Vaisala Veriteq
Continuous Monitoring System

Installation and Operational Qualification Protocol for Vaisala Veriteq viewLinc Software Version 4.3

Document #:	M211681EN-A
Date Prepared:	March 6, 2014
Prepared by:	Paul Daniel, Sr. Regulatory Compliance Manager
Reviewed by:	Jeff Chesman, Technical Support Representative

PROTOCOL PRE-APPROVAL

This Protocol has been reviewed and approved by the following 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 study. The following responsible functional areas have approved this Installation / Operational Qualification Protocol for the Vaisala Veriteq viewLinc Software Version 4.3:

Approved By:

Information Technology	Date
Operations	Date
Quality Assurance	Date

Disclaimers

- Prior to execution of this Protocol, the following conditions must be met:
  - Devices (Loggers and Transmitters) have been attached to the system either directly via a cable connection or indirectly via a vNet PoE Network Interface or Digi PortServer Ethernet Adaptor.
  - All cables being used that require drivers have been properly installed on the viewLinc Server.
  - All vNet and Digi PortServer Ethernet Adaptors being used have been set up with IP addresses and correct network information, and have had the appropriate drivers installed on the viewLinc Server.
  - All computers used in the Continuous Monitoring System meet the minimum requirements as specified in the viewLinc documentation.
  - The Vaisala Veriteq vLog software has been installed on the viewLinc Server used in this validation. vLog 4.3 or newer is recommended. Using older versions may result in test discrepancies.
- The procedures in this Protocol assume that the default templates have not been changed. If the installation of this software is an upgrade and previous settings are imported, test discrepancies may occur because of changes made to templates in previous versions.
- Administrative permissions to the viewLinc Server are required to complete some sections of this Protocol.
- Unless otherwise specified, the procedures in this Protocol assume that the default five (5) minute sample interval in the Vaisala Veriteq Loggers has not been changed. Test discrepancies may occur if different sample intervals are used.
- The data connection between test Loggers and the viewLinc server must not become disconnected during testing (unless otherwise specified within the test procedure). Test Loggers must contain an adequate amount of data (unless otherwise specified within the test procedure).
- Some Logger Channel types have non-editable descriptions. Procedures requiring the alteration of Channel descriptions may not succeed when performed on a Logger with these Channel types. The Logger and Channel Descriptions of the 300 Series Transmitters are not editable.
- Loggers used in this Protocol must not be linked to vLog audit trails unless specifically required in a test, 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 modification of the system configuration, settings, and templates is highly recommended following validation.

Vaisala
Tel: (604) 273-6850
Fax: (604) 273-2874

Toll-free in North America: 1-888-VAISALA
Email: helpdesk@vaisala.com
Web: www.vaisala.com/en/lifescience

Table of Contents

1 Purpose

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

Note: 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 Qualification Protocol CD in the directory \Qualification Protocol\.

1.1 Installation Qualification

The Installation Qualification (IQ) Protocol was written, executed, and approved to ensure that the system, composed of both the hardware and the software, 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 minimal Quality System elements necessary to support system operation in a GxP environment.

1.2 Operational Qualification

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

2 Responsibilities

2.1 Vendor Responsibilities

Vaisala is responsible for the following:

- IQ/OQ Protocol Template Creation
- Initial Logger Calibration

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 Veriteq Continuous 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 (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 Veriteq viewLinc 4.3 software; Microsoft Windows® based PCs with an approved web browser; Vaisala Veriteq Data Loggers (or Vaisala 140 Series Loggers or Vaisala 300 Series Transmitters); and connectivity cabling.

The Vaisala Veriteq Continuous Monitoring System consists of Server and Client components. For the purposes of the Protocol, a Server is any computer on which the viewLinc software is installed. The Server component is the core of the Continuous 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 see real-time conditions at the points being monitored, or to make configuration changes.

The Continuous Monitoring System supports the use of a variety of Vaisala Devices, including Vaisala Veriteq Loggers, Vaisala 140 Series Wi-Fi Data Loggers and Vaisala 300 Series Transmitters.

The Vaisala Veriteq Continuous Monitoring System also includes user-based security and unique file identifiers for data integrity. The Vaisala Veriteq Continuous Monitoring System allows the end user to set alarm thresholds and notifies the end user(s) visually and via Email to computer, phone, pager, or other mobile messaging devices, when an alarm condition is triggered, acknowledged, or when a Logger communication problem exists. The software has built-in trending and reporting, and can schedule downloads of Logger data (historical data) for later review, graphing, and filing.

4 Objective

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

_____.

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

5 Validation Approach

5.1 Basic Risk Assessment

5.1.1 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.

5.1.2 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 nonconfigured elements.

5.1.3 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 functions will be included in the testing where they impact the operation of these two critical areas.

5.1.4 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.

5.2 Installation Qualification (IQ)

5.2.1 Quality System

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 system documentation and supporting SOPs. Several documentation items to be verified are considered to be customer responsibilities, such as a Monitoring SOP or a Calibration Program, and will not be supplied by Vaisala. Furthermore, this verification is not definitive of all documentation that is appropriate or that should be present.

5.2.2 Hardware

The IQ will document the baseline hardware (Loggers, Transmitters, Ethernet Adaptors, and Servers) associated with the Vaisala Veriteq viewLinc CMS, and the configuration of these items to function on the customer network. 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 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.

