Innotech Service & Event Analyser

INSTALLATION INSTRUCTIONS

INNOTECH®

Proprietary

Trademark

The term ‘Innotech’ used in this manual is a trademark of Mass Electronics Pty Ltd trading as Innotech Control Systems Australia.

'Microsoft' and 'Windows' are registered trademarks of Microsoft Corporation in the United States and other countries.

Disclaimer

While great efforts have been made to assure the accuracy and clarity of this document, Mass Electronics Pty Ltd assumes no liability resulting from any omissions in this document, or from misuse of the information obtained herein. The information in this document has been carefully checked and is believed to be entirely reliable with all of the necessary information included. Mass Electronics Pty Ltd reserves the right to make changes to any products described herein to improve reliability, function, or design, and reserves the right to revise this document and make changes from time to time in content hereof with no obligation to notify any persons of revisions or changes. Mass Electronics Pty Ltd does not assume any liability arising out of the application or any use of any product or circuit described herein; neither does it convey licence under its patent rights or the rights of others.

Document Management

Document Title: Innotech® Service and Event Analyser Installation Instructions

Revision History

Version Number	Date	Summary of Changes
1.0	December 2011	First Version of Document
1.1	February 2012	Added details for starting and stopping the iSEA service
1.2	September 2012	Document Updated for iSEA v1.1
2.0	April 2013	Document Updated for iSEA v2.0. Added details for new Configuration, Virtual Points and Notification windows
3.0	November 2013	Document style update, contact details update
3.1	March 2014	Updated for iSEA v2.1
3.2	June 2014	Updated for iSEA v2.2
3.3	April 2016	Updated for iSEA v2.3
3.4	July 2017	Updated for iSEA v2.4
3.5	February 2020	Updated for iSEA v2.5, removed Chronicle dongle references

Contents

Innotech Service & Event Analyser

INSTALLATION INSTRUCTIONS

1 Preliminary Information

INNOTECH®

1-1 Introduction

This manual is intended to provide the customer with complete and comprehensive documentation to set up and configure the Innotech Service and Event Analyser (iSEA) on a Building Management System (BMS) computer.

iSEA is a Windows® based application that resides in the system tray. Its main purpose is to provide notifications to the user of events that occur in Innotech Service based applications that may not have a dedicated application status monitoring tool, such as Chronicle Server. It also facilitates restarting Innotech services if they are unexpectedly terminated, in order to reduce the need for human intervention.

Customers should familiarise themselves with the content of this manual before attempting installation and setup of iSEA on their computer.

Throughout this manual there are icons to illustrate notes and points of caution, as illustrated below:

These notices indicate a piece of useful information which should be read.

IMPORTANT

*These notices contain information about the software that **must be done** before proceeding further to ensure success.*

1-1.1 Systems Covered by this Manual

The manual covers the preparation and configuration of iSEA and its features for use with the Innotech Chronicle and iComm server programs.

1-1.2 Scope of this Technical Manual

This technical manual contains the following Chapters:

Table 1-1: Chapter List

Chapter Name	Description
Chapter 1 - Preliminary Information	Contains initialisation related information of a general nature such as computer requirements and pre-installation materials.
Chapter 2 - Functionality of iSEA	Contains information about the various features of iSEA.
Chapter 3 - Configuring iSEA	Contains instructions for configuring the various features within iSEA.

1-2 System Requirements

1-2.1 Computer System Requirements

Minimum System Requirements:

- Intel® Pentium® Dual-Core 2.8GHz dual-core processor or equivalent
- 4GB of RAM
- 10MB Hard Disk Drive space required
- 1024 x 768 display with 16-bit video card
- DVD-ROM drive
- Keyboard and mouse or compatible pointing device

Supported Operating Systems:

- Windows® 10 64-bit
- Windows® Server 2012 R2
- Windows® Server 2016
- Windows® Server 2019

- Requires Microsoft .NET™ Framework (v4.0 or later)
- Requires the latest versions of Innotech iComm (available from our website)

Windows 10 builds are supported for approximately 18 months after release. It is recommended that you should upgrade your operating system if using an unsupported build.

1-2.2 iSEA Software Requirements

The software requirements for iSEA vary slightly depending on the functionality required. The various functions of iSEA and the software that each requires is listed below.

Table 1-2: iSEA Software Requirements

Functionality	Software Requirements
Monitoring Chronicle Server Status	Chronicle Server 2.1 or greater
Virtual Points	iComm (latest version from Innotech website)
Alarm generation for Chronicle Server Status	Chronicle 2.1 or greater iComm (latest version from Innotech website) Facility Manager 1.20D or greater
Tenant Target Monitoring with Alarm Generation	Chronicle Server 2.1 or greater ATOM 3.2 or greater iComm (latest version from Innotech website) Facility Manager 1.20D or greater

Innotech Service & Event Analyser

INSTALLATION INSTRUCTIONS

2 Functionality of iSEA

INNOTECH®

2-1 Introduction

iSEA is a Windows® based application that resides in the system tray. Its main purpose is to provide notifications to the user of events that occur in Innotech Service based applications that may not have a dedicated application status monitoring tool. It also facilitates restarting of Innotech services if they are unexpectedly terminated, in order to reduce the need for human intervention.

iSEA monitors Chronicle Server, iComm & SQL Server.

2-2 Installation of iSEA

iSEA is automatically installed along with Chronicle Server 2.0 or greater. Therefore there are no additional steps required for the installation of iSEA.

2-3 Overview of iSEA

iSEA is automatically started when the user logs in. It is visible as a icon on the windows taskbar as shown below in Figure 2-1.

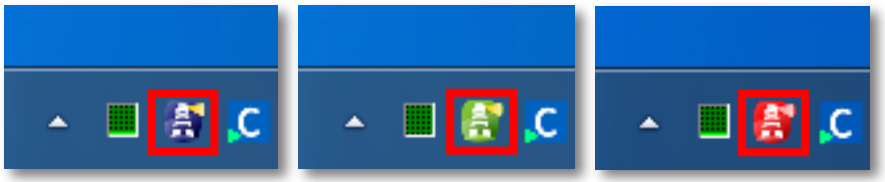


Figure 2-1: iSEA icon in the Windows Taskbar

The iSEA icon is static blue if there are no notifications in the notification list. It flashes green/blue if there are notifications in the notification list. It continually flashes red/green if there are active critical errors, but as soon as the errors are resolved, it will return to flashing green/blue to advise you of new notifications.

The iSEA icon may be hidden due to the default settings in Windows. These hidden icons can be viewed by expanding the task bar. The settings for individual elements may be set by selecting customize.

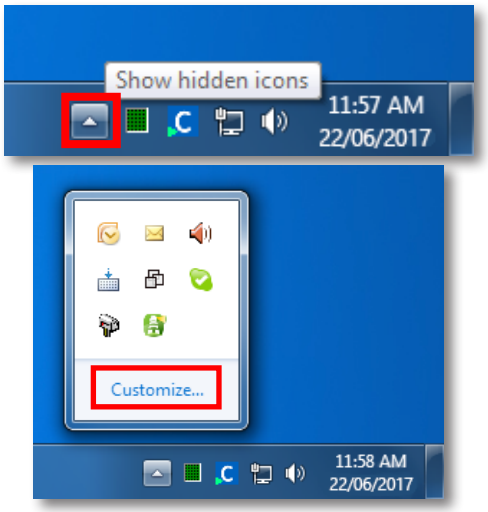


Figure 2-2: Viewing hidden icons in Windows Taskbar

Table 2-1: iSEA Features and Functions

ISEA Features	Function
Configuration	Change the port configuration for iSEA. Default is 21001.
Service Status	Check the status of monitored applications.
Monitored Points	This functionality enables monitoring of points so that timely notifications of excessive usage may be generated, and actions taken to notify customers promptly.
Notifications	View the monitored application notifications and alerts.
Virtual Points	Create virtual points to perform calculations on real point values.

Configurable items for these features may be accessed via right clicking on the iSEA icon in the windows system tray as shown below in Figure 2-3.

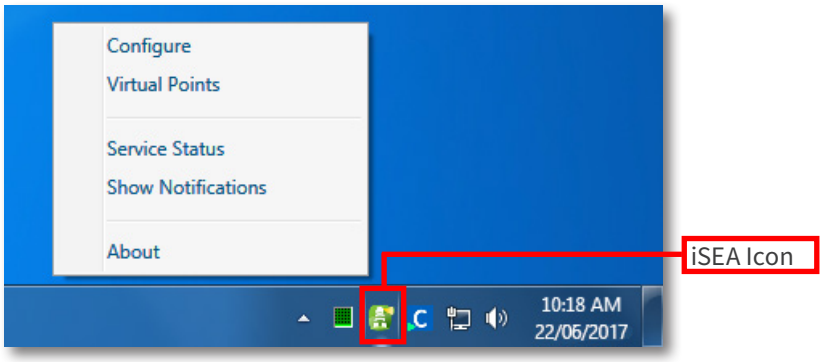


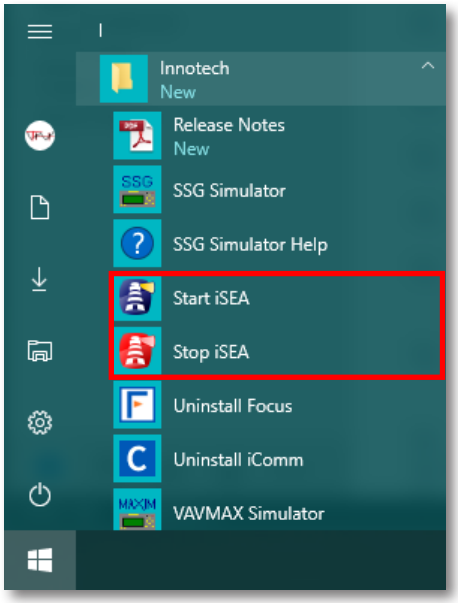
Figure 2-3: iSEA Right Click Context Menu

2-3.1 Stopping and Restarting the iSEA Service

The iSEA service automatically starts when you login to the computer. In the event that iSEA requires manual stopping and restarting, such as when Innotech software is being installed or upgraded, this can be achieved from the iSEA shortcuts located in the iSEA program group.

