ADPRO
XO Client Software

User Manual

For FastTrace 2 Series, iFT Series, and eFT Series

March 2023
Doc. 21796_19
Software version XO 5.3

Honeywell

Disclaimer

The contents of this document are provided on an "as is" basis. No representation or warranty (either express or implied) is made as to the completeness, accuracy or reliability of the contents of this document. The manufacturer reserves the right to change designs or specifications without obligation and without further notice. Except as otherwise provided, all warranties, express or implied, including without limitation any implied warranties of merchantability and fitness for a particular purpose are expressly excluded.

Intellectual Property and Copyright

This document includes registered and unregistered trademarks. All trademarks displayed are the trademarks of their respective owners. Your use of this document does not constitute or create a license or any other right to use the name and/or trademark and/or label. This document is subject to copyright owned by Honeywell. You agree not to copy, communicate to the public, adapt, distribute, transfer, sell, modify, or publish any contents of this document without the express prior written consent of Honeywell.

Trade Name Statement

ADPRO, FastTrace, iFT, iFT-E, eFT, iFT Gateway, IntrusionTrace, LoiterTrace, XO, iTrace, iCommand, iCommission, iPIR, and FMST are trademarks and/or registered trademarks of Honeywell and/or its subsidiaries in the United States and/or other countries. Other brand names mentioned herein are for identification purposes only and may be trademarks of their respective holder(s). Your use of this document does not constitute or create a licence or any other right to use the name and/or trademark and/or label.

General Warning

This product must only be installed, configured and used strictly in accordance with the General Terms and Conditions, User Manual and product documents available from Honeywell. All proper health and safety precautions must be taken during the installation, commissioning, and maintenance of the product. The system should not be connected to a power source until all the components have been installed. Proper safety precautions must be taken during tests and maintenance of the products when these are still connected to the power source. Failure to do so or tampering with the electronics inside the products can result in an electric shock causing injury or death and may cause equipment damage. Honeywell is not responsible and cannot be held accountable for any liability that may arise due to improper use of the equipment and/or failure to take proper precautions. Only persons trained through an Honeywell accredited training course can install, test and maintain the system.

Liability

You agree to install, configure, and use the products strictly in accordance with the User Manual and product documents available from Honeywell.

Honeywell is not liable to you or any other person for incidental, indirect, or consequential loss, expense or damages of any kind including without limitation, loss of business, loss of profits, or loss of data arising out of your use of the products. Without limiting this general disclaimer the following specific warnings and disclaimers also apply:

Fitness for Purpose

You agree that you have been provided with a reasonable opportunity to appraise the products and have made your own independent assessment of the fitness or suitability of the products for your purpose. You acknowledge that you have not relied on any oral or written information, representation, or advice given by or on behalf of Honeywell or its representatives.

Total Liability

To the fullest extent permitted by law that any limitation or exclusion cannot apply, the total liability of Honeywell in relation to the products is limited to:

i. in the case of services, the cost of having the services supplied again; or
ii. in the case of goods, the lowest cost of replacing the goods, acquiring equivalent goods or having the goods repaired.

Indemnification

You agree to fully indemnify and hold Honeywell harmless for any claim, cost, demand, or damage (including legal costs on a full indemnity basis) incurred or which may be incurred arising from your use of the products.

Miscellaneous

If any provision outlined above is found to be invalid or unenforceable by a court of law, such invalidity or unenforceability will not affect the remainder which will continue in full force and effect. All rights not expressly granted are reserved.

Document Conventions

The following typographic conventions are used in this document:

Convention	Description
Bold	Used to denote: emphasis. Used for names of menus, menu options, toolbar buttons…
Italic	Used to denote references to other parts of this document or other documents. Used for the result of an action.

The following icons are used in this document:

Icon	Description
	Note. This icon indicates information of special interest that will help the reader make full use of the product, optimise performance, etc. Failure to read the note will not result in physical harm to the reader, or damage to equipment or data.
	Caution! This icon indicates danger to equipment. The danger can be loss of data, physical damage to the equipment, or permanent corruption of configuration details.
	Warning! This icon indicates danger of physical harm to the reader. Not following instructions may lead to death or permanent injury.
	Warning! This icon indicates danger of electric shock. This may lead to death or permanent injury.

Contact Us

www.security.honeywell.com

Contents

1 About this Document 11
1.1 What is XO 5? 11
1.2 Scope 11

2 Installing the XO Client Software on Your PC 12
2.1 System Requirements for the Client PC 12
2.1.1 Hardware 12
2.1.2 Software 13
2.2 Installing the XO Client Software Using the Installer 13
2.3 Installing the XO Client Software via the XO Device's Web Page 16
2.3.1 Internet Explorer Settings 16
2.3.2 Changing the PC's IP Address 18
2.3.3 Installation 22
2.4 Launching and Initial Configuration 27
2.4.1 Launching the XO Client 27
2.4.2 Adding an XO Device to the XO Client 28
2.4.3 Demo Devices 30
2.4.4 Deleting an XO Device 31
2.4.5 Connecting to an XO Device 32
2.4.6 Filtering the Device List 34
2.4.7 Changing an XO Device 35
2.4.8 Changing the Work Folder 35
2.4.9 Setting the Date and Time 36
2.4.10 Manually Synchronising with NTP Server 38
2.4.11 Creating a Direct Shortcut to a Device 38
2.4.12 Reusing an Existing Device List 40
2.5 Software Updates 40

3. Connections 44
3.1 Network (Ethernet) 44
3.2 Telnet Connection 47
3.3 Restrictions for Port Number Usage 49
3.4 Communication with External Networks (Routers and Firewalls) 49
3.5 Bandwidth 51
3.6 Dynamic DNS 51
3.6.1 About Dynamic DNS 51
3.6.2 Setup 51
3.6.3 Troubleshooting Dynamic DNS 52
3.7 Restricting Access to the XO Device 53
3.8 PPP Connection (Modem) 54
3.8.1 About Modems 54
3.8.2 Dynamic DNS for Modems 54
3.8.3 PSTN or ISDN Modem Configuration 54
3.8.4 3G/4G Modem Configuration 56
3.8.5 Troubleshooting 3G/4G Modem Setup 57
3.9 4G Wingle Connection 58
3.9.1 Preparing the Wingle 58
3.9.2 Wingle PPP Configuration 62
3.10 Email 62
3.10.1 Setting up Email 62
3.10.2 Setting up Email with Gmail 64
3.10.3 Creating Mailing Lists 65
3.10.4 Verifying Email Communication 67
3.11 IP Camera Network 68
3.11.1 General Setup 68

3.11.2 IP Cameras in Multiple Network Segments (Static Routing) ... 70
3.12 I/O Cards (MIO and EIO) ... 74
3.12.1 Configuring the I/O Cards ... 74
3.12.2 Updating the MIO Card Firmware ... 76
3.12.3 MIO and EIO Cards Inputs/Outputs ... 77
3.13 Network I/O Units (Net I/O) ... 81
3.13.1 About Network I/O Units ... 81
3.13.2 Adding a Net I/O Unit with Known IP Address ... 82
3.13.3 Searching Net I/O Units on the Local Network ... 82
3.13.4 Modifying the Settings of a Net I/O Unit ... 83
3.13.5 Deleting a Net I/O Unit ... 83
3.13.6 Net I/O Unit Inputs and Outputs Setup ... 84
3.13.7 Net I/O Unit Inputs and Outputs ... 85
3.14 Connection to S3100 ... 88
3.14.1 Communication with S3100 Security Panels ... 88
3.14.2 Handling Inputs from S3100 Security Panels ... 89
3.14.3 Sending Triggers to the S3100 Security Panel ... 90
3.15 VPN connection ... 91
3.15.1 VPN configuration ... 91
3.15.2 Set up A L2TP/IPSec VPN in Windows Server 2019 ... 93
3.15.3 Add an account for XO NVR on Windows Server 2019 ... 105

4 Alarm Transmission ... 109
4.1 Alarm Transmission Channels ... 109
4.2 Life Check (Site Pulse) ... 110
4.3 General Alarm Transmission Settings ... 111
4.4 Primary Alarm Transmission Settings ... 112
4.5 Backup (Secondary) Alarm Transmission Settings ... 113
4.6 Parallel Transmission Settings ... 114

5 Using IP Cameras ... 115
5.1 Available IP Camera Channels ... 115
5.2 Prerequisites ... 115
5.3 Selecting Suitable IP Cameras ... 116
5.4 Analytic Resolution for IP Cameras ... 116
5.5 Streams with Different Aspect Ratios ... 117
5.6 Troubleshooting Analytic Resolutions ... 118
5.7 Using Cameras in Corridor Mode ... 120
5.8 Enabling IP Cameras ... 120
5.9 IP Camera Discovery ... 124
5.10 Changing a Camera's IP Address Using the Discovery Tool ... 126
5.10.1 Changing an IP Address for a Single Camera ... 126
5.10.2 Changing Multiple IP Addresses Using a Range ... 130

6. Using Analogue Cameras ... 136
6.1 Video and Audio Connections ... 136
6.2 Enabling Analogue Cameras ... 136

7 Camera Settings ... 138
7.1 General Settings ... 138
7.2 Video Settings ... 138
7.2.1 Brightness, Contrast, Saturation ... 138
7.2.2 Pixelation ... 139
7.2.3 Anonymization ... 141
7.3 Camera Calibration ... 142
7.3.1 About Camera Calibration ... 142
7.3.2 3D Calibration ... 142
7.3.3 3D Calibration from Live Images ... 143
7.3.4 3D Calibration from Recorded Images ... 147
7.3.5 Bounding Box Calibration for Different Aspect Ratios ... 148

7.4 Overlay 151
7.5 Live View and Multicast (Parameters) 152
7.6 PTZ Control for Analogue Cameras 153
7.6.1 PTZ Control via USB Port/MIO Card 154
7.6.2 USB Port/MIO Card Supported PTZ Protocols 155
7.6.3 PTZ Control via DTC Card 155
7.6.4 DTC Supported PTZ Protocols 156
7.7 PTZ Setup 156
7.8 Recording Parameters 158
7.9 Copying Camera Settings 159
7.10 Disabling Cameras 160
7.11 Remote Access to IP Camera 161

8 Audio 164
8.1 About Audio 164
8.1.1 Audio Input 164
8.1.2 Audio Output – Talkback 164
8.1.3 Full Duplex Mode 164
8.2 Audio Communication Setup 165
8.3 Setting up Audio Inputs 166
8.4 Setting up Audio Outputs 167
8.4.1 Specifying the Audio Switcher Type 167
8.4.2 Associating Cameras with Audio Outputs 167
8.5 Using IP Audio Devices 168

9 Recording Behaviour 170
9.1 Setting up Recordings 170
9.2 Creating Recording Conditions 170
9.3 Recording-Controlled Camera Actions 171
9.4 Setting up the Active Periods 173
9.4.1 Dates and Days of the Week 173
9.4.2 Time in the Days: Time-Based and Mode-Based Recording 174
9.5 Continuous Recording 174
9.5.1 Definition 174
9.5.2 Time-Based Continuous Recording 174
9.5.3 Mode-Based Continuous Recording 175
9.6 Recording on Event 176
9.6.1 Definition 176
9.6.2 Time-Based Recording on Event 177
9.6.3 Mode-Based Recording on Event 180
9.7 Changing or Deleting Recording Conditions 182
9.8 Automatically Erasing Old Video Recordings 183
9.9 Recording Modes 184
9.9.1 About Recording Modes 184
9.9.2 Recording Mode with Time Schedule 184
9.9.3 Recording Mode with Manual Selection 186

10 Watching Live Images 189
10.1 Watching Live Images in the Live Video Screen 189
10.2 Full Screen View 191
10.3 Changing the Image Quality (Resolution) 191
10.4 Info Display 192
10.5 Activating Outputs 192
10.6 Taking Snapshots 193
10.7 Local Video Recordings 194
10.8 Audio, Listening 195
10.9 Audio, Talkback 196
10.10 PTZ Control 196
10.10.1 Using PTZ Functions 196
10.10.2 Managing PTZ Preset Positions 198

10.11 Watching Live Images on a Monitor ... 200
10.11.1 About Using a Monitor ... 200
10.11.2 Setting up a Monitor ... 201
10.11.3 Disabling the Monitor ... 202
10.11.4 Switching Between Matrix View and Welcome Screen ... 202
10.12 Watching Live Images via a Web Browser ... 203

11 Recorded Video ... 205
11.1 About Recorded Video ... 205
11.2 Searching Recordings on the Timeline ... 205
11.2.1 Timeline Overview ... 205
11.2.2 Selecting a Timeframe on the Timeline ... 207
11.2.3 Searching Event Recordings on the Timeline ... 208
11.2.4 Playing the Selected Footage ... 209
11.2.5 Synchronised Playback ... 209
11.3 Searching Recordings via Advanced Search ... 211
11.4 Identifying the Storage Disk ... 212
11.5 Searching Recordings via Postmotion ... 212
11.6 Downloading and Storing Selected Video Recordings ... 214
11.6.1 Overview ... 214
11.6.2 Downloading Recordings to your Local Hard Disk ... 215
11.6.3 Downloading Recordings to USB Drive or CD/DVD ... 215
11.7 Managing Local Recordings ... 216
11.7.1 Overview of Local Files ... 216
11.7.2 Viewing or Deleting Local Files ... 217
11.7.3 Backing up Local Files ... 217
11.8 Locked Recordings ... 219

12 360° Camera Images ... 222

13 Arming and Disarming ... 224
13.1 About Arming/Disarming ... 224
13.2 Arming/Disarming Automatically ... 224
13.3 Arming/Disarming Manually ... 225

14 Alarm Profiles ... 227
14.1 About Alarm Profiles ... 227
14.2 Adding a New Profile ... 227
14.3 Deleting an Alarm Profile ... 229
14.4 Default Alarm Profiles ... 229
14.4.1 Normal Event Profile ... 230
14.4.2 Primary Event Profile ... 230
14.4.3 Backup Event Profile ... 231
14.4.4 Silent Message Profile ... 231
14.4.5 Single Event Profile ... 232
14.4.6 Active Sensor Event Profile ... 232

15 Input/Output Behaviour ... 234
15.1 About Inputs and Outputs ... 234
15.2 Inputs ... 235
15.3 Monitored Inputs ... 235
15.4 Filtering Inputs ... 235
15.5 Alarm Input Behaviour ... 236
15.6 PTZ Position on Input ... 239
15.7 Outputs ... 240
15.8 Filtering Outputs ... 241
15.9 Output Behaviour ... 241
15.9.1 Manual Operation ... 241
15.9.2 Recording-Controlled Outputs ... 243
15.10 Programmable Inputs and Outputs ... 245
15.10.1 Overview ... 245

15.10.2 Predefined Programmable Outputs ... 245
15.10.3 Programming Logical Functions ... 246

16 Video Content Analytics (VCA) ... 248
16.1 Overview ... 248
16.2 Rendering Analytic Bounding Boxes ... 248
16.3 Motion, Sabotage ... 251
16.3.1 About Motion, Sabotage Detection ... 251
16.3.2 Drawing Detection Zones ... 252
16.3.3 Motion Zone Detection Settings ... 255
16.3.4 Private Zones (Mask Zones) ... 258
16.3.5 Sabotage Detection ... 259
16.3.6 Advanced Settings for Sabotage Detection (Scene Profiles) ... 260
16.3.7 Scene Profile Settings ... 260
16.3.8 Default Scene Profile ... 260
16.3.9 Creating a Custom Scene Profile ... 260
16.3.10 Assigning Existing Scene Profiles to Cameras ... 262
16.3.11 Changing an Existing Scene Profile ... 262
16.3.12 Deleting a Scene Profile ... 263

17 PIR Detector Settings ... 264
17.1 Prerequisites ... 264
17.2 Configuring the Serial Port ... 264
17.3 Enable parallel PIR polling ... 266
17.4 Configuring IP Modules ... 267
17.4.1 Adding IP Modules ... 267
17.4.2 Deleting IP Modules ... 268
17.5 Configuring the Walk Test Port ... 268
17.6 Initiating the PIR Discovery ... 269
17.7 PIR Detector Status ... 270
17.8 PIR Alarm Inputs ... 270
17.9 Double-Knock Configurations ... 272
17.10 Double-Knock with Camera ... 273
17.11 Intelligent Double-Knock between PRO E PIR Detectors ... 274
17.12 Setting up the Fog Detection Input ... 276

18 Calendar ... 278

19 Users ... 279
19.1 About Users ... 279
19.2 About Strong Passwords ... 279
19.3 Adding New Users ... 281
19.4 User Rights ... 282
19.4.1 Pixelation ... 282
19.4.2 Live Video ... 283
19.4.3 Recorded Video ... 284
19.4.4 System ... 284
19.4.5 Status ... 285
19.4.6 General ... 285
19.5 Modifying an Existing User ... 286
19.6 Deleting Users ... 287
19.7 Granting the Technician ... 288
19.7.1 Granting Access to the XO Device ... 288
19.7.2 Generating a PIN of the Day ... 289
19.7.3 Disabling Technician Grants ... 290

20 Configuration Management ... 291
20.1 Storing a Configuration ... 291
20.2 Renaming a Configuration ... 292
20.3 Copying a Configuration ... 292
20.4 Activating a Configuration ... 293

20.5 Resetting the Active Configuration to Factory Defaults 294

21 Downloading and Uploading Files 296
21.1 Downloading Files from the XO Device 296
21.2 Uploading Files to the XO Device 298
21.2.1 Overview 298
21.2.2 Uploading Configurations 298
21.2.3 Uploading Calibration Pictures 299
21.2.4 Uploading Other Files 301
21.3 Firmware Rollback 301
21.4 Configuration Template 302

22 Starting and Stopping 303
22.1 Restarting the System 303
22.2 Stopping the System 303

23 Status 305
23.1 Front LED Indicators 305
23.2 Status Indicators in the Status Window 305
23.3 Isolating an Alarm Input 308
23.4 General Status of the System 308

24 System Information 312
24.1 Software and License Information 312
24.2 Licenses 314
24.2.1 Overview 314
24.2.2 System License 314
24.2.3 Encoder Card Licenses (Analogue Video Channels) 315
24.2.4 IP Video Channel Licenses 315
24.2.5 Application Licenses 316
24.3 Viewing Active Connections 317
24.4 PTZ Overview 319
24.5 Logs 320
24.5.1 About Logs 320
24.5.2 Generating a Log 321
24.5.3 Saving a Log 322
24.5.4 Example of a Log Record 323
24.5.5 Example of an Event Log 323
24.5.6 Example of a Command Log 325
24.6 Hard Disks 326
24.6.1 Hard Disk Information 326
24.6.2 Calculating the Write Speed 328
24.6.3 Hard Disk Lockdown Mode 329

Appendix A – Networks, Subnet Masks, and IP Addresses 332
A.1 The Basics 332
A.2 Calculation Examples 333
A.3 Subnet Mask Notations 335

Appendix B – Abbreviations 336

1 About this Document

1.1 What is XO 5?

XO™ is ADPRO's Security+ Operating System software. The XO software consists of:

- the server firmware = the software that runs on your ADPRO® NVR+ device.
- the client software = the software that runs on your PC.

The XO software is suitable for the following ADPRO NVR+ devices:

- FastTrace 2 Series: FastTrace 2, FastTrace 2X, and FastTrace 2E.
- iFT Series: iFT and iFT-E.
- eFT Series: eFT4/16P, eFT2/8P, and eFT2

Note

The XO 5.0 firmware is supported on FastTrace 2 Series devices with a PH10LU motherboard, and a DOM of min. 2 GB. Furthermore, for upgrading to XO 5.0, min. firmware XOa 3.0 is required. For details, see the *XO 5.0 Release Notes* (26598_18).

Wherever **server** or **XO device** is mentioned in this document, it applies to all the devices above unless specifically mentioned otherwise.

1.2 Scope

This user manual covers the following topics:

- Installation of the XO client software
- Setup and configuration of the XO device and its peripheral devices (cameras, I/O units, PIR detectors…) in the XO client software
- Event and alarm transmission
- User management
- Configuration management.

This user manual does not cover:

- The usage of XO on the iFT Gateway devices: see XO Client Software User Manual for iFT Gateway (33103).
- Installation of hardware: see the Hardware Installation Manual of your XO device (FastTrace 2 Series: 21790; iFT Series: 27817; eFT Series:35450).
- Overview of supported IP cameras: see the Supported IP Camera List (26742).
- Setup and use of the analytic applications: see the documentation of the IntrusionTrace and LoiterTrace applications.
- License and firmware management using Xchange2: see the Xchange2 user manual (27816).

You can find the latest versions of this document and any referenced document on the Security Solutions Support site https://myhoneywellbuildingsuniversity.com/ (logon may be required). If a document number is indicated (between parentheses), you can enter it in the Keywords box on the site, and search for the document.

2 Installing the XO Client Software on Your PC

There are several ways to install the XO client on your PC:

- Using the stand-alone client installer, which you can download from My Honeywell Building University https://myhoneywellbuildingsuniversity.com/. For instructions, see *2.2 Installing the XO Client Software Using the Installer*.
- Using the device's web page, if you have a connection to your XO device but no internet connection. If you use the device's web page, you need to add the device's web page to the trusted sites in Internet Explorer. Furthermore, your PC must have an IP address in the same network range as the XO device. For instructions, see *2.3 Installing the XO Client Software via the XO Device's Web Page*.

2.1 System Requirements for the Client PC

2.1.1 Hardware

The following are the recommended hardware requirements to run the XO client on a PC:

- Intel Core i5 processor with 8GB RAM
- Graphics card with DirectX 12 support and the capability for using YUV surfaces and hardware stretching. Intel® HD Graphics 630 is recommended.

Honeywell recommends to use a graphics card that allows YUV surfaces and hardware stretching. If not, the XO client software will force the graphics card to GDI mode, which will increase CPU load.

- It is recommended to install the latest drivers of your graphics card.

  For NVIDIA cards, check www.nvidia.com.

  For ATI/AMD cards, check www.amd.com/en/support.

- If necessary, you can always force the client into GDI mode (not recommended, because of CPU load). Add the line ‘gdi=1’ in the [General] section of the hydra.ini file. The default location for this file is:

  C:\Users\username\Appdata\Roaming\Hydra\

  (where username is the name of the Windows user that is currently logged on).

The rendering switches to the GDI mode when the graphics card does not have this support. Rendering in GDI mode is not recommended because of high CPU utilization.

Note

you can use hardware decoding on your client PC to enhance the rendering performance. On a typical system (i7-4790 @3.60GHz), the XO client can handle decoding and rendering of up to 20 full HD (1920x1080) streams. This performance is not guaranteed and depends on several other factors.

If you are using an additional discrete GPU (Nvidia, AMD Radeon…), then you need to activate the on-board Intel GPU in your PC's BIOS. For details, consult your PC's documentation.

If you are using Windows 7, you need to attach a monitor to the on-board VGA connector of your PC, because DirectX 9 needs a monitor to create the necessary hardware surfaces.

The embedded client application is now by default a 64-bit application, and the customers who require a 32-bit version can download it from the support site.

Caution!

HD cameras can be used more optimally in a PC with better system specifications. Please take into account that double resolution, on average, results in 4 times more performance.
Honeywell advises to test the settings to make sure that your PC can handle your configuration.

2.1.2 Software

The following are the recommended software requirements to run the XO client on a PC:

- Windows 10 (64-bit)
- DirectX 12 drivers
- Internet Explorer 11

Note

Firmware with hardware version 2.0.0.0 and software version 1.0.0.1 is needed to decode firmware in the older devices still running the HIPI card hardware.

It is strongly recommended to download the latest drivers for your video card from the site of the manufacturer of your card. Doing this will resolve a number of issues that you would probably encounter.

- NVIDIA: www.nvidia.com
- ATI/AMD: http://ati.amd.com

The client can be forced to use GDI mode. Just put **gdi=1** in the [General] section of the **hydra.ini** file located in your data directory. The default location is: **c:\users\<username>\AppData\Roaming\Hydra\hydra.ini**.

2.2 Installing the XO Client Software Using the Installer

Note

The procedure below describes how to install the XO client software **on a new system**. For **updating** the client software, see *Software Updates*.

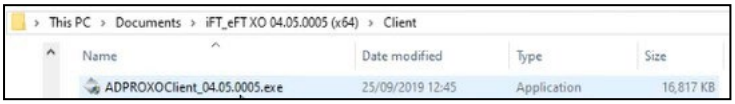
To install the XO client software using the XO client's installer, proceed as follows:

1. Download the installer from the Security Solutions Support website https://myhoneywellbuildingsuniversity.com/. Type **32689** in the **Keywords** box and search, or filter on **Product** = **XO/XOa**, and then on **Information Type** = **Software Setup**.

   Note

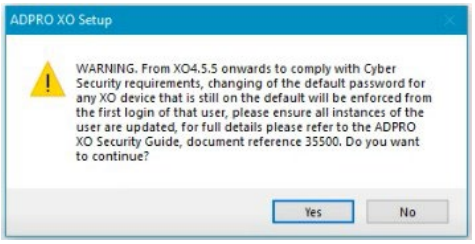
   Your virus scanner may block this download. Disable your virus scanner temporarily if this occurs. Remember to switch it back on after installation.

2. Unzip the downloaded file.

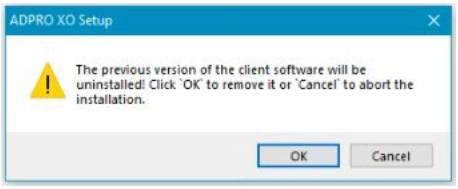
   

   Double-click the **ADPROXOClient_04.05.0007.exe** file to start the installer.

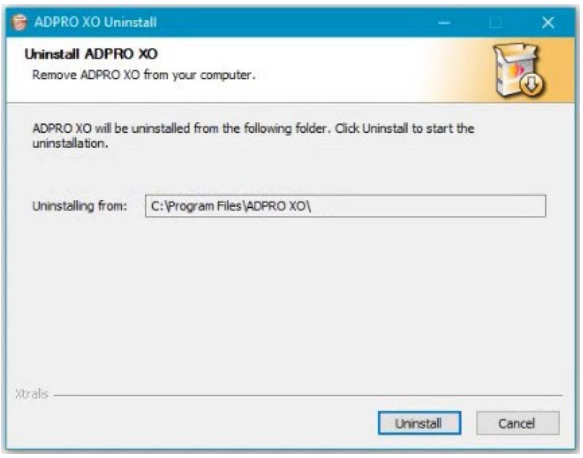
3. The following warning message may appear:
   Do you want to allow the following program from an unknown publisher to make changes to this computer?
   In this case, click **Yes** to start the installation.
4. Click **Yes** in the following message. This message is displayed as changing the default password for XO device from first login is made mandatory since XO 04.05.005.



5. Click **OK** to uninstall the previous XO client.



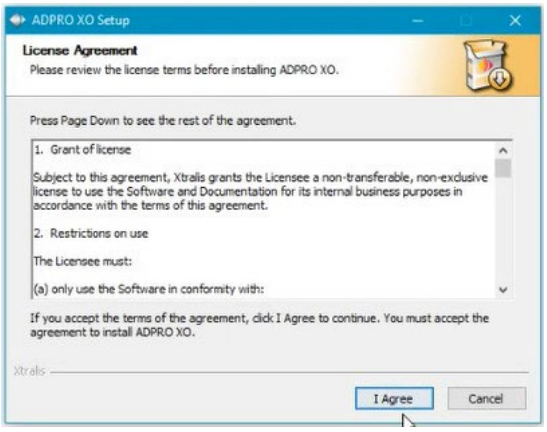
6. Click **Uninstall** to confirm. When finished, the following screen appears:



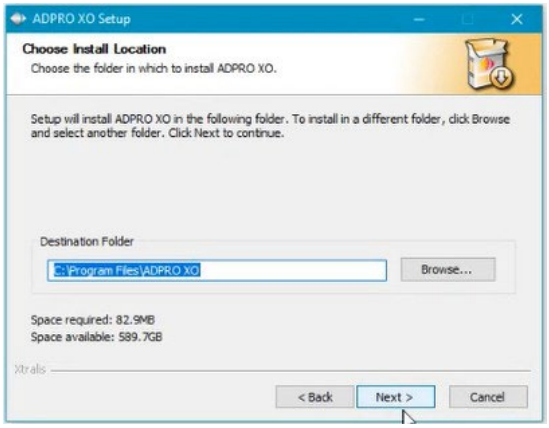
7. Click **Finish**. The new version will now install.



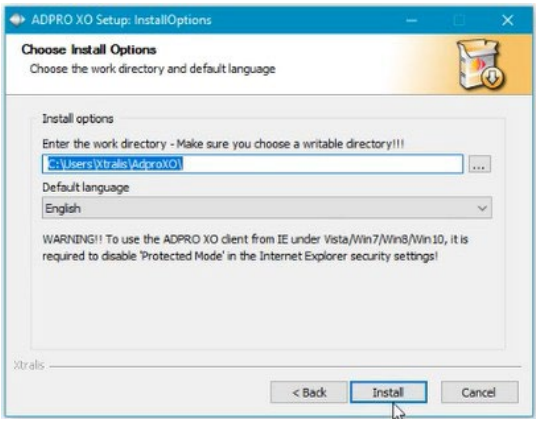
8. Click **I Agree** to agree with the terms of the license agreement.



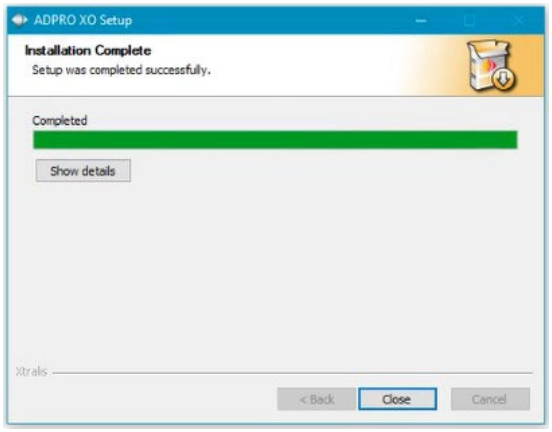
9. Accept or modify the installation folder. Click **Next**.



10. Accept or modify the default work folder (= the folder for storing snapshots and downloaded recordings). Also select your preferred language. Click **Install**, and wait for the following screen to appear:



11. When the installation is completed, click **Close** to exit the installation Wizard. The new client version is now installed.



Before you can add an XO device and connect to it using the client, your PC must have an IP address in the same network range as the XO device. For instructions, see *Changing the PC's IP Address*.

2.3 Installing the XO Client Software via the XO Device's Web Page

Note

Webserver is disabled by default starting with ADPROXO 5.0. It can only be reenabled by a technician on a system in which an admin user has enabled the technical grant. To install the client software using the XO device's web page, the webserver must be enabled by the technician which is a security risk. You can get the client software from the release DVD or from the support site (https://myhoneywellbuildingsuniversity.com/).

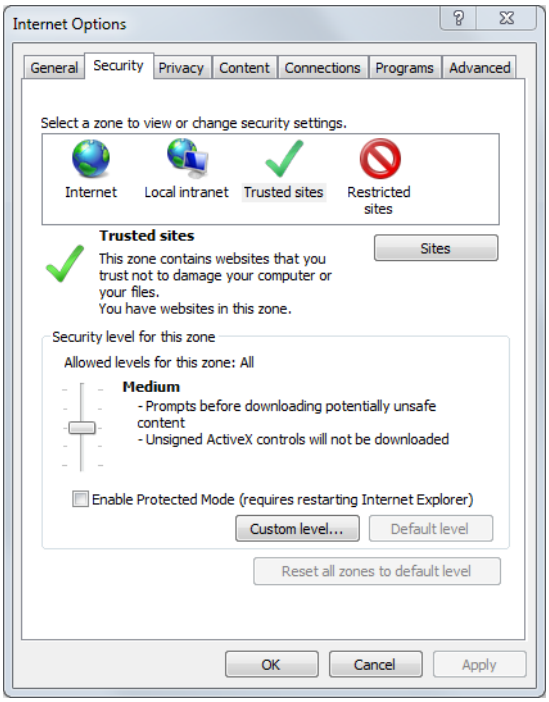
2.3.1 Internet Explorer Settings

Note

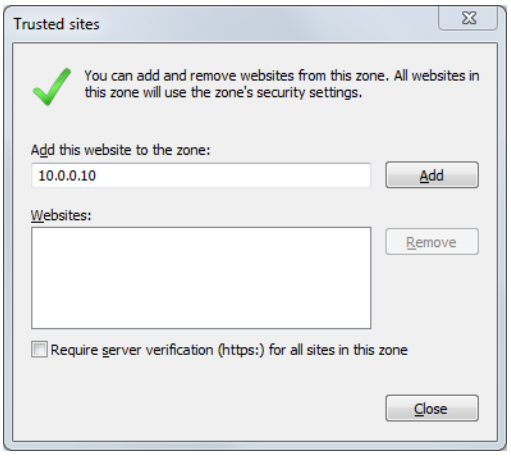
If you will install the XO client software via the XO device's web page, the preferred browser is Internet Explorer. If you cannot use Internet Explorer, try any other internet browser. In this case, you have to install the MeadCo Neptune plugin. You can download the plugin from www.meadco.com/Neptune/Download.