5.2.3 Software

The IQ will document the correct installation of the viewLinc software and record critical installation parameters.

5.3 Operational Qualification (OQ)

5.3.1 General

The OQ portion of the IQOQ Protocol documents the correct operation of the Vaisala Veriteq 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.

5.3.2 Risk-Based Approach

Based on the rationale presented in Section 5.1, OQ testing will focus on the two highest risk areas of the system: Data Collection and Alarming.

5.3.3 Data Collection

The correct run-time configuration of the data collection process will be verified in the IQ activities described above. System security pertinent to the data collection configuration and process will be verified in the OQ. Furthermore, the data reporting process and the accuracy of the associated statistics will be verified.

5.3.4 Alarming

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).

5.4 Performance Qualification (PQ) Considerations

5.4.1 The OQ portion 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.

5.5 Other Considerations

5.5.1 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 User's Guide.

5.5.2 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.

5.5.3 From the perspective of the viewLinc system, any single input is identical to another input whether it is derived from a Channel from a Vaisala Veriteq Data Logger, a Vaisala 140 Series 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.

5.5.4 Vaisala Series 140 Loggers are unique among Vaisala devices compatible with viewLinc, as they can store a single high and a single low threshold locally in the Logger memory. This capability ensures local alarming in the event of disconnection of these wireless devices preventing 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 Series 140 Loggers (if applicable). However, since the 140 Series Logger is slaved to the viewLinc Server, it is only considered necessary to test the viewLinc Server functions in this IQOQ. Specific testing of local thresholds in Series 140 Loggers is considered to be performance testing appropriate for a PQ, and therefore out of scope of this IQOQ.

5.5.5 This validation Protocol is written to utilize a pre-existing test configuration that must be input into the viewLinc System prior to beginning OQ testing. The test configuration can be input manually using the configuration document "Test Configuration.doc" as a guide. The test configuration may also be input automatically into the viewLinc System using the executable "Protocol_DB.exe" configuration tool. Both files can be found in the directory \Configuration\ on the Qualification Protocol CD. Instructions for inputting the test configuration into the system are included in the test procedure for Section 8.3.

5.5.6 Before testing involving Locations can occur, the Locations created via the validation test configuration must be linked to Channels and Devices on the viewLinc System. Linkage instructions are included in the test procedures in Sections 8.3 and 8.23.

Note: Depending on device type, one or two connected devices will be required to complete the testing described in this Protocol. For more information, refer to 5.5.7.1 and 5.5.8.3 below.

5.5.7 The Location Alarm Test is created when the validation test configuration is utilized. This Location must be linked to a temperature Channel on an existing Device on the viewLinc System. This Location is referenced in the majority of the OQ Test Sections, except Section 8.22 and Section 8.23.

5.5.7.1 Only a single device with a temperature Channel is required for the majority of the testing in this Protocol. The temperature Channel must be configured to display Celsius.

5.5.7.2 The instructions for linking the Location Alarm Test are provided in the test procedures for Section 8.3.

5.5.8 In the final OQ Test Sections (Section 8.22 and Section 8.23), Location A and Location B are utilized. These Locations are created when the validation test configuration is utilized and must be linked to Channels on existing Devices on the viewLinc System. Location A and Location B are referenced only in Section 8.22 and Section 8.23.

5.5.8.1 Instructions for linking the Location A and Location B are provided in the test procedures for Section 8.22.

5.5.8.2 Provided that all other OQ tests are completed, these Locations may be linked to the device that may have been used for the Location Alarm Test, described previously.

5.5.8.3 If the devices used have only one Channel per device, a minimum of two devices will be required. If using Vaisala Veriteq VL-2000 Loggers, or other two Channel Loggers, only a single device will be required.

5.5.9 In this Protocol, bold text is used to refer to items and text that are visible on the viewLinc interface, such as windows, panes, buttons, and names of Locations, etc. Navigation instructions are provided in bold with arrows to indicate navigation to deeper menu levels, such as **Options > System Configuration > Locations Manager** to open the **Locations Manager** window. If the command string is preceded by a name and a colon, such as **Device Browser: Options > Expand All Devices**, this indicates that the commands should take place on a specific pane (in this case, the **Device Browser** pane) of the current window.

5.5.10 The computer used to access the viewLinc system for execution of this Protocol must have specific software installed. Refer to the viewLinc User's Guide for a comprehensive list of compatible software. The following software is required:

- A viewLinc compatible web browser.
- A spreadsheet application, such as Excel, capable of opening .csv files.
- A PDF reader application, such as Adobe Reader, capable of opening .pdf files.

6 Documentation Procedures

6.1 Data generated during the execution of this Protocol will be collected and recorded on the data sheets provided.

6.2 During the execution, the executor's initials and date will be provided at the time of completion for each activity.

6.3 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.

6.4 Charts, printout, notes etc. generated during the execution will be dated, signed, and attached to the completed Protocol document.

6.5 All test sections will be reviewed and signed by appropriate _____ personnel to verify document completeness.

6.6 The IQ Test Sections of the document should be completed prior to beginning the OQ Test Sections, with the following exceptions:

6.6.1 Completion of IQ Test **Section 7.2 – Vaisala Documentation** is not required prior to initiating OQ tests.

6.6.2 Completion of IQ Test **Section 7.3 – Customer Quality System Documentation** is not required prior to initiating OQ tests.