IMPORTANT

If you are upgrading your software, the iSEA service must be stopped **before** *upgrading.* ***The iSEA service must be restarted after upgrading your Innotech software****, to ensure correct operation of the Innotech services being monitored.*



Windows 10

- Click the Windows icon on the taskbar.
- Scroll the programs list and navigate to the Innotech folder.
- Click either "Start iSEA" or "Stop iSEA" as required as shown in Figure 2-4.

Figure 2-4: iSEA Program Group in the Windows 10 Start Menu

2-3.2 Services and Process Status Monitoring

iSEA monitors the status of the following programs and services:

- Chronicle Server
- iComm
- SQL Server Express

Right Click the iSEA icon and select the Service Status option in the iSEA menu as shown below in Figure 2-5.

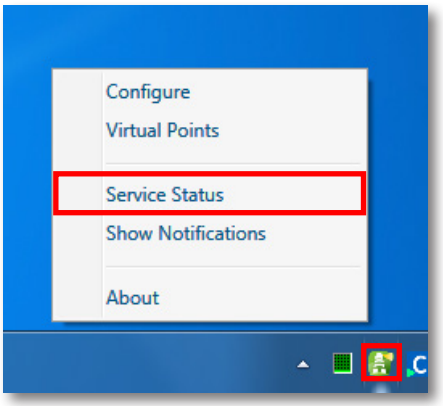


Figure 2-5: iSEA Context Menu - Service Status

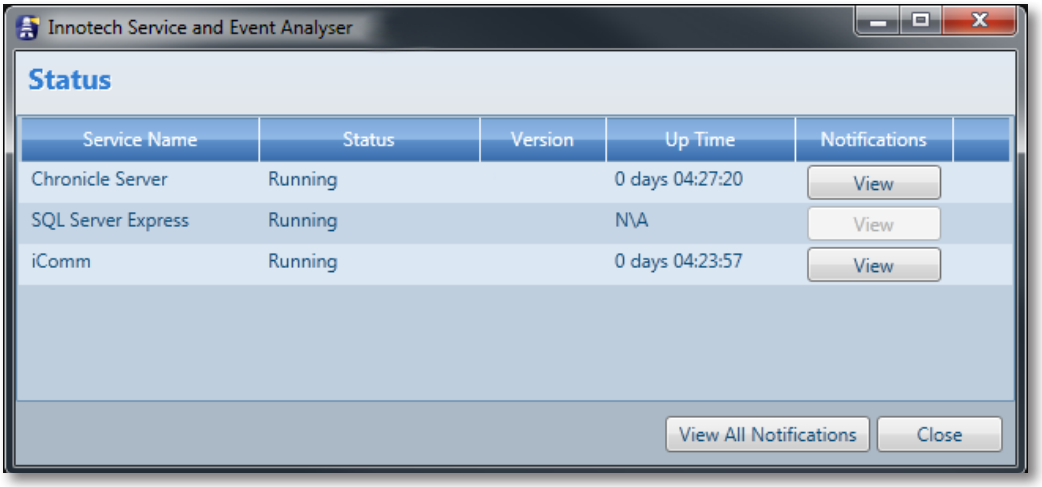


Figure 2-6: Services and Programs monitored in iSEA

2-3.3 Notifications in iSEA

iSEA displays several types of notifications in order to provide the user with information regarding the operation of Innotech Software. See the configuration section for details on configuring iSEA notifications.

Table 2-2: Types of Notifications in iSEA

Notification Icon	Notification Type	Information covered by Notification
	Information	Indicates general information e.g. - • Database backup progress • Starting of Services and Processes • Virtual Point Creation
	Warning	Indicated import information that may indicate a potential problem e.g. - • Disconnection from iComm
	Error	Indicates a problem with a monitored service or process e.g. - • Disconnection from Chronicle Server • Inability to connect to iComm

Important notifications such as Errors and other significant notifications will be written to the Windows Application log. This log is accessible from the Windows Computer Management Interface.

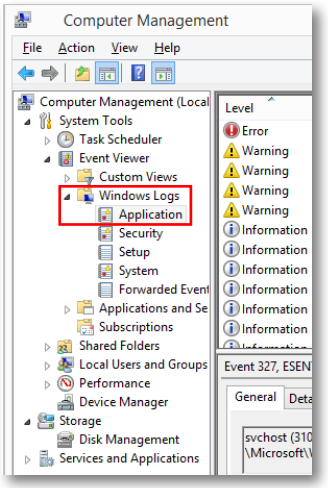


Figure 2-7: Windows Application logs

To access Windows Computer Management:
Windows 10: Right click the Windows button on the desktop mode taskbar and select Computer Management.

Innotech Service & Event Analyser

INSTALLATION INSTRUCTIONS

3 Configuring iSEA

INNOTECH®

3-1 Introduction

This section provides the instructions on how to configure the functions of iSEA including the setup of Virtual points and setup for Monitoring of Chronicle & iSEA using Facility Manager.

3-1.1 iSEA Configuration Window

Right click the iSEA icon in the system tray and select Configure from the context menu to open the Configuration window.

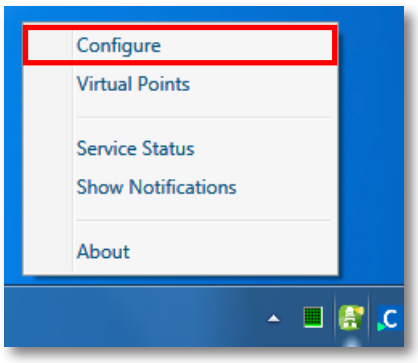


Figure 3-1: iSEA System Tray Icon Context Menu

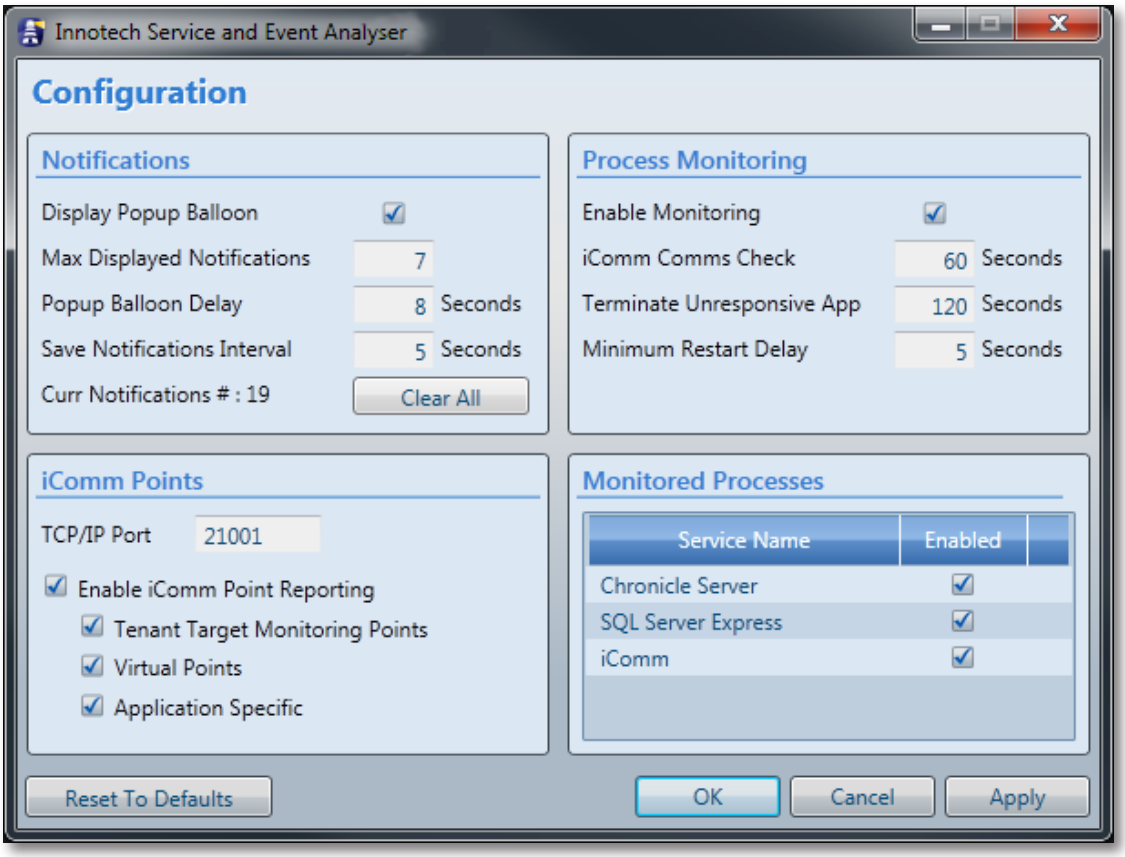


Figure 3-2: iSEA Configuration Window

3-1.1.1 Notifications

Table 3-1 describes the function of each setting for the Notifications. These settings configure how messages from iSEA are displayed.