When installing the XO client software via the XO device's web page, you need to add the XO device's IP address to your **Trusted sites** in Internet Explorer. The XO device's default IP address is 10.0.0.10 with subnet mask 255.255.255.0. Proceed as follows:

1. In Internet Explorer, choose **Tools** > **Internet options**.
2. Click the **Security** tab.

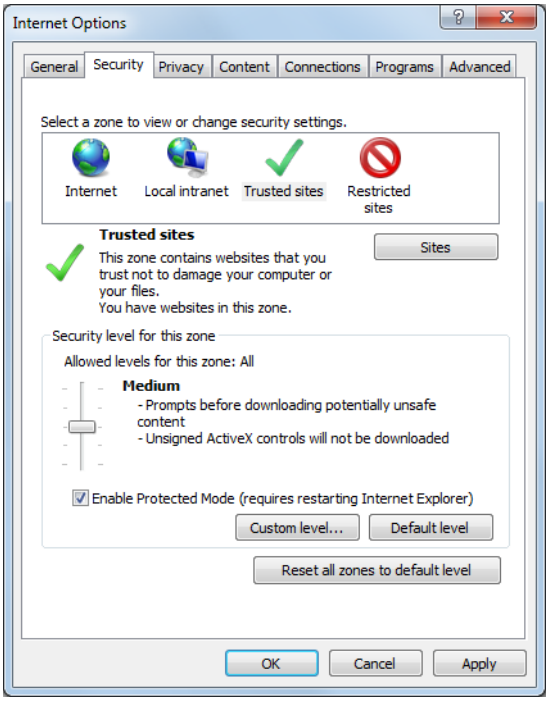


3. In the **Select a zone…** box, click **Trusted sites**, and then click **Sites**.



4. In the **Add this website…** box, type **https://** followed by the XO device's IP address. For example: https://10.0.0.10
5. Click **Add**, and then click **Close**.
6. Click **OK** to close the **Internet Options** window.

If installation is still not possible, you may try clearing the Enable Protected Mode checkbox in the Security tab.



Caution!

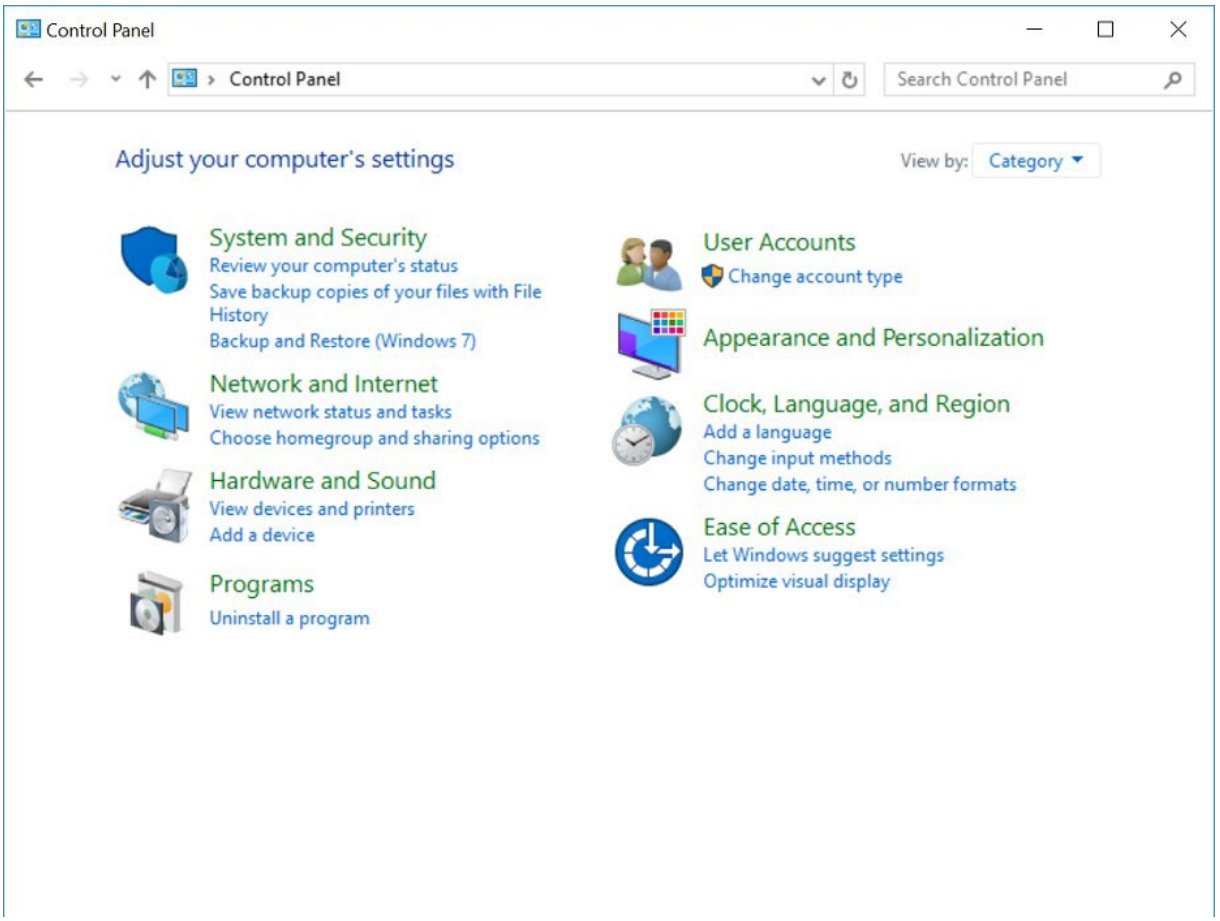
Check with the IT department if you are allowed to switch off protected mode, because it may lead to IT issues.

2.3.2 Changing the PC's IP Address

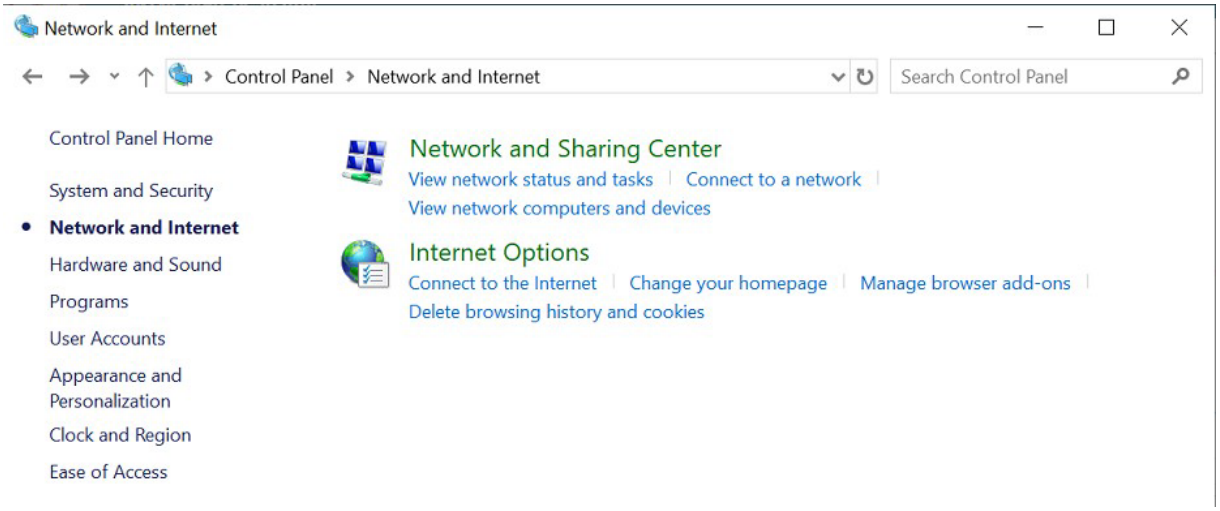
The XO device's default IP address is 10.0.0.10 with subnet mask 255.255.255.0. If you install the client software via the device's web page, or if you want to configure a device using the XO client, you need to put your PC in the same IP range (for example, IP address 10.0.0.2 with subnet mask 255.255.255.0).

To change the PC's IP address in Windows 10, proceed as follows:

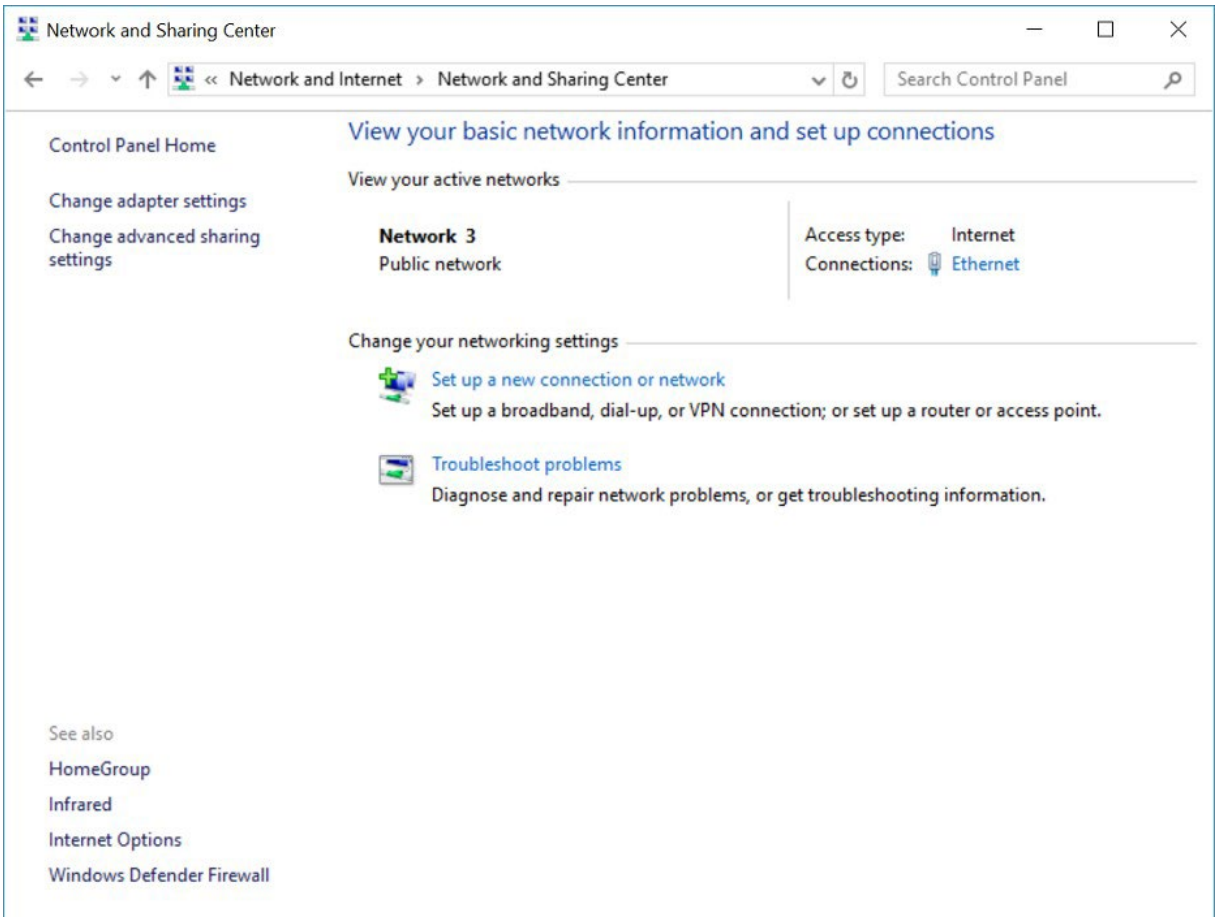
1. Click **Start**, and then click **Control Panel (View by: Category)**.



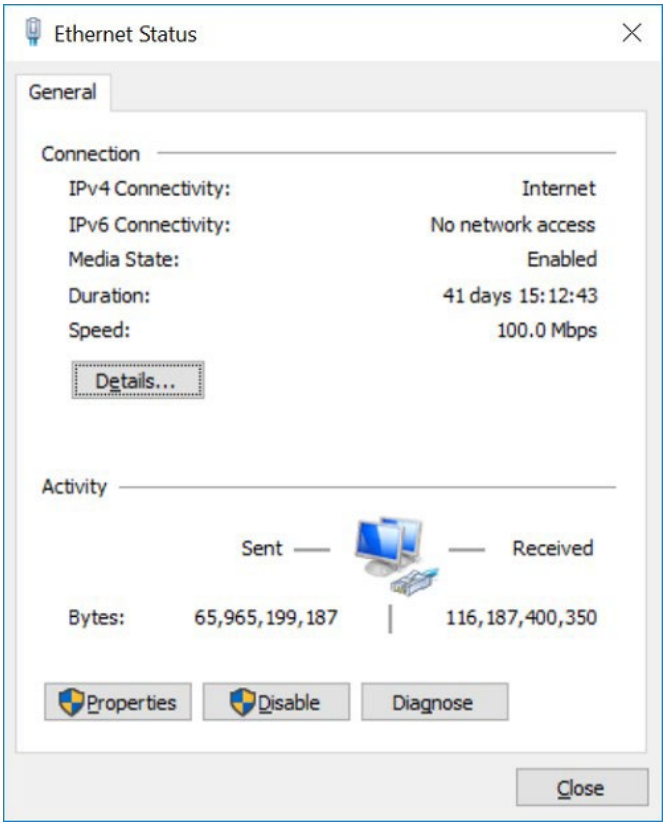
2. Click **Network and Internet**.



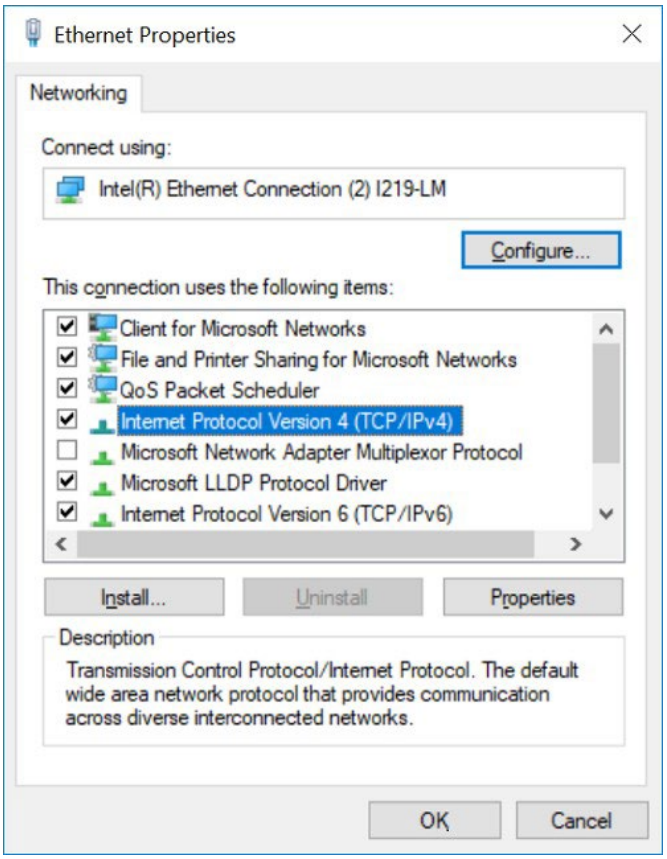
3. Click **Network and Sharing Center**.



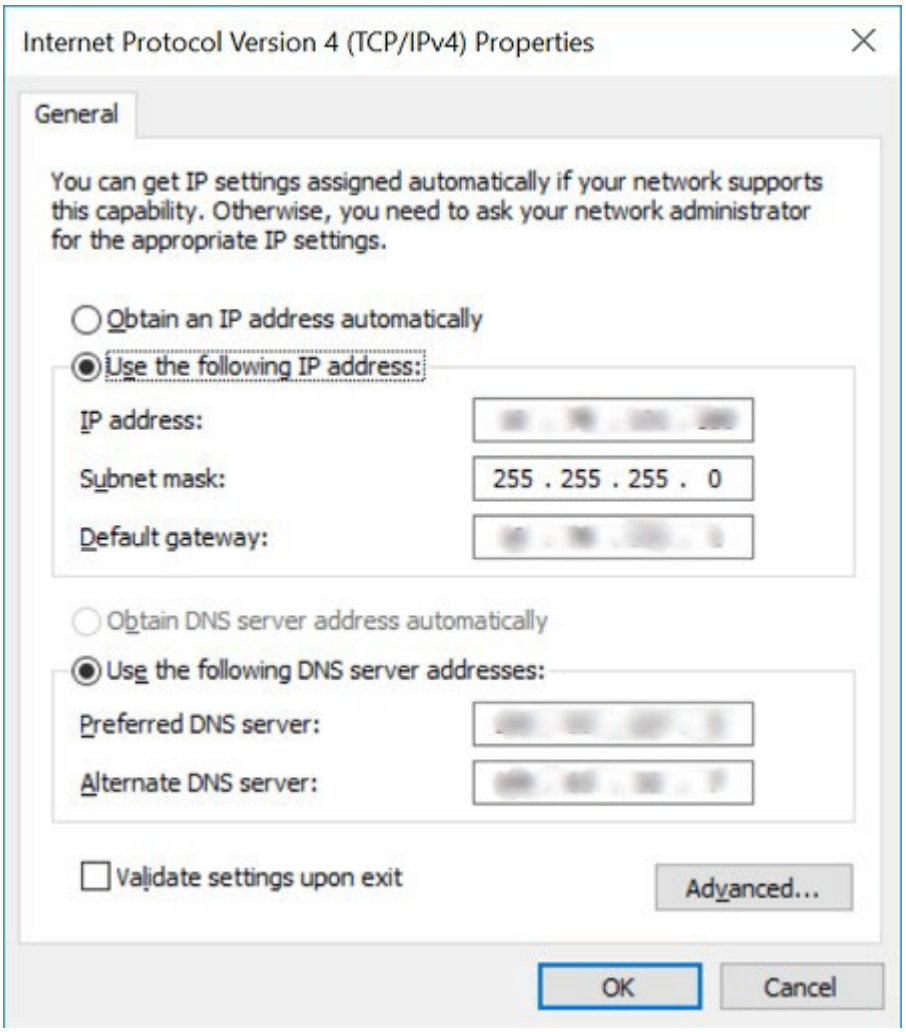
4. Click **Connections**.



5. Click **Properties**.



6. Click **Internet Protocol Version 4 (TCP/IPv4)**.



7. For ease of initial setup, change the PC's TCP/IP settings to the following:

IP address	10.0.0.2
Subnet mask	255.255.255.0

8. Click **OK** to return to the **Local Area Connection** window.
9. Click **OK** to close the window.

Note

You can check the XO device information by running the following commands when you are connected to the device with a monitor and keyboard.

ALT + F1	To display the IP details
ALT + F7	To display the cameras in matrix layout

2.3.3 Installation

Note

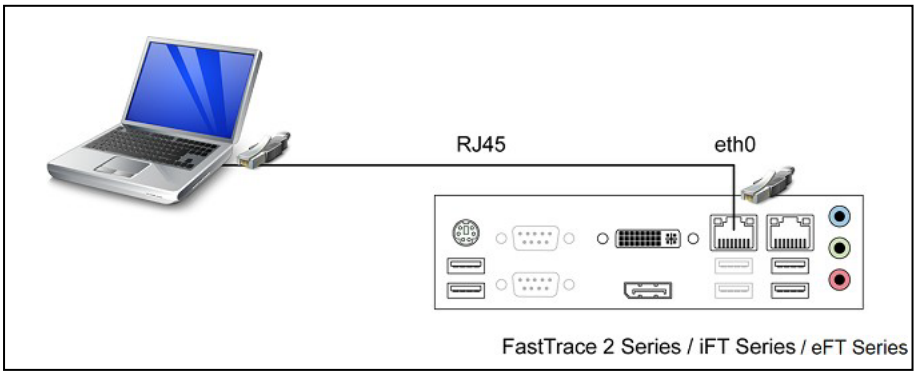
The procedure below describes how to install the XO client software **on a new system**. For **updating** the client software, see *2.5 Software Updates*.

Note

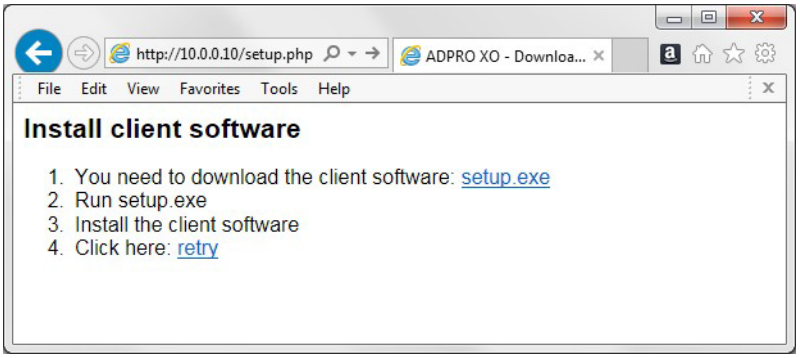
Webserver is disabled by default starting with ADPRO XO 5.0. It can only be reenabled by a technician on a system in which an admin user has enabled the technical grant. To install the client software using the XO device's web page, the webserver must be enabled by the technician which is a security risk. You can get the client software from the release DVD or from the support site (https://myhoneywellbuildingsuniversity.com/).

To install the XO client software via the XO device's web page, proceed as follows:

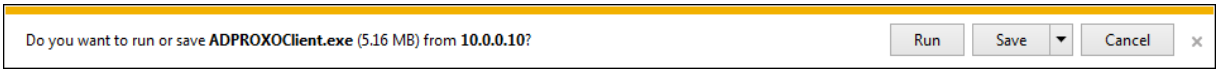
1. Connect your PC to the XO device's eth0 port with an RJ45 network cross cable or via the network switch/router on the eth0 port.



2. Open Internet Explorer and enter the XO device's IP address, followed by /setup.php
   For example: https://10.0.0.10/setup.php



3. Click **setup.exe**.

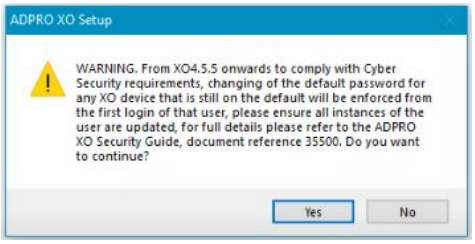


4. Click **Run** to start the installation.

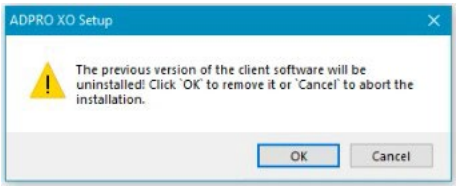
Note

Your virus scanner may block this download. Disable your virus scanner temporarily if this occurs. Remember to switch it back on after installation.

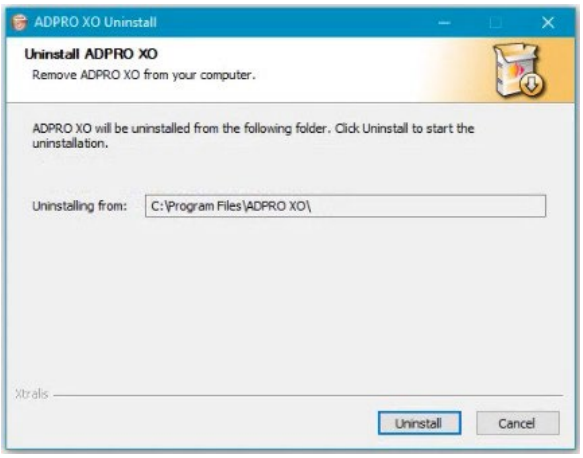
5. The following warning message may appear:
   Do you want to allow the following program from an unknown publisher to make changes to this computer?
   In this case, click **Yes** to start the installation.
6. Click **Yes** in the following message. This message is displayed as changing the default password for XO device from first login is made mandatory since XO 04.05.005.



7. Click **OK** to uninstall the previous XO client.



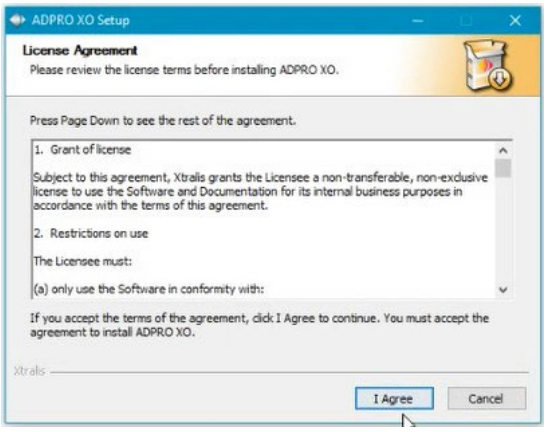
8. Click **Uninstall** to confirm. When finished, the following screen appears:



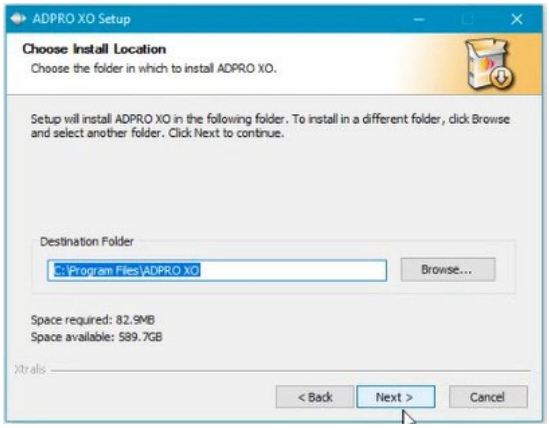
9. Click **Finish**. The new version will now install.



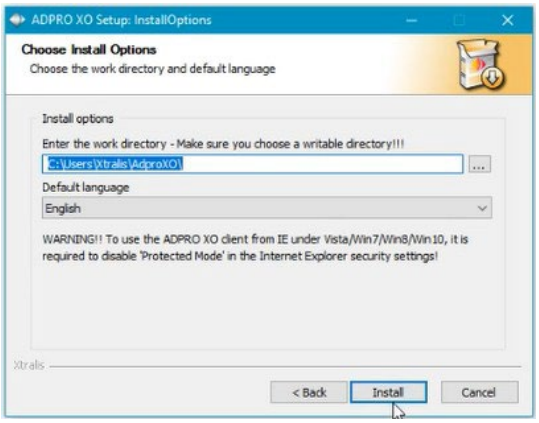
10. Click **I Agree** to agree with the terms of the license agreement.



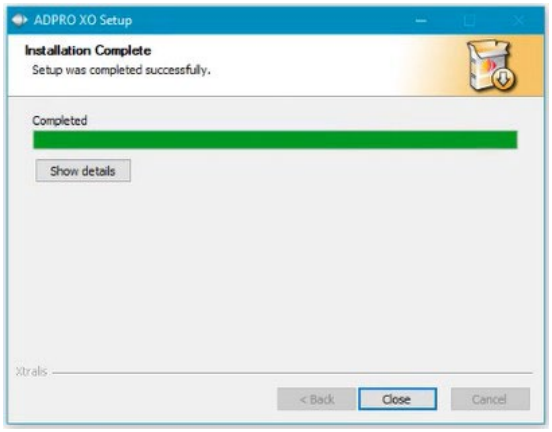
11. Accept or modify the installation folder. Click **Next**.



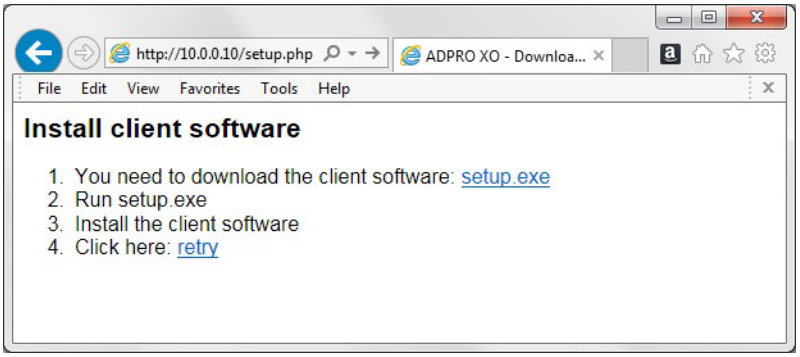
12. Accept or modify the default work folder (= the folder for storing snapshots and downloaded recordings). Also select your preferred language. Click **Install**, and wait for the following screen to appear:



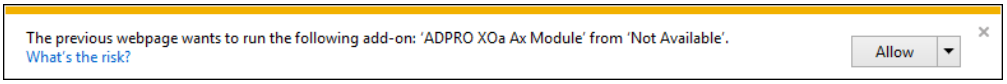
13. When the installation is completed, click **Close** to exit the installation Wizard. The new client version is now installed.



If you have installed the client via the XO device's web page, and you try to start the client, it may occur that the internet browser is opened instead of the login screen. If this is the case, just click **Retry**.



If you receive a warning message such as the one below (at the bottom of the browser window), click **Allow** to continue:

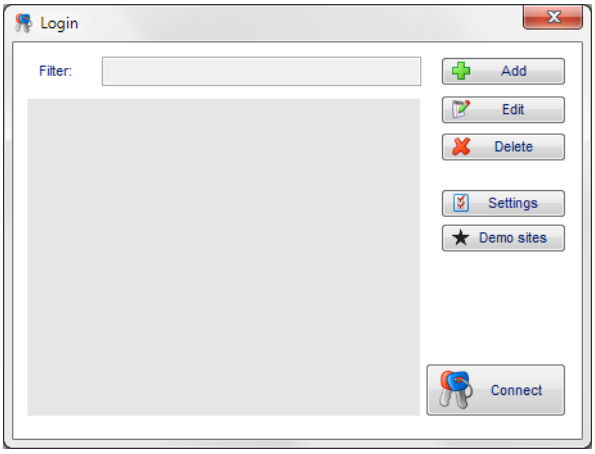


2.4 Launching and Initial Configuration

2.4.1 Launching the XO Client

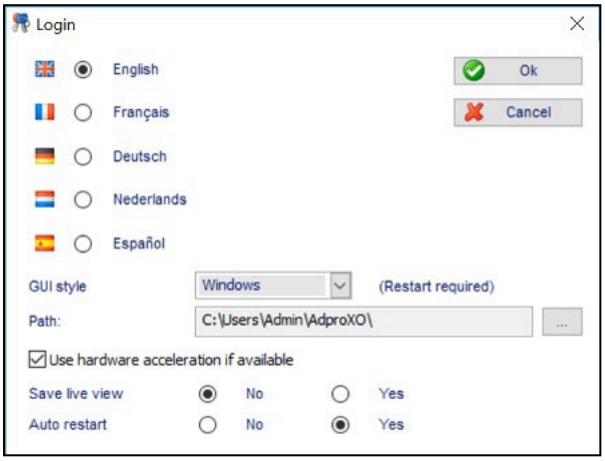
To launch the XO client, proceed as follows:

1. On the desktop, double-click the XO client icon .
   If the icon is not available, you can press **Start** and choose **All Programs** > **ADPRO XO** > **AdproXO**. The following window appears:



   The **Login** window displays all your XO devices so that you can quickly connect to them. When using the XO client for the first time, the list is empty.

2. To set up how the client launches, click **Settings**.



3. Provide the following information:

Item	Description
English, Français…	Select the desired language for the application.
GUI style	Select a style to change the appearance of the application. The changes will only take effect after you restart the client software.
Path	If required, change the default work folder (= the folder for storing snapshots and downloaded recordings).
Use hardware acceleration if available	Select this option if you want to use hardware decoding on your client PC. Hardware decoding may enhance the rendering performance. For system requirements, see *System Requirements for the Client PC*.

Item	Description
Save live view	Set this option to **Yes** if you want to show the last used camera matrix in the live view. If you set it to **No**, the live view window is empty when you start the client, and you have to select the cameras for the live view matrix each time you start the client.
Auto restart	Set this option to **Yes** if you want the login window to reappear when you close the client software. This allows you to quickly connect to another XO device.

4. Click **OK** to save the settings.
5. If you have changed the **GUI style**, close the **Login** window, and then restart the client application for the changes to take effect.

You can now add an XO device and connect to it.

2.4.2 Adding an XO Device to the XO Client

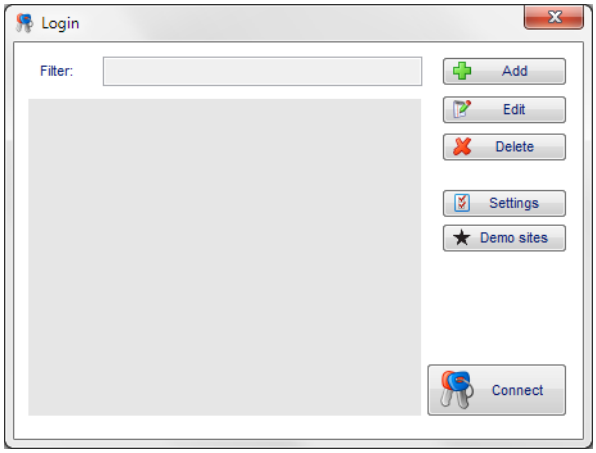
Note

The system stores the list of XO device connections added to your XO client in the HydraSiteList.xml file. You can reuse this list on a different PC (or for another PC user), so you do not have to add all XO devices again. For details, see *2.4.12 Reusing an Existing Device List*.

