be created in viewLinc and assigned rights and members.

9.1.4 Password Complexity Verification

viewLinc 5.2 requires that passwords be complex and include a mix of upper-case letters, lower case letters, numbers and special characters, when using native viewLinc security features. This test will verify that simple passwords are rejected, and only suitably complex passwords are accepted by the system.

9.1.5 Password Change Verification

viewLinc 5.2 requires password changes on system accounts, when using native viewLinc security features. Passwords can be changed at any time by a user, and password change will be forced by the system at specific instances, such as initial login. The system will also prevent the re-use of existing passwords. This test will verify that password changes in the system operate correctly.

9.1.6 Failed Login Lockout Verification

viewLinc 5.2 will lockout any account that fails multiple login attempts, when using native viewLinc security features. This test will verify that the lockout function engages successfully when challenged by multiple failed login attempts.

9.1.7 Security Preferences Verification

viewLinc 5.2 utilizes settings known as Preferences to control global features within viewLinc. Two of the preferences options directly affect security and transparency within the system, by controlling repeat authentication and commenting. This test will verify that the system requires authentication and commenting when configured to require these actions.

9.1.8 Security Rights Verification

viewLinc 5.2 utilizes Rights to determine general user abilities within viewLinc. Rights cannot be assigned to users directly and may only be assigned to groups which may include any number of users. This test will verify that users may only perform those abilities in viewLinc that have been specifically granted to the members of a group that includes the user.

9.1.9 Access Permissions Verification

viewLinc 5.2 utilizes Permissions to limit access to Zones and Locations. Permissions may be assigned to groups only, and users receive only the permissions granted to groups in which they are members. This test will verify that users may only access and control those Zones and Locations in viewLinc that have

been specifically permitted to the user by their group membership.

9.1.10 **Notification and Threshold Template Verification**

viewLinc 5.2 provides notification and threshold templates to simplify the management of threshold alarming in viewLinc. This section will verify the management of threshold alarms using Alarm Notification and Threshold Alarm templates.

9.1.11 **Email Alarm Notification Verification**

Email notification is the primary mode used by viewLinc 5.2 to communicate events to system users when they are not actively logged in to the system. This section will specifically test the generation of alarm notification emails in response to an alarm condition.

9.1.12 **SMS Alarm Notification Verification**

SMS notification is another mode by which viewLinc 5.2 can communicate events to system users when they are not actively logged in to the system. Use of this feature requires SMS Settings be configured to use either an SMS modem installed on the viewLinc server, or an approved SMS Web Service. This section will specifically test the generation of an SMS notification in response to an alarm condition.

9.1.13 **Voice Alarm Notification Verification**

Telephone voice message notification is another mode by which viewLinc 5.2 can communicate events to system users when they are not actively logged in to the system. Use of this feature requires Voice Settings to be configured to use an approved telephone web service provider. This section will specifically test the generation of a telephone voice notification in response to an alarm condition.

9.1.14 **Low Threshold Alarm Verification**

An important function of viewLinc 5.2 is the generation of threshold alarms when monitored conditions are found to be below specified limits. This section will specifically test the activation of Low Threshold Alarms.

9.1.15 **High Threshold Alarm Verification**

An important function of viewLinc 5.2 is the generation of threshold alarms when monitored conditions are found to be above specified limits. This section will specifically test the activation of High Threshold Alarms.

9.1.16 **Multi-Threshold Verification**

Management of threshold settings in viewLinc 5.2 is simplified with the use of Multi-Thresholds. This section will specifically test the generation of multiple threshold alarms configured using the Multi-Threshold feature.

9.1.17 **RFL100-Series Local Threshold Verification**

Vaisala RFL100-series data loggers have the capability to store HighHigh, High, Low, and LowLow thresholds locally in the data logger memory for each channel. This test section will verify the ability to manage local thresholds in a RFL100-series data logger. In addition, the functioning of the local thresholds will be verified for a single RFL100-series data logger.

9.1.18 **HMT140-Series Local Threshold Verification**

Vaisala HMT140-series data loggers have the capability to store high and low thresholds locally in the data logger memory for each channel. This test section will verify the ability to manage local thresholds in an HMT140-series data logger. In addition, the functioning of the local thresholds will be verified for a single HMT140-series data logger.