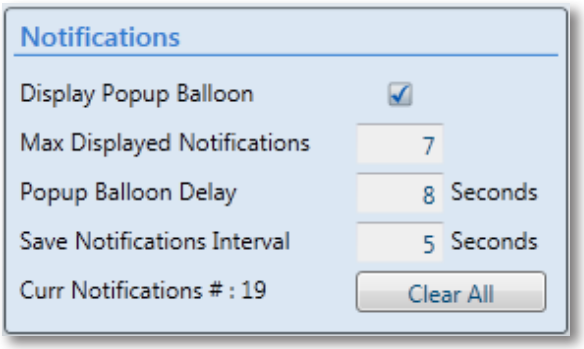


Figure 3-3: Notifications Configuration Settings

Table 3-1: Notification Settings

Setting	Function
Display Popup Balloon	When checked, iSEA will display a notification balloon in the Windows notification area.
Max. Displayed Notifications	Sets the number of notifications that can be displayed in the notification balloon.
Popup Balloon Delay	Amount of time that the notification balloon will be displayed for.
Save Notifications Interval	Notifications will be saved to a backup file at the interval in this setting.
Current Notifications	Displays the current number of notifications in the Notification Window.
Clear All	Click to clear all notifications from the notification window.

3-1.1.2 iComm Points

iSEA utilises a specific TCP Port in order to communicate with iComm. By default, iSEA utilises TCP Port 21001. In order to specify a different TCP Port, type a new port number into the configuration window. These settings are important as it is used in the setup of Monitored points and Virtual Meters in iSEA and iComm.

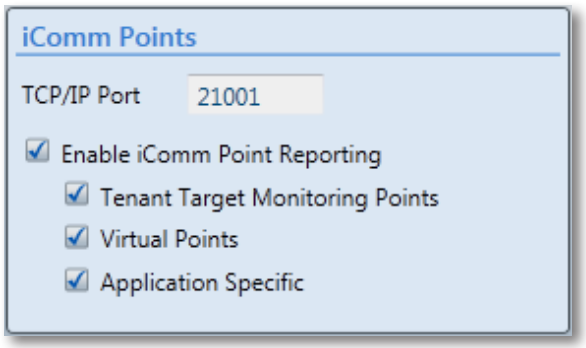


Figure 3-4: iComm Points Configuration Settings

Table 3-2: iComm Points Settings

Setting	Function
TCP/IP Port	Sets the port number for iSEA connection to iComm.
Enable iComm Point Reporting	Enables iSEA to send selected point values to iComm.
Tenant Target Monitoring Points	iSEA will report tenant target values for the local Chronicle server on the target monitoring device.
Virtual Points	iSEA will report virtual point values on the virtual point device.
Application Specific	Enables application specific devices to report to iComm. ie iSEA's Internal Points. **iSEA:** • ChronicleRunning~Output • SQL_Express~Output **Chronicle Server:** • DbConnected~Output • iCommConnected~Output • AllocatedDB~Output • ReportingUsage~Output • DatabaseLogging~Output

3-1.1.3 Process Monitoring

These settings enable or disable monitoring of monitored processes and sets the delay in seconds for process checking and restarting.

IMPORTANT

Disabling monitored processes will impact data integrity and should only be used for troubleshooting or maintenance.

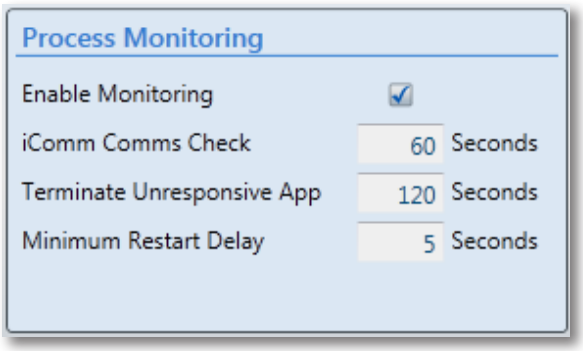


Figure 3-5: Process Monitoring Configuration Window

Table 3-3: Process Monitoring Settings

Setting	Function
Enable Monitoring	Click to enable or disable monitoring of selected Innotech processes and services.
iComm Comms Check	Time delay before iSEA reports a communications failure with iComm, after at least two failed attempts.
Terminate Unresponsive App	Time delay before iSEA terminates an unresponsive application. Only applications with user interfaces (iComm) can be terminated and restarted using this feature.
Minimum Restart Delay	Time delay before iSEA restarts an application that is detected as not running.

3-1.1.4 Monitored Processes

These settings enable or disable monitoring of selected Innotech processes and services. Check or uncheck items as required.

IMPORTANT

Notifications and service status for disabled processes will not be displayed, nor will they be restarted if not running.

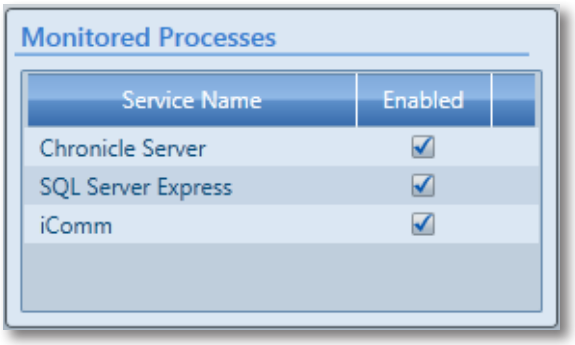


Figure 3-6: Monitored Processes Configuration Window

Table 3-4: Monitored Processes Settings

Setting	Function
Chronicle Server	Allows Chronicle Server to be monitored by iSEA.
SQL Server Express	Allows SQL Server Express to be monitored by iSEA.
iComm	Allows iComm to be monitored by iSEA.

3-2 Configure iSEA

3-2.1 Setup of Monitoring in iSEA

The steps below describe how to enable Facility Manager (FM) to monitor the Chronicle Server service and some of its components to ensure it is running, and setup an alarm if the service fails unexpectedly.

Notifications in FM may be set up to alert maintenance staff of various potential faults that may occur when Chronicle is logging data, such as if the database connection fails. Database usage may also be monitored, so that precautions may be taken when the database approaches capacity to ensure no data is lost.

This guide assumes that the Point Reporting settings in the iSEA Configuration window are enabled, all software detailed above has been installed and configured as specified in the relevant setup guides, and that the user is familiar with the operation of a Microsoft Windows computer.

1. In the iComm window, click the Add New Connection button and click iSEA.

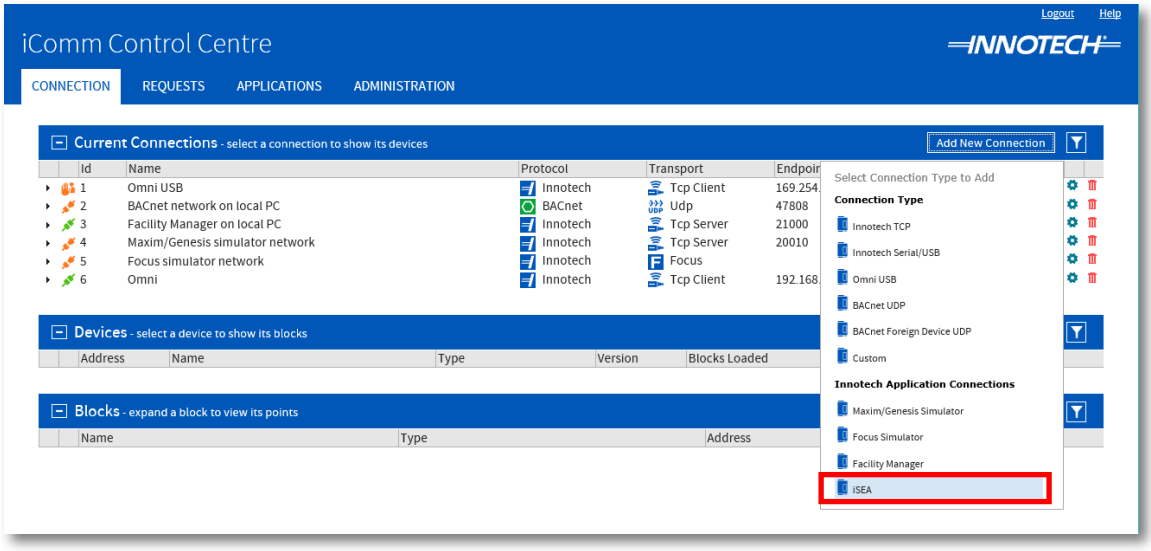


Figure 3-7: Creating a new iSEA Connection in iComm

To edit the connection later, click the settings cog at the right end of the connection in the Current Connections panel.

