Operating Manual

Honeywell

Touchpoint Pro Webserver
Version 7.0.0.0

LEGAL NOTICES

Revision History

Revision	Comment	Date
Issue 1	A04643	Jul 2015
Issue 2	A04938	Dec 2016
Issue 3	A05034	Oct 2017

LEGAL NOTICES

Disclaimer

In no event shall Honeywell be liable for any damages or injury of any nature or kind, no matter how caused, that arise from the use of the equipment referred to in this manual.

Strict compliance with the safety procedures set out and referred to in this manual, and extreme care in the use of the equipment, are essential to avoid or minimise the chance of personal injury or damage to the equipment.

The information, figures, illustrations, tables, specifications, and schematics contained in this manual are believed to be correct and accurate as at the date of publication or revision. However, no representation or warranty with respect to such correctness or accuracy is given or implied and Honeywell will not, under any circumstances, be liable to any person or corporation for any loss or damages incurred in connection with the use of this manual.

The information, figures, illustrations, tables, specifications, and schematics contained in this manual are subject to change without notice.

Unauthorised modifications to the gas detection system or its installation are not permitted, as these may give rise to unacceptable health and safety hazards.

Any software forming part of this equipment should be used only for the purposes for which Honeywell supplied it. The user shall undertake no changes, modifications, conversions, translations into another computer language, or copies (except for a necessary backup copy).

In no event shall Honeywell be liable for any equipment malfunction or damages whatsoever, including (without limitation) incidental, direct, indirect, special, and consequential damages, damages for loss of business profits, business interruption, loss of business information, or other pecuniary loss, resulting from any violation of the above prohibitions.

Warranty

Honeywell Analytics warrants the Touchpoint Pro system against defective parts and workmanship, and will repair or (at its discretion) replace any components that are or may become defective under proper usage within 12 months from the date of commissioning by a Honeywell Analytics approved representative* or 18 months from shipment from Honeywell Analytics, whichever is sooner.

This warranty does not cover consumables, batteries, fuses, normal wear and tear, or damage caused by accident, abuse, improper installation, unauthorized use, modification or repair, ambient environment, poisons, contaminants or abnormal operating conditions.

This warranty does not apply to sensors or components that are covered under separate warranties, or to any 3rd-party cables and components.

Any claim under the Honeywell Analytics Product Warranty must be made within the warranty period and as soon as reasonably practicable after a defect is discovered. Please contact your local Honeywell Analytics Service representative to register your claim.

This is a summary. For full warranty terms please refer to the Honeywell Analytics' General Statement of Limited Product Warranty, which is available on request.

* A Honeywell Analytics approved representative is a qualified person trained or employed by Honeywell Analytics, or a qualified person trained in accordance with this manual.

Copyright Notice

Microsoft, MS and Windows are registered trademarks of Microsoft Corp.

Other brand and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective holders.

Honeywell is the registered trademark of Honeywell International Inc.

Touchpoint is a registered trademark of Honeywell Analytics.

Find out more at www.honeywellanalytics.com

LEGAL NOTICES

This page deliberately blank.

CONTENTS

Contents

INTRODUCTION

1 Important Information

The Equipment referred to in this manual contains components and assemblies that are each certified for use in a variety of differing environments, and it is the site owner's responsibility to confirm the suitability of the equipment prior to its installation and use.

The Equipment assemblies referred to in this manual are collectively certified for use in a flammable gas detection system only. Any other use is not currently certified and is not authorised by the manufacturer.

For installation in Canada and the USA, for both ordinary and hazardous locations, all connections, cabling, overcurrent protection and installations must strictly adhere to both the National Electrical Code (NEC) and the Canadian Electrical Code (CEC).

Check the product rating plate and look for the following marks to ensure that the supplied equipment is suitable for its intended location and purpose:

Products bearing the CE mark conform to all applicable European Directives as stated on the Honeywell product specific EU Declaration of Conformity.

Products bearing the CSA mark conform to the requirements for Ordinary Locations, and where marked on components and apparatus, Zone 2 and Division 2 Hazardous Locations.

Products, components and apparatus bearing the ATEX Explosion Protection mark conform to the requirements for Zone 2 Potentially Explosive Atmospheres.

WARNING
FOR SAFETY REASONS THIS EQUIPMENT MUST BE OPERATED BY QUALIFIED PERSONNEL ONLY. READ AND UNDERSTAND THE INSTRUCTION MANUAL COMPLETELY BEFORE OPERATING OR SERVICING THE EQUIPMENT.

ATTENTION
POUR DES RAISONS DE SÉCURITÉ, CET ÉQUIPEMENT DOIT ÊTRE UTILISÉ, ENTRETENU ET RÉPARÉ UNIQUEMENT PAR UN PERSONNEL QUALIFIÉ. ÉTUDIER LE MANUEL D'INSTRUCTIONS EN ENTIER AVANT D'UTILISER, D'ENTRETENIR OU DE RÉPARER L'ÉQUIPEMENT.

1.1 Intended Readers

This Manual should be read by everyone who accesses the TPPR gas detection system remotely. In addition this manual may be used to train people who access the TPPR gas detection system remotely.

1.2 Conventions Used

The following conventions are used in this manual:

- **TPPR** refers to the Touchpoint Pro Gas Detection System.
- **Webserver** refers to the TPPR's inbuilt remote access interface.

INTRODUCTION

1.3 TPPR Documentation Suite

The TPPR documentation is supplied on CD-ROM with new systems, and is available to download from the Honeywell Analytics website (see below).

The downloadable TPPR documentation suite consists of:

- Touchpoint Pro Technical Handbook
- Touchpoint Pro Operating Manual
- PC Configuration Operating Manual
- Webserver Operating Manual (this document)
- Touchpoint Pro Safety Manual
- Other Bulletins and Advisories as released from time-to-time

Note: Honeywell Analytics recommends that you regularly visit your Internet Location (below) and click on **Additional Docs** to check for the latest releases and information.

1.4 Document Translations and Optional Software

The Touchpoint Pro Technical Handbook (from Issue 4) is available in English only, but other TPPR end-user documents and software are available to download from: http://www.honeywellanalytics.com/

Open the link, select your language, locate **Products/Touchpoint Pro** and click on **Additional Docs** and **Software** to check for the latest releases.

Note: Honeywell Analytics recommends that you visit the website above, click on **Products/Touchpoint Pro/Software**, and register for email notification of updates, newsletters and technical bulletins.

1.4.1 Available Document Languages

- Deutsch
- English
- Español
- Français
- Italiano
- Nederlands
- русский

1.5 Associated Documents

TPPR documents should be read in conjunction with 3rd-Party or ancillary component and sensor documentation.

1.6 How to Use this Document

This document is not designed to be read 'end-to-end'. Rather it is intended to be used as an authoritative reference work and source of safety information and operational procedures. As such it is organised into logical sections and chapters that allow all levels of reader to quickly access the required information.

This document is organised so that individual sections, chapters or pages can be copied or printed as a quick reference source. All new chapters start on an odd facing page to allow them to 'stand-alone' when printed, and some end pages are deliberately blank for the same reason.

It is strongly recommended that the hyperlinked Contents, Figures, and Table lists, and the PDF bookmark tool are used for easy navigation.

1.7 Further Information and Help

Contact Honeywell Analytics Technical Support for advice if you notice any conflicts between this and other documents.