9.1.19 **Notification Escalation Verification**

Intelligent alarm notification through notification escalation is an important function element of the viewLinc 5.2 alarm response. This section will specifically test the functions that support escalation of an alarm notification.

9.1.20 **User Schedule Verification**

viewLinc 5.2 is designed primarily as a continuous monitoring system. Some users will desire not to be notified when they are not on duty. For these users, viewLinc uses a scheduling function to define when notifications will be sent to a given user. This section will specifically test the application of the scheduling function to a user.

9.1.21 Threshold Schedule Verification

viewLinc 5.2 is designed primarily as a continuous monitoring system. Some applications require monitoring that is not continuous. For these applications, viewLinc uses a scheduling function to define when threshold alarming will be active for a given Location. This section will specifically test the application of the scheduling function to a threshold alarm.

9.1.22 Alarm Pause Verification

viewLinc 5.2 provides the ability to pause alarms to assist in the management of active alarms. This section will verify the pause alarm functionality in viewLinc.

9.1.23 Communication Alarm Verification

viewLinc collects data from a network of sensors. Consistent communication with the sensors is vital to ensure that sensor data is received in a timely manner, and the related alarming functions are evaluating fresh data. If viewLinc loses connection with a sensor, it can generate a communication alarm to notify system users that communication has been lost. This test will challenge the Communication Alarm functions in viewLinc.

9.1.24 Device Historical Data Alarm Verification

viewLinc 5.2 collects data from a network of data loggers. The condition of the data loggers is continually evaluated by viewLinc. If viewLinc detects an error in a data logger that will affect data collection, a Device Historical Data Alarm may be generated. For instance, a Device Historical Data Alarm would be generated for a missing sensor probe, or for expected historical samples missing from the data logger memory. This monitoring of the data loggers helps ensure consistent data collection within the viewLinc system. This test will challenge the Device Historical Data Alarm functions in viewLinc.

9.1.25 Configuration Alarm Verification

viewLinc 5.2 collects data from a network of data loggers. The condition of the data loggers is continually evaluated by viewLinc. If viewLinc detects an error in a data logger that will affect data collection, a Configuration Alarm may be generated. For instance, a Configuration Alarm would be generated for a missing sensor probe. This monitoring of the data loggers helps ensure consistent data collection within the viewLinc system. This test will challenge the Configuration Alarm functions in viewLinc.

9.1.26 Host Communication Alarm Verification

viewLinc 5.2 collects data from a network of sensors. The network of sensors is often connected by intermediate server hosts to improve performance for large systems. For RFL100-series data loggers, an AP10 access point serves as a host for connection to the viewLinc system. Consistent communication with the hosts is vital to ensure that all data, and the resulting alarming functions, are up to date. If viewLinc loses connection with a host, it can generate a communication alarm to notify system users that communication to the specific host has been lost. This test will challenge the host communication alarm functions in viewLinc.

9.1.27 Data Presentation Verification

The primary way to view historical data in viewLinc 5.2 is with the Location History Report. This is a presentation quality report that is highly adaptable and can be easily configured to meet the needs of multiple users. Data can also be viewed in the Trends window, providing immediate access to data graphs.

9.1.28 Calculation Verification

viewLinc 5.2 can provide a standard suite of general statistics with the Location History Report, including Average, Standard Deviation, and Mean Kinetic Temperature (MKT). In addition, the Alarm Report performs basic calculations to determine Maximum and Minimum values during an alarm period. This test will verify the calculations performed by viewLinc within the Location History and Alarm reports.

9.1.29 Time Zone Verification

viewLinc 5.2 is designed to support an enterprise installation involving devices and client PCs in time zones different than the time zone of the viewLinc Enterprise Server. This test section challenges the functions of the viewLinc software that pertain to localization of time settings.

9.1.30 System Watchdog Verification

viewLinc 5.2 is supported by a Watchdog Service, which monitors the viewLinc application and restarts it

automatically in the event of a problem. This test section will verify the ability of the System Watchdog to restart the viewLinc Enterprise Server after being manually stopped. In addition, an in-process Communication Alarm will be interrupted by the shutdown and verified to continue notification following the shut-down and restart.

SAMPLE

9.2 Event Log and Audit Trail Verification

Goal

viewLinc 5.2 has an Event Log in which it records events occurring in the system. The Event Log is also an Annex 11/Part 11 compliant Audit Trail to record changes to electronic records in the viewLinc application. This test will verify that the Event Log accurately and effectively records instances of record creation, modification, and deletion.