IMPORTANT

Prior to setup, ensure that the configuration settings in iSEA are correct for your installation.

2. Specify the Connection name as 'iSEA Monitoring', change the IP Address and port number is necessary.
3. Set the Address of the first device to 1, and the Address of the last device to 2.
4. Click the OK button to confirm the settings as shown below.

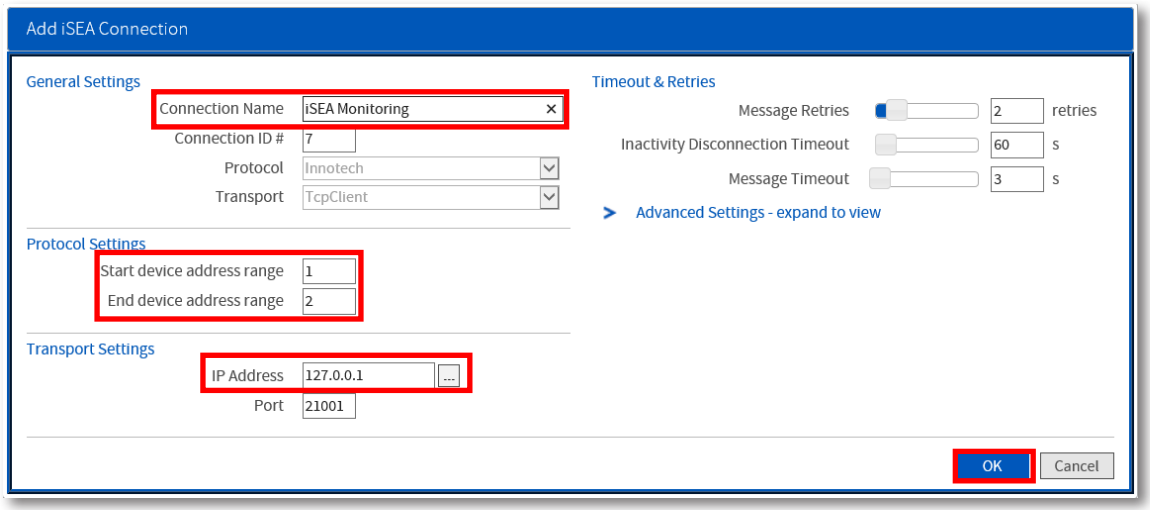


Figure 3-8: iComm TCP Connection General Properties

5. Two devices will be listed under the connection if the settings are correct and iSEA is running. The first device will have the device name 'iSEA', and will have a green tick when the connection to iSEA is successful. Two blocks will be loaded for this device.
   The second device is named 'Chronicle Server', and will only be alive when iSEA has connected to Chronicle Server. There will be 6 blocks loaded for this device as shown below.

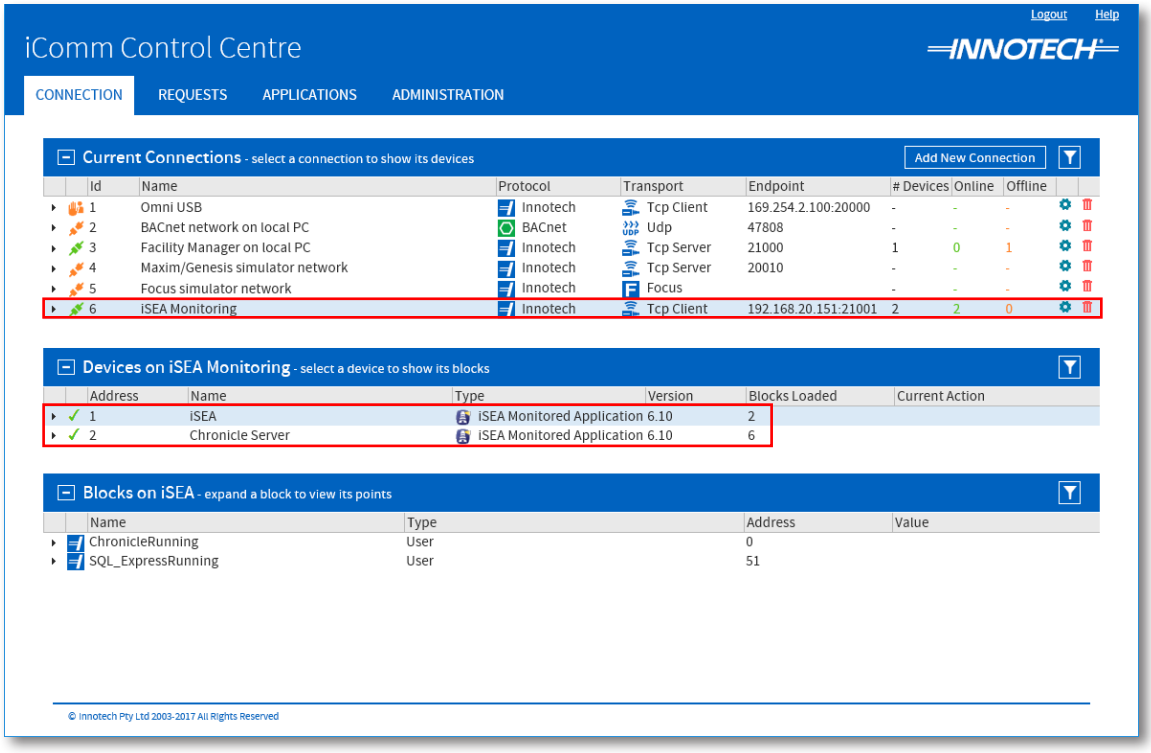


Figure 3-9: iSEA Connection Devices

3-2.2 Set up Facility Manager

6. Open FM Builder, and create a new project or open an existing one.

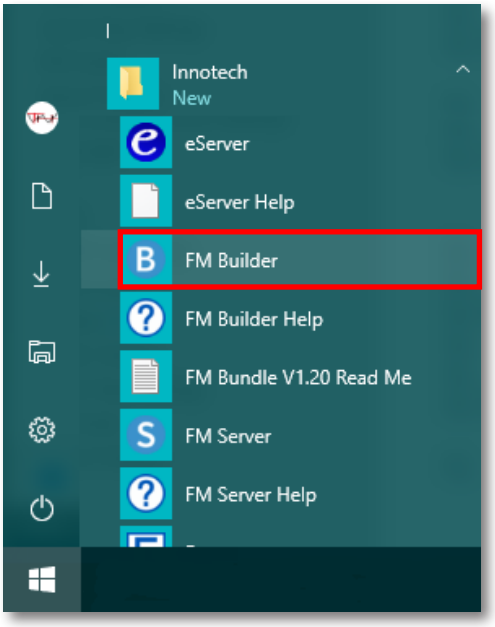


Figure 3-10: Open FM Builder

7. Click on the 'Alarm Groups' tab.

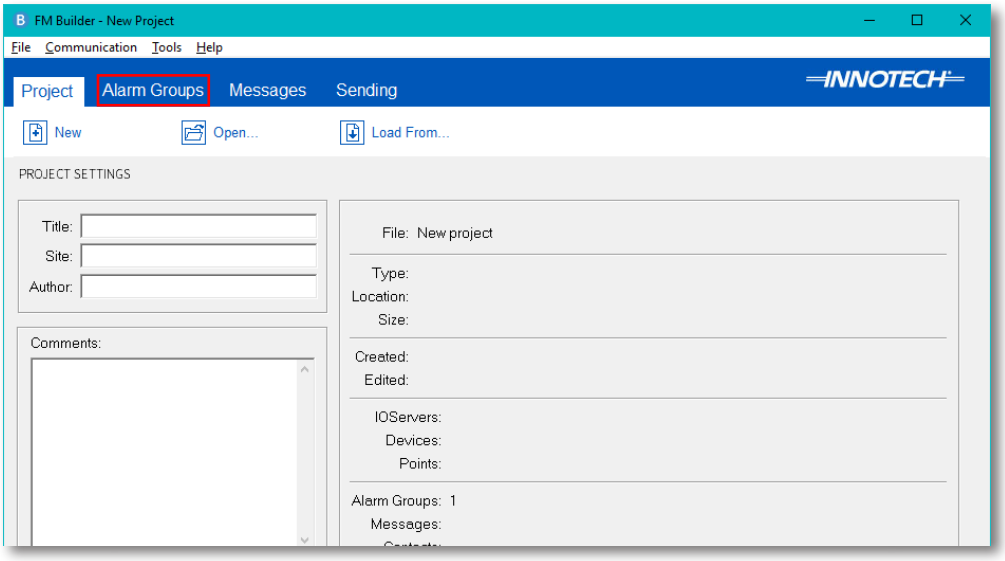


Figure 3-11: FM Builder Alarm Groups Tab

8. Add a new Server using the 'New Server' button if iComm does not already exist in the project.
9. Enter a name for the server, and the address of the iComm computer, then click the 'Ok' button.