Contact Honeywell Analytics Sales Support for a list of TPPR-compatible sensors, filters, test gases or other components.

The Honeywell contact details are on the back page of this document.

SAFETY

2 Safety Hazards, Warnings and Cautions

2.1 Safety

Incorrect set-up, maintenance, operation or modification of the Touchpoint Pro gas detection system *or its installation* may constitute a serious hazard to the health and safety of personnel and their environment. It is therefore imperative that the contents of the *Touchpoint Pro Operating Manual* are thoroughly understood by everyone who has access to the gas detection system or its associated equipment.

The *Touchpoint Pro Operating Manual* is available to download from the Honeywell Analytics website, whose address is on the back page.

> **DANGER**
>
> Always read the *Touchpoint Pro Operating Manual* in conjunction with this manual as it contains important safety notices and operational procedures.

> **DANGER**
>
> TPPR configuration settings are complex and incorrect settings can render the TPPR Gas Detection System dangerous, unreliable or inoperative, which may lead to multiple deaths and/or serious injury.
>
> Do not allow unauthorised or untrained people to access or use PC Configuration Software.

> **WARNING**
>
> Accessing TPPR over the Internet can expose you to security risks. It is strongly recommended that you use server-based firewall protocols and a VPN for additional security.

2.2 Online Security

Personal Computers and Networks are considered to always be at high risk of being deliberately compromised by third-parties, and by being inadvertently compromised by poor IT discipline, poor maintenance or simply through lack of user knowledge.

Touchpoint Pro is protected by security protocols, but it cannot protect itself against deliberate intrusion or damage from *compromised PCs*. This is especially so when a compromised PC is connected directly to TPPR without going through protected network servers, or when a disaffected employee is allowed privileged access.

PC users should always take the following basic safety precautions with their PCs, regardless of whether or not they use PC Configuration software or Webserver:

1. Follow your organisation's IT protocols at all times.

2. Always ensure that you have up-to-date OS patches and software installed.

3. Always ensure that you have the latest anti-virus database installed.

4. Only install approved software acquired from a reputable site or organisation.

5. Ensure that you restrict your online time to the minimum necessary.

6. Do not leave an unsecured or unlocked PC unattended.

7. Ensure that passwords and login names are kept hidden and secure.

8. Do not store unencrypted passwords on your PC.

9. Always take a TPPR backup whenever its configuration changes.

10. Log off from TPPR and websites as soon as you are finished.

11. Do not visit other online or social networking sites while connected to TPPR.

12. Do not discuss your TPPR system over the internet.

This page deliberately blank.

3 Touchpoint Pro Webserver – Introduction

Touchpoint Pro Webserver is an optional tool that allows users to remotely view Touchpoint Pro events and information, and to view and print reports, using a standard Web browser.

The Touchpoint Pro Webserver software is pre-installed on all Honeywell TPPR systems. The Webserver is activated by purchasing and installing a Product Key Licence.

Centralised Control Rooms have the option to manage multiple TPPR installations from one or more computers. Each TPPR Controller must have a unique IP address and an activated licence.

Any number of computers can be authorised but the recommended maximum is five simultaneous users for each controller.

3.1 Devices and Operating Systems

The Webserver software may be used with devices or computers with a browser that can support the https protocol, and can import and install a certificate from the TPPR webserver. Systems include:

- Windows
- iOS (iPad)
- Android

Note: as browsers and operating systems change frequently, it is not possible to list all suitable versions.

For security, client devices should use a current and maintained version of operating system.

3.1.1 Installation and Activation

Remote licence activation and certificate installation require a computer running a current and supported version of Windows.

3.2 Webserver Life-Cycle Process

1. Webserver software is installed on TPPR during manufacture.
2. The customer obtains a Product Key from their Honeywell Analytics sales representative to activate its licence.
3. End-users install an initial Webserver Certificate using the downloadable Webserver Certification Tool (WSCT).
4. End-users use a browser to connect to the TPPR to download and install a certificate to their computer.
5. End-users can then connect to Webserver using a browser for the licence period.
6. After 12 months from installation the certificate expires and may be renewed.

Note: A licence is required only for the TPPR Webserver. Client computers do not need a licence.

3.3 Security

TPPR has Network functionality that can only be accessed using the appropriate Honeywell tools and registered certificates. However, it is the user's responsibility to ensure that their own Network and Site security protocols are able to prevent unauthorised access.

3.3.1 Certification

Touchpoint Pro Webserver provides a secure (https://) connection to authorised network clients. System security is achieved by the following process:

1. The Touchpoint Pro must have a Webserver certificate installed using the Honeywell **Webserver Certification Tool** (WSCT), which must then be activated by entering a valid Product Key within 3 months from the day of installation.
2. The activated certificate must then be downloaded and installed to client computers to enable secure web access.
3. The Webserver certificate must be renewed annually and installed using the WSCT.

Note: Certificates are specific to each TPPR controller and cannot be transferred.

Note: Ensure that you only download Honeywell software from the official Honeywell Analytics website. Please speak to your Sales representative if you experience difficulties in accessing or downloading the software.

INTRODUCTION TO WEBSERVER

3.3.1 Touchpoint Pro Security Guide

Refer to the **Touchpoint Pro Security Guide** for further information. This can be obtained from your service representative or downloaded from the Honeywell TPPR web site.

3.4 Webserver Licence Status

The Webserver licence and certificate status can be checked from the controller touch screen, or from a remote computer on the same network.

3.4.1 Check Status from Controller

To check the current Webserver licence status, log into the TPPR Touchscreen and navigate to `Toolbox>Help>About`.

Click on the Webserver button to display the current licence status.

3.4.2 Check Status Remotely

To check the licence status from a connected device or computer, type:

`http://[TPPR IP]//misc/wslicense.asp`

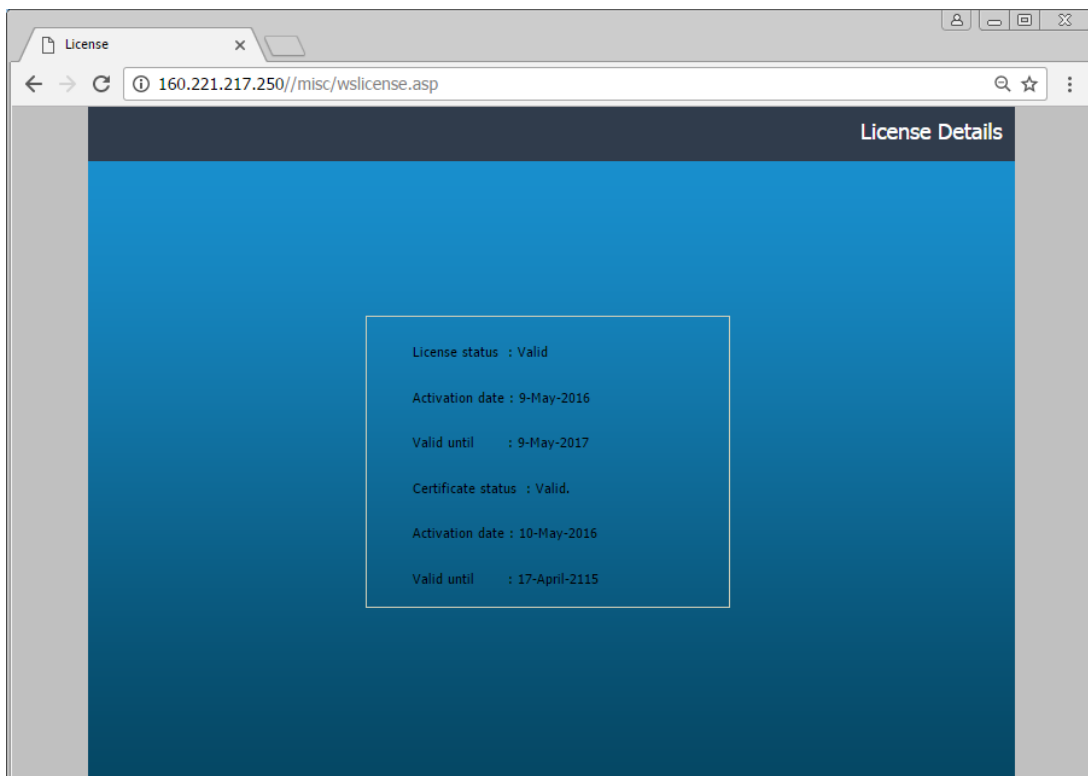in the address bar, where [TPPR IP] is the IP address of the TPPR controller.