Rationale

The Audit Trail function of the Event Log will be challenged by creating, editing, and deleting a new and unused Location in viewLinc. Evidence will be documented to show that the Event Log accurately records the events, including the timestamps, the identity of the user, and before and after values within the record. Please note that monitoring data records cannot be created, accessed, or altered by any user, and therefore are not included in this test of the Audit Trail.


Prerequisites/Guidance

The following prerequisites and guidance apply to this test:



- This test procedure is written with the assumption that the tester is an experienced user of the viewLinc application. Utilize the *viewLinc User Guide* or online Help to gain familiarity with the viewLinc functions required for this test procedure (see "Events").
- Read the test procedure prior to executing the test procedure.
- All test steps shall be performed by a user with administrative access.
- When instructed to record the current time, record the HH:MM clock display in viewLinc window header. When instructed to record a timestamp, record the timestamp associated with the record or event under test.

9.2 Event Log and Audit Trail Verification		
Test Instructions	Actual Results	Initials / Date
<p>1. Create a new temperature Location in viewLinc and save the change. Do not link the Location to a device. Record the following items:</p> <ul style="list-style-type: none">• User performing action• New Location name• Date / Time of save action	<p>1a User name:</p> <p>1b Location name:</p> <p>1c Date / Time:</p>	
<p>2. Edit the name of the new Location. Save the change. Record the following items:</p> <ul style="list-style-type: none">• Edited Location Name• Date / Time of save action	<p>2a Location name:</p> <p>2b Date / Time:</p>	
<p>3. Delete the edited Location. Save the change. Record the following items:</p> <ul style="list-style-type: none">• Date / Time of save action	<p>3a Date / Time:</p>	

9.2 Event Log and Audit Trail Verification

Test Instructions	Actual Results	Initials / Date
<p>4. Locate the Event Log entry for the creation of the Location in Step 1. Record the following items:</p> <ul style="list-style-type: none"> • Event ID • User performing action • Location name • Event timestamp 	<p>4a Event ID:</p> <p>4b User name:</p> <p>4c Location name:</p> <p>4d Timestamp:</p>	
<p>5. Locate the Event Log entry for the editing of the Location Name in Step 2. Record the following items:</p> <ul style="list-style-type: none"> • Event ID • User performing action • Properties before (Name) • Properties after (Name) • Event timestamp 	<p>5a Event ID:</p> <p>5b User name:</p> <p>5c Properties before:</p> <p>5d Properties after:</p> <p>5e Timestamp:</p>	
<p>6. Locate the Event Log entry for the deletion of the Location in Step 3. Record the following items:</p> <ul style="list-style-type: none"> • Event ID • User performing action • Event timestamp 	<p>6a Event ID:</p> <p>6b User name:</p> <p>6c Timestamp:</p>	
<p>7. Print and attach the Event Log page(s) that contain the events related to this test.</p>	<p>7a Printout attached? Yes <input type="checkbox"/> No <input type="checkbox"/></p> <p>7b Attachment #:</p>	
<p>8. Verify the recorded test data for the creation of the new Location (Step 1) against the recorded Event Log data:</p> <ul style="list-style-type: none"> • User performing action • Location name • Event timestamp <p> Verified test data may not be identical in format.</p>	<p>8a 1a agrees with 4b? Yes <input type="checkbox"/> No <input type="checkbox"/></p> <p>8b 1b agrees with 4c? Yes <input type="checkbox"/> No <input type="checkbox"/></p> <p>8c 1c agrees with 4d? Yes <input type="checkbox"/> No <input type="checkbox"/></p>	

9.2 Event Log and Audit Trail Verification

Test Instructions	Actual Results	Initials / Date
<p>9. Verify the recorded test data for the editing of the new Location (Step 2) against the recorded Event Log data:</p> <ul style="list-style-type: none">User performing actionBefore valueAfter valueEvent timestamp <p> Verified test data may not be identical in format.</p>	<p>9a 1a agrees with 5b? Yes <input type="checkbox"/> No <input type="checkbox"/></p> <p>9b 1b agrees with 5c? Yes <input type="checkbox"/> No <input type="checkbox"/></p> <p>9c 2a agrees with 5d? Yes <input type="checkbox"/> No <input type="checkbox"/></p> <p>9d 2b agrees with 5e? Yes <input type="checkbox"/> No <input type="checkbox"/></p>	
<p>10. Verify the recorded test data for the deletion of the new Location (Step 3) against the recorded Event Log data:</p> <ul style="list-style-type: none">User performing actionEvent timestamp <p> Verified test data may not be identical in format.</p>	<p>10a 1a agrees with 6b? Yes <input type="checkbox"/> No <input type="checkbox"/></p> <p>10b 3a agrees with 6c? Yes <input type="checkbox"/> No <input type="checkbox"/></p>	