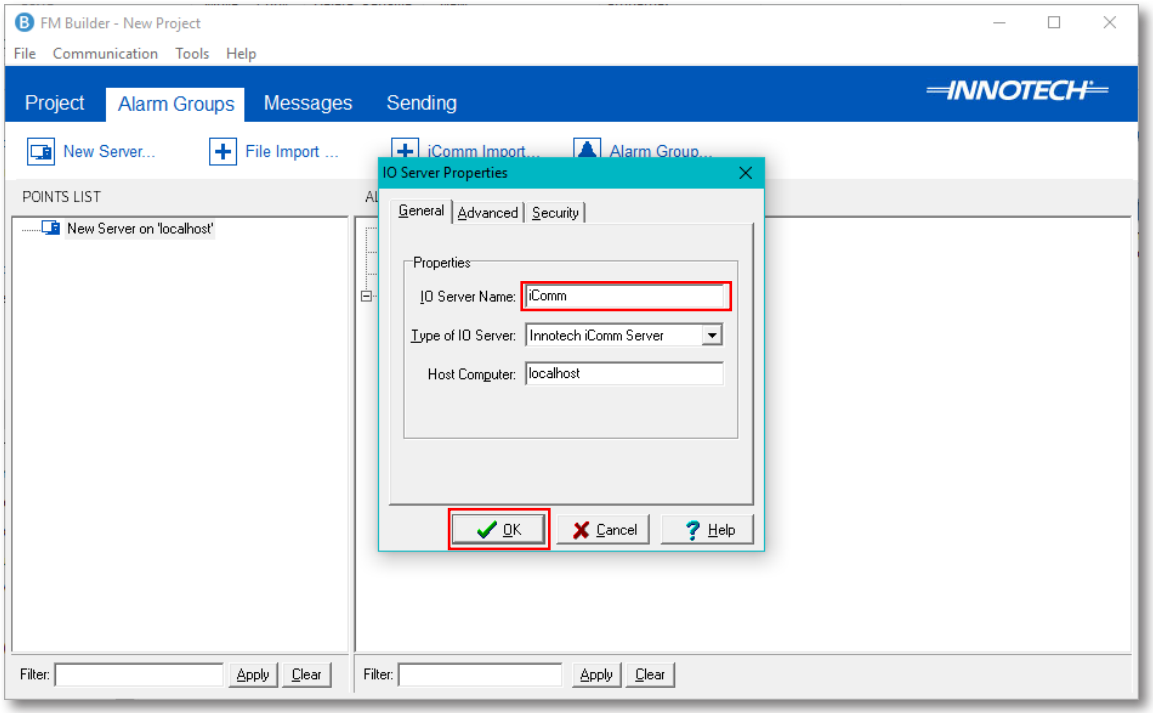


Figure 3-12: FM Builder - Create a new IO Server

10. Create 2 new devices on this server using the Device ID and Connection ID as listed in iComm.

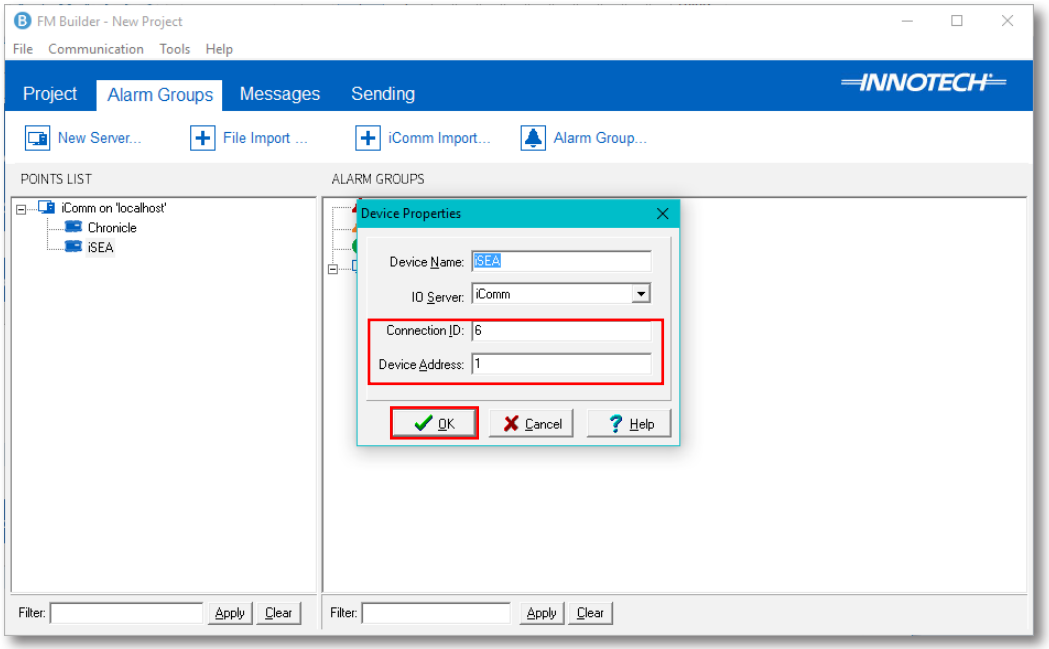


Figure 3-13: FM Builder - Create new iSEA Devices

11. Create 1 digital point on the ‘iSEA’ device with the address ‘ChronicleRunning~Output’, and a recommended update rate of 1 second (1000 milliseconds).

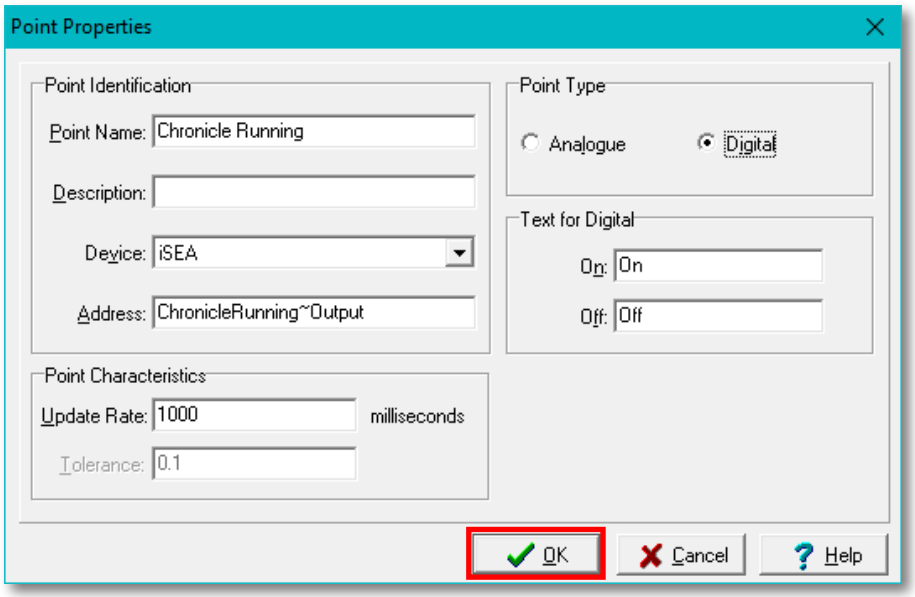


Figure 3-14: Create a new Point called ‘Chronicle Running’