Figure 1.   Webserver Licence and Certificate Status

Note: the device or computer does not need to have a Webserver certificate installed (described later) to carry out this check.

4 Webserver Operation

Once the Webserver has been activated and server certificate installed, any user can open a Webserver session on a client device or computer that has a matching certificate installed.

4.1 Users

Any user may **view** all Webserver screens and obtain and print reports. It is not necessary to have a TPPR account, or to log in to use most Webserver functions.

4.1.1 System Operations

Webserver permits a limited set off system operations.

- Reset
- Acknowledge
- Inhibit and Clear Inhibit

Users must log in to a valid account on the TPPR controller to carry out these operations.

4.1.2 Configuration

It is not possible for any user to change the system configuration, or view more than basic configuration details, from the Webserver interface.

4.2 Launching a Webserver Session

You can launch a Webserver session by typing the chosen Touchpoint Pro IP Address in your browser address bar and pressing **Return**.

Note: The address must be prefixed by **https;//**

Alternatively you may create a browser bookmark or desktop shortcut to connect to the Webserver.

4.2.1 Ending a Webserver Session

Webserver sessions do not time out, and remain open indefinitely. To end a session, close the browser window and exit the browser. On some browsers, simply closing the browser window is not adequate as the window can be re-opened.

Logged in users should log out before closing the window.

Note: Logged in users will be timed out and their login closed after a period of inactivity. No warning is provided. The Webserver session will remain open, but the user must log in again to carry out further operations.

4.3 Client Window

A webserver window, similar to that shown below, will open. Use the normal screen navigation tools, such as keyboard and mouse, to navigate the screen or to make selections.

Figure 2.   Webserver Home Page Example

WEBSERVER OPERATION

4.4 Menu Buttons

The following buttons are shown on the menu bar. Their functions are described in the following section.

KEY			
🏠	Home	🕐	View Event History
📕	View Active Events	➕	View Tool Box / Print Reports
📄	View Inputs	🔒	Locked / Log in
📄	View Outputs	🔓	Unlocked / Log out

4.5 Webserver Screens

The Webserver screen is similar to the controller touch screen, and enables many aspects of system status and operation to be viewed remotely. These include the following:

Note: For detailed descriptions of screens refer to the **Touchpoint Pro Operating Manual** or **Technical Handbook**.

4.5.1 Viewing Active events

View alarm, fault and warning details. Pop-out menus allow input and output details and input trend graphs to be viewed.

Figure 3.   Active Events Screen

4.5.2 View Input Status

The status of each input channel may be viewed. Similarly, pop-out menus allow the input details and trend graphs to be viewed for each input.
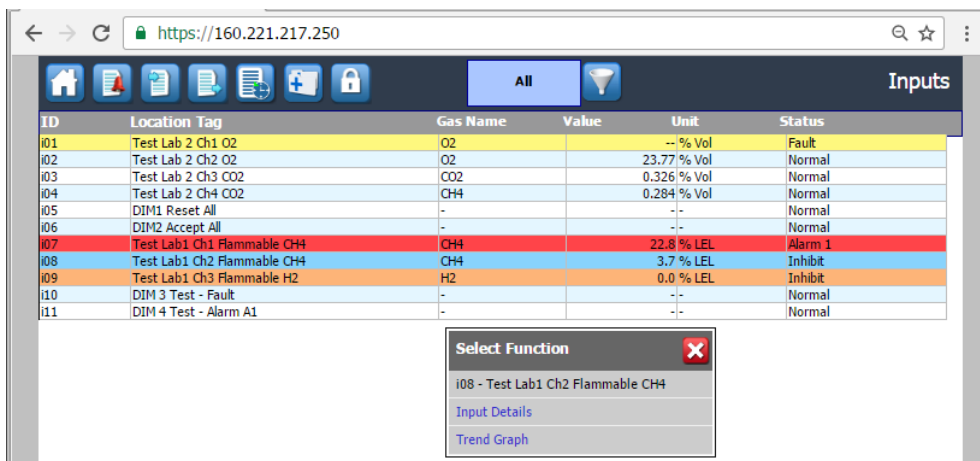

Figure 4.   Input Details Screen

4.5.3 View Output Status

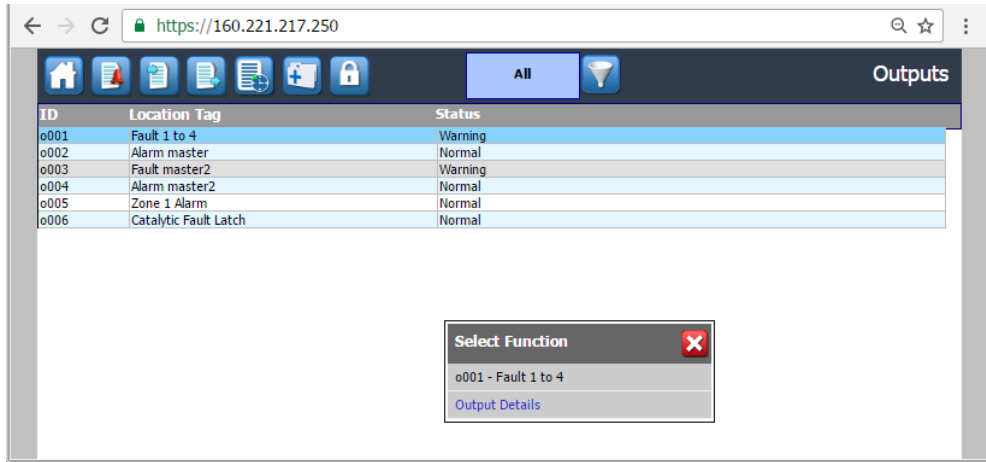The status of each output channel may be viewed.

Figure 5.   Output Details Screen

4.5.4 Event History

The event history records all events, including alarms, faults, warnings and system actions. The displayed events may be filtered by type and a time range set.