6.6.3 Completion of IQ Test **Section 7.9 – Calibration Verification** is not required prior to initiating OQ tests.

6.6.4 Completion of IQ Test **Section 7.10 – IQ Final Approval** is not required prior to initiating OQ tests.

6.7 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. However, if necessary, the following Test Sections may be performed out of sequence:

6.7.1 Section 8.12 – 140 Series Logger Local Threshold Validation

6.7.2 Section 8.18 – System Watchdog

6.7.3 Section 8.19 – Preferences Security Testing

6.7.4 Section 8.20 –Historical Database Validation

6.7.5 Section 8.21 –Rights Testing

6.8 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.

6.9 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, etc.

6.10 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 (e.g., M211681EN-A), reference section and step (e.g., Step 8.6.12, or Section 8.6, Step 12), total number of pages (e.g., 6 pages), and the Date/Initial of the test executor.

6.11 Protocol Definitions

6.11.1 A discrepancy is defined as a difference between the expected results and the actual results.

6.11.2 An exception is defined as a difference between the approved Protocol procedure and the procedure followed in testing.

6.11.3 A deviation is defined as a discrepancy or exception that prevents meeting the acceptance criteria.

6.11.4 Discrepancies, exceptions, and deviations to approved Protocols may occur. It is the responsibility of the 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 SOP for Deviation Reporting (if applicable).

6.11.5 Deviations, exceptions, and discrepancies must be approved by the Quality Assurance group according to current standard operating procedures, prior to any further execution of the Protocol test section in which the deviation occurred.

7 INSTALLATION QUALIFICATION

7.1 Test Plan

Testing will be performed to verify that the installation of the Vaisala Veriteq Continuous Monitoring System is in conformance with manufacturer's specifications and customer requirements. The test plan consists of eight sections. These are:

7.1.1 Vaisala Documentation

This section will verify the presence of the vendor documentation necessary to properly operate, administer, and maintain the viewLinc system.

7.1.2 Customer Quality System Documentation

This section will verify the presence of the customer Quality System documentation suggested for proper GMP operation, administration, and maintenance of the viewLinc system.

7.1.3 Server Hardware Requirements and Configuration

This section will verify that the computer selected for the role of viewLinc Server (and additional Hosts, if applicable) meets the hardware requirements of the Vaisala Veriteq Continuous Monitoring System.

7.1.4 Software Installation Verification

This section will verify that the Vaisala Veriteq viewLinc Software is properly installed on the viewLinc Server.

7.1.5 Email Configuration Verification

This section will verify that Email settings of the viewLinc Server are properly configured for successful Email notifications.

7.1.6 SMS Configuration Verification

This section will verify that SMS settings of the viewLinc Server are properly configured for successful SMS notifications.

7.1.7 System Hardware Configuration

This section will capture the baseline hardware configuration of the viewLinc System.

7.1.8 Calibration Verification

This section will verify that the Vaisala Data Loggers and Transmitters connected to the viewLinc System are calibrated.

7.4 Server Hardware Requirements and Configuration

Record the specified information for the computer to be used as a Server in the Vaisala Veriteq viewLinc Continuous Monitoring System. Compare the Hardware Specifications and Operating System against the requirements listed in the table below. It may be necessary to consult with the facility IT Department to obtain the information requested in this test section.

Note 1: This form may be duplicated if there are Logger Hosts or Multiple servers in use in this installation. If this form is duplicated, follow the guidelines in Section 6 for labeling duplicate pages.

Note 2: The information requested in Steps 1, 2, 5 and 6 may be found in the System area of the Control Panel menu of the viewLinc Server.

Step	Procedure	Expected Results	Are actual results as expected? Initials/Date
7.4.1	Record the Full Name and Domain of the viewLinc Server. Server Full Name: _____ Server Domain: _____	The Full Name and Domain of the viewLinc Server has been recorded.	
7.4.2	Record the Operating System of the viewLinc Server. Operating System: _____	The Operating System of the viewLinc Server has been recorded. The Operating System is MS Windows 7 (SP1, 32 or 64-bit), Server 2003 (SP2, 32-bit), Server 2008 (SP3, 64-bit) or Server 2012 (64-bit).	
7.4.3	Record the number of Locations (Channels) to be installed on the viewLinc system. Number of Locations: _____ Determine the size of the viewLinc installation by circling the corresponding size indicator: Small: <20 Locations Medium: 20 to 400 Locations Large: > 400 Locations	The number of Locations (Channels) to be installed on the viewLinc system has been recorded. The number of Locations was used to determine installation size.	
7.4.4	Determine if the viewLinc server will be dedicated to viewLinc only, or if it will be shared with other applications. Circle the appropriate value below: DEDICATED SERVER / SHARED SERVER	The required parameter for the viewLinc Server has been recorded. The parameter is appropriate for the size of the installation. · Small/Medium: Server may be SHARED. · Large: Server must be DEDICATED.	