Adding a device to the XO client means that you define and store a set of connection parameters for the device, such as the IP address, ports, and a user ID or username and password. This allows for a 'one-click' connection to a device.
You can define several connections to the same physical devices, for example for different users (Admin and Technician), or for connecting from an internal and an external network.
To prevent unauthorised access to a device from your PC, you can leave the password setting blank, forcing a user to always manually enter the password when connecting.

To add an XO device to the client, proceed as follows:

1. Launch the XO client.

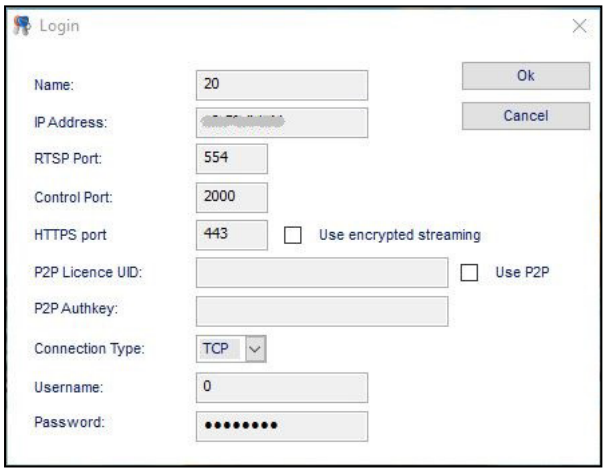


Note

If you have installed the XO client for the first time on this PC, you can add a few demo devices to familiarise yourself with the XO client before adding your own device(s). Access to the demo devices is limited; not all features are available. For details, see *Demo Devices*.
Once you have added your own device(s) to the client, you can no longer add the demo devices.

2. If you want to add the demo devices, click **Demo sites**. Continue with the next step to add your own devices.

3. Click **Add**. The following window appears:

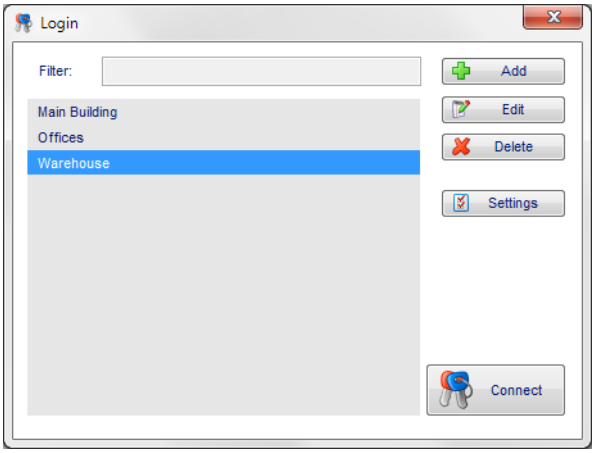


4. Provide the following information:

Item	Description
Name	Type a meaningful name for the XO device.
IP Address	Type the IP address or DNS hostname of the XO device (default IP address is 10.0.0.10). If you are connecting from an external network (via routers/firewalls), make sure to type the external (public) IP address as set in the router's/firewall's network address translation (NAT) table.
RTSP Port **Control Port**	Type the RTSP port number (default is 554) and the control port number (default is 2000). These values have to correspond with the RTSP/control port numbers as specified in the client software under **System** > **Connections** > **Ethernet / PPP**. For more information, see *Network (Ethernet)*. If you are connecting from an external network (via routers/firewalls), make sure to type the external port numbers as set in the router's/firewall's network address translation (NAT) table.
HTTPS Port	The HTTPS port number (default is 443) Select the **Use encrypted streaming** checkbox for secure video streaming. **Note** Restart the XO device after the secure streaming is enabled. Encryption is applied only on the input video stream and not on the input audio stream. The Honeywell Miracle cameras will not support audio-out functionality when encrypted streaming is used.
P2P License UID	Enter the UID for P2P connection same as that of the XO server and select **Use P2P**. Enable P2P on the XO server from **System** > **Connections** > **Ethernet / PPP** > **P2P configure** for this field to display on the client login page. For more details, see *Network (Ethernet)*.

Item	Description
P2P Authkey	Enter the Authkey for P2P connection same as that of the XO server and select Use P2P. Enable P2P on the XO server from **System** > **Connections** > **Ethernet / PPP** > **P2P configure** for this field to display on the client login page. For more details, see *Network (Ethernet)*. **Note** Only Administrative and technician users have rights to generate and display Authkey.
Connection Type	Select the TCP or UDP protocol. UDP is recommended, but TCP may be required if the connection goes through a router that blocks the UDP packets.
Username **Password**	Enter the user ID/username and password of an existing user to log on to the XO device. The default user ID is 0. The XO device has 666777 as the initial password which is changed at the first login. **Note** Entering a **password** is optional. If you leave the **Password** box blank, you have to fill in the password manually each time you connect to the device.

5. Click **OK**. The new XO device appears in the list.
6. Repeat for any other XO devices that you want to add.



2.4.3 Demo Devices

If you start from a clean installation of the XO client (no update, no devices added), you can choose to add the demo devices that Honeywell provides. You can use them to familiarise yourself with the XO client before starting with your own devices.

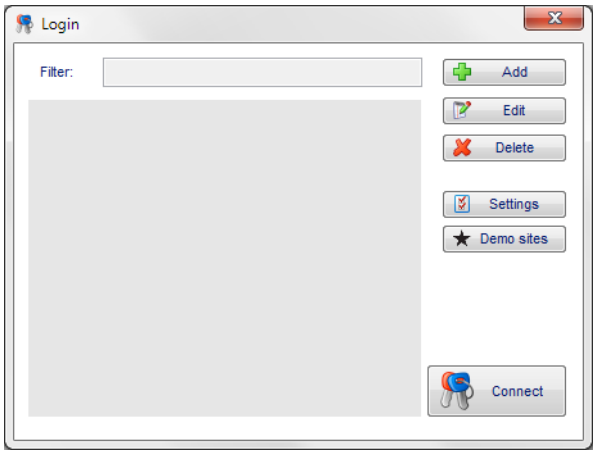
Access to demo devices is limited: the **System** menu is not available.

Note

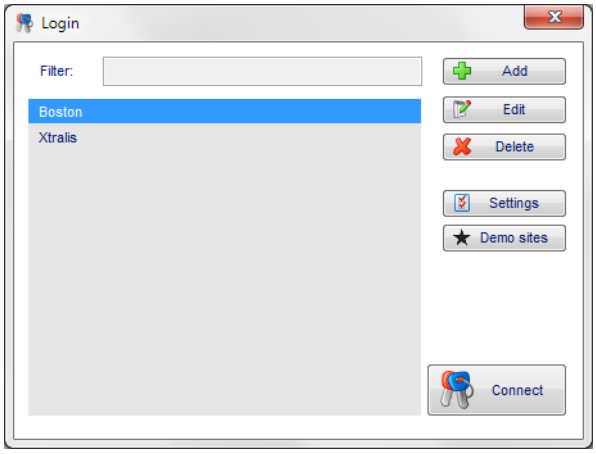
Once you have added your own device(s) to the XO client, you can no longer add demo devices. The **Demo Sites** button will disappear.

To add demo devices to your XO client, proceed as follows:

1. Launch the XO client.



2. Click **Demo Sites**. The system adds the demo devices to the XO client.



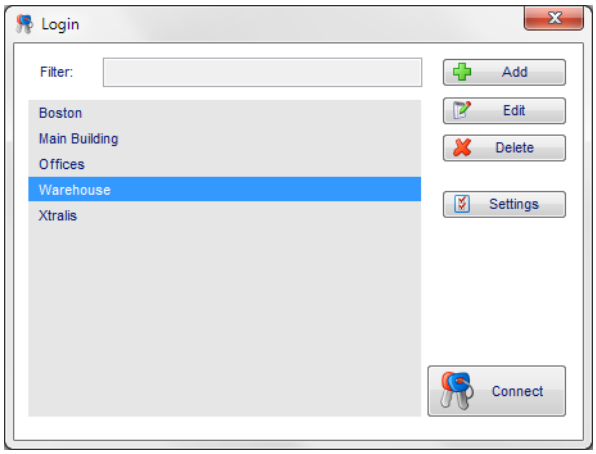
You can connect to the demo devices in the same way as other devices.

2.4.4 Deleting an XO Device

You can delete devices that you no longer use.

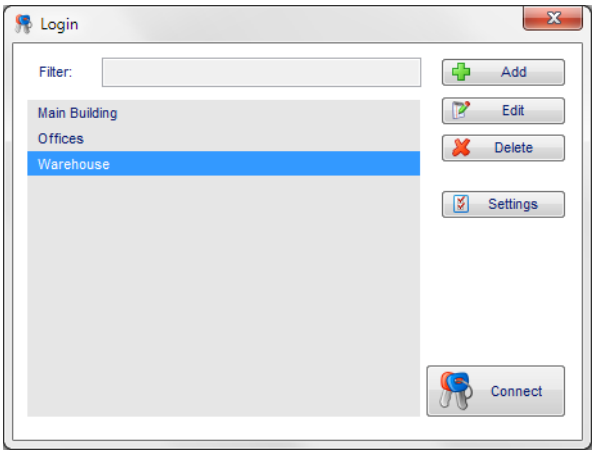
To delete an XO device, proceed as follows:

1. Launch the XO client.



2. Click the desired XO device in the list, and then click **Delete**.

3. Click **Yes** to confirm.



2.4.5 Connecting to an XO Device

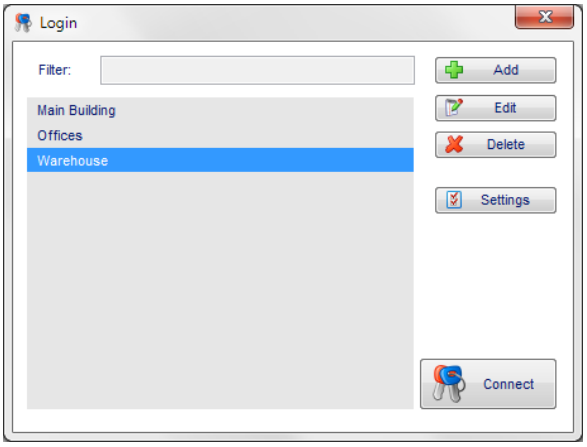
You can connect to an XO device:

- From the **Login** window in the XO client (recommended)
- From Internet Explorer.

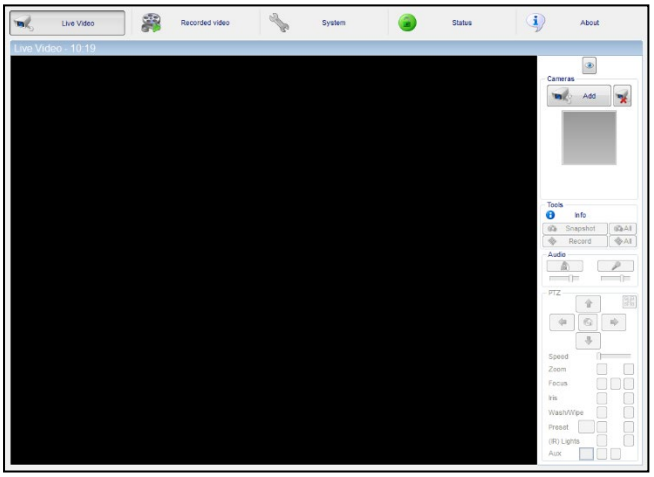
2.4.5.1 Connecting to an XO Device via the Login Window

To connect to an XO device via the **Login** window, proceed as follows:

1. Launch the XO client. The list of XO devices appears. The system automatically selects the last used XO device.

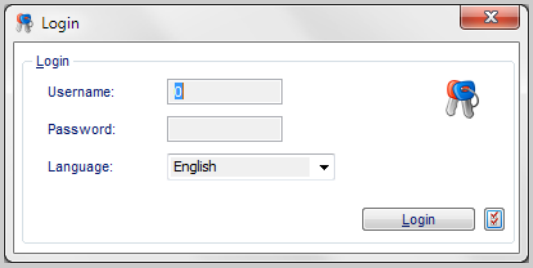


2. Click the desired XO device in the list, and then click **Connect**.
   Alternatively, double-click the desired XO device in the list.
   The **Live Video** screen appears:



Note

If you did not specify a password for connecting to the device, the following screen appears:



Enter the password and click **Login**.

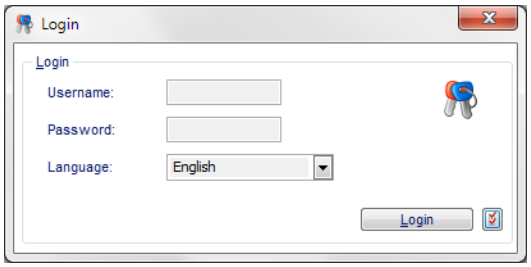
2.4.5.2 Connecting to an XO Device in Internet Explorer

Caution!

If you want to use the ActiveX control for displaying the client in Internet Explorer, then you have to configure Internet Explorer to run 64-bit processes. Enable the Enhanced Protected Mode and activate protected mode for local and internet zones (Internet Options > Advanced > Security).

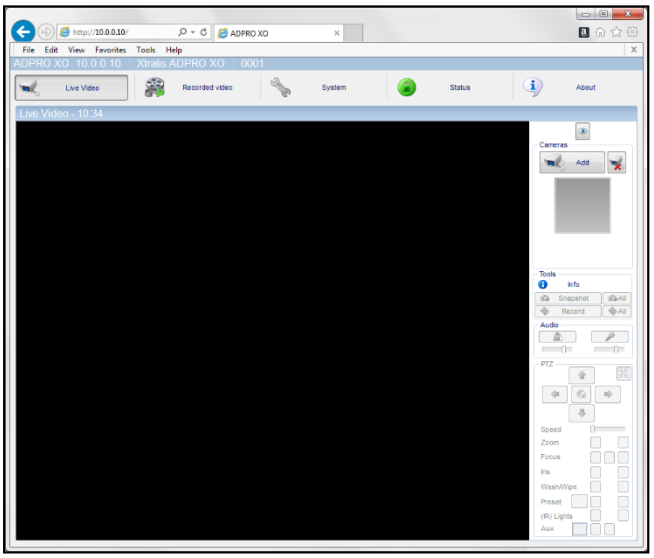
To connect to an XO device in Internet Explorer, proceed as follows:

1. Open Internet Explorer and type the XO device's IP address in the address bar (the default IP address is 10.0.0.10). The login screen appears:



2. Enter the user ID/username and password of an existing user to log on to the XO device. The default user ID is 0. The XO device has 666777 as the initial password which is changed at the first login.
3. Set alphanumeric password in the password change dialog.
4. In the **Language** box, select the desired language for the application.

5. Click **Login**. The **Live Video** screen appears:

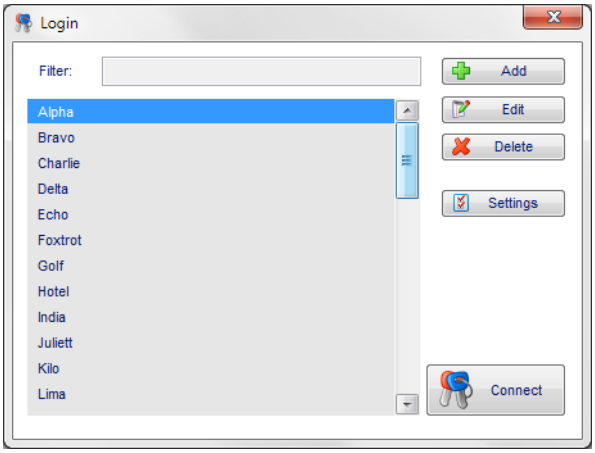


2.4.6 Filtering the Device List

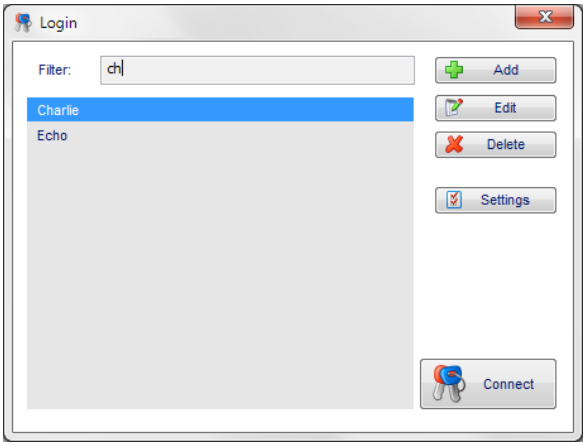
If you have many devices in the list, you can use the filter in the **Login** window to quickly find the desired device and connect to it.

To filter the device list in the **Login** window, proceed as follows:

1. Launch the XO client.



2. In the **Filter** box at the top, type a part of the name of the desired device. The system filters the list as soon as you start typing.



3. Double-click the desired device in the list to connect to it.

Note

The filter remains active when you close the client window and return to the **Login** window (if **Auto restart** is active), although the filter text is not visible. To remove the filter and display all devices, click in the empty **Filter** box and press **Delete**.

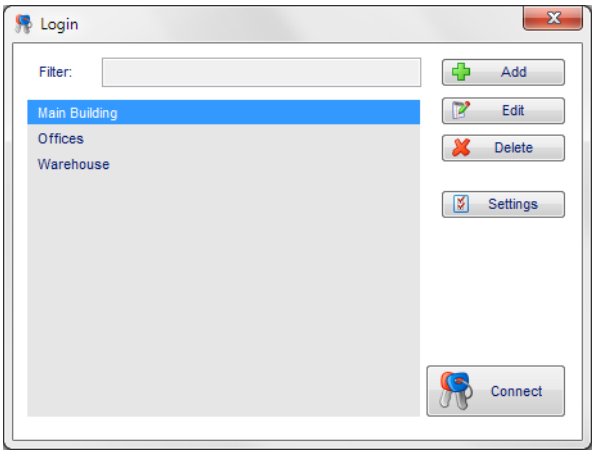
When you close the **Login** window, the system removes the filter. The next time you start the client, the **Login** window will display all devices.

2.4.7 Changing an XO Device

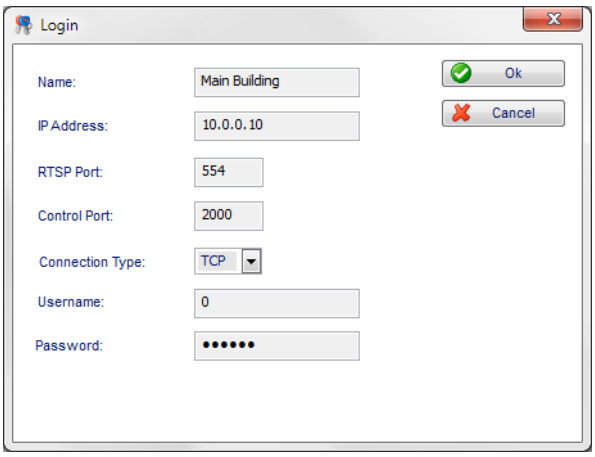
The first time you connect to an XO device, you use the default values. If you have modified any related settings related to the connection using the XO client (IP address, ports, password…), you also have to change these in the **Login** screen.

To change an XO device, proceed as follows:

1. Launch the XO client (in its own window).



2. Select the desired XO device in the list, and then click **Edit**.



3. Change the necessary settings.
4. Click **OK** to confirm.

2.4.8 Changing the Work Folder

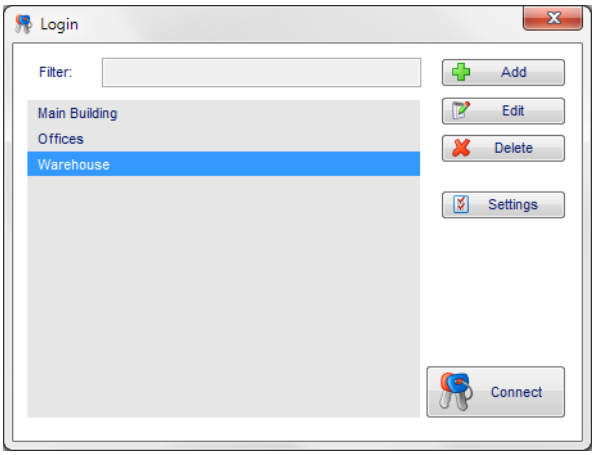
The work folder is the default folder on your PC where the XO device stores snapshots, local recordings, and downloaded recordings.
The default work folder is C:\Users*username*\AdproXO\
(where *username* is the name of the Windows user that is currently logged on).

For snapshots, local recordings, and downloaded recordings, the system will automatically create subfolders in the work folder for the different XO devices that you manage with your PC. The system does not create these subfolders for the files that you download using the **Transfer** screen; you have to select or create the desired subfolders yourself.

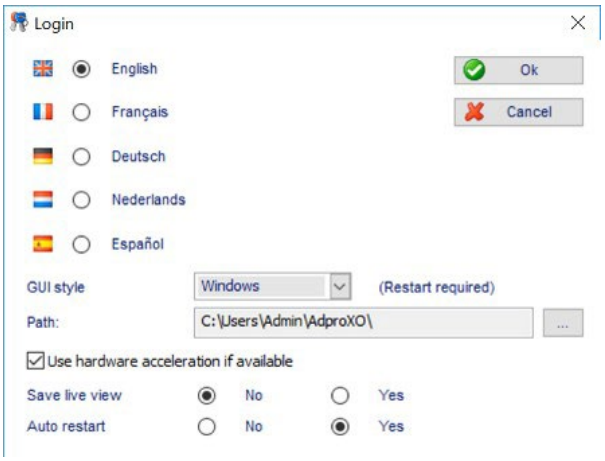
The subfolder name consists of the server unit ID (0001–99999) and the site name of the XO device, as specified in the **CMS Alarm transmission** window. For example:
C:\Users*username*\AdproXO\0001 - MySiteName

To change the default work folder, proceed as follows:

1. Close the client, and then reopen it from your desktop. **Do not connect** to any device yet.



2. In the **Login** window, click **Settings**.



3. To the right-hand side of the **Path** box, click the ... button.
4. Browse to the desired folder, and click **OK** to confirm.
5. Click **OK** to close the **Settings** window.

2.4.9 Setting the Date and Time

The first time that you connect to an XO device, set the date and time. This ensures that the correct timestamp appears on recordings and logs.

Changing the date/time settings requires a system restart.

> ***Caution!***
>
> If you turn back the clock, the system may erase existing recordings. For example, you need to turn the clock back from 16:00 h to 15:30 h. Any existing recordings that were already made between 15:30 h and 16:00 h may be erased after you set the clock back to 15:30 h.

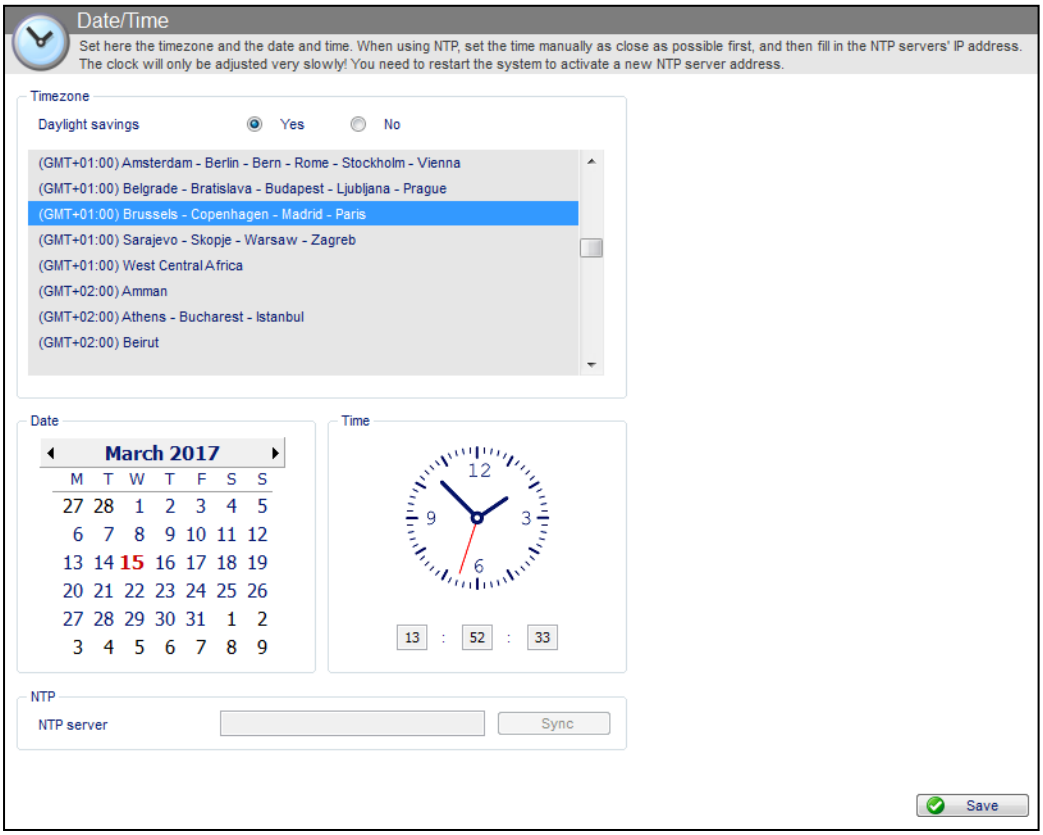
If available, you can let the XO device synchronise with an NTP server (Network Time Protocol server).

Note

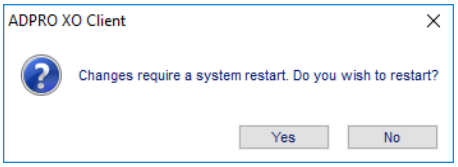
If you experience any instability with the NTP server when using a dynamic NTP address, then enter the DNS server of your Internet Service Provider in the advanced settings for the Ethernet connection: choose **System** > **Connections** > **Ethernet / PPP**, click **Advanced mode**, and fill in the **Provider DNS server** box.

To set the date and time, proceed as follows:

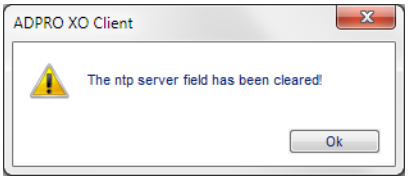
1. Choose **System** > **General** > **Date/Time**.



2. To switch automatically between summer and winter time, set **Daylight savings** to **Yes**.
3. Click the correct time zone in the list.
4. In the **Date** box, click the correct date.
5. In the **Time** box, type the correct time in hours, minutes, and seconds. Enter the time in 24 h notation.
6. If you want to use an NTP server to synchronise time: in the **NTP server** box, type the NTP server's IP address, or its dynamic name.
7. Click **Save**. The following message appears:



8. Click **Yes** and wait for the device to restart.
   If you click **No**, the system undoes your changes. If you had filled in the **NTP server** box, the system clears the box, and the following message appears:

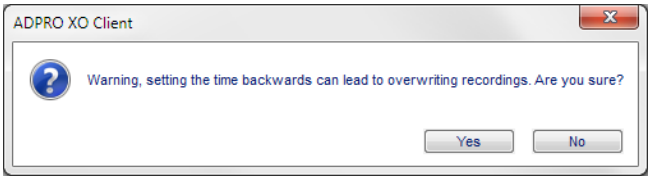


9. Click **OK** to close the message box.

2.4.10 Manually Synchronising with NTP Server

If you have filled in an NTP server, the system will automatically synchronise with the NTP server. However, you can synchronise manually as follows:

1. Choose **System** > **General** > **Date/Time**, and then click **Sync**. The following warning appears:



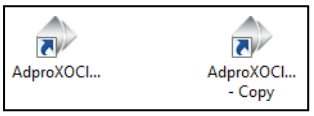
2. Click **Yes** to continue.

2.4.11 Creating a Direct Shortcut to a Device

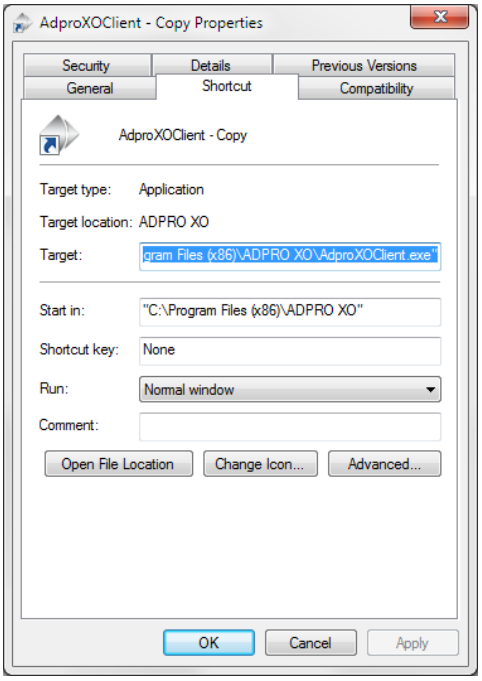
From version XOa 3.02, you can create a shortcut on your PC desktop to start the client software and connect to a specific device immediately, without first showing the **Login** window with the list of devices.

To create a direct shortcut to a device, proceed as follows:

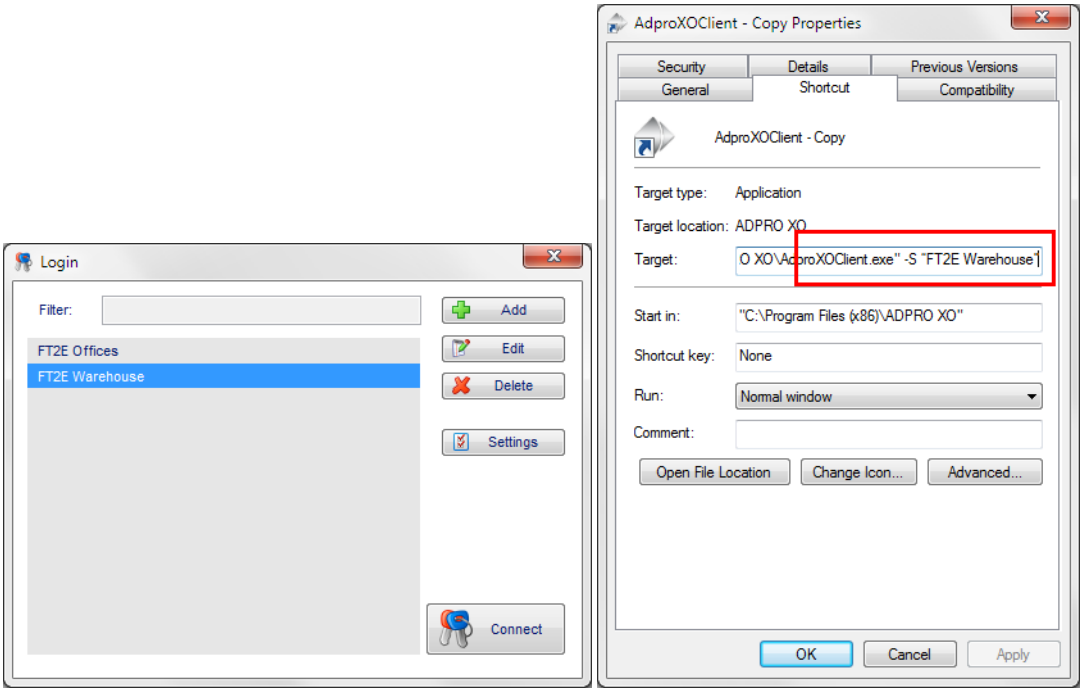
1. On your PC desktop, locate the shortcut to the XO client.
2. Right-click the shortcut and select **Copy**, and then right-click the desktop and select **Paste**. Alternatively, you can click the shortcut once, and then press Ctrl+C, and then Ctrl+V. Windows creates a copy of the shortcut:



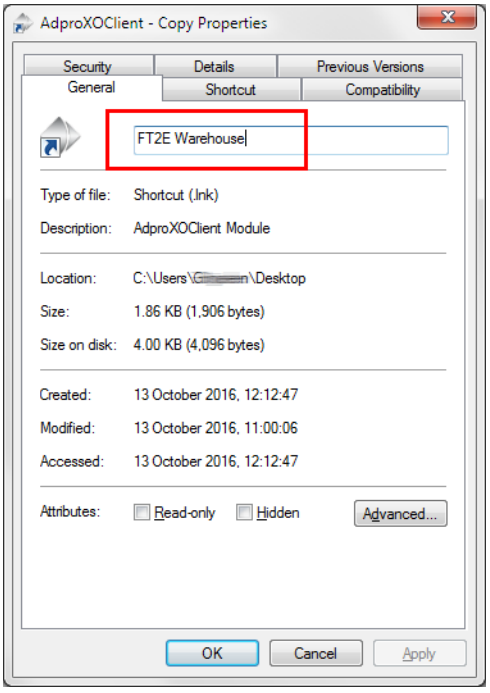
3. Right-click the copy, and then select **Properties**.