Figure 6.   Event History Screen

4.5.5 Tool box – SD card, Reports and Help

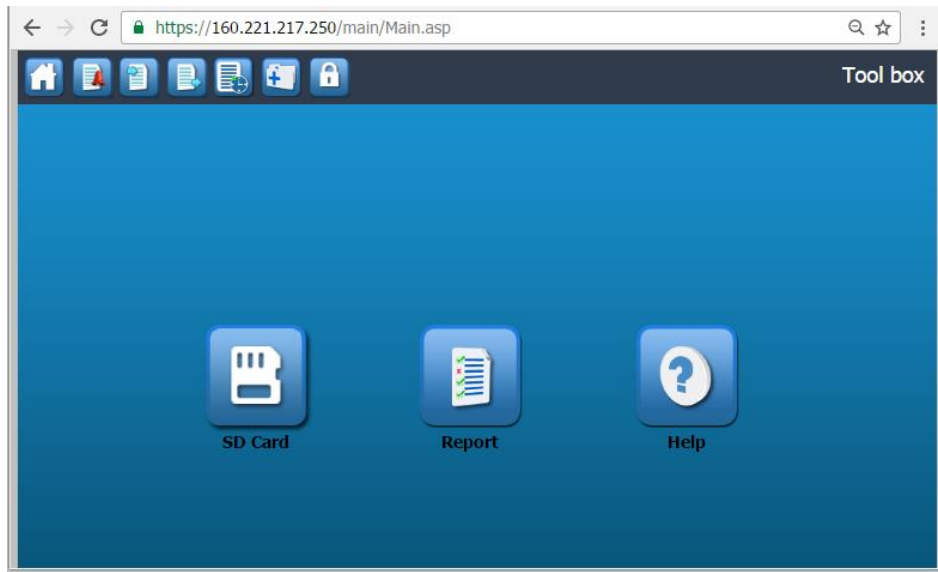The Tool box menu displays the following options:

Figure 7.   Tool Box Screen

- **SD Card** – Shows SD card status and usage
- **Help** – Displays controller software versions, service contact information, and configuration information
- **Report** – Allows a range of reports to generated, as described below:

4.5.5.1   Report Generation

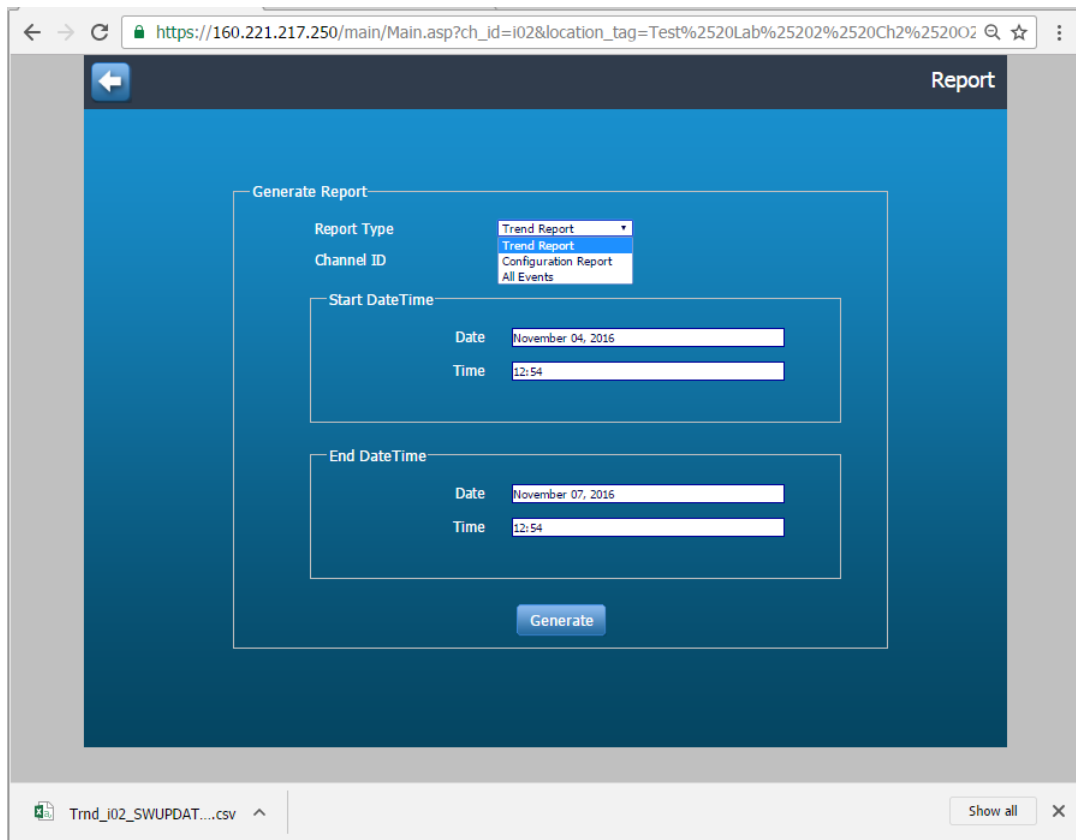The Webserver can generate Trend, Configuration and Event reports.

Figure 8.   Report Generation

Select the report type, date range and where appropriate the required channel, and click on **Generate**.

WEBSERVER OPERATION

A pop-up window provides options to:

- Open the file in the system's default spreadsheet application. The Webserver does not save the file, the user must save the file from the application.
- Save the file. The report is placed in the browser's designated Downloads folder. Reports are saved as comma separated .csv files and may be opened by a spreadsheet application or a text editor.
- Save the file to a specific location ("Save As") with required file name. .

Note: The options presented may vary between browsers, and browser settings. Some browsers may save automatically.

4.5.5.2   Browser pop-up permissions

Webserver uses a browser pop-up window when a report is generated. Webserver needs to know whether to open or save the file, and the destination when saving.

It may be necessary to enable pop-ups for the Webserver. This is normally found in your browser **Privacy** settings.

4.5.6   System Operations

Users with suitable account permissions can carry out the following system operation:

- Reset
- Acknowledge
- Inhibit and Clear Inhibit

Users must log in to a valid account on the TPPR controller to carry out these operations. System operations are available from the **Active Events**, **Inputs** and **Outputs** screens.

Figure 9.   System Operation Example
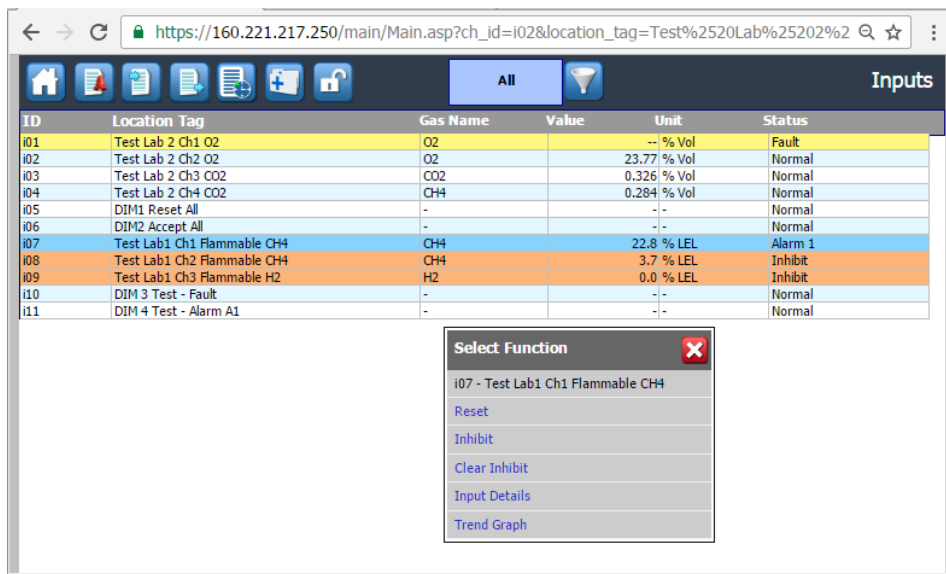
To access the system operations, select the required item on the display. A pop-out menu shows the available actions for that channel.