Step	Procedure	Expected Results	Are actual results as expected? Initials/Date
7.4.5	Record the CPU Speed and CPU Core Type of the viewLinc Server. CPU Speed: _____ Core Value (Quad/Dual/Single): _____	The CPU Speed and CPU Core Type of the viewLinc Server have been recorded. The recorded CPU Speed and CPU Core Type meet or exceed the minimum value for the size of the installation. Small: 1.6 GHz Single Core Medium: 1.6 GHz Dual Core Large: 3.2 GHz Quad Core	
7.4.6	Record the amount of installed memory (RAM) for the viewLinc Server. RAM: _____	The installed memory (RAM) of the viewLinc Server has been recorded. The recorded RAM exceeds the minimum value for the size of the installation. Small: 2 GB RAM Medium: 4 GB RAM Large: 4 GB RAM	
7.4.7	Record the Application Install Drive and amount of Free Disk Space in the Application Install Drive for the viewLinc Server. Application Install Drive: _____ Free Disk Space: _____	The Application Install Drive and amount of Free Disk Space in the Application Install Drive for the viewLinc Server has been recorded. The recorded Free Disk Space exceeds 350 MB.	
7.4.8	Record the Database Drive and amount of Free Disk Space in the Application Database Drive for the viewLinc Server. Application Database Drive: _____ Actual Free Disk Space: _____	The Application Database Drive and amount of Actual Free Disk Space in the Application Database Drive for the viewLinc Server has been recorded. The Actual Free Disk Space in the Application Database Drive exceeds the following calculated value: (# of Locations) x (75 MB/Location/Year): _____MB/Year	

Step	Procedure	Expected Results	Are actual results as expected? Initials/Date
7.4.9	Record the following network configuration information for the viewLinc Server: MAC Address: _____ IP Address: _____ IP Address is (circle one): DYNAMIC / STATIC	The requested network configuration information for the viewLinc Server has been recorded. **Note**: Use the DOS commands **getmac** and **ipconfig** in a Windows command box on the viewLinc Server to determine the MAC and IP addresses, respectively. Otherwise, consult the facility IT Department.	

Comments/Deviations: _____

Acceptance Criteria: The viewLinc Server (and any viewLinc Device Hosts) meets the hardware and operating environment requirements specified in the test steps.

Acceptance Criteria Met? Pass/Fail: _____ Initials/Date: _____/_____

Reviewed by: _____ Date: _____

8 OPERATIONAL QUALIFICATION

8.1 Test Plan

Testing will be performed to verify that the operation of the Vaisala Veriteq Continuous Monitoring System is in conformance with manufacturer's specifications and customer requirements. The Acceptance Criteria for all sections are derived from Vaisala's recommendations. The test plan will consist of twenty-two areas of functionality as defined below.

8.1.1 System Event Log Validation

All system and user actions are recorded within the Events section of the Continuous Monitoring System. Where applicable, test sections in the OQ include verification that the representative events from the test procedure are captured accurately within the Events Log. This test will verify that the Event Log is tamper-proof and that any alterations to the Event Log generate an alarm.

8.1.2 Test Configuration Setup

This validation Protocol is written to utilize a pre-existing test configuration that must be input into the viewLinc System prior to beginning OQ tests involving Locations. This test section provides the instruction necessary to configure the system for validation testing.

8.1.3 User Creation

This test will verify that system users can be created in the viewLinc software and can be assigned various system rights, group memberships, authentication types, and notification schedules, depending on their needs.

8.1.4 Group Management

This test will verify that groups can be created in the viewLinc software and assigned various system rights. Furthermore, it will be demonstrated that users may be assigned to groups depending on their needs.

8.1.5 Changing Passwords

This test will verify that Users with Rights to Manage Users can change the passwords & authentication types of other users. Furthermore, it will be demonstrated that Users who do not have the Manage Users Right, can change their viewLinc passwords, but not their Windows password or authentication type.

8.1.6 High Alarm Testing

This test will verify the Vaisala Veriteq Continuous Monitoring System's High Threshold Alarm functionality. A private threshold is configured containing representative variables for parameters such as color codes, messages, delays, notifications and comments. The alarm condition is simulated and the response of the system to the alarm condition verified.

8.1.7 Low Alarm Testing

This test will verify the Vaisala Veriteq Continuous Monitoring System's Low Threshold Alarm functionality. A saved Threshold Template and associated Alarm Template are used containing representative variables for parameters such as color codes, messages, delays, notifications and comments. The alarm condition is simulated and the response of the system to the alarm condition verified, including schedules for multiple users.

8.1.8 Alarm Template Modification

Threshold Templates may be directed to leverage an Alarm Template in lieu of entering alarm response parameters directly into the Threshold Template. This test will verify that selecting a new Alarm Template for an existing Threshold Template will update the settings for thresholds on individual Locations which utilize the same Threshold Template.

8.1.9 Threshold Schedule Verification

This test will verify the threshold alarm scheduling functions of the viewLinc software by editing the schedule and verifying that alarming function follows the defined schedule parameters.

8.1.10 Multi-Threshold Alarm Verification

This test will verify that the multi-threshold alarm of the Vaisala Veriteq viewLinc software functions as intended.

8.1.11 Vaisala 140 Series Logger Local Threshold Validation

This test will verify the viewLinc software may be used to set local thresholds on Vaisala 140 Series Loggers by editing the Channel properties of a compatible device. Furthermore, this test will verify that thresholds set on Locations can be directly uploaded to a Channel of a compatible device.

8.1.12 Communication Alarm Testing

This test will verify the Vaisala Veriteq Continuous Monitoring System's Communication Alarm functionality. The system default Communication alarm template containing variables for parameters such as color codes, messages, delays, notifications and comments, is challenged in this test. The alarm condition is simulated by removing a device from the system and the response of the system to the alarm condition verified.