4. In the **Target** box, add a space to the end of the text, followed by:
   -S "*YourDeviceName*"
   where *YourDeviceName* is the name of the device as shown in the **Login** window. For example, for a device named FT2E Warehouse, add:
   -S "FT2E Warehouse"



5. Click the **General** tab.
6. In the box at the top, type a new name for the shortcut.



7. Click **OK** to confirm.



8. Double-click the shortcut to start the client and immediately connect to the specified device.

Note

If you change the name in the device list, adjust the shortcut too. If not, the device list will appear when you double-click the shortcut.

2.4.12 Reusing an Existing Device List

The system stores the list of XO devices added in your XO client software in the **HydraSiteList.xml** file. The default location for this file is:
C:\Users*username*\Appdata\Roaming\Hydra\
(where *username* is the name of the Windows user that is currently logged on).

You can copy/paste this file to any other PC and/or other PC user to obtain the same connected devices without having to add all the XO devices again.

Note

The AppData folder is a hidden folder in Windows, so it may not be visible on your PC. To make Windows display hidden folders, proceed as follows: in Windows Explorer, choose **Tools** > **Folder options**; then click the **View** tab, and select the **Show hidden files, folders, and drives** option. Press F5 to refresh the Explorer view.

You can also reuse the list of devices from a previous (XOa/XO) version of the client.
In this case, you have to copy:

- for XOa: the HydraApp.ini file that you can find in the following folder:

  C:\Users\username\Appdata\Roaming\AdproXOa\

- for XO 5.0: the the HydraSiteList.xml file that you can find in the following folder:
  C:\Users\username\Appdata\Roaming\Hydra\

Paste the HydraApp.ini or HydraSiteList.xml file in the C:\Users*username*\Appdata\Roaming\Hydra\ folder for the XO client. The system will automatically convert it to a HydraSiteList.xml file. If there already is a file named HydraSiteList.xml file in the folder, you have to delete it before you paste the HydraApp.ini or HydraSiteList.xml file.

2.5 Software Updates

Honeywell regularly provides software updates for your XO device, which you can easily download and install via the Xchange2 tool. For more information, see the *Xchange2 user manual* (27816).

Caution!

Honeywell issues upgrade information with every major software upgrade. Upgrade information may consist of system requirements, special upgrade instructions, etc. Before installing new software, make sure that you **read and understand the upgrade information** first. Always follow the instructions in the upgrade documentation. If in any doubt, do not install the new software.
You can find upgrade instructions on the Security Solutions Support site https://myhoneywellbuildingsuniversity.com/ (listed under Field Alerts). Also check the Release Notes (listed under Product Release) for information on solved bugs or known issues.

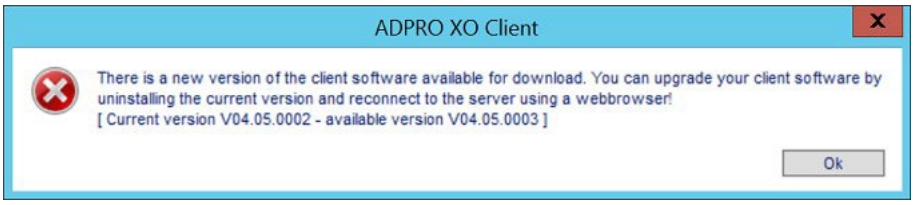
Caution!

When upgrading to XO 5.0, the system will first uninstall the old version of the client. Note that the default install path and work folder are different.

Caution!

The FastTrace 2 Series device firmware is available in a 32-bit and a 64-bit version. This enhances the device's performance and makes it future-proof. FastTrace 2 Series devices with analogue encoder cards (DS42xx) can only run the 32-bit version. Other FastTrace 2 Series models can run the 64-bit version, if they meet the other requirements: PH10LU motherboard, DOM min 2 GB…. For details, see *the XO 5.0 Release Notes* (26598_16).

Honeywell recommends to use the same version for server and client software. However, it is possible to use a newer client version to connect to servers running lower firmware versions. The opposite is not possible: you cannot use an older client software to configure a server running on a newer version. In this case, the following message appears when you open the XO client:



Click **OK** to close the message box. The client software opens, but the following warning appears:



Click **OK** to close the message box. The **System** menu is unavailable until you update the client software. You can update the client using the client installer (downloadable from the Security Support site), or, if you do not have an internet connection for downloading, you can update the client via the device's web page, as described below.

Note

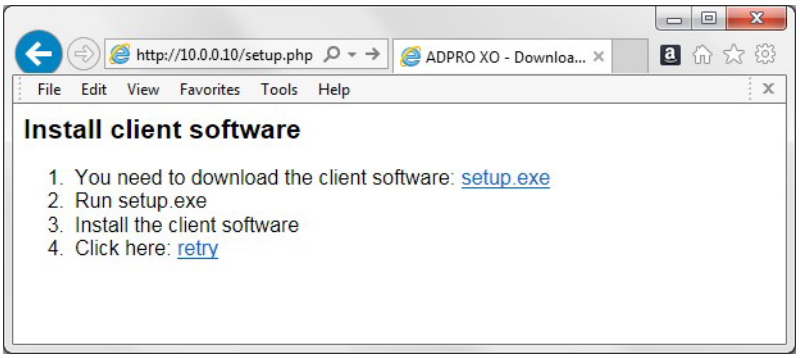
Webserver is disabled by default for security reasons. It can only be reenabled by a technician on a system in which an admin user has enabled the technical grant. To install the client software using the XO device's web page, the webserver must be enabled by the technician which is a security risk. You can get the client software from the release DVD or from the support site (https://myhoneywellbuildingsuniversity.com/).

Honeywell recommends to uninstall the current client first. (In Windows, go to **Programs and Features**, search for **ADPRO XO**. Right-click it and then click **Uninstall**.)

To update the client software to the same version as the server, proceed as follows:

1. Close the XO client.
2. Open Internet Explorer.

3. In the address box, type the XO device's IP address followed by /setup.php. For example: http://10.0.0.10/setup.php
   The following window appears:



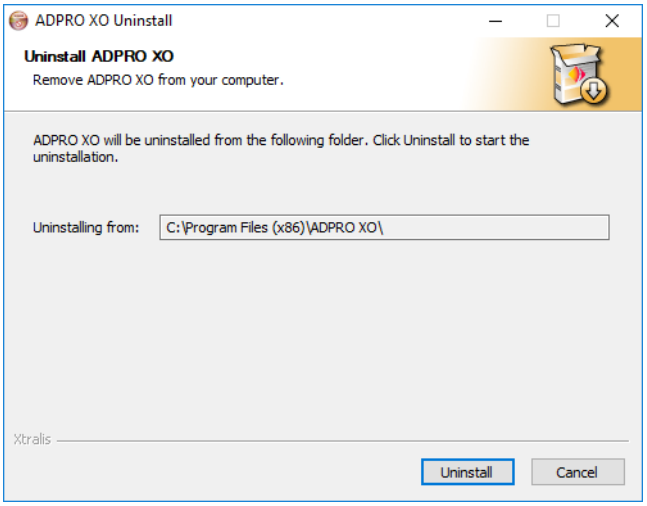
Note

If you are experiencing issues when updating the XO client software, see *Internet Explorer Settings* for instructions.

4. Click **setup.exe** to download the setup file.



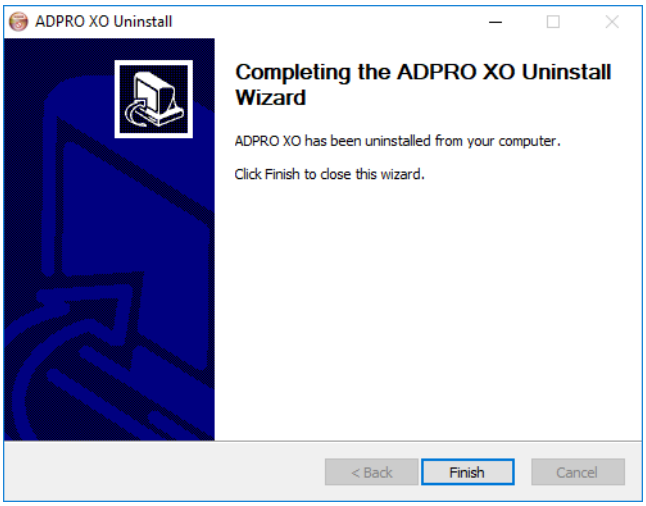
5. Click **Run**.
   Alternatively, you can download the installation file, and launch it from the download folder.
   The system will uninstall the previous XO or XOa client version first.



Note

The uninstaller will preserve the devices that you have added to your current version. They will be immediately available in the new version.

6. Click **Uninstall** to confirm. When finished, the following screen appears:



7. Click **Finish**, and then follow the instructions of the installation Wizard to install the new version.

3. Connections

3.1 Network (Ethernet)

You connect the XO device to a local network (eth0) for communicating with the client PC and the CMS: for transmission of alarms, messages, live and quad images… The local network also provides the communication line to Net I/O units and S3100 panels.

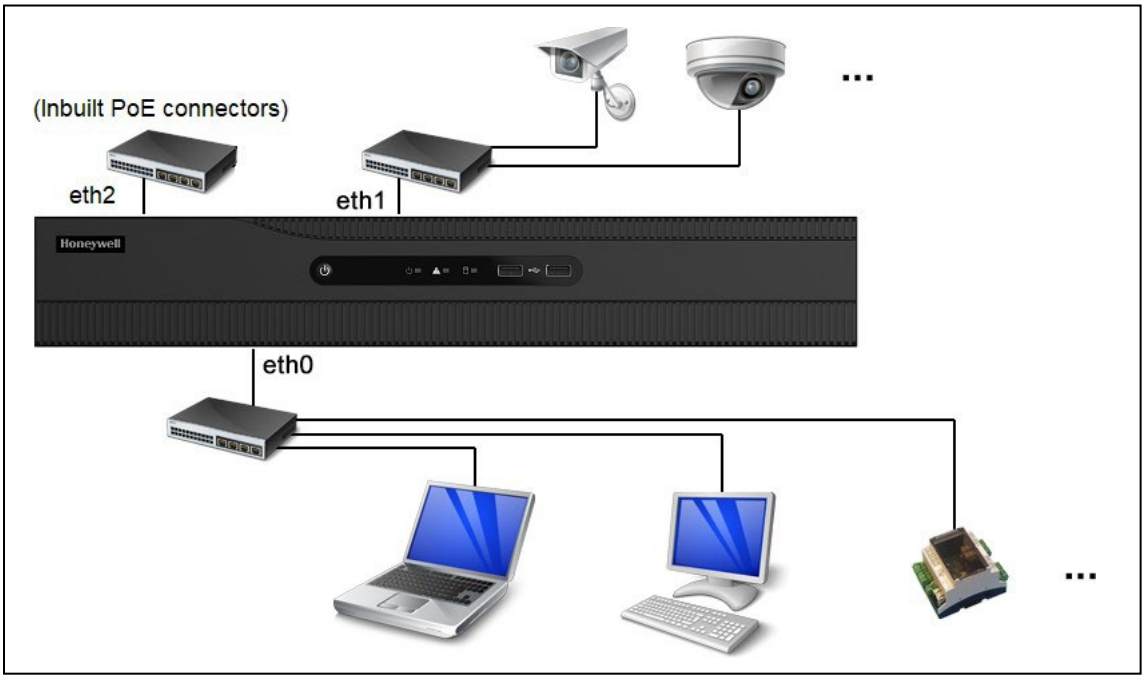
You connect the IP cameras to a separate network (eth1). For more information, see *IP Camera Network* . This makes sure that the video streams from the IP cameras do not interfere with alarm transmission on the local network.

Note

Although it is technically possible to connect other IP devices, such as Net I/O units, to the IP camera network (eth1) instead of the local network (eth0), Honeywell does not recommend it.

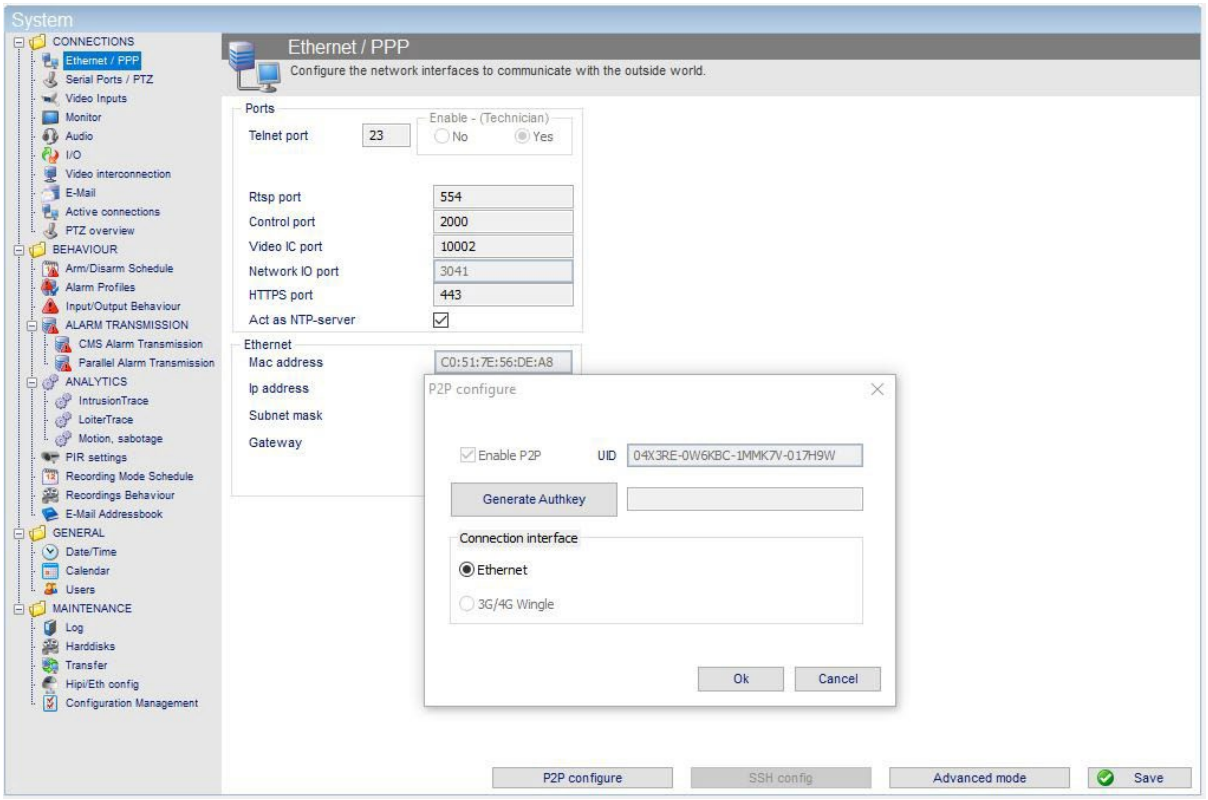
It is not possible to have overlapping IP address ranges in eth0 and eth1; these must be separate. The system will check and issue a warning if the IP addresses of eth0 and eth1 are in the same range. The additional Ethernet connector (eth2) provides the physical interface to connect to PoE cameras on the eFT-T4/16P and eFT-T2/8P devices.

Besides the local network connection, you can also set up a remote (PPP dial-in) network using an external modem. For more information, see *PPP Connection (Modem)* .



To set up the local network connection (eth0), proceed as follows:

1. Choose **System** > **Connections** > **Ethernet / PPP**.



2. Provide the following information:

Item	Description	Default value
Ports		
Telnet port	For security reasons, the Telnet connection is disabled by default. A Technician user can activate the Telnet connection and set the Telnet port. For details, see *Telnet Connection* .	Disabled, port 23
Webserver port	Type the port number for the http protocol. **Note** Webserver is disabled by default.	Disabled, port 80
Rtsp port	Type the port number for the real-time streaming protocol: the client uses this port to control the video streaming. If you change this port number, you also need to change it in the settings for the device in the **Login** window.	554
Control port	Type the port number for exchanging information between the XO device and the XO client software (for example, the status of inputs and outputs). If you change this port number, you also need to change it in the settings for the device in the **Login** window.	2000
Video IC port	Type the port number for interconnecting with S3100 security panels. Use the same port as the one selected in the S3100 configuration.	10002
Network I/O port	This box displays the port used to poll the Net I/O units. This port is fixed, you cannot change it.	3041
Act as NTP-server	The option to disable NTP server running on the main NIC when not required.	Enabled

Item	Description	Default value
Ethernet		
P2P configure	The **Enable P2P server** window is displayed on clicking the **P2P configure** button.	NA
Generate Authkey	Click the Generate Authkey button to create an authkey. **Note** For new P2P connections, create an authkey before enabling P2P. Using authkey is essential for security (previously, P2P worked with just the UID, but now UID and authkey are required). Authkey will take effect in the next P2P connection and doesn't affect the currently established P2P. Generate Authkey will create a new authkey even if an authkey already exists, and the users must always use the latest authkey. Ensure securely saving the authkey.	NA
Enable P2P server	Select the **Enable P2P Server** checkbox and paste the unique P2P authentication identifier in the **UID** field (by selecting from the TUTK list) to enable P2P connection between the server and the connected clients. **Note** Instant access between the devices (without the use of IP address) is enabled using the P2P (peer-to-peer) network technology. TUTK is the vendor providing the P2P license UIDs. The P2P connection option is displayed on the XO client login page after applying it on the XO server. The same UID can be used for all the XO clients connecting with the XO server. To login to the XO Client with P2P connection, paste the same UID in the **P2P License UID** field and authkey in the **P2P Authkey** field, and then select **Use P2P**. Do not leave the IP address, control port, rtsp ports fields blank when you select the enable P2P server option. IP address field can have a dummy value. The control port and rtsp port values must be the same as those in the device. For example, if control port is 2001 and that port is port forwarded to port 2000 of the actual device you need to enter 2000 and not 2001. P2P supports connections via 4G wingle.	NA
MAC address	This box displays the MAC address of the XO device. You cannot change the MAC address.	–
IP address	Type the IP address of the XO device. Do not use reserved addresses! If you change the IP address, you also need to change it in the settings for the device in the **Login** window.	10.0.0.10
Subnet mask	Type the subnet mask.	255.255.255.0
Gateway	Type the gateway address (= IP address of the router).	10.0.0.1

> ***Caution!***
>
> Honeywell strongly recommends using the default ports. If you have to use other port numbers, consider the restrictions as described in *Restrictions for Port Number Usage*. **Do not use** the reserved port numbers **3040 and 3041**.
>
> In addition, you have to document the use of the new ports thoroughly. You will need this information to configure the routers/firewalls in your network.

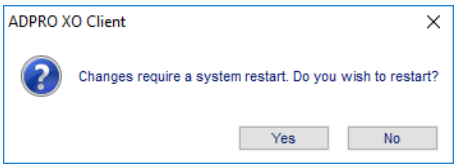
3. Click **Save**. If you have changed the IP address, the following message appears:



The system automatically clears the list of client PCs allowed to connect to the device. For details, see *Restricting Access to the XO Device* .

4. Click **OK** to close the message box. Changing the network settings may require a system restart.

If this is the case, the following message appears:



Click **Yes**, and wait for the device to restart.

If no system restart is required, The following message appears:



Click **OK**. The client will close.

5. Make any necessary changes in the client's **Login** window, and then connect to the device again.

3.2 Telnet Connection

In software version XOa 3.02.0033 and above, the Telnet connection is disabled by default for security reasons. Technician users can enable/disable the Telnet connection in the XO client. Technician users can only log on to the XO client if an Administrator or another user has granted them access. For details on user types, access rights, and granting access to Technician users, see *Users* .

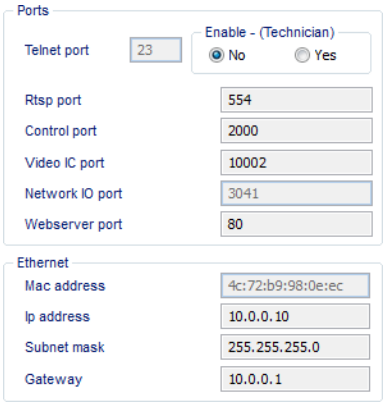
Once the Telnet connection is activated, any user (with suitable access rights) can change the default Telnet port if required. Changing the Telnet port requires a system restart.

> ***Caution!***
>
> If you use your XO device with M3000, you must enable the Telnet connection. Without Telnet, there is no communication between the systems.

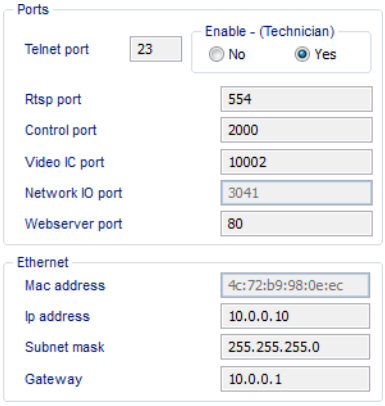
To enable the Telnet connection, proceed as follows:

1. Log on to the XO client as an Administrator user (or any other user that can enable the Technician user).
2. Choose **System** > **General** > **Users**.

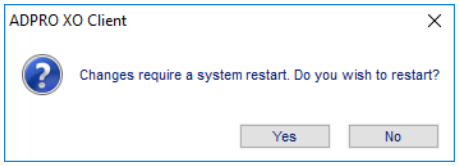
3. Under **Technician grant**, click **Enable**.
4. Close the XO client.
5. Log on to the XO client as a Technician user.
6. Choose **System** > **Connections** > **Ethernet / PPP**.



7. To enable the Telnet connection: under **Enable - (Technician)**, click **Yes**.
   The **Telnet port** box becomes available.



8. If you want to change the default port number, type the IP port number for the Telnet connection in the **Telnet port** box.
9. Click **Save**. If you have changed the Telnet port, the following message appears:



10. Click **Yes**, and wait for the device to restart.

Note

The system automatically disables the technician grant when you restart the XO device. If you want to enable the Telnet connection again, you have to re-enable the Technician user first which may enforce password reset.

Caution!

Enable telnet only in rare scenarios such as when you are remotely investigating a field issue and disable it soon after. Honeywell recommends that you disable the Telnet connection when no longer needed. Only Technician users can disable the Telnet connection.

Technician user can establish SSH session with the XO client using the telnet window. Use the keyboard command `kb,<user name>,<password>` to establish SSH connection with the XO device. The alphanumeric password must be enclosed in quotes. The technician can White List the XO device IP for SSH, and the SSH connection over the control port can be used to debug errors on the XO device.

To disable the Telnet connection, proceed as follows:

1. If required, enable the Technician user first.
2. Log on to the XO client as a Technician user.
3. Choose **System** > **Connections** > **Ethernet / PPP**.
4. To disable the Telnet connection: under **Enable - (Technician)**, click **No**.
5. Click **Save**.
6. If required, disable the Technician grant again.

3.3 Restrictions for Port Number Usage

Listed below are the default port numbers used for ADPRO XO communication. Although it is possible to change most of these port numbers via the XO client, **do not use the default port numbers for anything else than their default purpose as described in the table below**.

Default port number	Purpose	Fixed
80	Webserver port	–
554	RTSP port (streaming video)	–
2000	Control port	–
3000	Audio server port (see also Note below)	–
3040	NetFinder port.	Yes
3041	Network I/O port (for Net I/O units)	Yes
5555	Walk test port (iPIR).	–
10002	Video interconnection port (S3100/FOXnet Plus).	–
15020	Presidium port (obsolete).	–
443	HTTPS port for video stream	–
33300 ～ 33400	Camera event feedback port	–

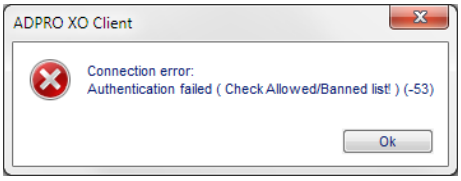
Note

In a network with multiple XO devices, and if you need to access the devices from an external network (for example, a CMS via router/firewall), you have to specify a **unique audio server port number** for each device. For example: 3000 for the first device, 3001 for the second… Remember to add all port numbers to the port forwarding configuration of your router/firewall.

3.4 Communication with External Networks (Routers and Firewalls)

If you need to communicate with the XO device from an external network, make sure that the routers and firewalls in the network are set up correctly: network address translation (port forwarding), firewall settings, etc. If not, the XO devices will not be able to send alarm and other information to the CMS or other destinations in the

external network. In addition, you will not be able to connect to the device from the external network. You will receive the following error message when trying to log on:



In the XO client **Login** window, add a device using its external IP address and external port numbers.

For instructions on setting up routers and firewalls, see the documentation of your router/firewall. If you are using the ADPRO ADSL 1202/1302 Router, see the router's *Installation Guide* (29448). The table below lists the standard services and port numbers that are required for communication:

Service Name	Service Type	Port Number (From/To)
Control Port TCP	TCP	2000–2001
Control Port UDP	UDP	2000–2001
Audio Port TCP	TCP	3000
Audio Port UDP	UDP	3000
Alarm Port TCP	TCP	10000
RTSP Port TCP	TCP	554
RTSP Port UDP	UDP	554
Debug Port (must be closed at all times; open only when needed)	UDP	2222
iPIR Port	UDP	5555

Caution!

For security reasons, **always keep debug port 2222 closed**. Open it **only on request** (for example, by Honeywell technical support staff), and **always close it afterwards**.

Note

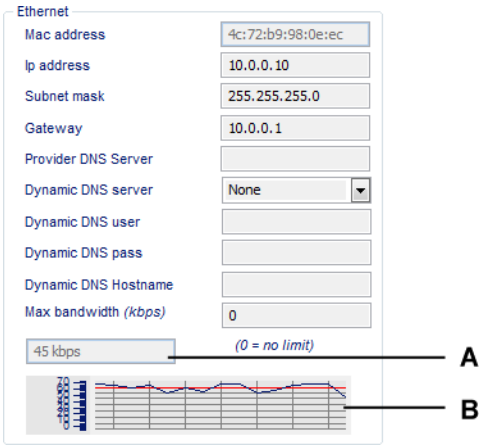
If you are using **non-standard** port numbers, make sure to specify them instead of the standard ports.

3.5 Bandwidth

You can limit the total bandwidth that the system uses. This may affect image rate, but not image quality, during live viewing.

To limit the bandwidth, proceed as follows:

1. Choose **System** > **Connections** > **Ethernet / PPP**.
2. Click **Advanced mode**. The advanced Ethernet options appear:



   The graph (**B**) at the bottom indicates the bandwidth that the local network is currently using. The horizontal red line in the graph indicates the average used bandwidth. The box above the graph (**A**) displays the current bandwidth value in kbps.

3. In the **Max bandwidth (kbps)** box, type the desired maximum bandwidth in kbps (kilobits per second). If you do not want to limit the bandwidth, type **0**.
4. Click **Save**.

3.6 Dynamic DNS

3.6.1 About Dynamic DNS

Dynamic DNS provides the capability for a networked device, such as a router or modem, to notify a Domain Name System (DNS) to change, in real time, the active DNS configuration of its configured hostnames, addresses, or other information. In this way, you can use a hostname instead of the IP address, which is convenient for DHCP-attributed IP addresses. Especially with 3G/4G, DHCP often attributes the IP address.

To register to a Dynamic DNS service provider, the XO device needs access to the internet and to a DNS server to resolve the host name of the service provider. This internet connection can be provided by the Ethernet connection or a 3G/4G connection. If the internet connection is only available through 3G/4G, you have to enter the correct Provider DNS server when setting up Dynamic DNS in the client software.

Note

- If you configure a Dynamic DNS service for both the Ethernet and the PPP (3G/4G, modem) connection, you have to use different host names (only 1 account required, but 2 host names).
- If the XO device is behind a router, the Dynamic DNS service will use the external IP address. The XO device will set this automatically, so no changes in the XO client are necessary.

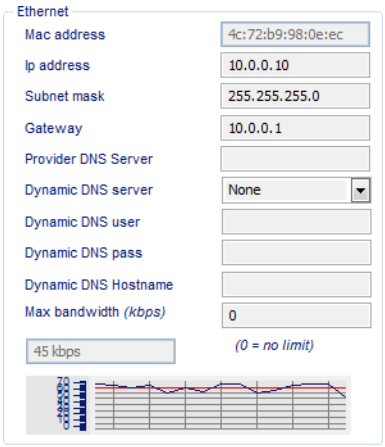
3.6.2 Setup

Note

You have to set up a Dynamic DNS account (with any Dynamic DNS service provider) first.

To configure the XO device for Dynamic DNS, proceed as follows:

1. Choose **System** > **Connections** > **Ethernet / PPP**.
2. Click **Advanced mode**. The advanced Ethernet options appear:



3. Provide the following information:

Item	Description
Provider DNS server	Enter the provider DNS server. If you will connect to internet over Ethernet, you can leave this box blank, because certain protocols have been pre-programmed in the software. If the internet connection is only available via 3G/4G (in **Advanced mode** under **PPP**), then you have to fill in this box.
Dynamic DNS server	Select the correct provider in the list.
Dynamic DNS user	Enter the username you have received from your provider for the Dynamic DNS account.
Dynamic DNS pass	Enter the password you have received from your provider for the Dynamic DNS account.
Dynamic DNS host	Enter the host you have received from your provider for your Dynamic DNS account.

4. Click **Save**, and wait for 10–20 seconds while the system establishes a connection to the Dynamic DNS server.
   - If no error messages appear, the connection to the Dynamic DNS is successful.
   - If error messages appear, see the troubleshooting section below.

3.6.3 Troubleshooting Dynamic DNS

If the system cannot connect to the Dynamic DNS service, an error message will pop up. At the same time, the system will activate system input 0055 – [SYST] – DYN DNS FAILED. Typical errors are incorrect username, password, or host name. The most common errors are described below.

Note

An error message is displayed only once. If you want to view the message once again, set the Dynamic DNS server to **None**, and then click **Save**. Re-enter your DNS provider, and click **Save** again. Wait for a few seconds and the message will reappear.

'Warning: Unable to determine IP address'

If you receive this error message, the XO device could not resolve the service provider's host name:

- Check the provider DNS server settings in the **Ethernet** screen.
- Check the internet connection of the XO device.

'No update required'

If you change settings for the Dynamic DNS, the XO device will write a new configuration and force an update of this configuration. Some service providers may return a message such as *No update required* or *Attempts to change to the current address are considered abusive*. This system will automatically reset this error on the next automated check, after one minute.

3.7 Restricting Access to the XO Device

To restrict the access to the XO device via the local network, you can:

- Create a list of authorised clients in the **Allowed** list.

  If you use the Allowed list, the system automatically adds the IP address of your PC (on which the XO client software is running) to the Allowed list when you add any other IP address. If this were not the case, your own PC would become an unauthorised client and you would no longer be able to connect to the device from your PC.

  You cannot delete your PC's IP address from the Allowed list.

  If you leave only your own IP address in the Allowed list, no other client will be able to connect to the XO device.

- Create a list of non-authorised clients in the Banned list.

  If you use the Banned list, you cannot add the IP address of your PC. If this were not the case, your own PC would become an unauthorised client and you would no longer be able to connect to the device from your PC.

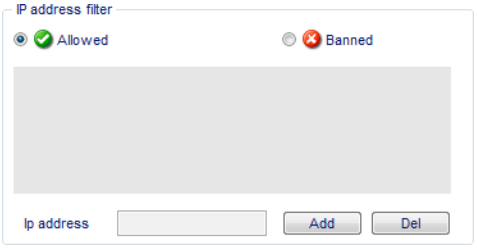
You cannot use both lists at the same time. Choose the list that suits your situation best. Leave the lists empty if you do not want to restrict access.

Note

If you change the IP address of the device, the system will automatically clear the **Allowed** list.

To restrict access to the XO device, proceed as follows:

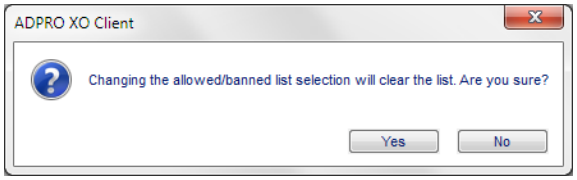
1. Choose **System** > **Connections** > **Ethernet / PPP**.
2. Click **Advanced mode**. The IP address filter appears:



3. Proceed as follows:
   - To create a list of authorised clients, click Allowed.
   - To create a list of non-authorised clients, click Banned.
4. In the **IP address** box, type the IP address that you want to ban/allow.
5. Click **Add** to add the IP address to the selected list.
6. Repeat for all other IP addresses that you want to ban/allow.
7. To remove an IP address from the list, click the IP address, and then click **Del**.

8. To quickly remove all addresses:
   - From the **Allowed** list, click **Banned**.
   - From the **Banned** list, click **Allowed**.