Comments/Deviations:

Acceptance Criteria Evaluation

Event Log and Audit Trail Verification: Event Log captures changes to electronic records, including the date and time of the change, the identity of the person making the change, and the original and new values.

Acceptance Criteria Met? PASS ☐ FAIL ☐ Initial/Date: _____

Reviewed By: _____ Date: _____

9.3 User Creation and Password Verification

Goal

viewLinc 5.2 utilizes user accounts to control access to viewLinc. Each user must be created and assigned various rights and permissions to control what actions the user can perform, and what areas may be accessed by the user. This test will verify that users can be created in viewLinc, and that the created users may access the viewLinc application to maintain their individual user profile.


Rationale

The user creation functions in viewLinc will be challenged by creating users and challenging the new users through login and password updates. Evidence will be documented to show that users can be created, users may update their passwords, and that native viewLinc security will prevent system access if the correct password is not supplied.

Prerequisites/Guidance

The following prerequisites and guidance apply to this test:

- This test procedure is written with the assumption that the tester is an experienced user of the viewLinc application. Utilize the *viewLinc User Guide* or online Help to gain familiarity with the viewLinc functions required for this test procedure (see "Groups and Users").
- Read the test procedure prior to executing the test procedure.
- Step 1 must performed with a user profile that has administrative rights within the viewLinc Application.
- If the Windows Authentication feature is not utilized on this installation, skip steps 9 to 12 and mark them "N/A".
- Tables referenced in the test instructions may be found at the end of this test section following the Acceptance Criteria.

9.3 User Creation and Password Verification		
Test Instructions	Actual Results	Initials / Date
<p>1. Create and save a primary test user profile per Table 9.3-a. Record the following items for the new user:</p> <ul style="list-style-type: none">• User name• Email• Mobile number• viewLinc PIN <p> This user will be referred to hereafter as <newadmin>. For privacy, the last 4 digits of the mobile number may be represented by "XXXX".</p>	<p>1a User name:</p> <p>1b Email:</p> <p>1c Mobile number:</p> <p>1d viewLinc PIN:</p>	
<p>2. Verify the test user profile custom 5.2 per Table 9.3-b. If the user does not exist, create it now. Provide user custom 5.2 with a unique email address and record the address.</p>	<p>2a Profile verified? Yes <input type="checkbox"/> No <input type="checkbox"/></p> <p>2b Email:</p>	
<p>3. Edit user custom 5.2 and change the password to Custom52!. Exit viewLinc.</p>	<p>3a New password:</p>	
<p>4. Verify user custom 5.2 is denied access to viewLinc when using password Test123!.</p>	<p>4a Access denied? Yes <input type="checkbox"/> No <input type="checkbox"/></p>	