8.1.13 Device Configuration Alarm Testing

This test validates that the Logger is actively collecting historical data within its on-board memory. Each Logger transmits both recorded and real-time readings to the system on each update, allowing for multiple sample points per update. Should the Historical logging fail internally, a configuration alarm will be generated for that Logger, and sent to the Administrator for system alert.

8.1.14 Location History Report Verification

The viewLinc system allows reports to be generated listing historical data from monitored Locations. Reports may be configured for instantaneous or scheduled generation. They may be further configured to define what Locations are included in the report and what types of data are included in the report, such as statistics calculations, raw data, trend graphs, etc. This test will verify that a representative report can be generated by the system in both a .pdf format and a format readable by Microsoft Excel.

8.1.15 Location History Statistical Validation

Location History Reports generated in viewLinc optionally include various statistics calculated from the historical samples. This test will verify the accuracy of the statistics

calculations in viewLinc through direct comparison to the equivalent statistics calculated by Microsoft Excel utilizing the same data set.

8.1.16 Time Zone Validation

The viewLinc software is designed to accommodate use across multiple time zones. The clock and time zone of the viewLinc Server as a master clock for all data. However, each log in session is automatically adjusted to the time zone of the Client. Reports, regardless of the Client time zone, will default to the time zone of the viewLinc Server, but may be set to report in any time zone. This test will verify the ability of the viewLinc software to correctly identify the Client time zone. Furthermore, this test will verify that reports can be generated in any time zone, correctly labeled for time zone, and with properly adjusted timestamps.

8.1.17 System Watchdog

The viewLinc system has an auto-recovery feature known as the System Watchdog Service, which monitors the viewLinc application and restarts it in the event of a problem. This test will verify the operation of the System Watchdog. The viewLinc service will be stopped to simulate a failure with the viewLinc application.

8.1.18 Preferences Security Testing

Among viewLinc Preference settings are two settings that can increase security and transparency within the database. The system may be set to require comments for all changes and to require repeat user authentication at intervals. This test section will verify that the security preferences in viewLinc can be configured and operate as intended.

8.1.19 Historical Database Validation

The viewLinc database is considered to be ‘tamper-proof’. Attempts to alter the data make the system inaccessible, thereby preventing any changes to the records. The system must be restored to an earlier data backup before the system can be accessed. This test section will verify the operation of the system functions that prevent tampering of the database.

8.1.20 Rights Testing

Access control within viewLinc is based on Rights. Rights may be assigned to individual users, or may be assigned to groups which may include any number of individuals. This test section will verify that each access Right in viewLinc provides only the intended Rights and no others, whether assigned to an individual or a group.

8.1.21 Permissions Testing - Users

Access control within viewLinc may be further refined by using Access Control permission which provides a user or a group with permissions to individual Zones, Locations and Views. This test section will verify that each permission level in viewLinc provides only the intended abilities and no others, when assigned to an individual user.

8.1.22 Permissions Testing - Groups

Access control within viewLinc may be further refined by using Access Control permission which provides a user or a group with permissions to individual Zones, Locations and Views. This test section will verify that each permission level in viewLinc provides only the intended abilities and no others, when assigned to a group.

8.2 System Event Log Validation

The viewLinc software checks each of the log entries of each Event generated. Any modification to the Event Log renders that single entry invalid, and changes the Record status to either **missing** or **Invalid Checksum**. This test will be performed with the administrative user, admin.

Follow the steps below to ensure that any modification is presented to the user as a modification alert and emailed to the administrator.

Note: If this is a fresh installation of viewLinc 4.3, or an upgrade from a viewLinc version earlier than 3.4, start at Step 1. If this is an upgrade from viewLinc 3.4, 3.5, or 3.6, start at Step 5. Mark all unused spaces, 'N/A'.

Step	Procedure	Expected Results	Are actual results as expected? Initials/Date
8.2.1	Click **Options > Events**. Record the Event Log Report Status from the status bar located beneath the **Events: Options** button. Status:_____	The **Events** page opens. The Event Log Report Status has been recorded. (If the status is **CORRUPTED**, continue to Step 2. If the status is **VALID**, continue to Step 5. Mark all unused spaces 'N/A'.)	
8.2.2	Click **Options > Alarms**. In the alarm listing, locate and highlight an alarm with the Description, '**Event Validation Alarm: Default Event Validation Alarm for Event Logging System'**.	The **Alarms** page opens. The specified alarm is located and highlighted.	
8.2.3	Click **Alarms: Options > Acknowledge**. Type **Event Log alarm acknowledged** in the **Action Taken** field. Enter, **This alarm was triggered as a normal part of the installation process** in the **Comments** field.	The **Acknowledge Alarms** dialog box appears and the rest of the interface is grayed out. The **Action Taken** field displays a value of **Event Log alarm acknowledged.** The **Comments** field displays a value of **This alarm was triggered as a normal part of the installation process**.	
8.2.4	Click the **Save** button.	The **Acknowledge Alarms** dialog box disappears and you are returned to **Alarms** window.	
8.2.5	Click **Options > System Configuration > Templates > Alarm Templates**. Highlight the **Default Event Validation Alarm** in the template listing on the left side of the screen.	The **Alarm Templates** window opens. The specified template is highlighted. The details for the template **Default Event Validation Alarm** are displayed in the right pane of the window.	
8.2.6	Click the **Notifications** tab, and click **Add > Add Email Notification**. In the **Send Email to:** field, enter a valid tester accessible Email address. Click **Alarm Templates: Options > Save**.	The tester accessible Email address entered in the **Send Email to:** field. **Default Event Validation Alarm** template is saved with the new address.	