   The following message appears:



9. Click **Yes** to confirm.
10. Click **Save**.

3.8 PPP Connection (Modem)

3.8.1 About Modems

You can connect one modem to the XO device, to the /dev/ttyU1 USB port. To know which USB port is dev/ttyU1, see the *Hardware Installation Manual* of your XO device (FastTrace 2 Series: 21790; iFT Series: 27817; eFT Series:35450). You can use either a PSTN/ISDN or a 3G/4G modem. The setup of both modem types is described in detail in the following sections.

Alternatively, you can use the Huawei E8372 wingle for a 4G connection.

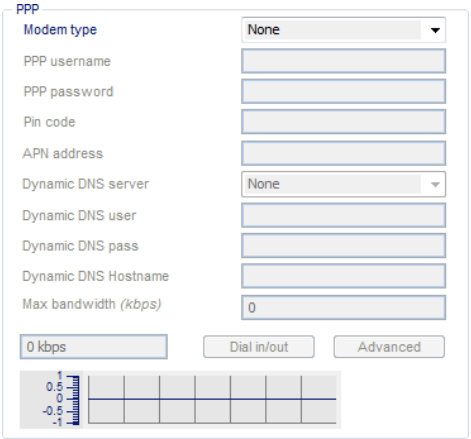
3.8.2 Dynamic DNS for Modems

If you configure a Dynamic DNS service for both the Ethernet and the PPP (3G/4G modem) connection, you have to use different host names (only 1 account required, 2 host names).

3.8.3 PSTN or ISDN Modem Configuration

Standard modems use the analogue line (AT modem) or digital line (ISDN). To set up a PSTN/ISDN modem, proceed as follows:

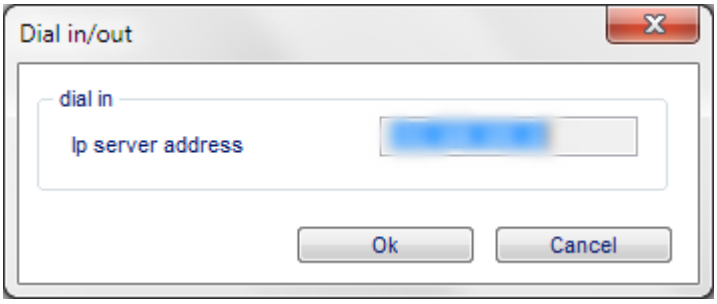
1. Choose **System** > **Connections** > **Ethernet / PPP**.
2. Click **Advanced mode**. The following section appears:



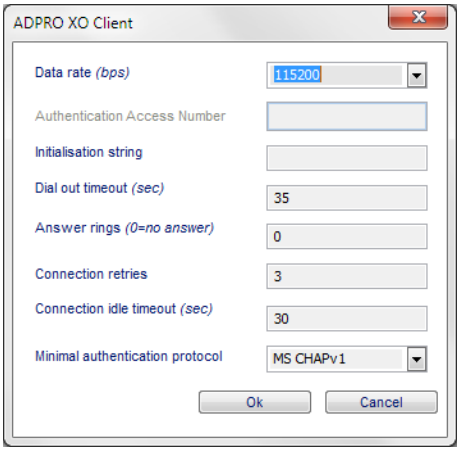
3. Provide the following information:

Item	Description	Default value
Modem type	Select **PSTN** for a PSTN or ISDN modem.	None
PPP username	Type the username of a user allowed to connect to the dial-in network (PPP authentication).	V3100
PPP password	Type the password of a user allowed to connect to the dial-in network (PPP authentication).	666777
Dynamic DNS server / user / pass / Hostname	Only required if you are using Dynamic DNS with the modem. The Dynamic DNS setup for modems is similar to the setup for the Ethernet connection. For details, see *Dynamic DNS* .	–
Max. bandwidth	Type the desired maximum bandwidth in kbps (kilobits per second) for the modem. If you do not want to limit the bandwidth, type **0**. The graph below this box indicates the bandwidth that the modem is currently using. The box just above the graph displays the current bandwidth value in kbps.	33 (suitable for V34 modem)

4. Click **Dial in/out**. The following screen appears:



5. In the **IP server address** box, type the IP address that will be assigned to the XO device when the client establishes a remote connection.
The default value is 192.168.100.10.
6. Click **OK**.
7. Click **Advanced**. The following screen appears:



8. Provide the following information:

Item	Description	Default value
Data rate (bps)	Select the baud rate of the modem.	115200
Initialisation string	Type the Hayes command string to initialise the modem.	–

Item	Description	Default value
Dial out timeout (sec)	Enter the time, in seconds, in which a connection to the remote client has to be established. If not successful, the XO device will retry. You can limit the number of attempts (see **Connection retries** below). Be aware that a PPP connection over PSTN can easily take 30 to 60 seconds.	35
Answer rings (0 = no answer)	Enter the number of rings on an incoming call before answering. Set to **0** to not answer any incoming call.	0
Connection retries	Enter the number of attempts the XO device will make to connect to the remote client.	3
Connection idle timeout (sec)	Enter the delay, in seconds, after which the XO device will disconnect if no more data is exchanged.	30
Minimal authentication protocol	Selects the authentication protocol used for establishing a remote connection: PAP/CHAP/MS CHAPv1/MS CHAPv2.	MS CHAPv1

9. Click **OK**.
10. Click **Save**.

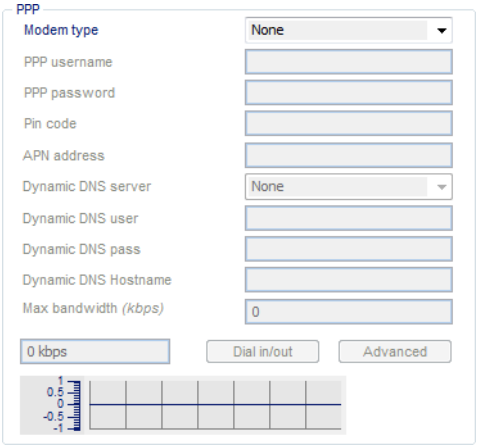
3.8.4 3G/4G Modem Configuration

Note

The XO device supports only the Sierra Wireless Airlink Raven XE modem. Honeywell does not guarantee that any other 3G/4G modem will work properly.
You can also use a compatible wingle such as the Huawei E8372 4G wingle. For details, see *4G Wingle Connection*.

To set up a 3G/4G modem, proceed as follows:

1. Choose **System** > **Connections** > **Ethernet / PPP**.
2. Click **Advanced mode**. The following section appears:

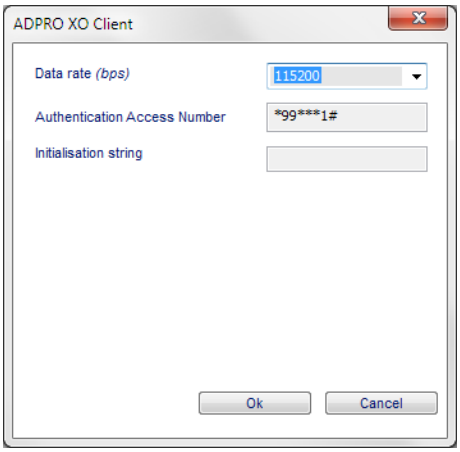


3. Provide the following information:

Item	Description	Default value
Modem type	Select **3G/4G** for a 3G or 4G modem.	None
PPP username	Type the username of a user allowed to connect to the dial-in network (PPP authentication).	V3100

Item	Description	Default value
PPP password	Type the password of a user allowed to connect to the dial-in network (PPP authentication).	666777
Pin code	Enter the PIN code for your 3G/4G SIM card.	–
APN address	Enter the APN (Access Point Name) address of your provider.	–
Dynamic DNS server / user / pass / Hostname	Only required if you are using Dynamic DNS with the modem. The Dynamic DNS setup for modems is similar to the setup for the Ethernet connection. For details, see *Dynamic DNS* .	–
Max. bandwidth	Type the desired maximum bandwidth in kbps (kilobits per second) for the modem. If you do not want to limit the bandwidth, type **0**. The graph below this box indicates the bandwidth that the modem is currently using. The box just above the graph displays the current bandwidth value in kbps.	1000

4. Click **Advanced**. The following screen appears:



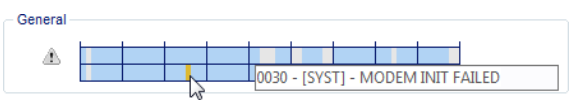
5. Provide the following information:

Item	Description	Default value
Data rate (bps)	Select the baud rate of the modem.	115200
Authentication Access Number	Enter the number that the 3G/4G modem will dial to set up a data connection. The number depends on the country and/or the provider. For example: Vodafone in Australia uses *99***2#.	*99***1#
Initialisation string	Type the Hayes command string to initialise the modem.	

6. Click **OK**.
7. Click **Save**.

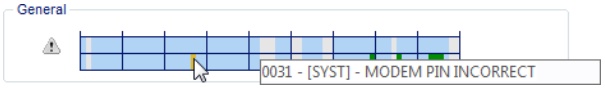
3.8.5 Troubleshooting 3G/4G Modem Setup

The XO device starts searching for the internal 3G/4G connection when you click **Save**. During the search, the system input 0030 – [SYST] – MODEM INIT FAILED is active (you can see this in the **Status** screen). After about 45 seconds (depending on the connection), when the XO device establishes the 3G/4G connection, the system automatically deactivates the input.



If the error message persists, there is an issue with the modem USB connection or the 3G/4G settings.

If you have entered an incorrect pin code, the system input 0031 – [SYST] – MODEM PIN INCORRECT is active.



If a 3G/4G connection is set up successfully, but the XO device cannot establish a connection, then try changing the control port (**System** > **Connections** > **Ethernet / PPP**, under **Ports**). The default control port is 2000, but many providers block it. Changing the control port to port 2001 may resolve the problem.

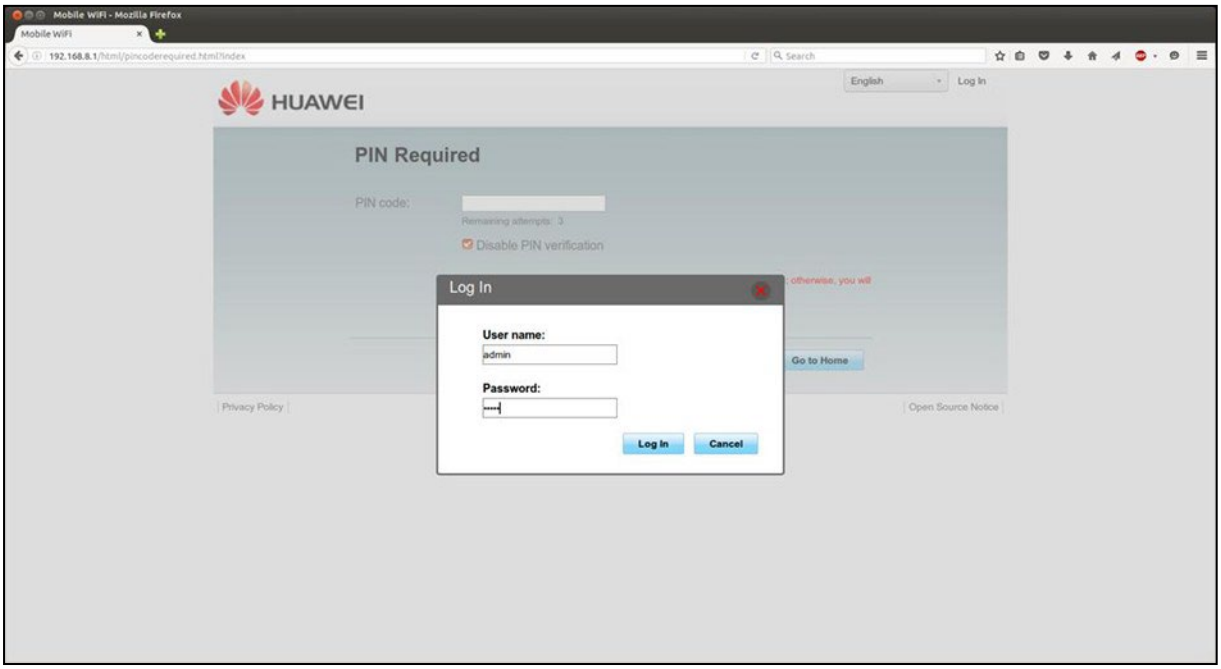
3.9 4G Wingle Connection

3.9.1 Preparing the Wingle

The Huawei E8372 wingle offers a 4G connection on your XO device. Before you can use the wingle, you need to prepare it on your PC. Then you can insert it into your XO device and specify the PPP settings in the XO client.

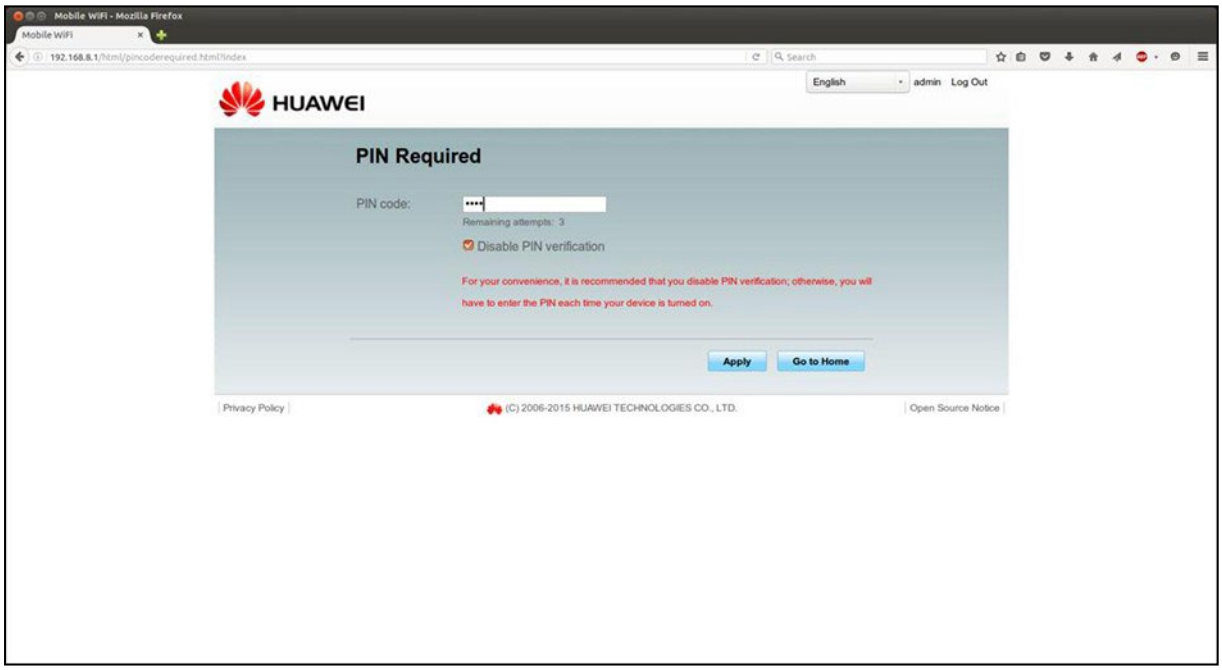
To prepare the wingle for use, proceed as follows:

1. Install the SIM card in the wingle. For details, see the Quick Start Guide that came with the wingle.
2. Write down the SSID and Wi-Fi key; you will need these later to connect to the Huawei Wi-Fi access point.
3. Insert the wingle into a free USB port on your PC.
4. Connect to the Huawei Wi-Fi access point.
   If the PC displays an additional Ethernet connection, you can use this connection instead of the Wi-Fi connection.
5. Open your browser and go to:
   https://192.168.8.1

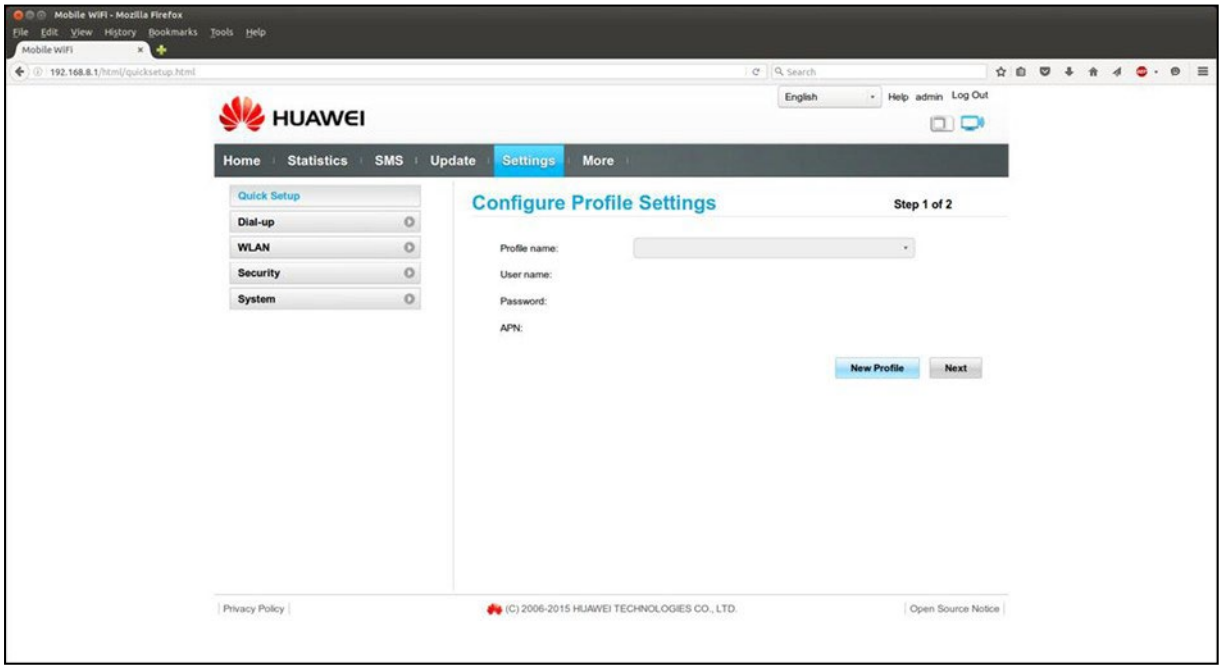


6. Log on with username = admin and password = admin.

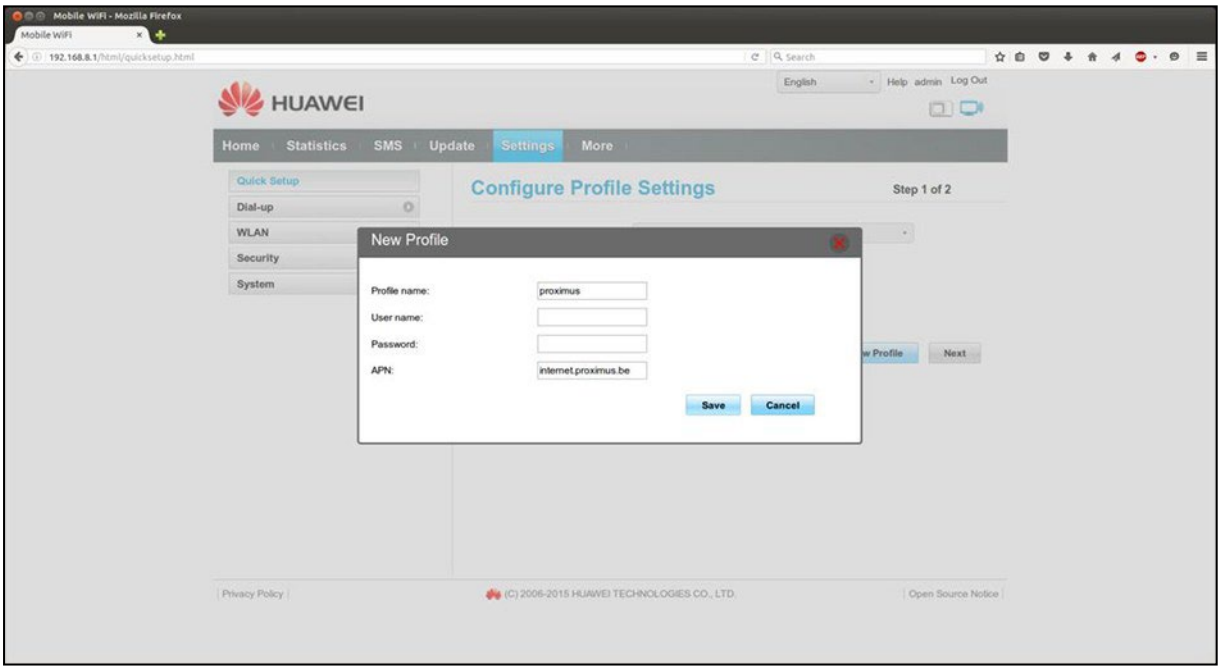
7. If the window below appears, fill in the PIN code of the SIM card.



8. Select the **Disable PIN verification** check box, and then click **Apply**.
9. In the menu at the top, click **Settings**.



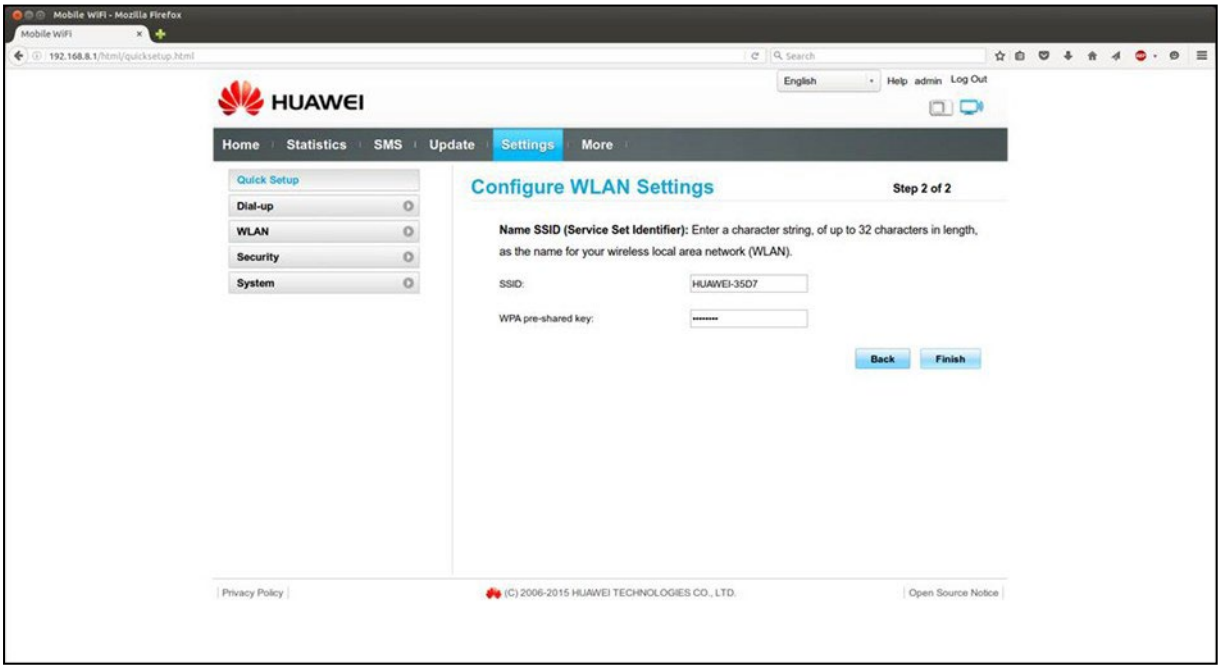
10. Click the **New Profile** button.



11. Provide the following information:

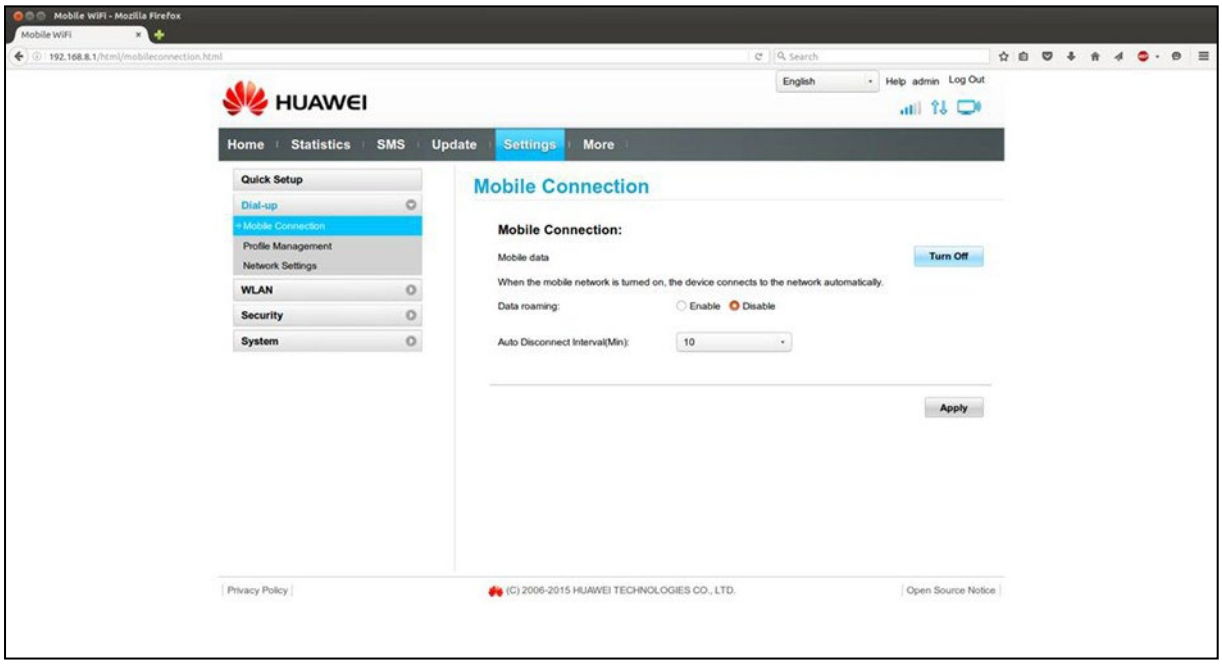
Item	Description
Profile name	Type a name for the connection.
User name	Type a username for the connection (if required – check with your provider).
Password	Type a password for the connection (if required – check with your provider).
APN	Enter the APN (Access Point Name) address of your provider.

12. Click **Save**, and then click **Next**.

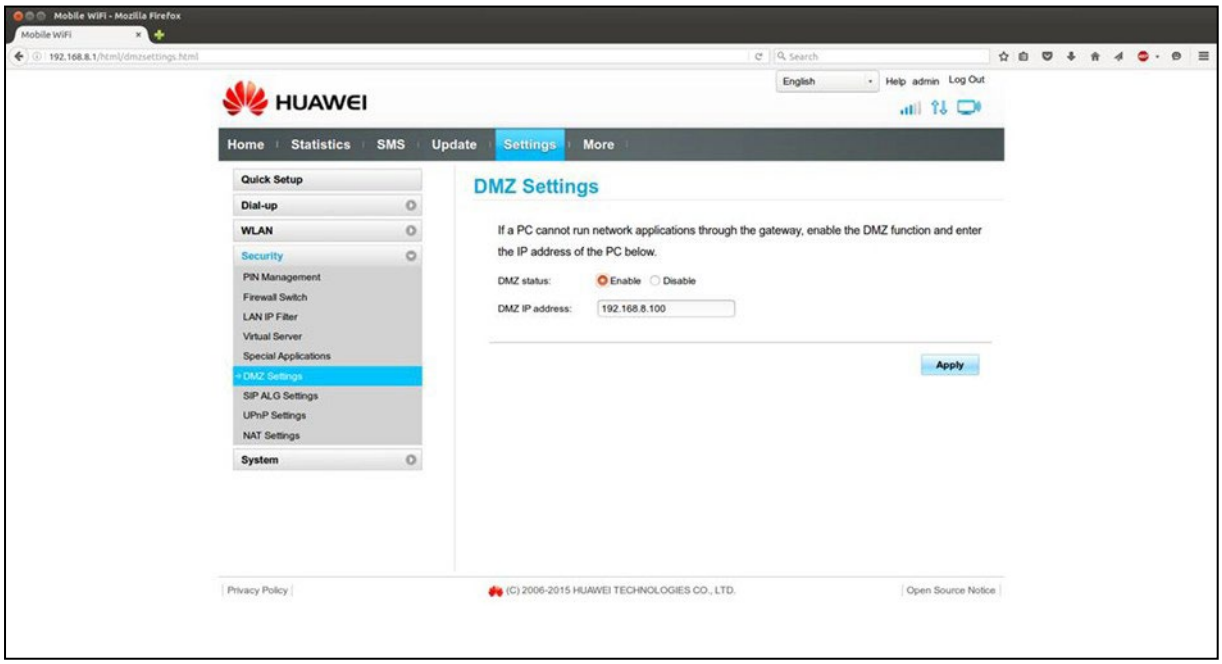


13. Optional: change the SSID and Wi-Fi key.
14. Click **Finish**.

15. In the menu on the left, choose **Dial-up** > **Mobile connection**.



16. Make sure that **Mobile data** is turned on (it is on if the screen displays the **Turn off** button).
17. In the menu on the left, choose **Security** > **DMZ settings**.



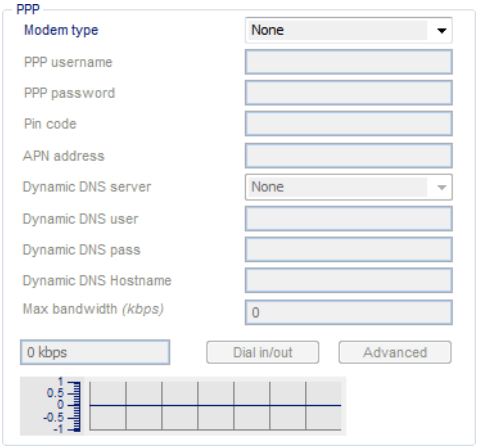
18. Set **DMZ status** to **Enabled**.
19. Set the **DMZ IP Address** to **192.168.8.100**.
20. Click **Apply**.
    The wingle is now configured.
21. Insert the wingle into the /dev/ttyU1 USB port on your XO device.
22. Restart the XO client.

Next, you will specify the PPP settings for the wingle in the XO client.

3.9.2 Wingle PPP Configuration

To specify the wingle PPP settings, proceed as follows:

1. Choose **System** > **Connections** > **Ethernet / PPP**.
2. Click **Advanced mode**. The following section appears:



3. Provide the following information:

Item	Description	Default value
Modem type	Select **3G/4G**.	None
PPP username	Type the username for connecting via the 4G wingle (PPP authentication).	V3100
PPP password	Type the password for connecting via the 4G wingle (PPP authentication). **Note** The default user ID is 0. The XO device has 666777 as the initial password which is changed at the first login.	666777
APN address	Enter the APN (Access Point Name) address of your provider.	–
Max. bandwidth	Type the desired maximum bandwidth in kbps (kilobits per second) for the PPP connection. If you do not want to limit the bandwidth, type **0**. The graph below this box indicates the bandwidth that the PPP connection is currently using. The box just above the graph displays the current bandwidth value in kbps.	1000

4. Click **Save**.

3.10 Email

3.10.1 Setting up Email

If you want the XO device to send emails on events/alarms (for example, for the iTrace app), set up the email SMTP server, and the email sender address. Ask the IT Department for the correct settings.

Note

The email address of the email sender may need to be an existing email account, depending on the SMTP server settings.

To set up email communication, proceed as follows:

1. Choose **System** > **Connections** > **Email**.



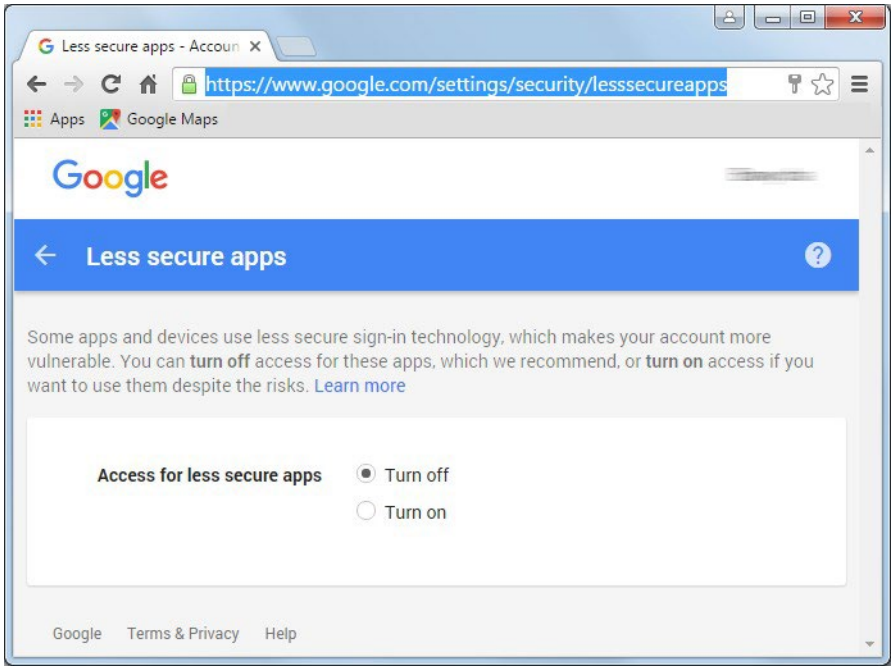
2. Provide the **SMTP server address**, **SMTP server port**, and **TLS** setting as specified by the IT Department.
3. If your email server requires authentication, provide a username and password in the **Username** and **Password** boxes.
4. In the **Sender email address** box, type the email address that will send the emails.
5. For emails to the iTrace app, specify the following additional settings:
   - **iTrace smtp retry time (1–10m)**: specify the time (between 1 and 10 minutes) in which the recipient has to respond to the iTrace email. If the recipient does not respond in time, iTrace sends the email again.
   - **iTrace retry attempts (1–10)**: the number of times (between 1 and 10) that iTrace sends an email for the same event. If there is still no response from the recipient after that, the XO device activates the system alarm 0041 – [SYST] – NO ITRACE REACTION. This alarm can warn CMS staff that there was no response to the iTrace emails, so that they can then take the appropriate action.
6. Click **Save**.