4.5.6.1   Safe Interaction

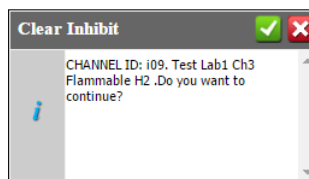If the Safe Interaction mode is enabled at the controller a confirmation pop-up is displayed for each action.

Figure 10.   Safe Interaction Confirmation

Confirm or cancel the operation as required.

WEBSERVER OPERATION

This page deliberately blank.

.

5 Activating the Webserver

The Webserver software is pre-installed on TPPR controllers. To use the Webserver:

5.1 Initial Licence Activation

The following steps are required to activate the Webserver licence for the first time. These steps are described in more detail below.

1. Obtain a Product Key code from your sales representative.

2. Enter the Product Key to activate the Webserver License.

3. Install the server certificate on the TPPR. The certificate is required to provide secure communications, and is locked to the IP address of the TPPR and the Product Key.

4. Install a matching certificate on each client device or computer to be used for Webserver sessions.

The certificate is created and optionally installed using the Webserver Certification Tool, which may be downloaded from the TPPR web page. The tool has two modes of operation, described later in this document:

- Online Mode– a direct Ethernet connection to the TPPR controller is available.
- Offline Mode – no direct connection is available.

5.2 Licence Renewal

To renew the licence:

1. Obtain a new Product Key code from your sales representative.

2. Enter it into the TPPR controller, either using the touchscreen or the Webserver Certification Tool as described below.

5.3 Obtaining a Product Key

To buy a product key, contact your sales representative. The following information is required:

1. The serial number of the controller. This will be on your shipping order or can be found on the product label on the back of the controller cover. It is a 13 digit number beginning with a G, for instance G017371501001.

2. The MAC Address of the controller. This can be found by logging into the Touchscreen and navigating to `Toolbox>Global Settings>TCP/IP settings.`

3. The controller software versions, accessible from the *Help, About* screen.

4. The name and work address of the person to whom the product key should be sent.

The product key is generated using this information and is sent by traditional mail to the named person.

Note: The product key cannot be sent electronically.

5.4 Webserver Licence Activation or Renewal

The Touchpoint Pro Webserver licence is activated by entering your Product Key using the Touchpoint Pro Touchscreen, or by using the Webserver Certification Tool (WSCT) described later in this document. To activate from the controller:

1. Log in to the TPPR Touchscreen as Administrator.

2. Navigate to `Extras>Global Settings>Component Update>Activate Webserver`.

3. Touch the **Enter Licence Key** box and enter your **Product Key** using the pop-up keyboard.

4. Press **OK** when done, and Touchpoint Pro will confirm if the licence is activated. Re-enter the product key and try again if you were unsuccessful.

5. Log out when done.

Note: The product key must be used within three months from the day the certificate was installed in the Controller. Contact your sales representative for advice if your key does not work.

5.4.1 Client Certificate

1. Connect a client computer to the TPPR and download the signing certificate as described in section 7.

You can now connect to Webserver at `https://<your TPPR IP address>`

ACTIVATING THE WEBSERVER

5.5 Webserver Certification Tool (WSCT)

The Webserver Certification Tool (WSCT) is used to install or renew the Webserver Certificate in the TPPR Controller. This could be done by your Service Contact during commissioning or annual maintenance, but full instructions are given in this chapter for those who do need or want to install their own certificates.

5.6 Installing the Webserver Certification Tool (WSCT) on a Windows PC

Note: Before downloading the WSCT tool, contact your sales or service representative to ensure that your TPPR system software is at a compatible software level.

To install or renew the TPPR Certificate you will first need to download and install WSCT on your local Windows PC:

1. Visit http://www.honeywellanalytics.com, select your language and navigate to **/products/Touchpoint-Pro**.

2. Click on **Software**, fill out the form and click **Download**

Figure 11.   Software Download Web Page

3. Click on the WSCT Software link and download the Webserver Certification Tool.

4. Run the downloaded program and install it on your PC.

5.7 Prerequisites for Running the WSCT

1. The TPPR system date, clock and time zone setting must be the same as the PC system's date, clock and time zone setting. (A valid licence may be judged invalid or connection delays may be experienced if they are not. See *Ch.9 Troubleshooting* for further information.)

2. The TPPR must have a unique static IP address.

3. You must know the TPPR's static IP address.

4. You must have Admin rights on the target PC to install and configure the software.

5. You must have the current printed Product Key.

6. You must not try to install the Product Key before its start date or more than 3 months after the start date.

Note: TPPR is delivered with a default static IP address, which should be changed prior to creating the certificate. Otherwise it will be necessary to re-install the certificate when the IP address is changed.

6 Installing the Licence and Certificate

There are two certificate installation modes when using the WSCT:

- **Online Mode**. Online Mode is used when the TPPR is already installed on a network and can be accessed from the PC being used for licensing. The network may be a simple peer to peer network or a corporate LAN.
- **Offline Mode**. This mode is when the IP address of the controller has been changed or a direct connection is not available, for instance if the network is not yet connected.

6.1 **Enabling the Remote Connection Port**

The Webserver Certification Tool uses the TPPR Remote Connection software port, which shares the Ethernet port. For security reasons the port must be enabled before a WSCT connection can be made. The port must be enabled at the TPPR controller touchscreen.

Note: The remote connection port is shared with the PC Configuration software tool. Terminate any PC Configuration session before opening a WSCT connection.

Log in at the controller and navigate to the TCP/IP Settings screen. Administrator access is required. Select the Tools icon and select the **Enable 2 Hours** option as shown below.

Figure 12.   Enabling the Remote Connection Port

The port will remain open for two hours, and will then automatically close. If for any reason the licensing is not completed within two hours, or the connection is disabled for other reasons, the port may be immediately re-opened by repeating the above steps. It is not necessary to remain logged in at the controller after enabling the port.

On completion it is recommended to navigate to the menu and select the **Disable** option to manually close the port.

Note: PC Configuration and Webserver Certification Tool software share Remote Connection Port, but only one connection can be active at a time.

Note: The Enable / Disable option does not affect the network status; it only affects the remote connection port. Other operations such as printing are not affected. It is not necessary to enable the Remote Connection port to use the Webserver after licencing is complete.

Note: All Enable / Disable events are recorded in the TPPR Event Log.

The Remote Connection port is described in more detail in the **Touchpoint Pro Technical Handbook**.

INSTALLING THE WEBSERVER CERTIFICATE

6.2 Installing the Licence and Certificate Using Online Mode

Installation is carried out in three parts:

- Activate the Webserver licence.
- Install the server certificate on the TPPR.
- Install client certificate(s) on client browser(s).

6.2.1 Installation Procedure – Online Mode

1. Enable the Remote Connection port and start the WSCT program by using the shortcut on your desktop or in your Start menu.