Step	Procedure	Expected Results	Are actual results as expected? Initials/Date
8.2.7	Log in to the viewLinc Server as an administrator. Open the Windows Services control panel (see IQ Section “Software Installation Verification”) and STOP both the viewLinc Watchdog and the viewLinc Enterprise Server services.	The viewLinc services stop.	
8.2.8	Navigate to the viewLinc Log folder (C:\Users\Public\Public Documents\Vaisala\Vaisala Veriteq viewLinc\log by default). Locate the **Events** folder and make a copy and save it to the same Location with the name, **Events Backup**.	The **Events** folder is located and copied. The copied folder is named **Events Backup**.	
8.2.9	Open the original **Events** folder and locate the file, **Events-<current year>** (file type SQLITE file).	The specified file is identified.	
8.2.10	Open the **Events-<current year>** file with Microsoft Notepad. Edit the file by deleting or adding text. Save the file.	The specified file is opened with Microsoft Notepad. The specified file is edited and saved.	
8.2.11	Return to the Windows Services control panel and start both viewLinc Watchdog and the viewLinc Enterprise Server services.	The viewLinc Watchdog and the viewLinc Enterprise Server services start.	
8.2.12	Log in to viewLinc. Click **Options > Events**. Record the Event Log Report Status from the status bar located beneath the **Events: Options** button. Status:_____	The **Events** page opens. The **Event Log Report Status** is **CORRUPTED**.	
8.2.13	Click **Options > Alarms**. In the alarm listing, locate and highlight an alarm with the Description, **Event Validation Alarm: Default Event Validation Alarm for Event Logging System**.	The **Alarms** page opens. An **Event Validation Alarm: Default Event Validation Alarm for Event Logging System** alarm is displayed.	

Step	Procedure	Expected Results	Are actual results as expected? Initials/Date
8.2.14	Click **Alarms: Options > Acknowledge**. Type **Log Validation alarm acknowledged** in the **Action Taken** field. Type **This alarm was triggered as part of the validation process** in the **Comments** field.	The **Acknowledge Alarms** dialog box appears and the rest of the interface is grayed out. The **Action Taken** field displays a value of **Log Validation alarm acknowledged.** The **Comments** field displays a value of **This alarm was triggered as part of the validation process**.	
8.2.15	Click the **Save** button.	The **Acknowledge Alarms** dialog box disappears and you are returned to **Alarms** window.	
8.2.16	Return to the **Events** window. Record the Event Log Report Status from the status bar located beneath the **Events: Options** button. Status:_____	The **Events** page opens. The Event Log Report Status is **Valid**.	
8.2.17	Open the **Events** window, and filter the Event Log for **System** and **Alarm Events**, and locate the entries that correspond to the following events and record the corresponding Event ID(s) : Activation of the Default Event Validation Alarm Event ID:_____ Email sent to the Administrator regarding the alarm. Event ID:_____ Event validation Alarm acknowledged. Event ID:_____ Print the appropriate page of events and attach it to the Protocol.	The Event Log entries for the specified events were identified and the corresponding Event ID(s) recorded. Each referenced Event Log entry indicates that the specified event occurred without error, displays the date/time of the event, and references the correct user.	
8.2.18	Return to the Windows Services control panel and STOP the viewLinc Watchdog service and the viewLinc Enterprise Server service.	The viewLinc services STOP.	
8.2.19	Return to Windows Explorer and navigate to the viewLinc Event Log folder location. Locate the **Events** folder and delete it.	The **Events** folder is located and deleted.	

Step	Procedure	Expected Results	Are actual results as expected? Initials/Date
8.2.20	Locate the **Events Backup** folder in the viewLinc **log** folder location. Rename the folder **Events**.	The folder **Events Backup** is located in the viewLinc data folder location and renamed **Events**.	
8.2.21	Return to the Windows Services control panel and start both viewLinc Watchdog and the viewLinc Enterprise Server services.	The viewLinc Watchdog and the viewLinc Enterprise Server services start.	
8.2.22	Log in to viewLinc. Click **Options > Alarms**. Acknowledge any **Event Validation** or **Configuration Changed** alarms present in the system.	The **Alarms** page opens. The specified alarm events are acknowledged, if present.	
8.2.23	From the **Locations Manager** window, right-click the root zone folder and select **Add Location** from the drop-down menu. Name the new Location and record the Location Name. Location Name: _____ Click **Locations: Options > Save**.	A new Location is created and the Location Name recorded. The action is saved.	
8.2.24	Right click the Location created in the previous step and select **Edit** from the drop-down menu. Edit the name of the selected Location and click **OK**. Record the new name. New Name: _____	The **Edit Location** dialog box appears. The **Edit Location** dialog box disappears. The new name appears for the Location in the **Locations Tree.**	
8.2.25	Click **Locations: Options > Save**. Record the time. Date/Time: _____	The save is performed and the time is recorded.	
8.2.26	Open the **Events** window, and filter the Event Log for all event types. Locate the entry that corresponds to the 'save' event in the previous step. Record the corresponding Event ID and the time stamp value: Event ID:_____ Timestamp:_____ Print the appropriate page of events and attach it to the Protocol.	The Event Log entry for the specified event was identified and the corresponding Event ID and timestamp recorded. The timestamp for the Event is consistent with the time value recorded in the previous step. Each referenced Event Log entry indicates that the specified event occurred without error, displays the date/time of the event, and references the correct user. The Event Log entry also displays the original name and the new name for the Location used in the test.	