You can now set up the mailing lists to send emails to.

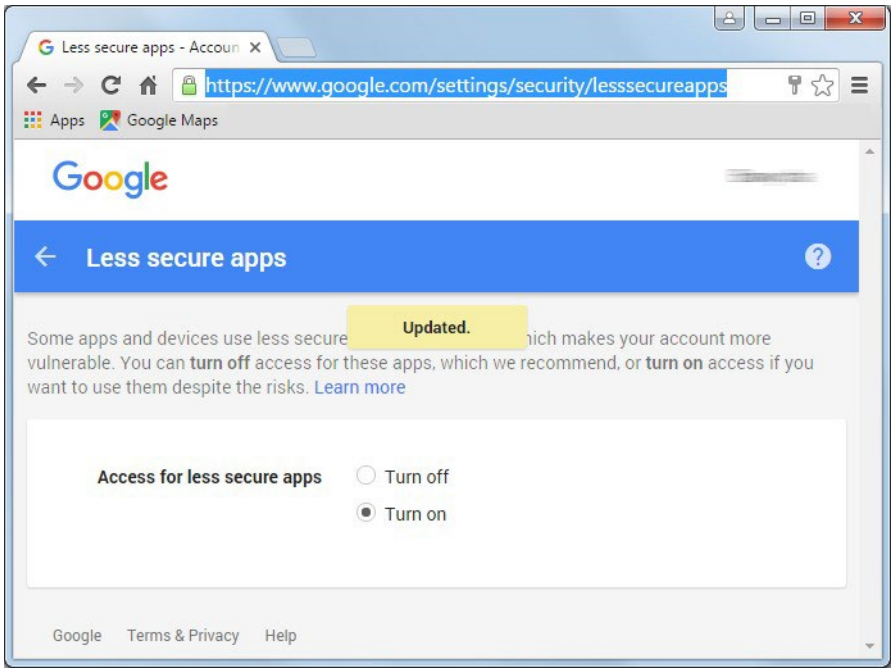
3.10.2 Setting up Email with Gmail

If you want to use a Gmail account to send emails, you have to set up Gmail too. Proceed as follows:

1. Open your web browser and go to:
   https://www.google.com/settings/security/lesssecureapps
2. Log on to your Gmail account if necessary. The following screen appears:

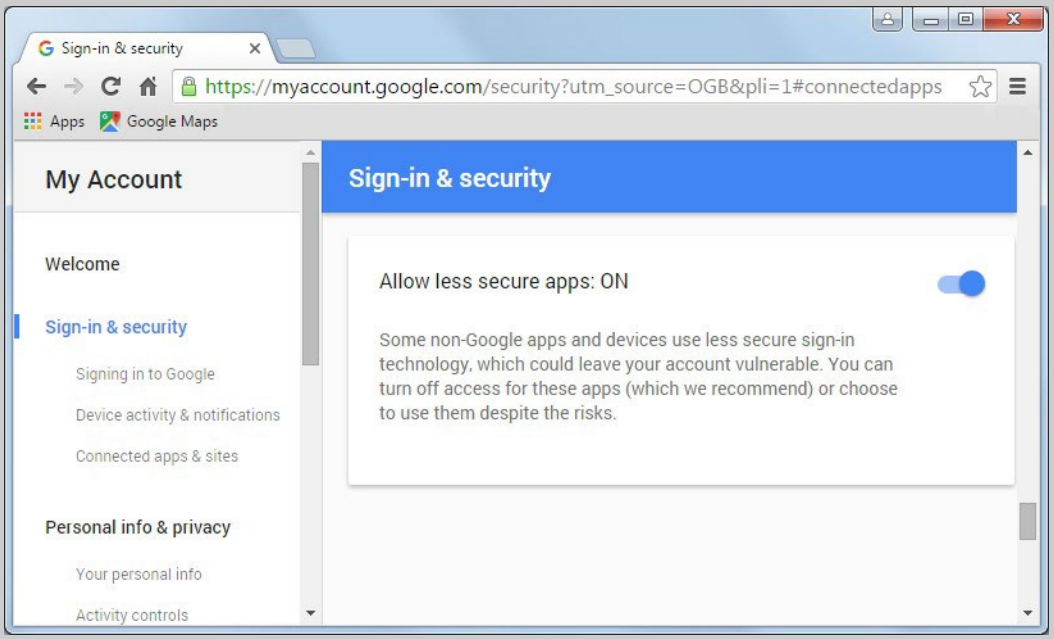


3. Make sure that **Turn on** is selected. The message **Updated** appears when you change the setting.



Note

If the link to the Gmail page does not work, you can log on to your Gmail account in your usual way. Choose **My Account** > **Sign-in & Security** > **Connected apps & sites**. Set **Allow less secure apps** to **ON**.



3.10.3 Creating Mailing Lists

The email address book defines the mailing lists for sending alarm messages. For each trigger (input), or set of triggers, you specify the email addresses of everyone who needs to be informed of the alarm or event.

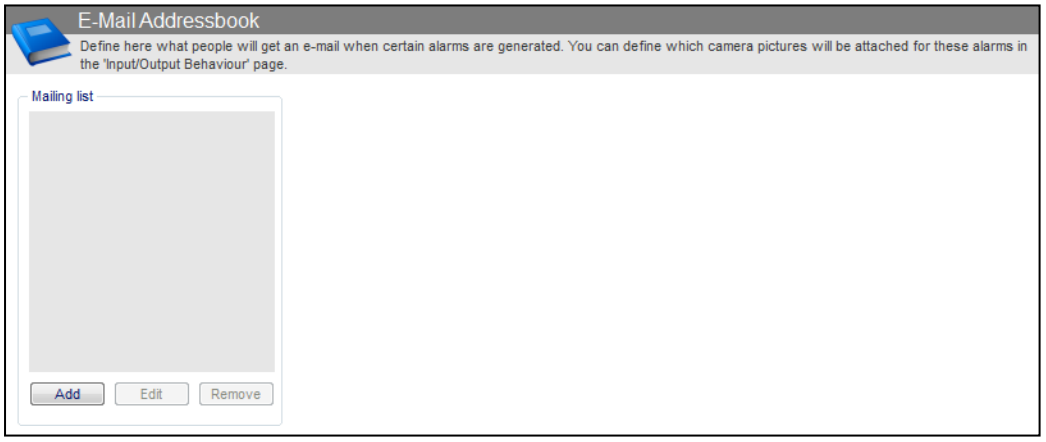
You can indicate that the mailing list is for specific use with iTrace. The emails then have a different layout with a link to the iTrace app.

Caution!

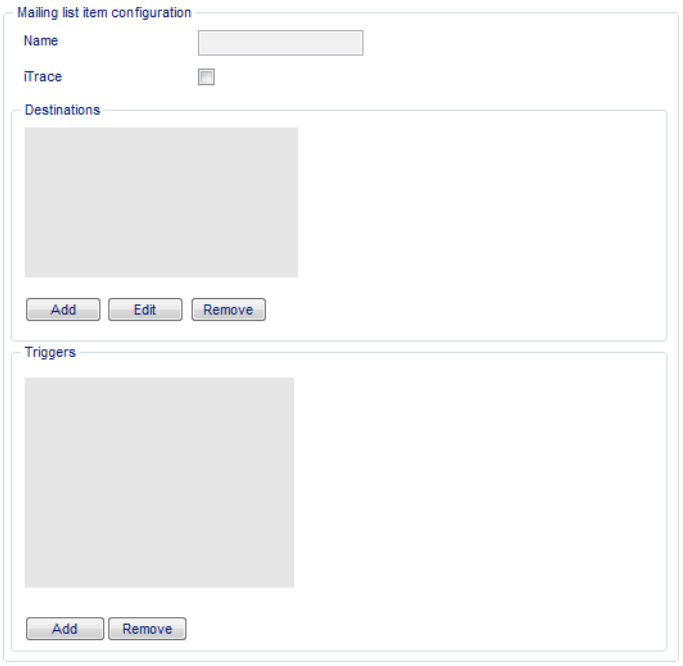
Make sure that you link all the inputs used for emails to alarm profiles with **Email transmission** enabled. For example, you cannot use inputs with alarm profile SILENT MESSAGE, because **Email transmission** is disabled for silent messages. If necessary, create a separate alarm profile. For details, see *Alarm Profiles*.

To create a mailing list, proceed as follows:

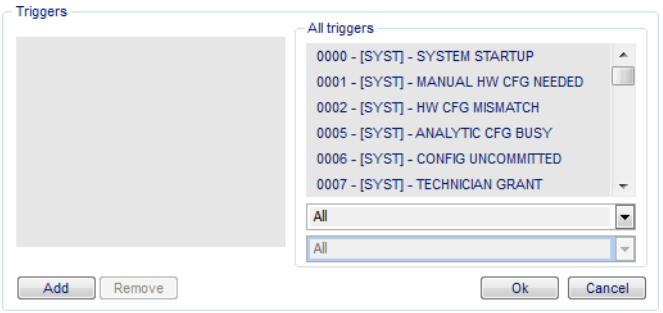
1. Choose **System** > **Behaviour** > **Email Addressbook**.



2. Click **Add**. The following screen appears:

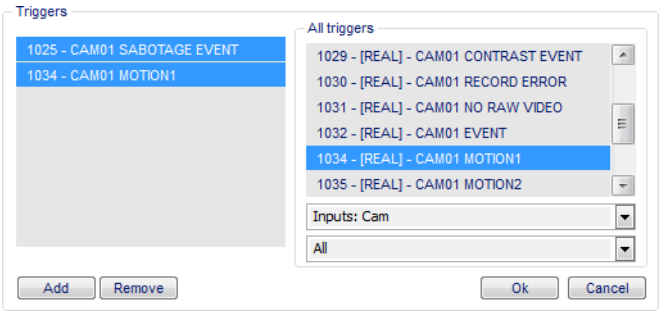


3. In the **Name** box, type a meaningful name for the mailing list.
4. If the mailing list is used with iTrace iCommand, select the **iTrace** checkbox.
   Next, you will add the required destination email addresses.
5. Under **Destinations**, click **Add**.
6. In the **Email address** box that appears, type the email address, and then click **OK**.
7. Repeat for all other required destination addresses.
8. To remove an email address, click on the address, and then click **Remove**.
9. To change an email address, click on the address, and then click **Edit**. Change the email address as required and then click **OK** to confirm.
   Next, you will add the inputs that will trigger the email.
10. Under **Triggers**, click **Add**. The list with all possible triggers appears.



Use the filters below the list to reduce the list. If you filter on camera inputs, you can filter further on camera number.

11. To add a trigger, double-click it in the **All triggers** list. The selected trigger now appears in the **Triggers** list on the left:



12. To remove a trigger from the **Triggers** list, double-click it.
13. Click **OK** to save the triggers.
14. Click **OK** to save the mailing list.
15. Click **Save** to save the email address book.

3.10.4 Verifying Email Communication

From firmware version V2.11, the XO device sends test emails to verify the email communication setup:

- When you save changes to the email setup, the system sends an SMTP server test email to the sender email address. Check if the sender has received the test email.

  If not, revise the email connection settings.

- When you save changes to the email address book, the system sends a trigger test email to the recipients.

  Check if the recipients have received this trigger test email.

  If not, revise the email connection settings and the email address book.

All firmware versions below V2.11 do not send these emails, so you must verify correct operation as mentioned below.

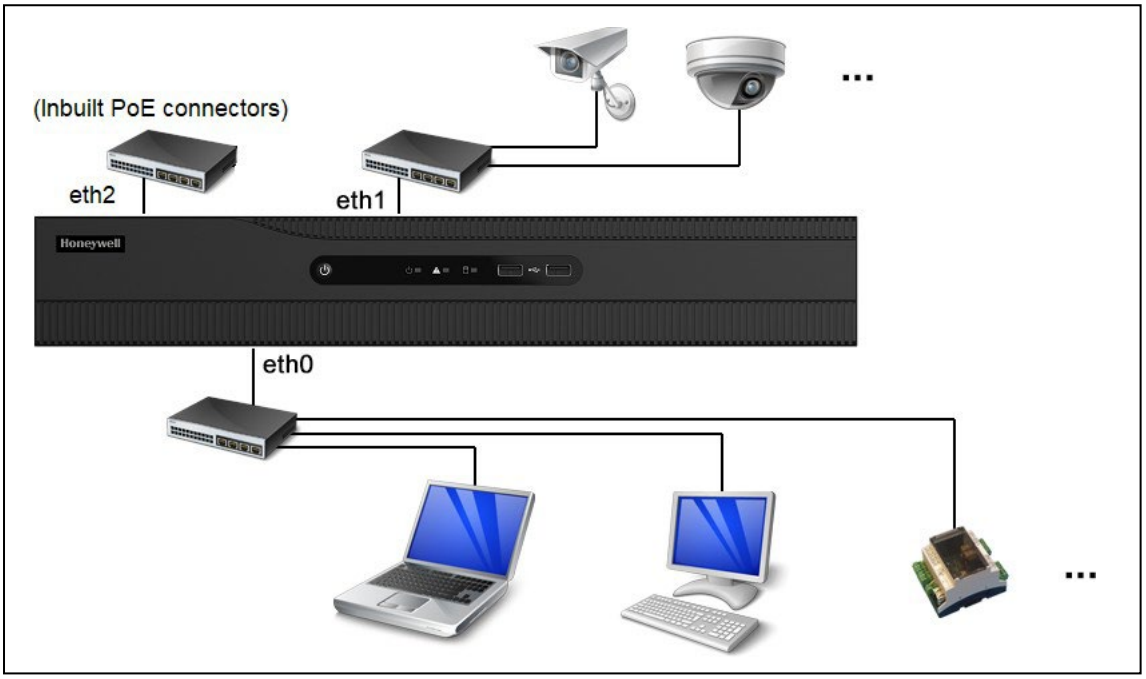
To verify email communication with firmware versions below V2.11, proceed as follows:

1. Select your mailing in the **Mailing list** box, and then click **Edit**.
2. Under **Triggers**, add any event that you can easily trigger (such as connecting to the XO device, or a physical input).
3. Click **OK**, and then click **Save** to save the changes.
4. Trigger the event.
5. Check if the recipients receive a notification email.
   - If not, revise the settings for the email connection and the email address book.
   - If yes, remove the test event from the **Triggers** list.
6. Click **OK** to save the triggers.
7. Click **OK**, and then click **Save**.

3.11 IP Camera Network

3.11.1 General Setup

The IP camera network (eth1) is separate from the local network (eth0) and uses a different IP range. This makes sure that the video streams from the IP cameras do not interfere with alarm transmission on the local network.



Note

It is not possible to have overlapping IP address ranges in eth0 and eth1; these must be separate. The system will check and issue a warning if the IP addresses of eth0 and eth1 are in the same range. The additional Ethernet connector (eth2) provides the physical interface to connect to PoE cameras on the eFT-T4/16P and eFT-T2/8P devices.

ADPRO devices with a PH10LU motherboard have two Ethernet ports on board.

All IP cameras connected to eth1 need an IP address in the same range as eth1. If you need to connect IP cameras in multiple IP address ranges, see *IP Cameras in Multiple Network Segments (Static Routing)* .

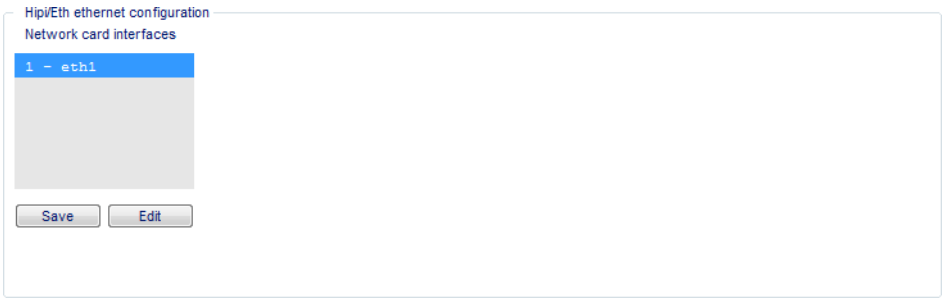
Note

Connect the camera network to eth1 of the XO device, not to eth0. Eth0 is reserved for the XO device network. Transferring video via eth0 may hinder alarm transmission.

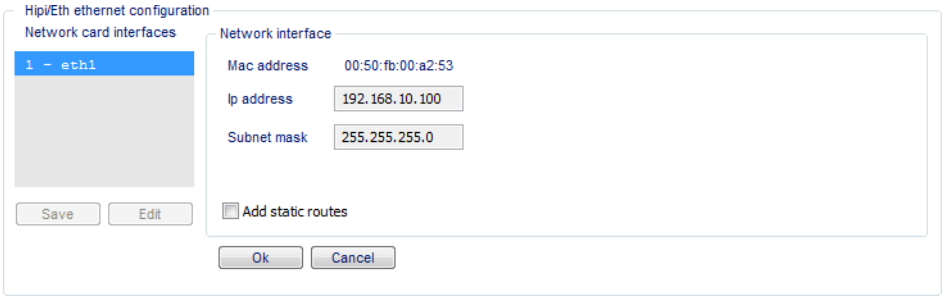
The IP address of your XO device and the IP address of the second Ethernet port have to be in different ranges.

To set up the IP camera network, proceed as follows:

1. Choose **System** > **Maintenance** > **Hipi/Eth config**.



2. Click **eth1**, and then click **Edit**.



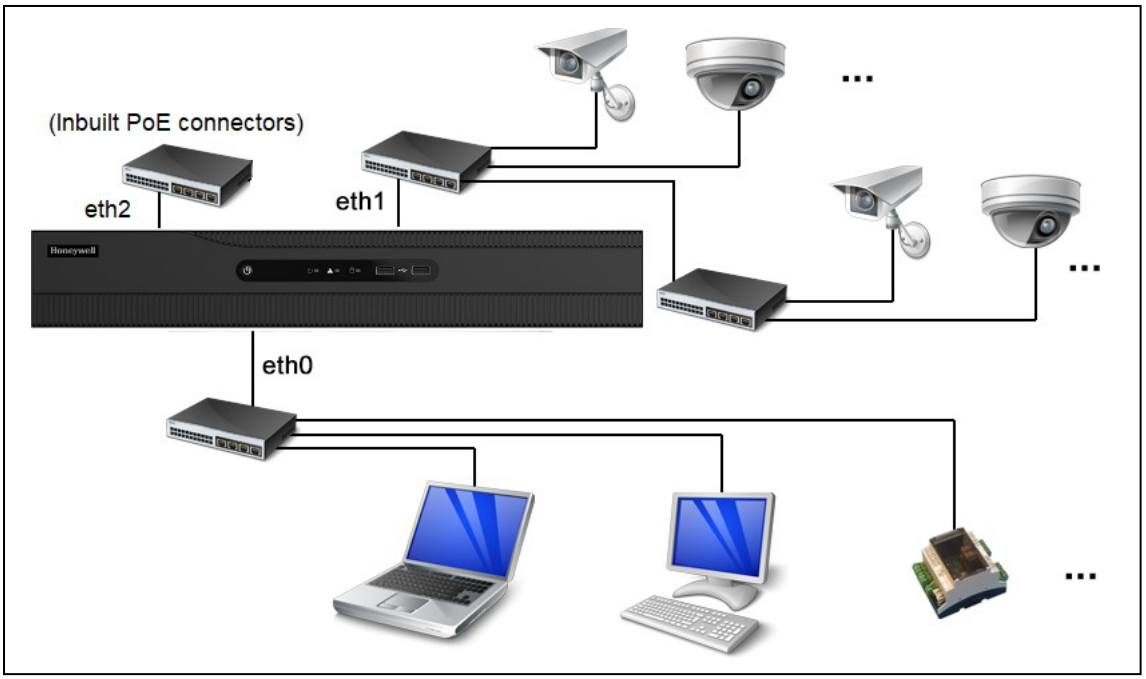
3. Enter the IP address and subnet mask.

> **Note**
>
> To make sure that eth1 is in a different IP range than eth0 (local network), use the same subnet mask for both.

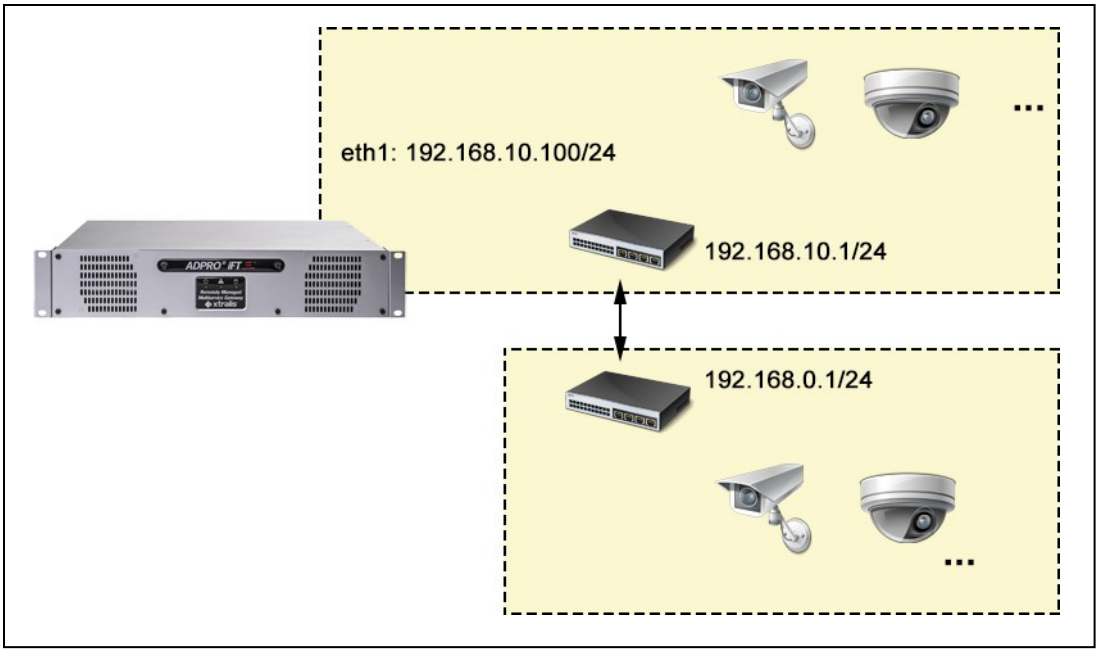
4. Click **OK**.
5. Click **Save**.

3.11.2 IP Cameras in Multiple Network Segments (Static Routing)

All IP cameras connected to eth1 need an IP address in the same range (same network segment). However, in larger buildings it may happen that the IP cameras are on multiple network segments using multiple IP address ranges. You can use **static routes** to extend the eth1 camera network to these other network segments.



In the example below, there are two IP camera networks. The route between the two networks runs via the gateways 192.168.10.1 (in the eth1 network) and 192.168.0.1 (in the second network).



To set up the static route to a second network in the XO client, you need:

- The IP address of the gateway in the eth1 network.

  Tip: by convention, gateway IP addresses usually end in '.1'. If eth1 is 192.168.10.100, then the gateway would be 192.168.10.1. Always check with the network administrator.

- The network identifier of the second network, in xxx.xxx.xxx.xxx format.
- The subnet mask of the second network, in xxx.xxx.xxx.xxx format. Ask the network administrator to provide the required information.

Note

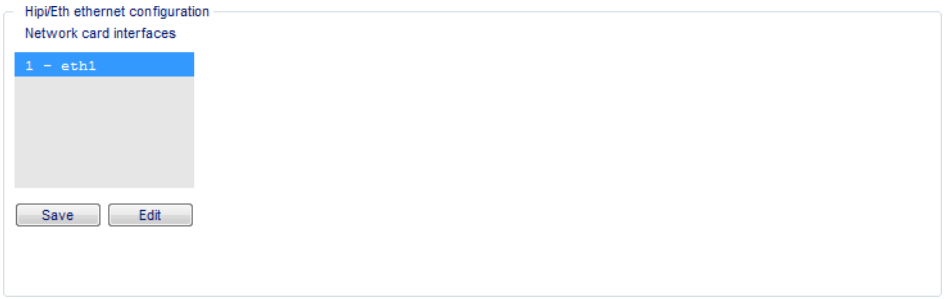
If the network administrator provides the information in a different format, or if you only get a range of IP addresses for the cameras in the second network, you can calculate the required values yourself. For details, see *Networks, Subnet Masks, and IP Addresses*.

Changing the static routes requires a system restart.

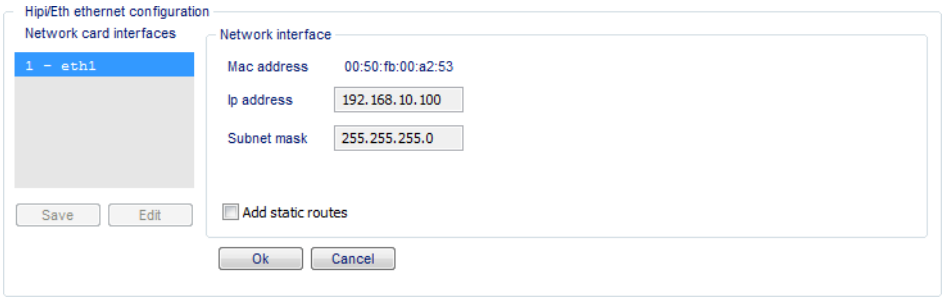
3.11.2.1 Adding Static Routes

To add static routes for the IP camera network, proceed as follows:

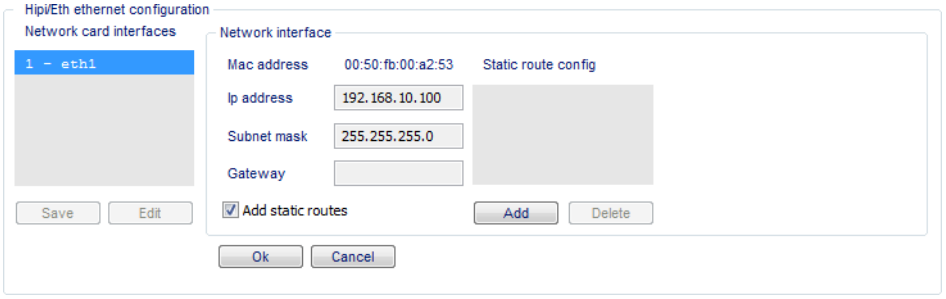
1. Choose **System** > **Maintenance** > **Hipi/Eth config**.



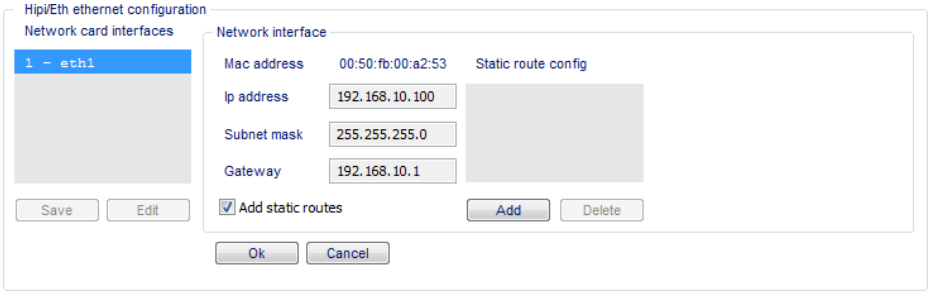
2. Click **eth1**, and then click **Edit**.



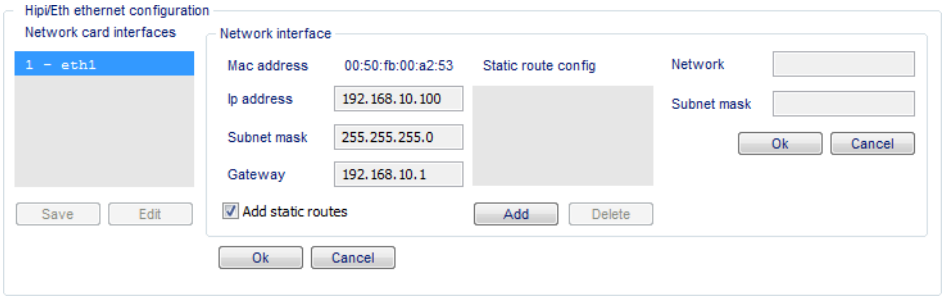
3. Select the **Add static routes** checkbox.



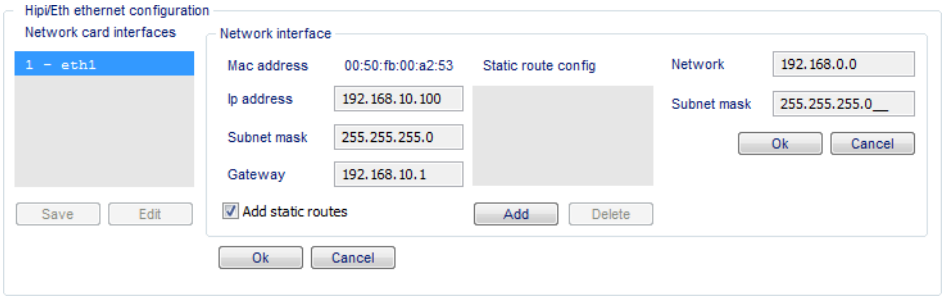
4. In the **Gateway** box, fill in the gateway for the eth1 camera network.



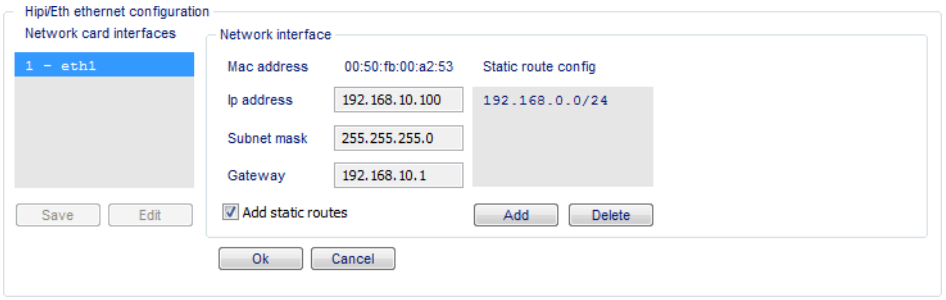
5. Click **Add**.



6. In the **Network** box, type the network address of the network segment that you want to add.
7. In the **Subnet mask** box, type the subnet mask of the network segment that you want to add.

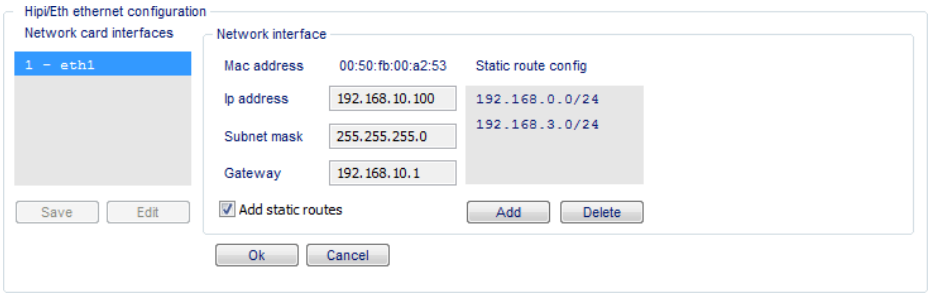


8. Click **OK**.

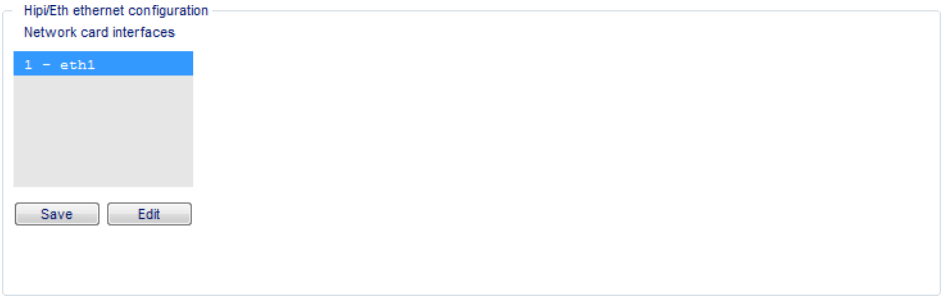


The added network appears in the **Static route config** box. The subnet mask is converted to CIDR notation (/24 in the example).