12. Drag the point to the required Alarm Group, and set the 'Activation Settings' to 'Changes to 0'.

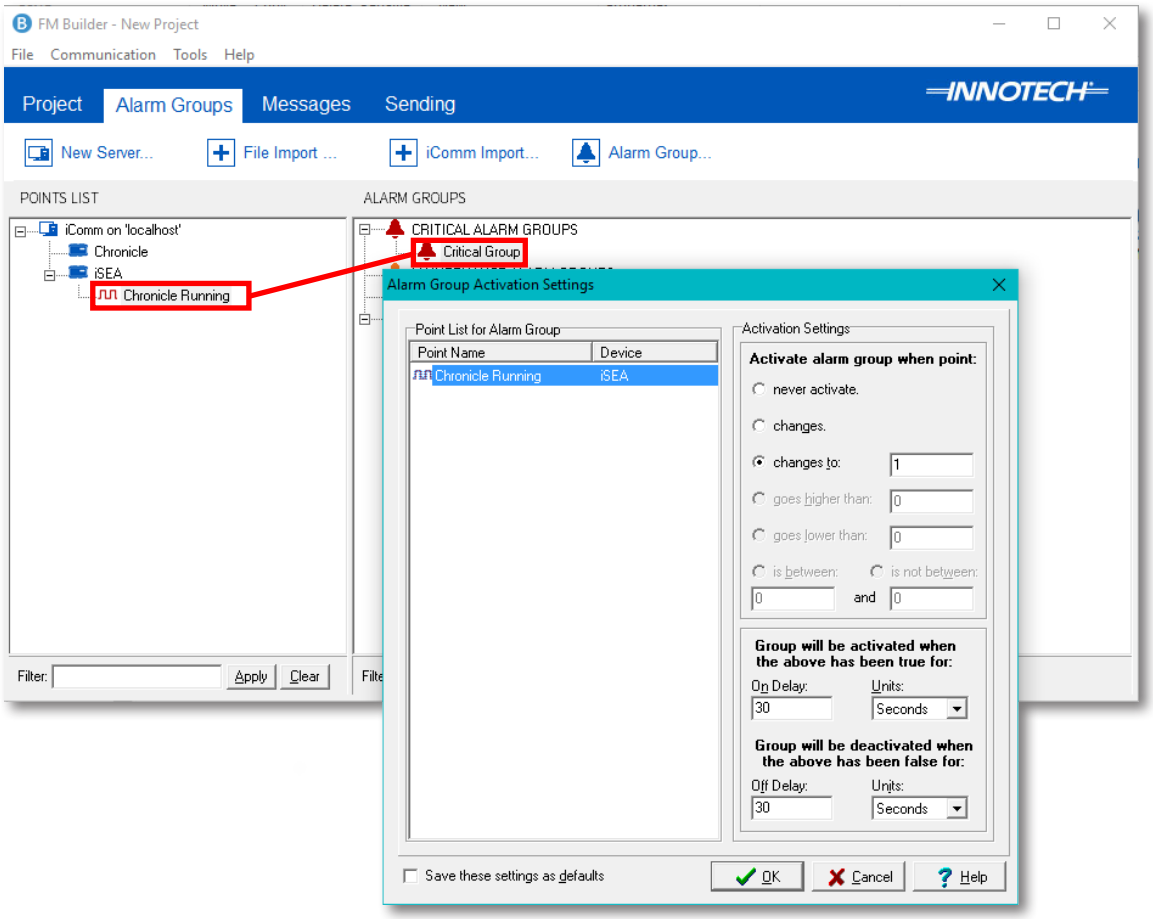


Figure 3-15: FM Builder - Add Point to an Alarm Group

13. Create 6 points on the 'Chronicle Server' device with the following addresses:

    - DbConnected~Output (Digital).
    - iCommConnected~Output (Digital).
    - AllocatedDB~Output (Analogue).
    - ReportingUsage~Output (Analogue).
    - DatabaseLogging~Output (Digital).

A point for SQL_ExpressRunning~Output can also be created if desired.

14. Drag each point to the required Alarm Group. The following 'Activation Settings' are recommended values and may be customised as required:

Table 3-5: FM Alarm Group Activation Settings

Point Name	Point Address	Alarm Activation Settings
DbConnected	DbConnected~Output	Set the 'Activation Settings' to 'Changes to 0'. A point value of 0 indicates that Chronicle Server can no longer communicate with the specified database.
iCommConnected	iCommConnected~Output	Set the 'Activation Settings' to 'Changes to 0'. A point value of 0 indicates that Chronicle Server can no longer communicate with an iComm.
AllocatedDB	AllocatedDB~Output	Set the 'Activation Settings' to 'Changes'. This value indicates the current maximum size of the database. The value should be 4 if 'SQL Express' is selected as the Database Server type in Chronicle Manager, or 10 if 'SQL Express 10GB' is selected.
ReportingUsage	ReportingUsage~Output	(Maintenance Alarm Group) set the 'Activation Settings' to 'Goes higher than 90'. (Critical Alarm Group) set the 'Activation Settings' to 'Goes higher than 97'. This value indicates the percentage used of the database allocated for reporting point logging. See note blow.

IMPORTANT

Once the ReportingUsage value exceeds 90, steps should be taken to ensure long term storage of backups are kept, as the earliest records in the database will be overwritten once the usage reaches 95%.

The Maintenance alarm for this point may be removed if this occurs, as the usage will never reduce below 90%, unless the reporting usage allocation is increased, or the Database type is changed from 'SQL Express' to 'SQL Express 10GB' (requires software licence).

If the usage exceeds 97% there is a critical issue with the database which may cause logging to fail if the reporting allocation is not increased.

The newly created "Chronicle Running" points are shown below.

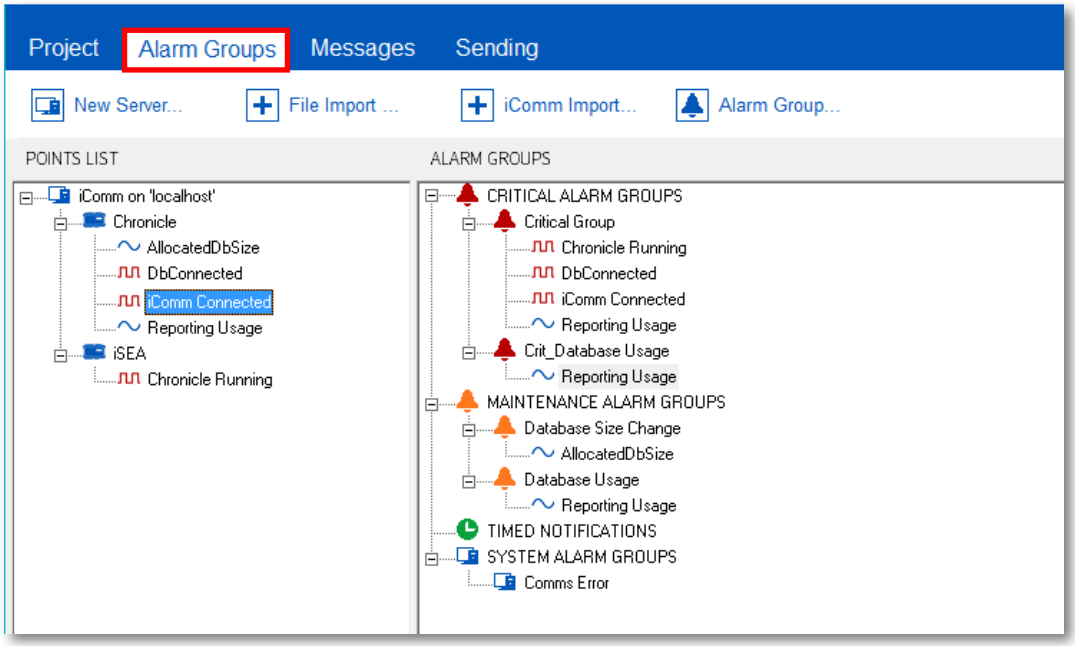


Figure 3-16: FM Builder Alarm Groups

15. Select the 'Messages' tab in FM, setup messages and recipients as required. Please refer to FM Help for more information.