Step	Procedure	Expected Results	Are actual results as expected? Initials/Date
8.2.27	Return to the **Locations Manager** window. Right-click the Location created in the previous steps and select **Permanently Delete Location** from the drop-down menu. Confirm the dialog box, then click **Locations: Options > Save**.	The Location created in the previous steps is deleted and the change is saved.	

Comments/Deviations: _____

_____

_____

_____

Acceptance Criteria: The event log was successfully corrupted, rendering the Event Log Report Status as Corrupt. The corrupted events were identified in the event log, an Email alert is sent to the system Administrator to notify of the issue, and an alarm generated in the Alarms window. Acknowledging the alarm returned the Event Log Report Status to a state of Valid. Furthermore, the 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: _____ Initials/Date: _____/_____

Reviewed by: _____ Date: _____

8.23 Permissions Testing – Groups

Access control within viewLinc may be further refined by using Access Control permissions which provide a user or a group with permissions to individual Zones, Locations and Views. This test section will verify that each permission level in viewLinc provides only the intended abilities and no others, when assigned to a group. This test will be started with the administrative user, <newadmin>. When prompted to log in as a different user, the password will be the same as the username.

Step	Procedure	Expected Results	Are actual results as expected? Initials/Date
8.23.1	Click **Options > System Configuration > Locations Manager**	**Locations Manager** window opens.	
8.23.2	Locate the existing thresholds for Location A and Location B and verify that they are enabled. If they are not enabled, enable them now.	The thresholds for Location A and Location B are enabled as specified.	
8.23.3	Click **Options > Alarms**. Wait for any necessary alarm delays.	The **Alarms** window opens. Location A and Location B are in active threshold alarm.	
8.23.4	Click **Options > Logout**.	User <newadmin> logs out.	
8.23.5	Log in as user adam. Click **Options > Alarms**. Highlight the threshold alarm listing for the Location associated with Location A and click **Alarms: Options > Acknowledge**.	The **Alarms** window opens. When the specified alarm is highlighted, the Acknowledge option is available in the drop-down menu.	
8.23.6	Do not acknowledge the alarm. Click **Cancel**.	**Acknowledge Alarms** dialog box disappears.	
8.23.7	Click **Options > System Configuration > Locations Manager** window. In the **Locations** pane, highlight Location A (in Zone A). Click the **Thresholds** tab. In the Thresholds tab, and click the **Options** button and select **Create <unit> Threshold** from the drop-down menu.	The **Locations Manager** window opens. Location A highlighted. **Thresholds** tab pane is displayed. The **Create <unit> Threshold** button is not available in the drop-down menu.	
8.23.8	Highlight Location B (in Zone B). Click the **Thresholds** tab. In the **Thresholds** tab, and click the **Options** button and select **Create <unit> Threshold** from the drop-down menu.	Location B highlighted. **Thresholds** tab pane is displayed. Edit Threshold window opens.	
8.23.9	Do not create a threshold. Click **Edit Threshold: Options > Cancel**.	**Edit Threshold** window disappears.	

Step	Procedure	Expected Results	Are actual results as expected? Initials/Date
8.23.10	Click **Options > Locations**. Highlight Location B in Zone B in the Zone tree. Right-click Location B. Select **Pause Threshold Alarming** from the drop-down menu.	The **Locations** window opens. Location B highlighted. The Pause Threshold Alarming button is not accessible in the drop-down menu.	
8.23.11	Click **Options > Logout**. Click **Yes** in the **Confirm logout** dialog box.	User adam is logged out.	
8.23.12	Log in as user brad. Click **Options > Alarms**. Highlight the threshold alarm listing for Location A and click **Alarms: Options > Acknowledge**.	The **Alarms** window opens. When the specified alarm is highlighted, the Acknowledge option is not accessible in the drop-down menu.	
8.23.13	Highlight the threshold alarm listing for Location B and click **Alarms: Options > Acknowledge**.	When the specified alarm is highlighted, the Acknowledge option is available to user brad. **Acknowledge Alarms** dialog box appears.	
8.23.14	Do not acknowledge the alarm. Click **Cancel**.	**Acknowledge Alarms** dialog box disappears.	
8.23.15	Click **Options > System Configuration > Locations Manager** window. In the **Locations** pane, highlight Location A (in Zone A).	The **Locations Manager** window opens. Zone A and Location A are visible to user brad.	
8.23.16	Highlight Location B (in Zone B). Click the **Thresholds** tab. In the Thresholds tab, click the **Options** button and select **Create <unit> Threshold** from the drop-down menu.	Location B highlighted. **Thresholds** tab pane is displayed. The **Create <unit> Threshold** option is not available in the drop-down menu.	
8.23.17	Click **Options > Logout**. Click **Yes** in the **Confirm logout** dialog box.	User brad is logged out.	
8.23.18	Log in as user chuck. Click **Options > System Configuration > Locations Manager**. Highlight Location A in Zone A in the Zone tree.	The **Locations Manager** window opens. Zone A is not visible to user chuck.	
8.23.19	Highlight Location B in Zone B in the Zone tree.	Zone B and Location B are visible to user chuck.	