9. If necessary, repeat steps 5 to 8 to add more static routes.



10. Click **OK**.

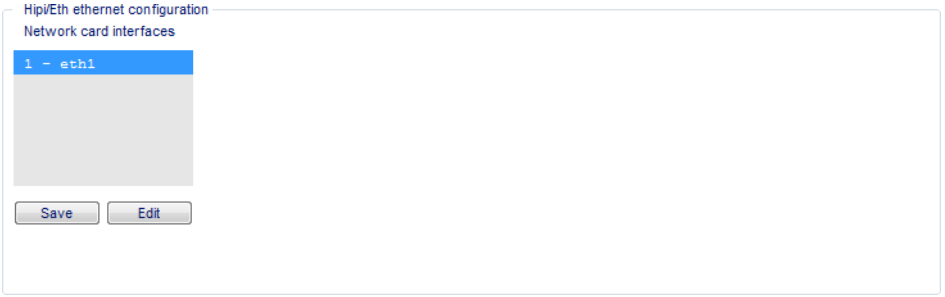


11. Click **Save**.

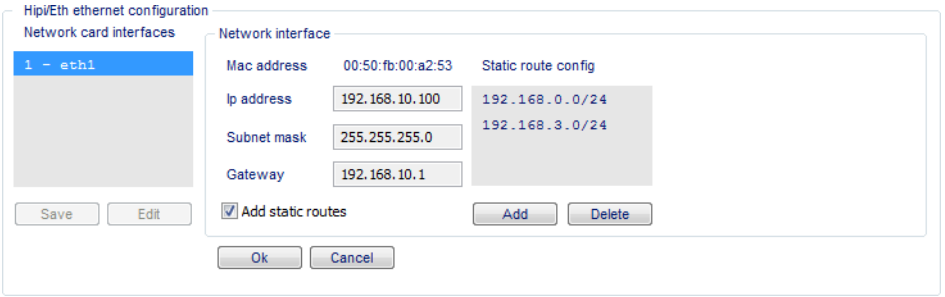
3.11.2.2 Removing Static Routes

To remove static routes for the IP camera network, proceed as follows:

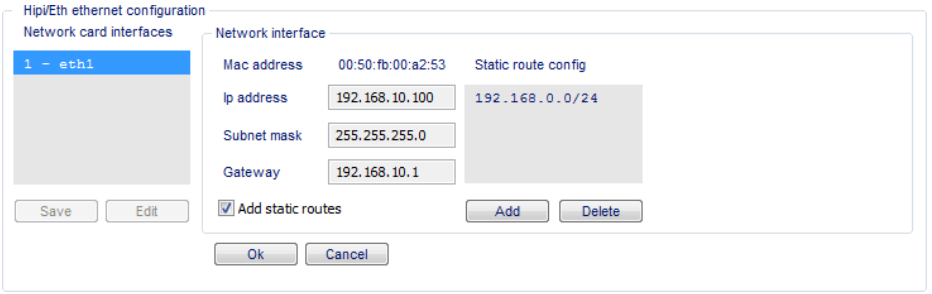
1. Choose **System** > **Maintenance** > **Hipi/Eth config**.



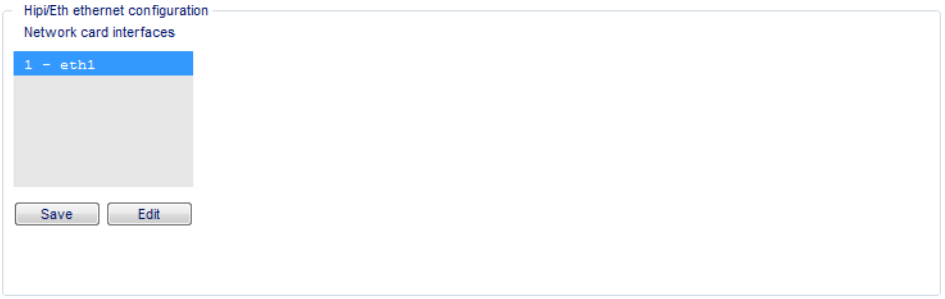
2. Click **eth1**, and then click **Edit**.



3. In the **Static route config** box, click the route that you want to remove, and then click **Delete**. The system removes the selected static route.



4. Click **OK**.



5. Click **Save**.

3.12 I/O Cards (MIO and EIO)

3.12.1 Configuring the I/O Cards

Note

If you are using XO I/O Interface USB modules with external I/O cards, make sure that you have performed the hardware mapping using the hardware configuration tool before configuring the cards in the XO client. For more information, see the *XO I/O Interface USB Module – Technical Manual* (32688).

The Main I/O (MIO) and Extension I/O (EIO) cards are internal (built into the ADPRO device) or external (XO I/O Interface USB module) I/O cards. They are also called OTB (on-the-box) cards. The MIO and EIO cards offer:

- Per MIO card: 8 tamper-protected inputs and 4 relay outputs.
- Per EIO card: 12 tamper-protected inputs and 4 relay outputs.

The XO Gateway I/O USB Module constitutes a single module connected to USB with 4 monitored Inputs/4 Relay outputs and a RS485 connection (contrary to the XO I/O Interface USB Modules there is NO VM22E interface).

XO Gateway I/O USB Module is primarily designed for iFT Gateway, but it can be added to any other XO device that does not already have 2 MIO cards via the hardware configuration page.

Perform the hardware mapping if you are using the XO Gateway IO USB module. For more information, see the *XO Gateway IO USB Module - Technical Manual* (<TBD>)

For correct operation, you have to indicate if the **inputs** are normally open (NO) or normally closed (NC), and if they are configured as NEOL, SEOL, or DEOL.

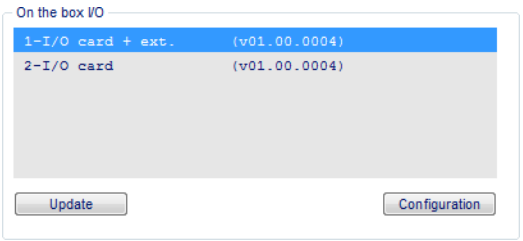
Furthermore, you can configure the **outputs** to operate in failsafe and/or watchdog mode:

- **Failsafe** mode means that the relay is activated during idle state, and drops when the output is driven. The advantage is that failsafe outputs drop to ‘alarm state’ when the power supply is cut.
- **Watchdog** mode means that the output is activated, after a certain timeout, when the system cannot reach the I/O card. This situation can occur when the system hangs. You can let the system automatically restart the motherboard to clear the situation.

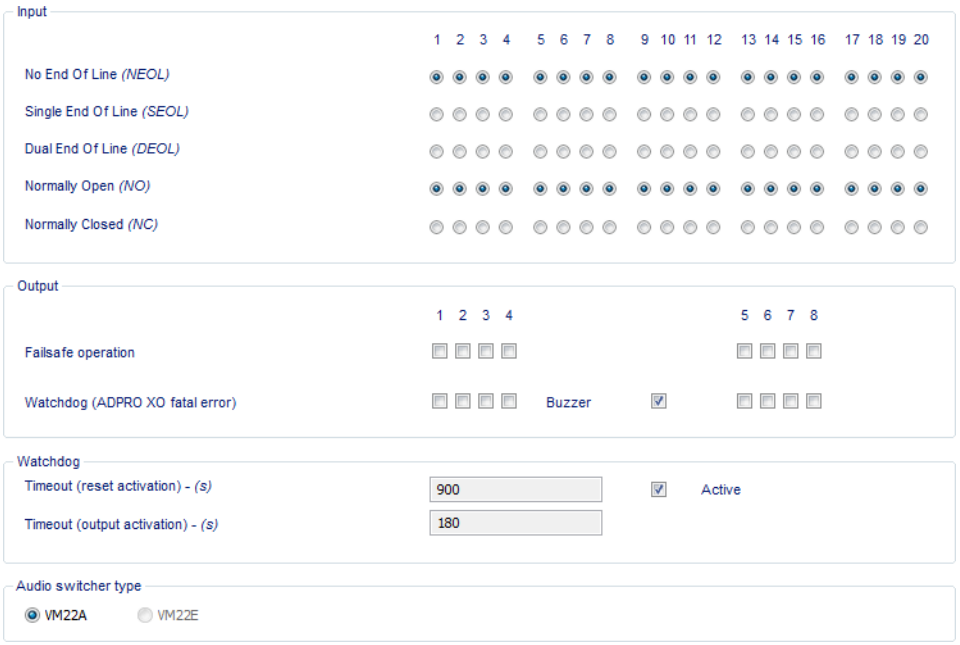
Finally, if you are using audio switchers (VM22A or VM22E), you have to indicate which type, so that the MIO card sends the correct signals to the switchers. The VM22A is only compatible with built-in MIO cards.

To configure the inputs and outputs of the MIO/EIO cards, proceed as follows:

1. Choose **System** > **Connections** > **I/O**. The screen shows the available I/O card sets. The example screen below shows a system with a first set of MIO+EIO card (**1–I/O card + ext.**) and a second MIO card (**2–I/O card**).



2. Click the desired I/O card set in the list, and then click **Configuration**. The following screen appears:



3. Provide the following information:

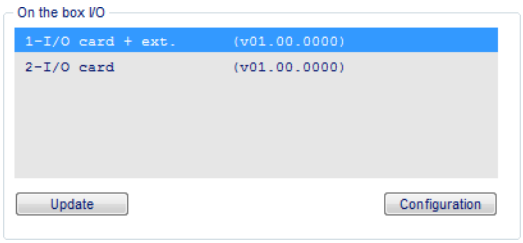
Item	Description
Input: Inputs 1–8 are the inputs on the MIO card, inputs 9–20 are the inputs on the EIO card.	
No End of Line (NEOL)	Select this option if the input is configured as NEOL.
Single End of Line (SEOL)	Select this option if the input is configured as SEOL.
Dual End of Line (DEOL)	Select this option if the input is configured as DEOL.
Normally Open (NO)	Select this option if the input is normally open.
Normally Closed (NC)	Select this option if the input is normally closed.
Output: Outputs 1–4 are the outputs on the MIO card, outputs 5–8 are the outputs on the EIO card.	
Failsafe operation	Select this checkbox for each output that has to operate in failsafe mode.
Watchdog	Select this checkbox for each output that has to operate in watchdog mode.
Buzzer	Select this checkbox if you want the buzzer to sound during a watchdog alarm.

Item	Description
Watchdog: specify the timeouts for the watchdog mode.	
Timeout (reset activation)	Type the timeout in seconds (181–1799) after which the system has to restart the motherboard.
Active	Clear this checkbox if you do not want to restart the motherboard automatically.
Timeout (output activation)	Type the timeout in seconds (61–599) after which the system has to activate the watchdog outputs and the buzzer.
Audio switcher type: if you are using an audio switcher for audio output, select the correct type.	
VM22A	Click this if you are using a VM22A audio switcher (only compatible with built-in MIO cards).
VM22E	Select this if you are using a VM22E audio switcher.

4. Click **OK**.
5. Click **Save**.

3.12.2 Updating the MIO Card Firmware

The list of installed I/O card sets displays the firmware version of the MIO card (v01.00.0000 in the example below).

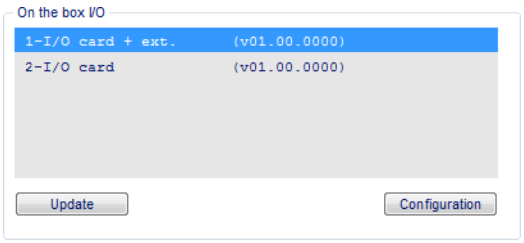


Note

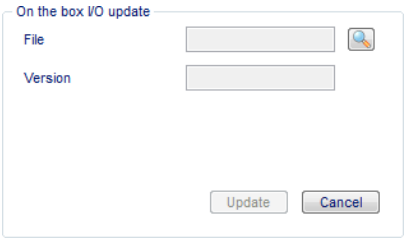
- For updating the MIO card firmware, you need **client version** XOa 3.00 or above. Older client versions are not suitable, even for FastTrace 2 Series devices with a **firmware version** below XOa 3.00.
- For using the VM22E audio switcher, Honeywell recommends minimum firmware version v01.00.0004 for the MIO card.
- Version v01.00.0002 of the MIO card is not compatible with FastTrace 2 Series devices that run firmware versions below XOa 3.00 (v2.11 and below).

To update the MIO card firmware, proceed as follows:

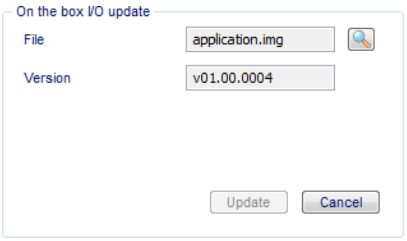
1. Choose **System** > **Connections** > **I/O**.



2. Click **Update**. The following section appears:



3. Click the  button and browse to the .img file with the latest firmware version.
4. Click **Open**. The **Version** box displays the firmware version that you will upload.



5. Click **Update**. The device beeps while the system installs the new firmware (about 5 seconds).
6. When finished, click **Cancel** to close the update box.
7. If you have a second MIO card, select the second card set in the **On the box I/O** list, and update its firmware in the same way.

3.12.3 MIO and EIO Cards Inputs/Outputs

The tables below list all the inputs and outputs in the XO client related to the MIO and EIO cards.

3.12.3.1 MIO and EIO Set 1

Real inputs:

MIO + EIO card, set 1		
Input (real)	**Default name**	**Description**
MIO card 1		
I2560	USBIO-1 PRESENCE FLT	I/O card absent
I2576	USBIO-1 INPUT01	Real alarm on input 1
I2577	USBIO-1 INPUT02	Real alarm on input 2
I2578	USBIO-1 INPUT03	Real alarm on input 3
I2579	USBIO-1 INPUT04	Real alarm on input 4
I2580	USBIO-1 INPUT05	Real alarm on input 5
I2581	USBIO-1 INPUT06	Real alarm on input 6
I2582	USBIO-1 INPUT07	Real alarm on input 7
I2583	USBIO-1 INPUT08	Real alarm on input 8
EIO card 1		
I2584	USBIO-1 INPUT09	Real alarm on input 9
I2585	USBIO-1 INPUT10	Real alarm on input 10
I2586	USBIO-1 INPUT11	Real alarm on input 11
I2587	USBIO-1 INPUT12	Real alarm on input 12

MIO + EIO card, set 1		
Input (real)	**Default name**	**Description**
I2588	USBIO-1 INPUT13	Real alarm on input 13
I2589	USBIO-1 INPUT14	Real alarm on input 14
I2590	USBIO-1 INPUT15	Real alarm on input 15
I2591	USBIO-1 INPUT16	Real alarm on input 16
I2592	USBIO-1 INPUT17	Real alarm on input 17
I2593	USBIO-1 INPUT18	Real alarm on input 18
I2594	USBIO-1 INPUT19	Real alarm on input 19
I2595	USBIO-1 INPUT20	Real alarm on input 20

Tamper inputs:

MIO + EIO card, set 1		
Input (tamper)	**Default name**	**Description**
MIO card 1		
I2596	USBIO-1 INPUT01	Tamper alarm on input 1
I2597	USBIO-1 INPUT02	Tamper alarm on input 2
I2598	USBIO-1 INPUT03	Tamper alarm on input 3
I2599	USBIO-1 INPUT04	Tamper alarm on input 4
I2600	USBIO-1 INPUT05	Tamper alarm on input 5
I2601	USBIO-1 INPUT06	Tamper alarm on input 6
I2602	USBIO-1 INPUT07	Tamper alarm on input 7
I2603	USBIO-1 INPUT08	Tamper alarm on input 8
EIO card 1		
I2604	USBIO-1 INPUT09	Tamper alarm on input 9
I2605	USBIO-1 INPUT10	Tamper alarm on input 10
I2606	USBIO-1 INPUT11	Tamper alarm on input 11
I2607	USBIO-1 INPUT12	Tamper alarm on input 12
I2608	USBIO-1 INPUT13	Tamper alarm on input 13
I2609	USBIO-1 INPUT14	Tamper alarm on input 14
I2610	USBIO-1 INPUT15	Tamper alarm on input 15
I2611	USBIO-1 INPUT16	Tamper alarm on input 16
I2612	USBIO-1 INPUT17	Tamper alarm on input 17
I2613	USBIO-1 INPUT18	Tamper alarm on input 18
I2614	USBIO-1 INPUT19	Tamper alarm on input 19
I2615	USBIO-1 INPUT20	Tamper alarm on input 20

Outputs:

MIO + EIO card, set 1		
Output	**Default name**	**Description**
MIO card 1		
C2560	USBIO-1 GREEN LED	Status of green LED (power)

MIO + EIO card, set 1		
Output	**Default name**	**Description**
C2561	USBIO-1 YELLOW LED	Status of yellow LED (fault)
C2562	USBIO-1 DISC LED	Status of disk LED (recording)
C2563	USBIO-1 BUZZER	Status of buzzer
C2576	USBIO-1 OUTPUT01	Status of output 1
C2577	USBIO-1 OUTPUT02	Status of output 2
C2578	USBIO-1 OUTPUT03	Status of output 3
C2579	USBIO-1 OUTPUT04	Status of output 4
EIO card 1		
C2580	USBIO-1 OUTPUT05	Status of output 5
C2581	USBIO-1 OUTPUT06	Status of output 6
C2582	USBIO-1 OUTPUT07	Status of output 7
C2583	USBIO-1 OUTPUT08	Status of output 8

3.12.3.2 MIO and EIO Set 2

Real inputs:

MIO + EIO card, set 2		
Input (real)	**Default name**	**Description**
MIO card 2		
I2624	USBIO-2 PRESENCE FLT	I/O card absent
I2640	USBIO-2 INPUT01	Real alarm on input 1
I2641	USBIO-2 INPUT02	Real alarm on input 2
I2642	USBIO-2 INPUT03	Real alarm on input 3
I2643	USBIO-2 INPUT04	Real alarm on input 4
I2644	USBIO-2 INPUT05	Real alarm on input 5
I2645	USBIO-2 INPUT06	Real alarm on input 6
I2646	USBIO-2 INPUT07	Real alarm on input 7
I2647	USBIO-2 INPUT08	Real alarm on input 8
EIO card 2		
I2648	USBIO-2 INPUT09	Real alarm on input 9
I2649	USBIO-2 INPUT10	Real alarm on input 10
I2650	USBIO-2 INPUT11	Real alarm on input 11
I2651	USBIO-2 INPUT12	Real alarm on input 12
I2652	USBIO-2 INPUT13	Real alarm on input 13
I2653	USBIO-2 INPUT14	Real alarm on input 14
I2654	USBIO-2 INPUT15	Real alarm on input 15
I2655	USBIO-2 INPUT16	Real alarm on input 16
I2656	USBIO-2 INPUT17	Real alarm on input 17
I2657	USBIO-2 INPUT18	Real alarm on input 18
I2658	USBIO-2 INPUT19	Real alarm on input 19
I2659	USBIO-2 INPUT20	Real alarm on input 20

Tamper inputs:

MIO + EIO card, set 2		
Input (tamper)	**Default name**	**Description**
MIO card 2		
I2660	USBIO-2 INPUT01	Tamper alarm on input 1
I2661	USBIO-2 INPUT02	Tamper alarm on input 2
I2662	USBIO-2 INPUT03	Tamper alarm on input 3
I2663	USBIO-2 INPUT04	Tamper alarm on input 4
I2664	USBIO-2 INPUT05	Tamper alarm on input 5
I2665	USBIO-2 INPUT06	Tamper alarm on input 6
I2666	USBIO-2 INPUT07	Tamper alarm on input 7
I2667	USBIO-2 INPUT08	Tamper alarm on input 8
EIO card 2		
I2668	USBIO-2 INPUT09	Tamper alarm on input 9
I2669	USBIO-2 INPUT10	Tamper alarm on input 10
I2670	USBIO-2 INPUT11	Tamper alarm on input 11
I2671	USBIO-2 INPUT12	Tamper alarm on input 12
I2672	USBIO-2 INPUT13	Tamper alarm on input 13
I2673	USBIO-2 INPUT14	Tamper alarm on input 14
I2674	USBIO-2 INPUT15	Tamper alarm on input 15
I2675	USBIO-2 INPUT16	Tamper alarm on input 16
I2676	USBIO-2 INPUT17	Tamper alarm on input 17
I2677	USBIO-2 INPUT18	Tamper alarm on input 18
I2678	USBIO-2 INPUT19	Tamper alarm on input 19
I2679	USBIO-2 INPUT20	Tamper alarm on input 20

Outputs:

MIO + EIO card, set 2		
Output	**Default name**	**Description**
MIO card 2		
C2624	USBIO-2 GREEN LED	Status of green LED (power)[1]
C2625	USBIO-2 YELLOW LED	Status of yellow LED (fault)[1]
C2626	USBIO-2 DISC LED	Status of disk LED (recording)[1]
C2627	USBIO-2 BUZZER	Status of buzzer[1]
C2640	USBIO-2 OUTPUT01	Status of output 1
C2641	USBIO-2 OUTPUT02	Status of output 2
C2642	USBIO-2 OUTPUT03	Status of output 3
C2643	USBIO-2 OUTPUT04	Status of output 4
EIO card 2		
C2644	USBIO-2 OUTPUT05	Status of output 5

[1] Front LED indicators and buzzer are always controlled by the MIO card in set 1.

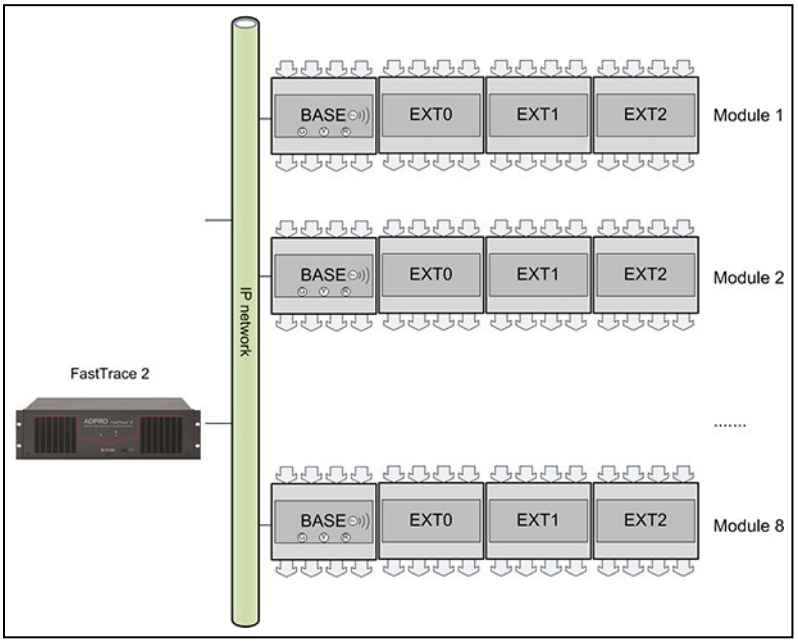
MIO + EIO card, set 2		
Output	**Default name**	**Description**
C2645	USBIO-2 OUTPUT06	Status of output 6
C2646	USBIO-2 OUTPUT07	Status of output 7
C2647	USBIO-2 OUTPUT08	Status of output 8

3.13 Network I/O Units (Net I/O)

3.13.1 About Network I/O Units

The Network (Net) I/O units offer extra inputs and outputs for your XO device via the local network. You can link up to 8 units to your XO device, each with 4 inputs and 4 outputs. You can expand each unit with up to 3 extension units, each with 4 inputs and 4 outputs. That allows for a total of 128 inputs and 128 outputs. Net I/O units also have LED indicators and a buzzer, controlled by the XO device.

The image below shows a configuration with a FastTrace 2 Series device. Setup is identical for iFT Series devices.



For the physical connection of the Net I/O units, assigning IP addresses… see the *ADPRO Network I/O Units Technical Manual* (33355).

You can add the Net I/O units to the XO client software, as follows:

- Manually, if you know the IP address of the Net I/O unit.
- Using the search function, which discovers all available Net I/O units on the local network (eth0). If you add a base unit, the system automatically adds the extension units too.

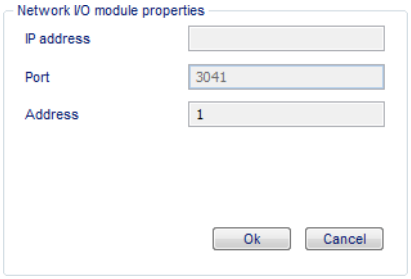
3.13.2 Adding a Net I/O Unit with Known IP Address

To add a Net I/O unit with a known IP address, proceed as follows:

1. Choose **System** > **Connections** > **I/O**. For Net I/O units, you will work in the **Network I/O** section:



2. Click **Add**. The following section appears:



3. Provide the following information:

Item	Description
IP address	Type the IP address of the Net I/O unit.
Port	This box contains the port number (the port to which the Net I/O unit is listening). The port number is fixed, you cannot change it.
Address	Type the sequence number of the Net I/O unit (1–8).

4. Click **OK**.
5. Click **Save**.

3.13.3 Searching Net I/O Units on the Local Network

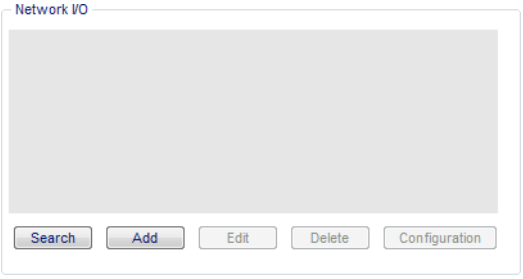
If you use the search function to add Net I/O units, the system will automatically fill in their IP address and sequence number (address). You can always change the sequence number afterwards.

Caution!

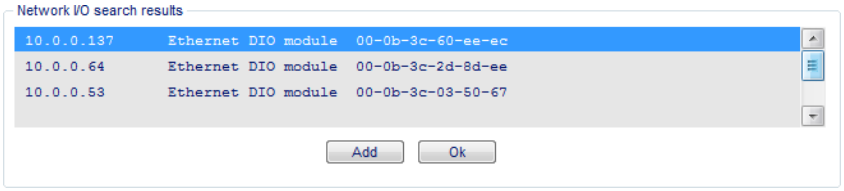
The search function scans only the local network (eth0). If you have Net I/O units on other networks (for example eth1), behind routers, or behind switches that block UDP, the search function will not discover these units.

To search for Net I/O units on the local network, proceed as follows:

1. Choose **System** > **Connections** > **I/O**. For Net I/O units, you will work in the **Network I/O** section:



2. Click **Search**. The system starts searching for Net I/O units on the local network and displays the found Net I/O units in the search results box.



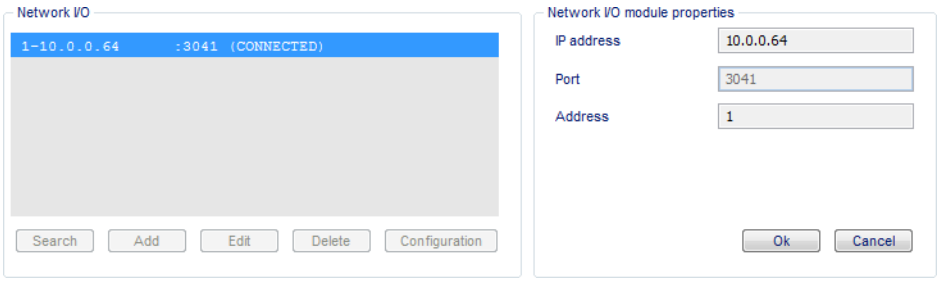
3. Select the desired Net I/O unit in the list and click **Add**. The selected Net I/O unit now appears in the **Network I/O** list.
4. Repeat for other Net I/O units that you want to add.
5. Click **OK** to close the search results box.
6. Click **Save**.

The system automatically fills in the address (sequence number 1–8) of the added Net I/O units.

3.13.4 Modifying the Settings of a Net I/O Unit

To modify the Net I/O unit settings, proceed as follows:

1. Choose **System** > **Connections** > **I/O**.
2. Click the desired Net I/O unit in the list, and then click **Edit**.



3. Provide the correct IP address and address (sequence number 1–8) as required.
4. Click **OK**, and then click **Save**.

3.13.5 Deleting a Net I/O Unit

To delete a Net I/O unit, proceed as follows:

1. Choose **System** > **Connections** > **I/O**.
2. Click the desired Net I/O unit in the list, and then click **Delete**.
3. Click **Save**.

3.13.6 Net I/O Unit Inputs and Outputs Setup

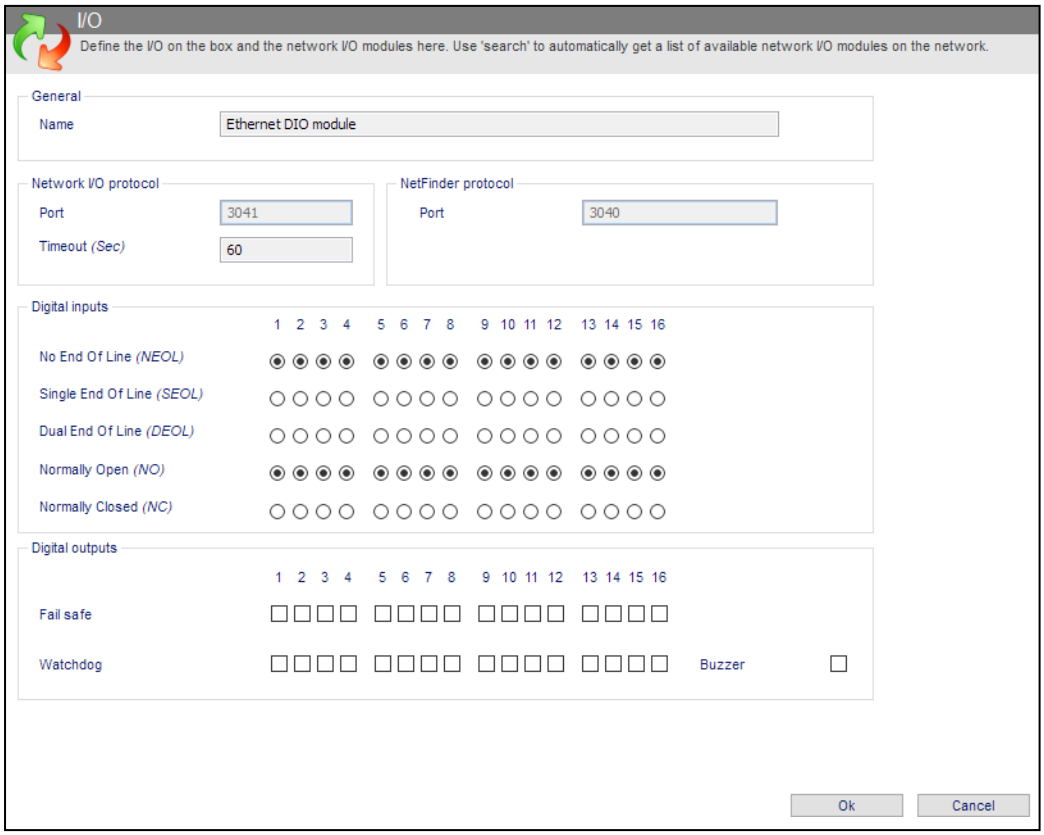
For correct operation, you have to indicate if the **inputs** are normally open (NO) or normally closed (NC), and if they are configured as NEOL, SEOL, or DEOL (SEOL and DEOL only with monitored inputs on V2 Net I/O units; for details see the *ADPRO Network I/O Units Technical Manual* (33355)).

Furthermore, you can configure the **outputs** to operate in failsafe and/or watchdog mode:

- **Failsafe** mode means that the relay is activated during idle state, and drops when the output is driven. The advantage is that failsafe outputs drop to 'alarm state' when the power supply is cut.
- **Watchdog** mode means that the output is activated, after a certain timeout, if the base unit detects that the XO device is not present. In this case, you can let the buzzer on the base unit sound.

To set up the inputs and outputs of a Net I/O unit, proceed as follows:

1. Choose **System** > **Connections** > **I/O**.
2. Click the desired unit in the **Network I/O** box, and then click **Configuration**.



Note

The configuration screen always shows 16 inputs and outputs (base unit + 3 extension units), even if there are no physical extension units attached.

3. Provide the following information:

Item	Description
General	
Name	Type a name (max. 20 characters) to describe the Net I/O unit. Use a description that is meaningful and relevant.