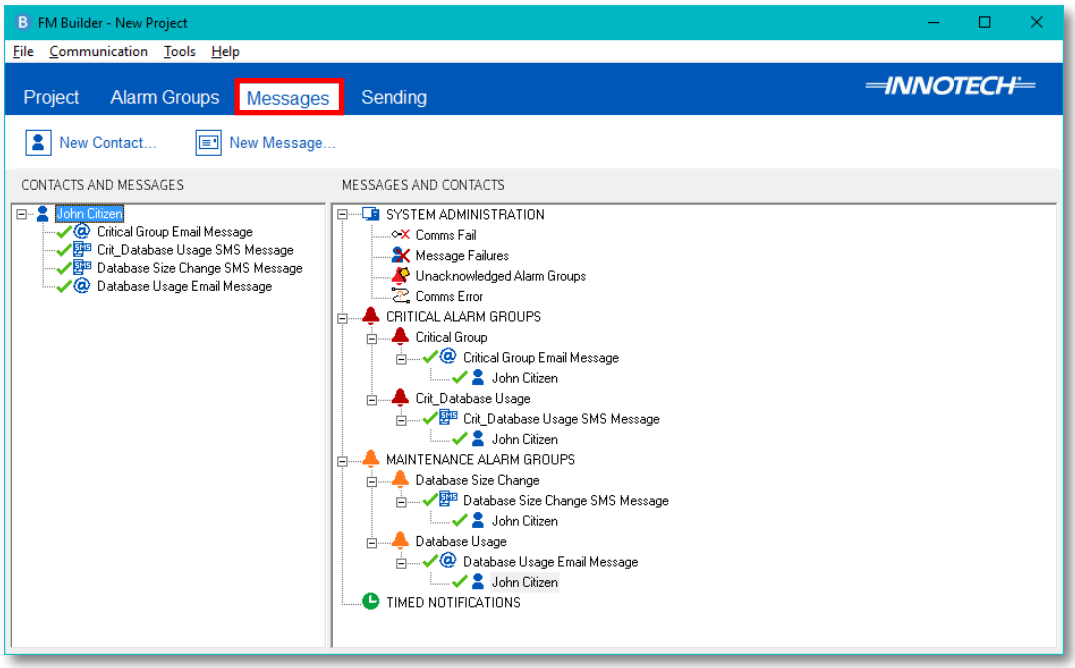


Figure 3-17: FM Builder Messages Tab

16. Select the ‘Sending’ tab, click ’Save’ and then click ’Send To’ to send the project to FM.

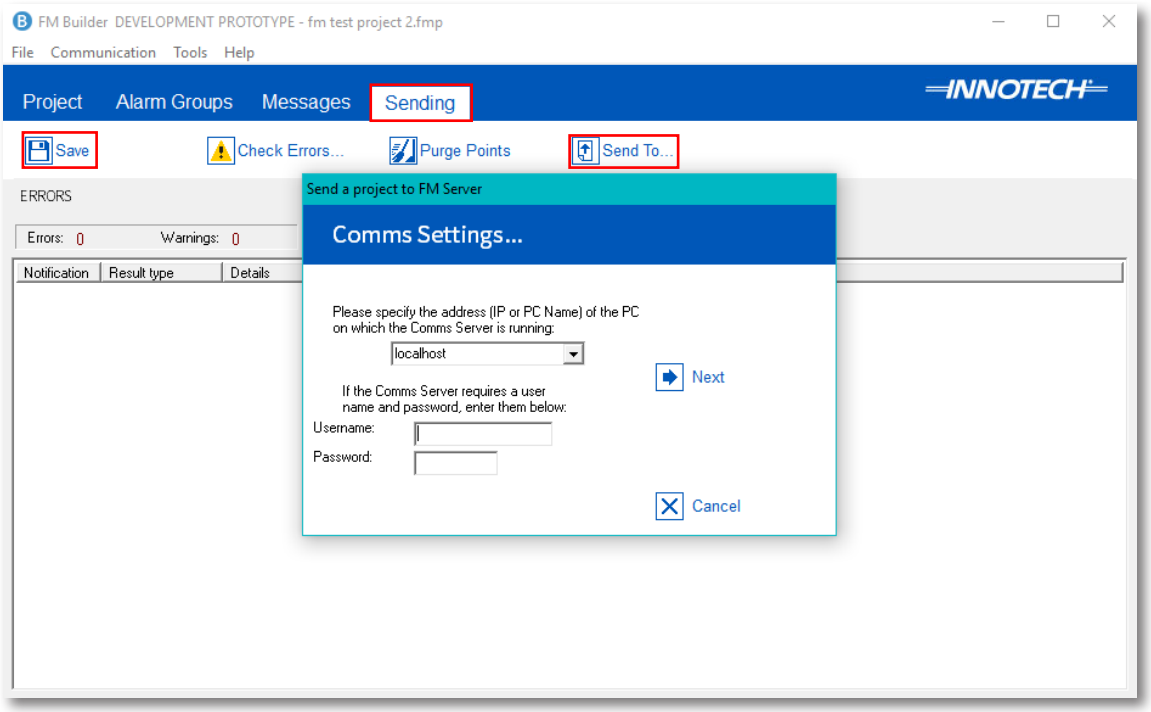


Figure 3-18: FM Builder Sending Tab

Transferring a project requires FM Server to be running.

3-2.3 Setup of Virtual Points in iSEA

Virtual points provides the ability to derive a single value from a set of available real point values by performing additions and subtractions as required. For example, multiple power meter values may be added together to derive the total power usage value.

In order to ensure compatibility with different devices, a multiplication factor can be set to convert between units, such as Watts to Kilowatts.

Virtual points are created by accessing the Virtual Points configuration interface within iSEA.

IMPORTANT

If a virtual point is created as an accumulated point, you can still log it as a reporting point in Chronicle but it is advisable to disable accumulating for this point to ease the CPU load.

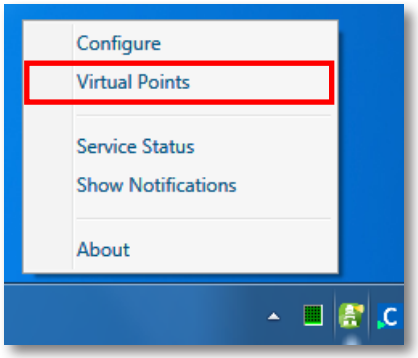


Figure 3-19: Accessing Virtual Points configuration in iSEA

1. In the Configure iComm Server section, enter the connection details for the iComm that contains the points you wish to create Virtual Points from. You must enter an iComm Address in order to use virtual points. The location of iComm may be configured as a DNS or IP Address. If necessary add the Username and Password of the iComm Server.

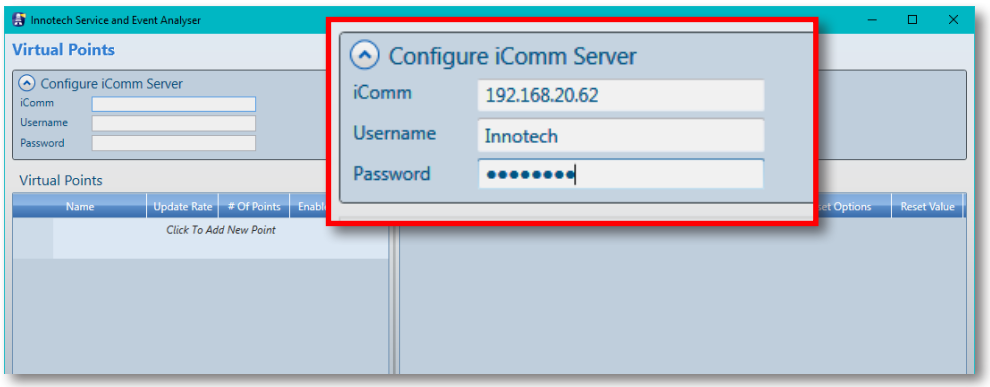


Figure 3-20: Virtual Points configuration - iComm Server settings

2. In the Virtual Points section, left click on the text “Click To Add New Point”. This will create a new row for you to enter the details of a virtual point.

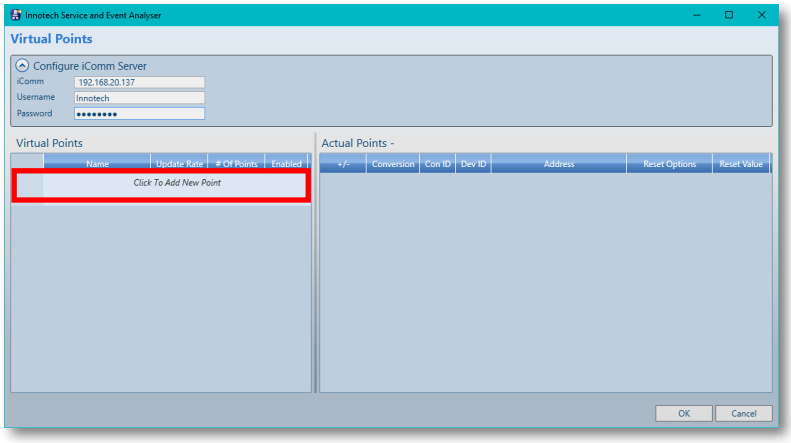


Figure 3-21: Add New Virtual Points

3. Enter a name for the virtual point under the Name column. By default, a Virtual Point is set to an update rate of 60 seconds. This value may be modified to any value between 5 and 300 seconds. (All actual points linked to this virtual point will be updated by iComm at this rate or faster).

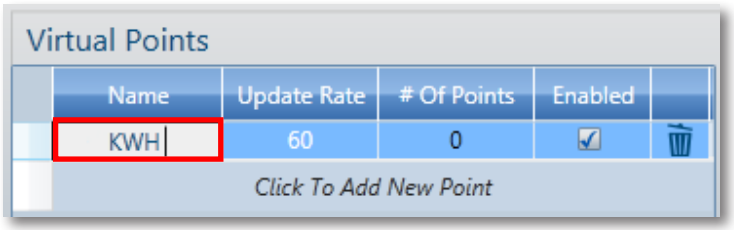


Figure 3-22: Enter Details for the Virtual Point

4. Click in the Name and Update Rate field to edit details, press enter when done.

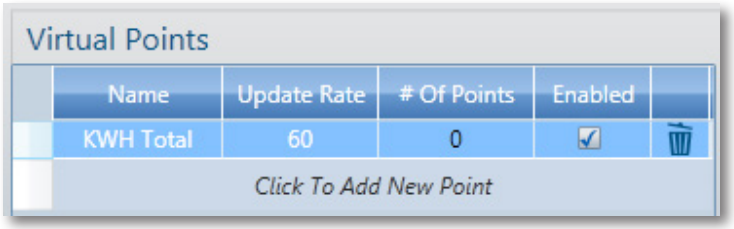


Figure 3-23: New Virtual Points Created

The Virtual point may not appear in iComm until the Update rate time interval has elapsed.

5. If you wish to temporarily disable a Virtual Point from sending values to iComm, uncheck the checkbox in the Enabled column.

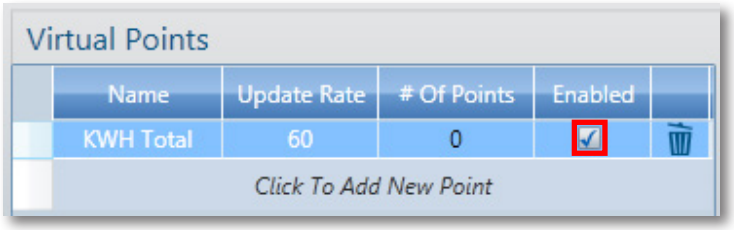


Figure 3-24: Enabling / Disabling Virtual Points

6. If you wish to permanently remove a Virtual Point from iSEA, click the *rubbish bin* icon at the end of the row you wish to delete.