Step	Procedure	Expected Results	Are actual results as expected? Initials/Date
8.23.20	Click **Options > Alarms**. Highlight the threshold alarm listing Location B and click **Alarms: Options > Acknowledge**.	The **Alarms** window opens. When the specified alarm is highlighted, the Acknowledge option is not accessible in the drop-down menu.	
8.23.21	Click **Options > Logout**. Click **Yes** in the Confirm logout dialog box.	User chuck is logged out.	
8.23.22	Log in as user donald. Click **Options > System Configuration > Locations Manager**. Highlight Location B in Zone B in the Zone tree.	The **Locations Manager** window opens. Location B is not visible to user donald.	
8.23.23	Highlight Zone A in the Zone tree. Right-click **Zone A**. Select **Rename** from the drop-down menu.	Zone A is highlighted. A text entry box appears on the selected Zone.	
8.23.24	Do not rename the zone. Click **Options > Logout**. Click **Yes** in the **Confirm logout** dialog box.	User donald is logged out.	
8.23.25	Log in as user earl. Click **Options > Locations**. Highlight Zone A in the Zone tree. Right-click **Zone A**. Select **Pause Threshold Alarming** from the drop-down menu.	The **Locations window** opens. Zone A is highlighted. The **Pause Threshold Alarming** dialog box appears.	
8.23.26	Do not pause alarming. Click **Cancel**.	**Pause Threshold Alarming** dialog box disappears.	
8.23.27	Click **Options > System Configuration > Locations Manager**. Right-click **Zone A**. Select **Rename** from the drop-down menu.	The Rename function is not accessible in the drop-down menu.	
8.23.28	Highlight Location B in Zone B in the Zone tree. Right-click **Location B**. Select **Edit** from the drop-down menu.	Location B is highlighted. The **Edit Location** dialog box appears.	
8.23.29	Do not edit the Location. Click **Cancel**.	**Edit Location** dialog box disappears.	
8.23.30	Click **Options > Logout**. Click **Yes** in the **Confirm logout** dialog box.	User earl is logged out.	

Step	Procedure	Expected Results	Are actual results as expected? Initials/Date
8.23.31	Log in as user fred. Click **Options > System Configuration > Locations Manager**. Highlight Location A in Zone A in the Locations pane. Click the **Thresholds** tab. In the **Thresholds** tab, click the **Options** button and select **Create <unit> Threshold** from the drop-down menu.	The **Locations Manager** window opens. Location A is highlighted. Thresholds tab pane is displayed. **Edit Threshold** window opens.	
8.23.32	Do not create a threshold. Click **Edit Threshold: Options > Cancel**.	**Edit Threshold** window disappears.	
8.23.33	Right-click **Zone B**. Select Rename from the drop-down menu.	The Rename function is not accessible in the drop-down menu.	
8.23.34	Click **Options > Locations**. Right-click **Zone A**. Select **Pause Threshold Alarming** from the drop-down menu.	The **Locations** window opens. The Pause Threshold Alarming selection is not accessible in the drop-down menu.	
8.23.35	Highlight Location B in Zone B in the Zone tree. Right-click **Location B**. Select **Pause Threshold Alarming** from the drop-down menu.	The Pause Threshold Alarming selection is available in the drop-down menu. **Pause Threshold Alarming** dialog box appears.	
8.23.36	Do not pause alarming. Click **Cancel**.	**Pause Threshold Alarming** dialog box disappears.	
8.23.37	Click **Options > Logout**. Click **Yes** in the **Confirm logout** dialog box.	User fred is logged out.	

Comments/Deviations: _____

_____

_____

_____

Acceptance Criteria: The Access Control permissions in viewLinc can be used to provide a group with permissions to individual Zones and Locations. Each permission level, when assigned to a group, provides the group members with only the intended abilities and no others.

Acceptance Criteria Met? Pass/Fail: _____ Initials/Date: _____/_____

Reviewed by: _____ Date: _____

8.24 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.

Note: The Final Approvers should be the same as the original Protocol Approvers, when available.

Implemented by: _____ Initials: _____ Date: _____

Name (Print): _____

Title: _____

Company: _____

Reviewed by: _____ Initials: _____ Date: _____

Name (Print): _____

Title: _____

Company: _____

Approved by: _____ Initials: _____ Date: _____

Name (Print): _____

Title: _____

Company: _____

QA Approved by: _____ Initials: _____ Date: _____

Name (Print): _____

Title: _____

Company: _____

9 Signature Identification 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. **Signature also indicates the individual has read and understands the protocol prior to task execution**. In the affiliation and title column fill in company name and designated title.

Printed Name	Signature	Title/Affiliation	Initials/Date

Comments/Deviations: _____

_____

_____

_____

Implemented by: _____ Date: _____

Reviewed by: _____ Date: _____

10 IQ/OQ DOCUMENT FINAL APPROVAL

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

Pass/Fail: _____ Initials: _____ Date: _____

Reviewed by: _____ Initials _____ Date: _____

Name (Print): _____

Title: _____

Company: _____

Approved by: _____ Initials _____ Date: _____

Name (Print): _____

Title: _____

Company: _____

QA Approved by: _____ Initials _____ Date: _____

Name (Print): _____

Title: _____

Company: _____