9.3 User Creation and Password Verification		
Test Instructions	Actual Results	Initials / Date
5. Verify user custom 5.2 is granted access to viewLinc when using password Custom52! .	5a Access granted? Yes <input type="checkbox"/> No <input type="checkbox"/>	
6. As user custom 5.2 , change the password for user custom 5.2 to 52Custom! . Logout of viewLinc.	6a New password:	
7. Verify user custom 5.2 is granted access to viewLinc when using password 52Custom! .	7a Access granted? Yes <input type="checkbox"/> No <input type="checkbox"/>	
8. Log in as an administrative user. Attempt to create a new user profile per Table 9.3-b . Verify the following: <ul style="list-style-type: none"> • “User name” field is outlined in red. • The warning “User name already exists” is provided when the cursor is placed on the User name field • The user profile can NOT be saved. 	8a Field outlined in red? Yes <input type="checkbox"/> No <input type="checkbox"/> 8b Warning provided? Yes <input type="checkbox"/> No <input type="checkbox"/> 8c User can NOT be saved? Yes <input type="checkbox"/> No <input type="checkbox"/>	
9. Log in as a user configured for Windows Authentication. <div> <i>i</i> This may be <newadmin> if properly configured. Otherwise, create an additional user for this test. If the Windows Authentication feature will not be used with this viewLinc installation, mark steps 9 through 12 as "N/A". </div>	9a Access granted? Yes <input type="checkbox"/> No <input type="checkbox"/> 9b User name: 9c Password:	
10. Verify that a user configured for Windows Authentication cannot change their user password in viewLinc.	10a Password NOT editable? Yes <input type="checkbox"/> No <input type="checkbox"/>	
11. Using the appropriate Windows tools outside of viewLinc, change the network password for the user recorded in step 9.	11a Password changed? Yes <input type="checkbox"/> No <input type="checkbox"/>	
12. Log in to viewLinc with the username and password for the user recorded in step 9.	12a Access denied? Yes <input type="checkbox"/> No <input type="checkbox"/>	
13. Print and attach the Event Log page(s) that contain the events related to this test.	13a Printout attached? Yes <input type="checkbox"/> No <input type="checkbox"/> 13b Attachment #:	

9.3 User Creation and Password Verification

Test Instructions	Actual Results	Initials / Date
14. Record the Event ID for the following events: <ul style="list-style-type: none">• Step 1: <newadmin> created.• Step 3: Password changed by administrator• Step 5: Login access granted to user "custom 5.2"• Step 6: Password changed by user "custom 5.2"	14a Step 1 Event ID: 14b Step 3 Event ID: 14c Step 5 Event ID: 14d Step 6 Event ID:	
15. Verify each Event Log entry for: <ul style="list-style-type: none">• Event occurred without error.• Includes timestamp• Includes correct user, if applicable.	15a Entries verified? Yes <input type="checkbox"/> No <input type="checkbox"/>	

Comments/Deviations:

Acceptance Criteria Evaluation

User Creation and Password Verification: Users may be created in viewLinc, and the users may access viewLinc when the correct password is provided. Access is denied to users without a correct password. The events were verified by observation and were also captured in the Event Log audit trail.

Acceptance Criteria Met? PASS ☐ FAIL ☐ Initial/Date: _____

Reviewed By: _____ Date: _____

Configuration Tables for User Creation and Password Verification

Table 9.3-a User Profile: <newadmin>


User name	<newadmin>
Full name	<any>
Email	<any accessible address>
Mobile number	<any accessible number>
Send alarm notifications	Always
viewLinc PIN	<any>
Groups	Everyone
Authentication	Windows (if Windows Authentication is utilized at test site, otherwise, viewLinc)
Password	N/A if Windows Authentication is utilized at test site, otherwise, <any>

Table 9.3-b User Profile: custom 5.2

User name	custom 5.2
Full name	<any>
Email	<any accessible address>
Send alarm notifications	Always
Groups	Everyone
Authentication	viewLinc
Must change password on next login	No
Password	Test123!

10. OQ Final Approval

The procedures in this section have been implemented, reviewed, and approved by the individuals listed below. All results have been documented and all deviations have been identified, documented, reviewed, and approved.

 The final approvers should be the same as the original protocol approvers, when available.

Implemented by (signature):		Date:
Name (print):		
Title:		
Company:		
Reviewed by (signature):		Date:
Name (print):		
Title:		
Company:		
Approved by (signature):		Date:
Name (print):		
Title:		
Company:		
QA approved by (signature):		Date:
Name (print):		
Title:		
Company:		

11. Signature ID Form

All personnel assigned to execute or review this executed Protocol, attached deviations, modifications, and/or supporting documentation must sign and initial in the space provided below. In the Title/Affiliation row fill in designated title and company name.

Printed Name	Signature	Title/Affiliation	Initials/Date

Comments:

Implemented
by:

Date:

Reviewed
by:

Date:

12. IQ/OQ Protocol Final Approval

The Vaisala viewLinc Monitoring System has passed all tests, and as such, is qualified to be used in the _____ environment:

Pass/Fail: _____ Initials: _____ Date: _____

Reviewed by (signature):	Initials:	Date:
Name (print):		
Title:		
Company:		
Approved by (signature):	Initials:	Date:
Name (print):		
Title:		
Company:		
QAapproved by (signature):	Initials:	Date:
Name (print):		
Title:		
Company:		