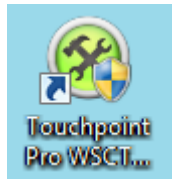**Figure 13.   WSCT Desktop Shortcut Icon**

2. Enter the TPPR's **IP Address** and click on **Connect**. The software should connect within a few seconds.
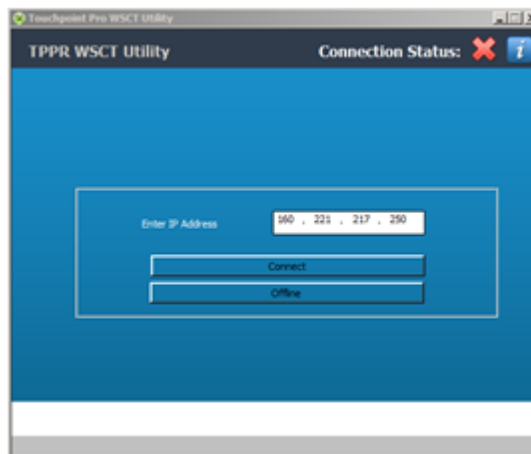

Figure 14.   WSCT Home Page Window

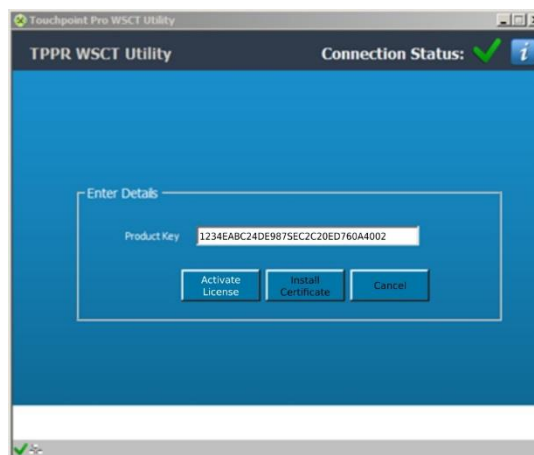3. Enter the 32 character product key and click on **Activate Licence**.

Figure 15.   WSCT Licence Activation Window

4. A pop up message is displayed to indicate success or warn of any errors.

6.2.2 Installing the Server Certificate

The certificate may be installed directly after activating the licence, or at a later time.

Note: Confirm that the date and time zone are correctly set on the controller and on the PC.

1. Enable the Remote Connection port as described above, if not already open.

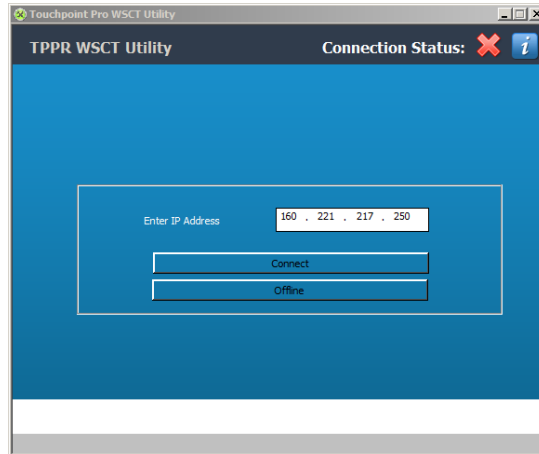2. Start the WSCT utility and connect to the TPPR by clicking **Connect**.

Figure 16.   WSCT Home Page Window

3. Ensure that the TPPR is not busy carrying out system operations such as calibration, configuration, or a backup or restore.

4. Click on **Install Certificate**.
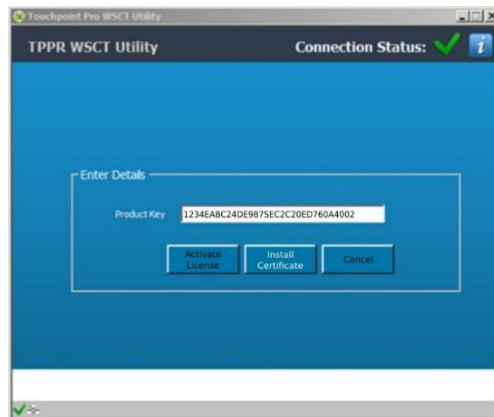
Figure 17.   WSCT Install Certificate Window

5. The controller will display a confirmation pop-up. Click on **OK**.

6. On completion, navigate to **Help, About** and click on **Webserver**. Verify that the certificate **Start and Finish dates** are set, and that the certificate status is shown as **Valid**.

6.2.3 Check the Installation

On completion, check that the installation was successful as described in section 3.4

6.2.4 Web Clients

When the certificate is installed on the controller, import the certificate details to each web client as described in Chapter 7, *Installing the Client Certificate.*

6.3 Installing the Server Certificate Using the Offline Mode

In this mode the WSCT tool generates a CAB file with the certificate details. The CAB file is saved to a USB memory device for installing on the controller.

This method is required if the IP address of the controller has been changed, or a direct connection is not available. Installing the CAB file overwrites any data still using the old IP address, and allows correct Webserver operation with the new IP address.

Note: The certificate must be installed within **three months** of issue. If not installed within three months a replacement product key must be obtained. Contact your sales representative for advice.

6.3.1 Installation Procedure – Offline Mode

1. Check that:

    a) The TPPR system clock and time zone are correctly set and match the host PC settings.

    b) You have the current printed Product Key.

    c) You know the current TPPR IP address. (`Tool box>Global Settings>TCP/IP Settings`)

    d) You know the TPPR MAC Address. (`Tool box>Global Settings>TCP/IP Settings`)

2. Create a short passphrase of up to 16 alphanumeric (ABC123) characters, without spaces or underscores. Note it down as you will need it more than once.

3. Start the WSCT utility and click on **Offline.**

Figure 18.   WSCT Offline Mode Selection

4. Enter the controller **IP address**, **MAC ID** and your passphrase.

5. Click on **Generate CAB**.

Figure 19.   WSCT Generate CAB Window

6. A message will be displayed showing the location of the CAB file. Note the location, or navigate to the file location, before dismissing the message.
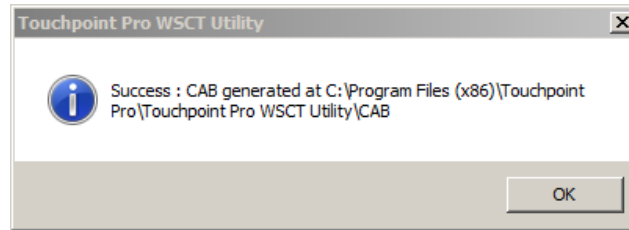

Figure 20. CAB File Generated Dialog

7. Locate the CAB file and copy it to a USB memory device.
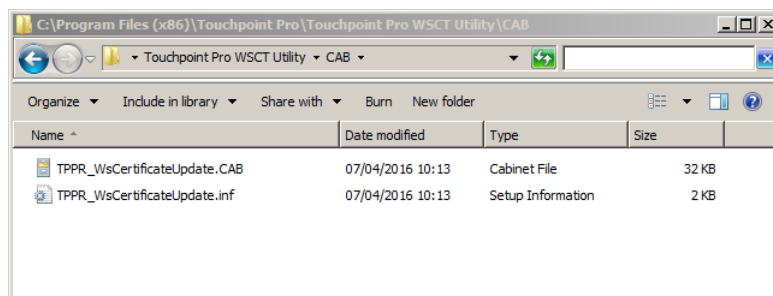
Figure 21. CAB File stored Dialog

8. Close the WSCT utility.

9. Connect the USB device to the TPPR controller. (See the *Touchpoint Pro Operating Manual*.)

10. Log in as an **Administrator**, and navigate to `Tool Box>Global Settings>Component Updates`.

11. Click on **Webserver Certificate Update** and enter your saved pass phrase when requested.

12. Finally click on **Activate Webserver** and type the Product Key.

13. Remove the USB memory device and return TPPR to normal (See the *Touchpoint Pro Operating Manual*.)

14. Use WSCT as required.

6.3.2 Web Clients

When the certificate is installed on the controller, import the certificate details to each web client as described in *Ch.3.6 Installing the Client Certificate on User PCs* above.