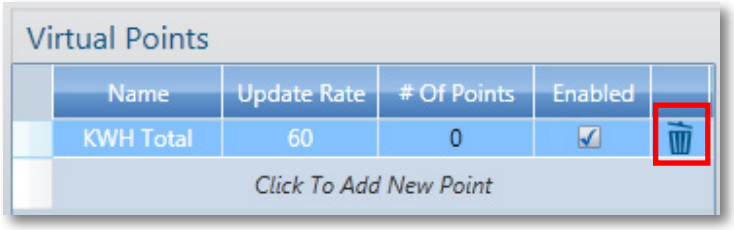


Figure 3-25: Permanently remove a Virtual Point

7. After creating a Virtual Point, you will be able to add Actual Points from which the value for the Virtual Point will be calculated. The Actual Points only relate to the currently selected virtual point.

8. To link an Actual Point to a Virtual Point, select the virtual point, then in the Actual Points panel, left click on the text “Click To Add New Point”.

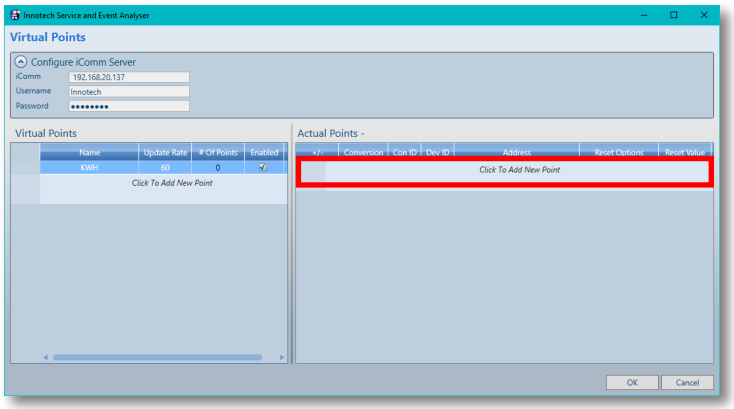


Figure 3-26: Creation of Actual Points under Virtual Points

9. Enter the Connection ID, the Device ID and the Point Address as required in the appropriate fields.

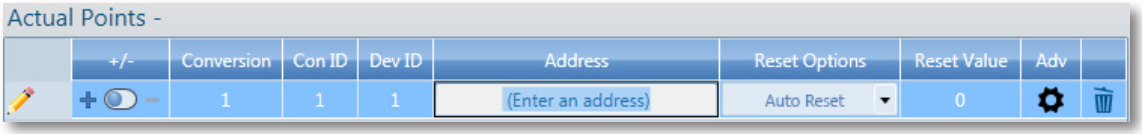
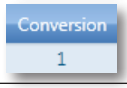
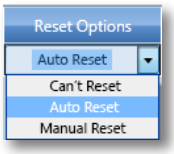


Figure 3-27: Creating Actual Points

Table 3-6: Elements of an Actual Point within a Virtual Point

Element	Function	Description
	Addition	The point is added to the Virtual point total.
	Subtraction	The point is subtracted from the Virtual point total.
	Conversion factor	Ranges between $1x10^{10}$ and $1x10^{9}$. This factor is multiplied with the Actual point value.
	Connection ID and Device ID	This is the Connection and Device IDs of your Actual Points.
	Reset Options	Auto Reset Default Setting. Accumulates at the highest received value from a point. Manual Reset The user defines the maximum value of the meter reset. Can't Reset This setting shows the "Live Value" of the meter. No Accumulation.
	Reset Value	This column will show the maximum meter value of the point at which it was reset.
	Advanced	Click the symbol to view or reset the Accumulated Reset Total for the point.

10. Enter a Conversion Factor if the value of the Actual Point needs to be converted.

11. If the Actual Point is to be subtracted from the total value of this Virtual Point, click on the +/- toggle switch in the first column of the current row.

12. Clicking the *rubbish bin* icon at the end of a row will delete that row. This action cannot be undone.

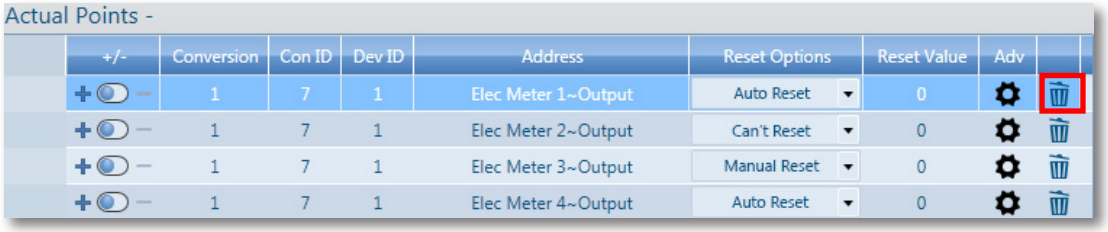


Figure 3-28: Deletion of Actual Points under Virtual Points

13. Once all Virtual Points and Actual Points have been created, click the OK button to create the new Virtual Points.

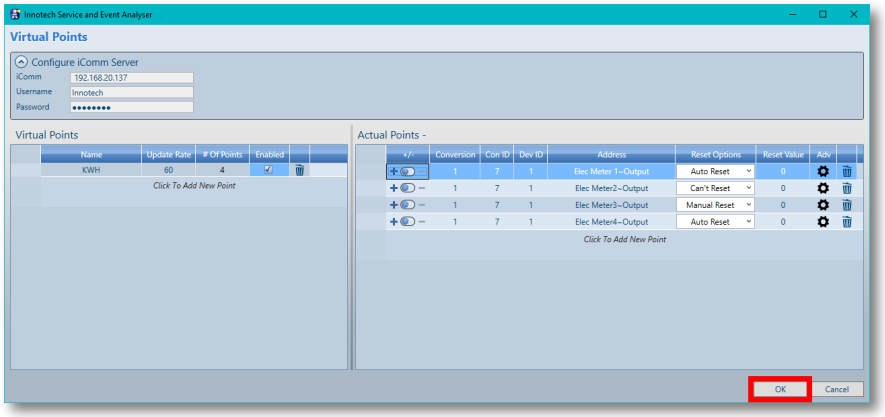


Figure 3-29: Click OK to create the Virtual Points

14. When the Virtual Points manager connects to iComm, a notification will be displayed by iSEA stating how many virtual points have been created. If the Virtual Points manager gets disconnected from iComm, iSEA will also show a notification for this event.

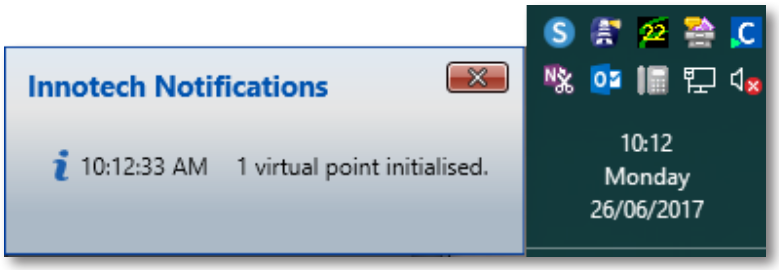


Figure 3-30: Virtual point creation notification

In order to log virtual points, the iSEA connection must first be setup in iComm, following the procedure specified in the Monitoring section, substituting the final device address with 4. This fourth device on the iSEA connection will contain all the virtual points setup on this instance of iSEA. These can then be imported into a Chronicle or Magellan project in the same way as standard device points.

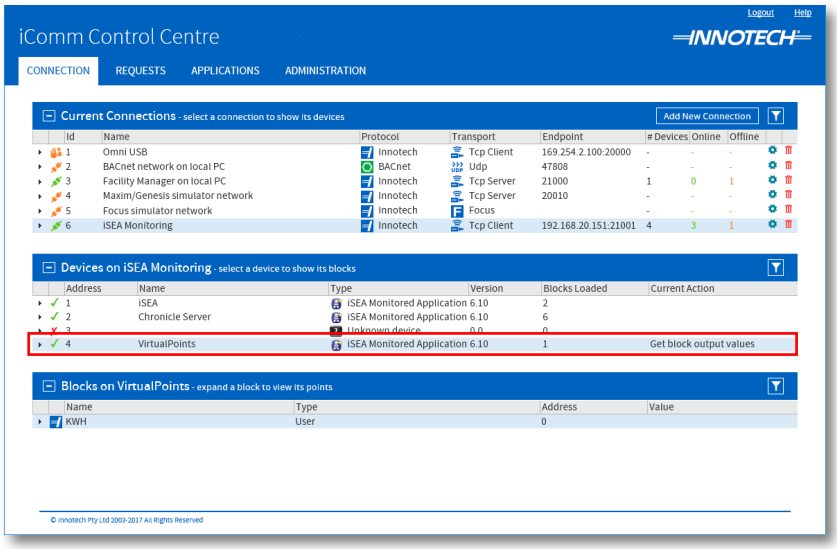


Figure 3-31: iComm with new virtual device

To ensure virtual points function correctly, the computer should be setup to automatically login after start-up.

Innotech Support

Innotech provides technical information on the Web to assist you with using its products.
At www.innotech.com, you can find technical manuals, user instructions, and data sheets for all our products.

For direct product support or product information, contact your local distributor, or an Innotech representative.

You can contact us via email, phone, or postal mail:

Website: www.innotech.com
Email: sales@innotech.com
Phone: +61 7 3421 9100
Mail: Innotech Control Systems
P.O. Box 292
Sunnybank
QLD 4109
Australia