INSTALLING THE WEBSERVER CERTIFICATE

This page deliberately blank.

7 Installing the Client Certificate

7.1 Introduction

To ensure that the Webserver connection is secure, TPPR uses a security certificate. A copy of the certificate must be installed on each device used to communicate with the Webserver. If a certificate is not present, the Webserver will not communicate with the device.

The certificate is downloaded from the TPPR using an initial Ethernet connection. It is then installed on the client device, after which the device can connect to the Webserver using the secure https protocol.

There is no limit to the number of client devices. However, performance may be degraded if more than five devices are connected simultaneously.

If multiple TPPR systems are in use, a separate certificate must be obtained from each system and installed.

7.1.1 Renewal

The certificate does not need to be renewed. A new certificate must be downloaded if the IP address of the TPPR is changed.

7.1.2 Downloading the certificate

The certificate may be downloaded by opening a browser and typing `http://[TPPR IP]/misc/caroottppr.cer` in the address bar then pressing **Enter**.

7.1.3 Installation Process

The installation process for Windows is described below. Other operating systems will have an equivalent method.

7.1.4 Internet Settings

TLS1.0 must be enabled on the client device.

In Windows this can be checked by navigating to the **Internet Properties** window, opening the **Advanced** tab and scrolling down to the required settings.

7.2 Certificate Installation on Windows

1. Locate and open the Internet Properties window, for instance by going to `Control Panel>Internet options`.

2. Open the **Advanced settings** tab and ensure that **Use TLS 1.0** is checked.

3. Select **OK** when ready to save the settings. You should not need to do this check again.

4. Type `http://[TPPR IP]/misc/caroottppr.cer` in your browser address bar and then press **Enter**.

5. A certificate download dialog will appear:
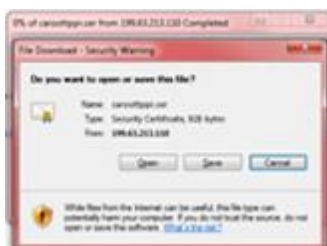
Figure 22.   Download the Client Certificate   **Figure 23.   Certificate Icon**

It may be necessary to first allow a pop-up and accept a site without a valid certificate.

6. Click **Save** to save the certificate to your PC. (Normally this will be your browser default save location, e.g. your **Downloads** folder.)

7. Double click on the saved certificate file to open it.

8. Select **Install Certificate…** and click **Next** when the Certificate Import Wizard appears.

INSTALLING THE CLIENT CERTIFICATE

9. Click **Install Certificate**.
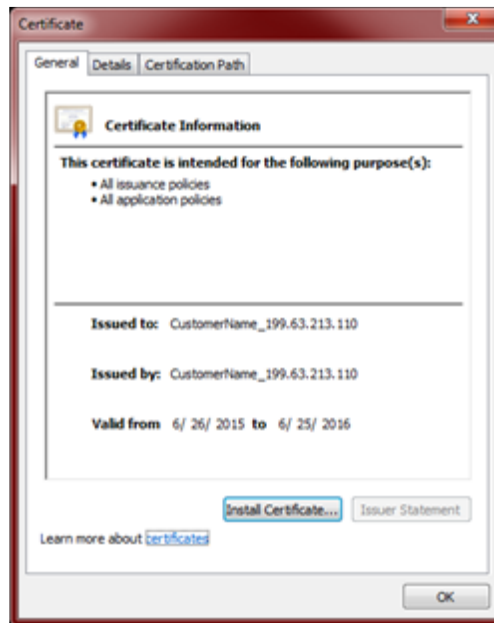
Figure 24.   Certificate Information

10. Ensure that **Place all certificates in the following store** is checked, then browse for and select the location **Trusted Root Certification Authorities.**
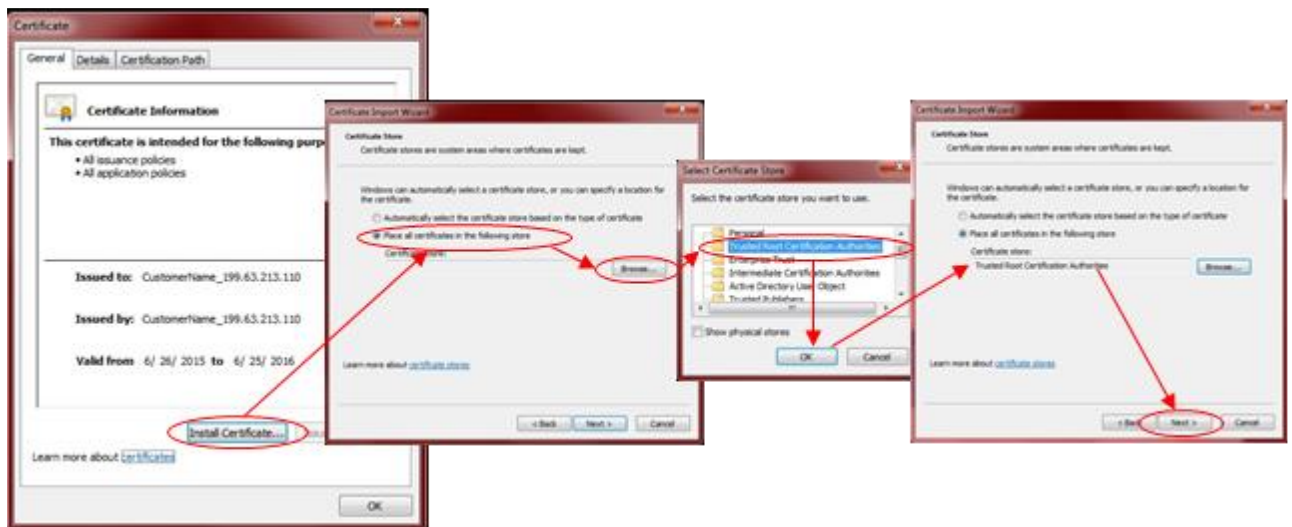
Figure 25.   Select Certificate Store

11. Click **OK** and **Next >,** followed by **Finish,** to import the certificate:

Figure 26.   Import Certificate and Finish

12. Click **OK** to exit the Wizard.

INSTALLING THE CLIENT CERTIFICATE

7.3 Certificate Installation on iPad

The certificate may be downloaded to an iPad but requires additional file management software to access the downloaded file.

A simple method is to send the certificate to the iPad as an email:

1. Download the certificate to a computer:

2. Type `http://[TPPR IP]/misc/caroottppr.cer` in your browser address bar and then press **Enter**.
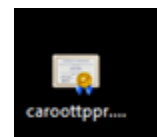
3. Attach the certificate file to an email and send to an account on the iPad.

4. Open the email and click on the attachment.

5. Follow the on-screen prompts to install the certificate.

INSTALLING THE CLIENT CERTIFICATE

This page deliberately blank.

8 Managing Certificates and Licence

8.1 Removing a Webserver Certificate

You can only remove a Webserver Certificate by using the TPPR Touchscreen.

To remove the certificate:

1. Log in to TPPR as **Administrator**

2. Navigate to `Extras>Global Settings>Component Updates`.

Figure 27.   Component Management Dialog

3. Click on **Webserver Certificate Remove**. (All connections will be terminated, effective after the next screen change.

4. Log out.

Note: The user can install further Webserver certificates using the same licence key, or a new one, but in either case it will be a different instance and users will need to re-import the web client certificate again. (You should delete the old certificate before installing a new one).

Note: This also applies if you generate a new CAB in offline mode, even when using the same key. However, if you installed the certificate offline using a CAB, you can re-install (Update) using the same CAB, which will restore the original Webserver certificate so that you can continue without replacing the client certificates.

8.2 Change of TPPR IP Address

If the TPPR IP address has changed, the Webserver will not work correctly with the new address.

To restore Webserver operation:

1. Ensure that you have the Product Key to hand, and a PC with the WSCT tool installed.

2. Change the TPPR IP address and check that it operates correctly.

3. Remove the old Webserver certificate, as described above.

4. Re-install the certificate using the Offline mode, as described above.

5. Re-new the Web Client certificates on each user PC.

MANAGING CERTIFICATES AND LICENCE

8.3 Renewing the Webserver Licence

To update the licence, obtain and install a new product key as described above.

Note: Check that the TPPR controller IP address has not changed. If it has, inform your sales representative when applying for a new Product Key.

Note: It is not necessary to renew the certificate when renewing the licence.

Note: Certificates on client devices do not need to be updated when the licence is renewed.

8.4 Activating Webserver Licences

When the new product key arrives, activate the licence as shown below.

8.4.1 Licence Renewal Using the Optional WSCT Utility

1. Start the WSCT utility.
2. Connect to the controller.
3. Enter the new product key.
4. Click on **Activate Licence**.

8.4.2 Licence Renewal Using the TPPR Controller

1. Log in as **Administrator**.
2. Navigate to `Extras>Global Settings>Component Updates` and click on **Activate Webserver**
3. Enter the new product key and any unexpired time on the existing licence will be transferred to the new licence.
4. Log out.

9 Troubleshooting

Please notify your Service representative or Honeywell Analytics if you experience any issues that are not explained below.

Problem	Solution
You cannot connect to the Touchpoint Pro Consider using a utility such as Ping to check the connection to the TPPR controller.	• Check that TPPR has a valid IP address, and that it is enabled. • Check if the TPPR IP address has changed • Check that you have a good network connection. • Check that TPPR is powered up and online. • Check that you have entered the correct IP address. • Check that there are no error messages on the Touchpoint Pro screen • Check for possible network or firewall restrictions.
Message seen on the Touchpoint Pro Controller: "The System has detected a conflict for statically assigned IP address <u>***</u> | <u>***</u> | <u>***</u> | <u>***</u> and with the system having hardware address <u>***</u> | <u>***</u> | <u>***</u> | <u>***</u>. The local interface has been disabled."	Another machine on the network is using the same IP address. Resolve the address conflict. Note that a change to the TPPR IP address will require the TPPR certificate and all client certificates to be re-installed. If changing the TPPR IP address, re-connect the system to the network before pressing Save. It may be necessary to re-enable the connection, from the same screen.
You see a timeout error message.	This may happen when you use a VPN and/or are routed through distributed servers. Try disconnecting from your VPN and using a clear connection. Try again when the network is less busy.
You cannot connect to the Webserver after installing the Licence.	The Licence validity period is controlled by the time setting on the PC running the certification tool. If the time on the TPPR controller is different from the time set on the PC, e.g. due to using Daylight Saving Time, there may be an initial connection refusal until the time difference has elapsed. This applies to both online and offline licensing modes.
You cannot connect to the Webserver after changing the TPPR IP Address	The Webserver Certificate is locked to the TPPR IP Address that was current when the certificate was installed. You will have to obtain a new Product code and install a new certificate using the new IP Address.
You cannot connect to the Webserver.	• Check that you are using **https**:// in your browser. • Check your Webserver Licence is still valid. • Check if the TPPR IP address has changed. It is necessary to reinstall the Webserver certificate and client certificates following a change. • Check the network connections, as above
You cannot log in to the Webserver.	Check that you have entered a valid TPPR username and password.
You cannot carry out executive actions from the Webserver.	• You are not logged in, or do not have sufficient user privilege.

MANAGING CERTIFICATES AND LICENCE

You cannot see generated Reports, and/or you got a Pop-Up warning message when you clicked the Generate button.	If the report did not download as a .csv file, your browser may be blocking it by default. To fix this issue, add the TPPR IP Address as an exception in your Pop-up notification. For Windows you may add it from: `Browser Settings>Privacy>Content Settings>Pop-ups`. You may need to generate the report again after adding the exception.
Error message: "Invalid License Key".	• Incorrect date set on the Touchpoint Pro • Incorrect date set on your PC (Daylight Saving Time error?) • Date and time not synchronized between TPPR and your PC • Product key validity genuinely expired
Webserver Operation is slow.	• Check the network operation • Check the number of connected clients. More than five connected clients can lead to reduced performance.

Find out more at

www.honeywellanalytics.com

Contact Honeywell Analytics:

Europe, Middle East, Africa

Life Safety Distribution GmbH

Javastrasse 2

8604 Hegnau

Switzerland

Tel: +41 (0)44 943 4300

Fax: +41 (0)44 943 4398

gasdetection@honeywell.com

Customer Service

Tel: 00800 333 222 44 (Freephone number)

Tel: +41 44 943 4380 (Alternative number)

Fax: 00800 333 222 55

Middle East Tel: +971 4 450 5800 (Fixed Gas Detection)

Middle East Tel: +971 4 450 5852 (Portable Gas Detection)

Americas

Honeywell Analytics Inc.

405 Barclay Blvd.

Lincolnshire, IL 60069

USA

Tel: +1 847 955 8200

Toll free: +1 800 538 0363

Fax: +1 847 955 8210

detectgas@honeywell.com

Asia Pacific

Honeywell Analytics Asia Pacific

7F SangAm IT Tower,

434 Worldcup Buk-ro, Mapo-gu,

Seoul 03922,

Korea

Tel: +82 (0)2 6909 0300

Fax: +82 (0)2 2025 0328

India Tel: +91 124 4752700

analytics.ap@honeywell.com

Technical Services

EMEA: HAexpert@honeywell.com

US: ha.us.service@honeywell.com

AP: ha.ap.service@honeywell.com

www.honeywell.com

Honeywell

DSA Suppliers

Thank you for reading this. For pricing or further information, please contact us.

W: https://dsasuppliers.com
E: sales@dsasuppliers.com
P: +441158390391

Leading UK Supplier
Brand New & Genuine OEM Parts
Delivered Worldwide

Worldwide Delivery   1000+ Genuine Parts & Equipment