Item	Description
Network I/O protocol	
Port	This box displays the port number (i.e. the port to which the Net I/O unit is listening). The port number is fixed, you cannot change it.
Timeout (sec)	Enter the communication timeout, in seconds (1–1199).
NetFinder protocol	
Port	This box displays the port number for the NetFinder tool. NetFinder is an external tool for programming the Net I/O unit's IP address and for updating its software. The port number is fixed; you cannot change it.
Digital inputs (1–16)	
No End of Line (NEOL)	Select this option if the input is configured as NEOL (default). For legacy Net I/O units (unmonitored inputs), always use this setting.
Single End of Line (SEOL)	Select this option if the input is configured as SEOL (monitored inputs only).
Dual End of Line (DEOL)	Select this option if the input is configured as DEOL (monitored inputs only).
Normally Open (NO)	Select this option if the input is normally open (default).
Normally Closed (NC)	Select this option if the input is normally closed.
Digital outputs (1–16)	
Fail safe	Select this checkbox for each output that has to operate in failsafe mode.
Watchdog	Select this checkbox for each output that has to operate in watchdog mode.
Buzzer	Select this checkbox if you want the buzzer on the base unit to sound during a watchdog alarm.

4. Click **OK**, and then click **Save**.

3.13.7 Net I/O Unit Inputs and Outputs

3.13.7.1 Inputs

The Net I/O units return fault conditions for power fault (POE LOSS) and unit not present (PRESENCE FLT).

Unit address								Default name
1	2	3	4	5	6	7	8	
I2050	I2114	I2178	I2242	I2306	I2370	I2434	I2498	NETIO-X POE LOSS
I2051	I2115	I2179	I2243	I2307	I2371	I2435	I2499	NETIO-X PRESENCE FLT

(X = unit number 1–8)

The tables below provide overviews of the real and tamper inputs on the base units and extension units.

Real inputs:

Input	Unit address								Default name
	1	2	3	4	5	6	7	8	
Base unit									
1	I2080	I2144	I2208	I2272	I2336	I2400	I2464	I2528	NETIO-X INPUT01 REAL
2	I2081	I2145	I2209	I2273	I2337	I2401	I2465	I2529	NETIO-X INPUT02 REAL
3	I2082	I2146	I2210	I2274	I2338	I2402	I2466	I2530	NETIO-X INPUT03 REAL
4	I2083	I2147	I2211	I2275	I2339	I2403	I2467	I2531	NETIO-X INPUT04 REAL
Extension unit 0									
1	I2084	I2148	I2212	I2276	I2340	I2404	I2468	I2532	NETIO-X INPUT05 REAL
2	I2085	I2149	I2213	I2277	I2341	I2405	I2469	I2533	NETIO-X INPUT06 REAL
3	I2086	I2150	I2214	I2278	I2342	I2406	I2470	I2534	NETIO-X INPUT07 REAL
4	I2087	I2151	I2215	I2279	I2343	I2407	I2471	I2535	NETIO-X INPUT08 REAL
Extension unit 1									
1	I2088	I2152	I2216	I2280	I2344	I2408	I2472	I2536	NETIO-X INPUT09 REAL
2	I2089	I2153	I2217	I2281	I2345	I2409	I2473	I2537	NETIO-X INPUT10 REAL
3	I2090	I2154	I2218	I2282	I2346	I2410	I2474	I2538	NETIO-X INPUT11 REAL
4	I2091	I2155	I2219	I2283	I2347	I2411	I2475	I2539	NETIO-X INPUT12 REAL
Extension unit 2									
1	I2092	I2156	I2220	I2284	I2348	I2412	I2476	I2540	NETIO-X INPUT13 REAL
2	I2093	I2157	I2221	I2285	I2349	I2413	I2477	I2541	NETIO-X INPUT14 REAL
3	I2094	I2158	I2222	I2286	I2350	I2414	I2478	I2542	NETIO-X INPUT15 REAL
4	I2095	I2159	I2223	I2287	I2351	I2415	I2479	I2543	NETIO-X INPUT16 REAL

(X = unit number 1–8)

Tamper inputs (available with monitored inputs only):

Input	Unit address								Default name
	1	2	3	4	5	6	7	8	
Base unit									
1	I2096	I2160	I2224	I2288	I2352	I2416	I2480	I2544	NETIO-X INPUT01 TAMPER
2	I2097	I2161	I2225	I2289	I2353	I2417	I2481	I2545	NETIO-X INPUT02 TAMPER
3	I2098	I2162	I2226	I2290	I2354	I2418	I2482	I2546	NETIO-X INPUT03 TAMPER
4	I2099	I2163	I2227	I2291	I2355	I2419	I2483	I2547	NETIO-X INPUT04 TAMPER
Extension unit 0									
1	I2100	I2164	I2228	I2292	I2356	I2420	I2484	I2548	NETIO-X INPUT05 TAMPER
2	I2101	I2165	I2229	I2293	I2357	I2421	I2485	I2549	NETIO-X INPUT06 TAMPER
3	I2102	I2166	I2230	I2294	I2358	I2422	I2486	I2550	NETIO-X INPUT07 TAMPER
4	I2103	I2167	I2231	I2295	I2359	I2423	I2487	I2551	NETIO-X INPUT08 TAMPER

Input	Unit address								Default name
	1	2	3	4	5	6	7	8	
Extension unit 1									
1	I2104	I2168	I2232	I2296	I2360	I2424	I2488	I2552	NETIO-X INPUT09 TAMPER
2	I2105	I2169	I2233	I2297	I2361	I2425	I2489	I2553	NETIO-X INPUT10 TAMPER
3	I2106	I2170	I2234	I2298	I2362	I2426	I2490	I2554	NETIO-X INPUT11 TAMPER
4	I2107	I2171	I2235	I2299	I2363	I2427	I2491	I2555	NETIO-X INPUT12 TAMPER
Extension unit 2									
1	I2108	I2172	I2236	I2300	I2364	I2428	I2492	I2556	NETIO-X INPUT13 TAMPER
2	I2109	I2173	I2237	I2301	I2365	I2429	I2493	I2557	NETIO-X INPUT14 TAMPER
3	I2110	I2174	I2238	I2302	I2366	I2430	I2494	I2558	NETIO-X INPUT15 TAMPER
4	I2111	I2175	I2239	I2303	I2367	I2431	I2495	I2559	NETIO-X INPUT16 TAMPER

(X = unit number 1–8)

3.13.7.2 Outputs

Unit address								Default name
1	2	3	4	5	6	7	8	
C2048	C2112	C2176	C2240	C2304	C2368	C2432	C2496	ETHIO-X GREEN LED
C2049	C2113	C2177	C2241	C2305	C2369	C2433	C2497	ETHIO-X YELLOW LED
C2050	C2114	C2178	C2242	C2306	C2370	C2434	C2498	ETHIO-X DISC LED
C2051	C2115	C2179	C2243	C2307	C2371	C2435	C2499	ETHIO-X BUZZER

(X = unit number 1–8)

Relay output	Unit address								Default name
	1	2	3	4	5	6	7	8	
Base unit									
1	C2080	C2144	C2208	C2272	C2336	C2400	C2464	C2528	DIGITAL OUTPUT E001
2	C2081	C2145	C2209	C2273	C2337	C2401	C2465	C2529	DIGITAL OUTPUT E002
3	C2082	C2146	C2210	C2274	C2338	C2402	C2466	C2530	DIGITAL OUTPUT E003
4	C2083	C2147	C2211	C2275	C2339	C2403	C2467	C2531	DIGITAL OUTPUT E004
Extension unit 0									
1	C2084	C2148	C2212	C2276	C2340	C2404	C2468	C2532	DIGITAL OUTPUT E005
2	C2085	C2149	C2213	C2277	C2341	C2405	C2469	C2533	DIGITAL OUTPUT E006
3	C2086	C2150	C2214	C2278	C2342	C2406	C2470	C2534	DIGITAL OUTPUT E007
4	C2087	C2151	C2215	C2279	C2343	C2407	C2471	C2535	DIGITAL OUTPUT E008
Extension unit 1									
1	C2088	C2152	C2216	C2280	C2344	C2408	C2472	C2536	DIGITAL OUTPUT E009
2	C2089	C2153	C2217	C2281	C2345	C2409	C2473	C2537	DIGITAL OUTPUT E010
3	C2090	C2154	C2218	C2282	C2346	C2410	C2474	C2538	DIGITAL OUTPUT E011
4	C2091	C2155	C2219	C2283	C2347	C2411	C2475	C2539	DIGITAL OUTPUT E012

Relay output	Unit address								Default name
	1	2	3	4	5	6	7	8	
Extension unit 2									
1	C2092	C2156	C2220	C2284	C2348	C2412	C2476	C2540	DIGITAL OUTPUT E013
2	C2093	C2157	C2221	C2285	C2349	C2413	C2477	C2541	DIGITAL OUTPUT E014
3	C2094	C2158	C2222	C2286	C2350	C2414	C2478	C2542	DIGITAL OUTPUT E015
4	C2095	C2159	C2223	C2287	C2351	C2415	C2479	C2543	DIGITAL OUTPUT E016

3.14 Connection to S3100

3.14.1 Communication with S3100 Security Panels

The XO device can connect with up to 16 S3100 security panels. Communication works in both directions:

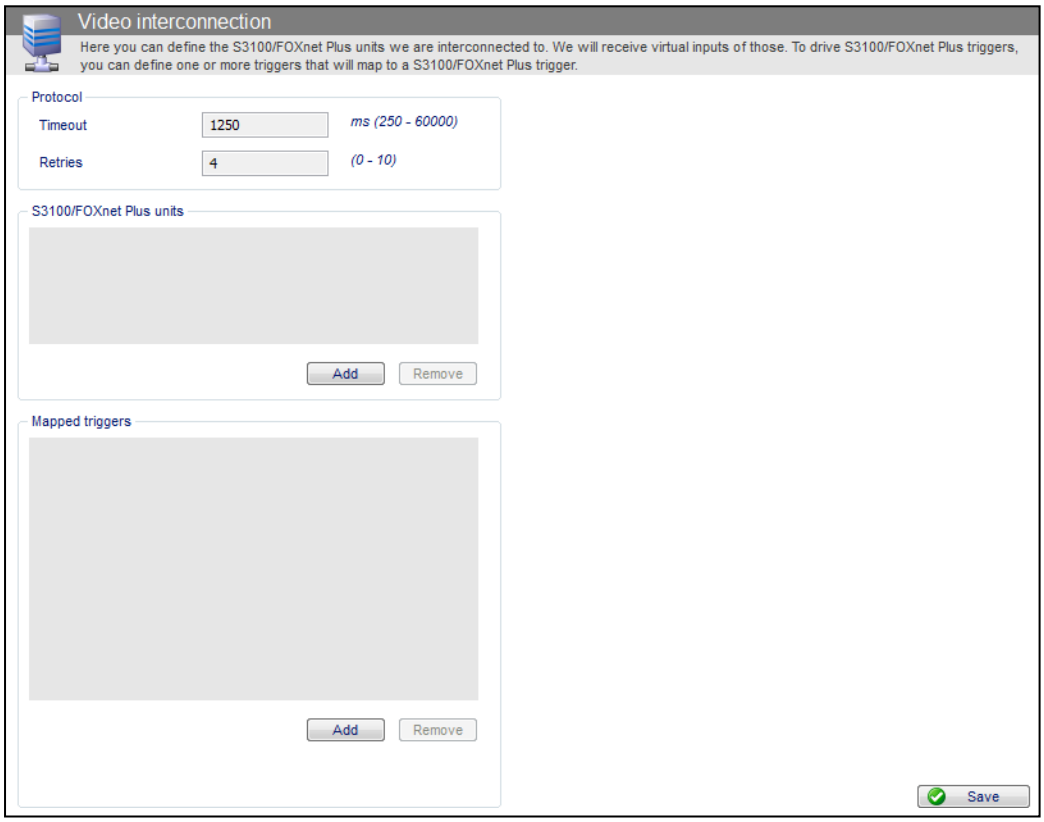
- From the S3100 to the XO device: there are 16 virtual inputs available on the XO device, which a S3100 security panel can activate.
- From the XO device to the S3100: a trigger (an input) from the XO device can activate an input on the S3100 security panel.

Note

Interconnection also works with the older FOXnet (Plus) security panels.

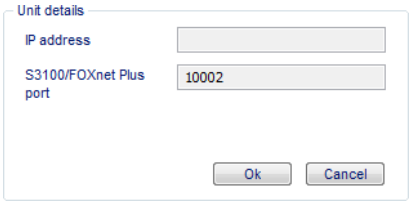
To set up connections to S3100 security panels, proceed as follows:

1. Choose **System** > **Connections** > **Video interconnection**.

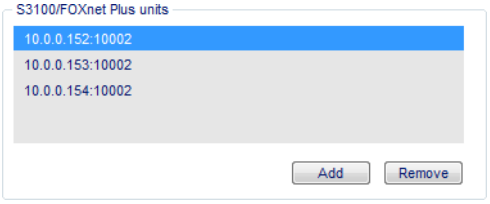


2. Under **Protocol**, provide the desired communication protocol settings. These settings apply to all connected S3100 panels:
   - In the Timeout box, enter the communication timeout in milliseconds. The default value is 1250 ms.
   - In the Retries box, enter the number of retries to establish communication. The default value is 4.

   The default values are sufficient for most cases, but you can increase them on slower networks if you observe communication faults between the devices.
3. To add an S3100 security panel: under **S3100/FOXnet Plus units**, click **Add**.



4. In the **IP address** box, enter the IP address of the S3100 security panel.
5. In the **S3100/FOXnet Plus port** box, enter the port number for communication (as defined in the S3100 security panel).
6. Click **OK** to confirm.
7. Add more S3100 panels as required. All added S3100 security panels appear in the list:



8. Click **Save**.

3.14.2 Handling Inputs from S3100 Security Panels

The table below provides an overview of the inputs on the XO device that are related to the S3100 connections. The system will trigger inputs I2816–I2936 if there is no communication between the XO device and the respective S3100 panel (1–16). The S3100 panels can trigger the 16 virtual inputs I2944–I2959. For instructions on setting up the S3100 panels to trigger the virtual inputs, see the S3100 technical documentation.

Input	Type	Default name	Description
I2816	REAL	VIC-H01 PRESENCE FLT	No communication with S3100 panel 1
I2824	REAL	VIC-H02 PRESENCE FLT	No communication with S3100 panel 2
I2832	REAL	VIC-H03 PRESENCE FLT	No communication with S3100 panel 3
I2840	REAL	VIC-H04 PRESENCE FLT	No communication with S3100 panel 4
I2848	REAL	VIC-H05 PRESENCE FLT	No communication with S3100 panel 5
I2856	REAL	VIC-H06 PRESENCE FLT	No communication with S3100 panel 6
I2864	REAL	VIC-H07 PRESENCE FLT	No communication with S3100 panel 7
I2872	REAL	VIC-H08 PRESENCE FLT	No communication with S3100 panel 8
I2880	REAL	VIC-H09 PRESENCE FLT	No communication with S3100 panel 9
I2888	REAL	VIC-H10 PRESENCE FLT	No communication with S3100 panel 10
I2896	REAL	VIC-H11 PRESENCE FLT	No communication with S3100 panel 11
I2904	REAL	VIC-H12 PRESENCE FLT	No communication with S3100 panel 12
I2912	REAL	VIC-H13 PRESENCE FLT	No communication with S3100 panel 13

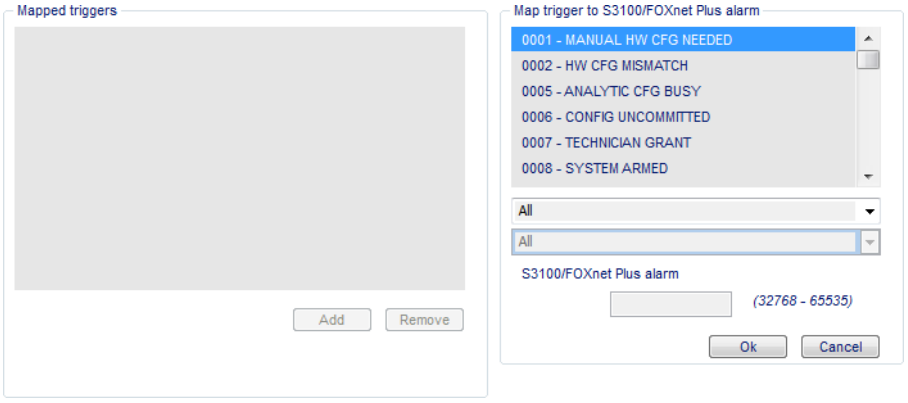
Input	Type	Default name	Description
I2920	REAL	VIC-H14 PRESENCE FLT	No communication with S3100 panel 14
I2928	REAL	VIC-H15 PRESENCE FLT	No communication with S3100 panel 15
I2936	REAL	VIC-H16 PRESENCE FLT	No communication with S3100 panel 16
I2944	REAL	VIRTUAL INPUT 001	Alarm from S3100 on virtual input 1
I2945	REAL	VIRTUAL INPUT 002	Alarm from S3100 on virtual input 2
I2946	REAL	VIRTUAL INPUT 003	Alarm from S3100 on virtual input 3
I2947	REAL	VIRTUAL INPUT 004	Alarm from S3100 on virtual input 4
I2948	REAL	VIRTUAL INPUT 005	Alarm from S3100 on virtual input 5
I2949	REAL	VIRTUAL INPUT 006	Alarm from S3100 on virtual input 6
I2950	REAL	VIRTUAL INPUT 007	Alarm from S3100 on virtual input 7
I2951	REAL	VIRTUAL INPUT 008	Alarm from S3100 on virtual input 8
I2952	REAL	VIRTUAL INPUT 009	Alarm from S3100 on virtual input 9
I2953	REAL	VIRTUAL INPUT 010	Alarm from S3100 on virtual input 10
I2954	REAL	VIRTUAL INPUT 011	Alarm from S3100 on virtual input 11
I2955	REAL	VIRTUAL INPUT 012	Alarm from S3100 on virtual input 12
I2956	REAL	VIRTUAL INPUT 013	Alarm from S3100 on virtual input 13
I2957	REAL	VIRTUAL INPUT 014	Alarm from S3100 on virtual input 14
I2958	REAL	VIRTUAL INPUT 015	Alarm from S3100 on virtual input 15
I2959	REAL	VIRTUAL INPUT 016	Alarm from S3100 on virtual input 16

You can set up the behaviour of these inputs in the same way as other inputs on the XO device: for transmitting alarms, starting recordings, etc.

3.14.3 Sending Triggers to the S3100 Security Panel

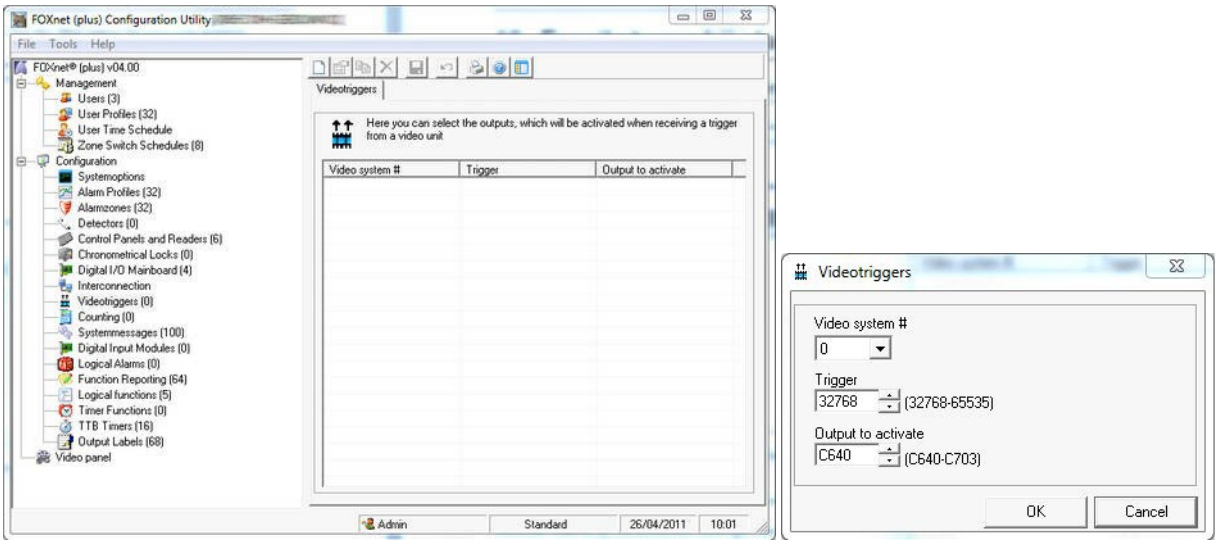
To define the triggers (inputs) to send from the XO device to the S3100, proceed as follows:

1. Under **Mapped triggers**, click **Add**. The following screen appears:



2. In the **Map trigger to S3100/FOXnet Plus alarm** list, select the desired input from the XO device. Use the filters below the list to reduce the list. If you filter on camera inputs, you can filter further on camera number.
3. In the **S3100/FOXnet Plus alarm** box, type the corresponding alarm number on the S3100 for the selected trigger. For information on the S3100 alarm numbers, see the S3100 technical documentation.
4. Click **OK**.
5. Repeat for all other triggers that you want to send to the S3100.

6. Click **Save**.
   You can now set up the S3100 and associate the triggers to outputs on the S3100 panel.
7. In the S3100 Configurator, open **Video triggers** and click **New** to associate the selected trigger to the output:



8. Select the trigger and the corresponding output to activate on the S3100 panel.

3.15 VPN connection

3.15.1 VPN configuration

XO NVR (gateway devices not included) can be connected to an L2TP/IPSec VPN (Virtual Private Network) and then obtain a virtual IP address. If the VCP is deployed on a computer connected to the same VPN, VCP can use the virtual IP address of the XO NVR to access this NVR even if the VCP and the NVR are not in the same real private network.

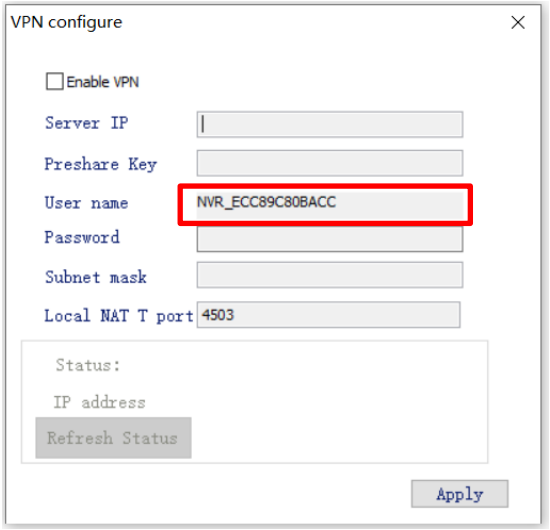
Before set VPN configuration on XO client, make sure to proceed as follows:

- Set up L2TP/IPSec VPN on Windows Server 2019 (refer to *Set up A L2TP/IPSec VPN in Windows Server 2019*).

  Make sure the VPN supports preshared key. XO NVR needs the preshared key to join the VPN.
- Deploy the VCP on the same Windows Server 2019.
- Add an access account for the XO device to join the VPN (refer to *Add an account for XO NVR on Windows Server 2019*).
- Disable 3G or 4G for XO device. (Choose System > CONNECTIONS > Ethernet / PPP and click Advanced mode. Select Modem type as None and click Save. Choose System >MAINTENANCE > Configuration Management to restart the XO device.)

After finishing the preparation above, you can specify VPN configuration by XO client by proceeding as follows:

1. Choose **System > CONNECTIONS > Ethernet / PPP** and click **VPN configure**.
2. On the **VPN configure** window, Fill in the following information:

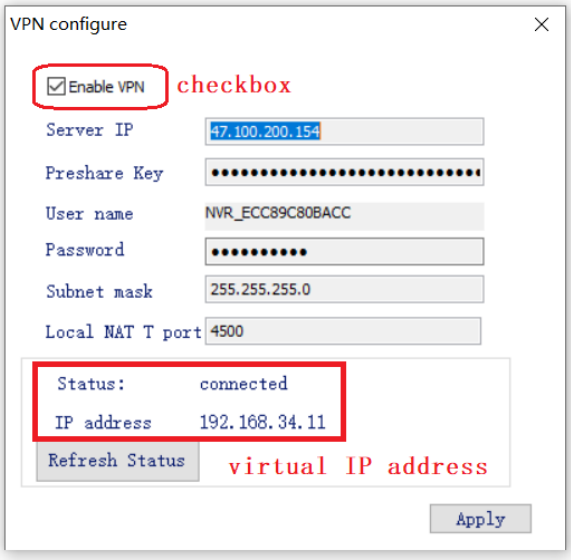


Item	Description
Server IP	Type the public IPv4 address of VPN server. **Note**: If you set up the L2TP/IPSec VPN on Windows Server 2019, type the public IPv4 address of Windows Server 2019.
User name	This user name is generated by the XO client. It is unique and unchanging.
Preshare Key Password Subnet mask	Type the preshared key/subnet mask of the VPN and the password of the account for the device to join the VPN. If you set up the L2TP/IPSec VPN on Windows Server 2019, to konw where to get the preshared key, password and subnet mask, refer to *Configure Pre-shared key, Add an account for XO NVR on Windows Server 2019* and *Configure static address pool*.
Local NAT T port	Type an UDP port number used by XO NVR to communicate with the VPN server. • To know more about NAT T (Network Address Translation Traversal, refer to https://docs.strongswan.org/docs/5.9/features/natTraversal.html • This port is used by XO NVR device itself and has nothing to do with the VPN Server. • If in the same private network, there are more than one XO NVR devices needing to join VPN, please type different NAT T ports for these devices, otherwise only one device can join the VPN successfully. • Default value: 4500 Recommended value ranges: 4500 ~ 4999

3. Check the **Enable VPN** checkbox and then click **Apply**.

   Click **Refresh Status** to refresh the real time status of XO NVR to VPN in time and you can get the virtual IP address.

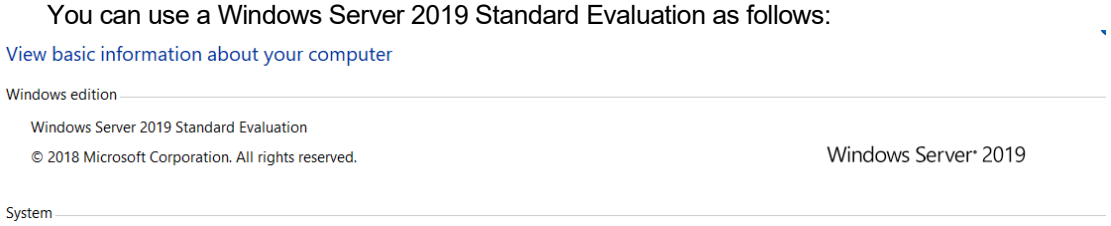
   If you want to let XO NVR exit the VPN, uncheck the **Enable VPN** checkbox and click **Apply**.



3.15.2 Set up A L2TP/IPSec VPN in Windows Server 2019

3.15.2.1 Preparation

1. Deploy Windows Server 2019 official version first.
   You can use a Windows Server 2019 Standard Evaluation as follows:

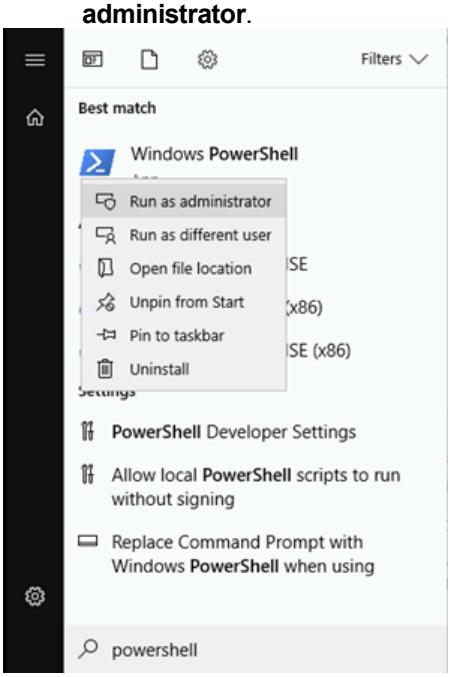


> **Note**
>
> If the Windows Server 2019 is deployed behind a firewall device:
>
> - Set the firewall device to ensure that Ping requests to the Windows Server 2019 are allowed.
> - Set the firewall device to ensure that accesses to the UDP ports 500, 1701 and 4500 of the Windows Server 2019 are allowed.

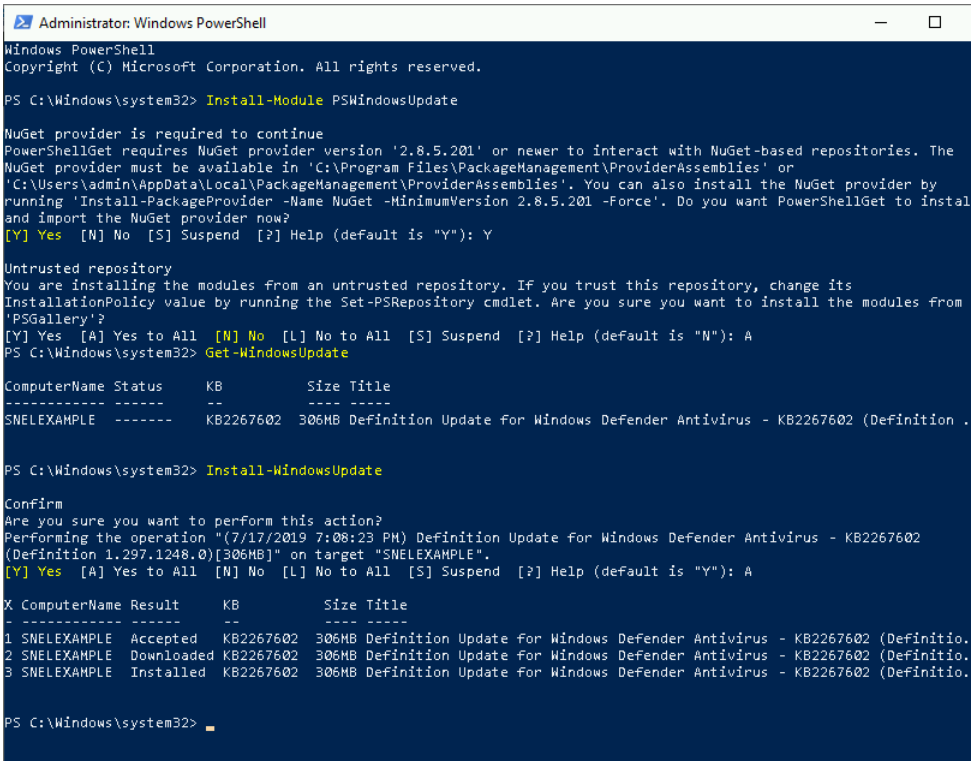
2. Log in Windows Server 2019 you have deployed as an administrative user.

3.15.2.2 Step 1 Update system.

1. Search for Windows Powershell and open it in Administrative mode by right-clicking and selecting **Run as administrator**.



2. Install Windows update module for Powershell by running the command in the Powershell:
   Install-Module PSWindowsUpdate
3. Press Y and enter all the time for confirmation.
4. Get the list of latest updates by running:
   Get-WindowsUpdate
5. Install the updates by running:
   Install-WindowsUpdate



6. Once updates are installed, restart the computer by running:
   Restart-Computer
7. After the computer is restarted, log in as an administrative user again to continue the remaining steps.

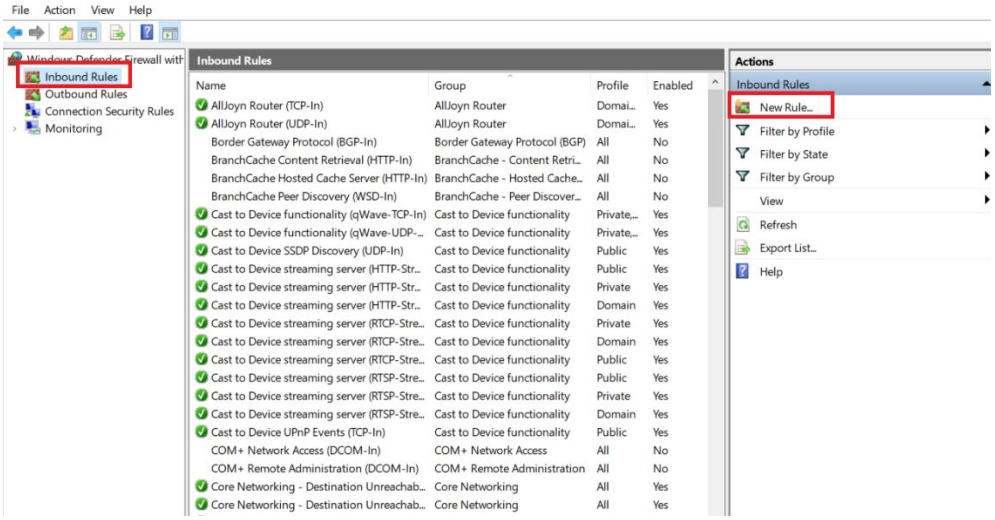
3.15.2.3 Step 2 Configure firewall to allow Pings

XO NVR checks whether the VPN server is online by ping.

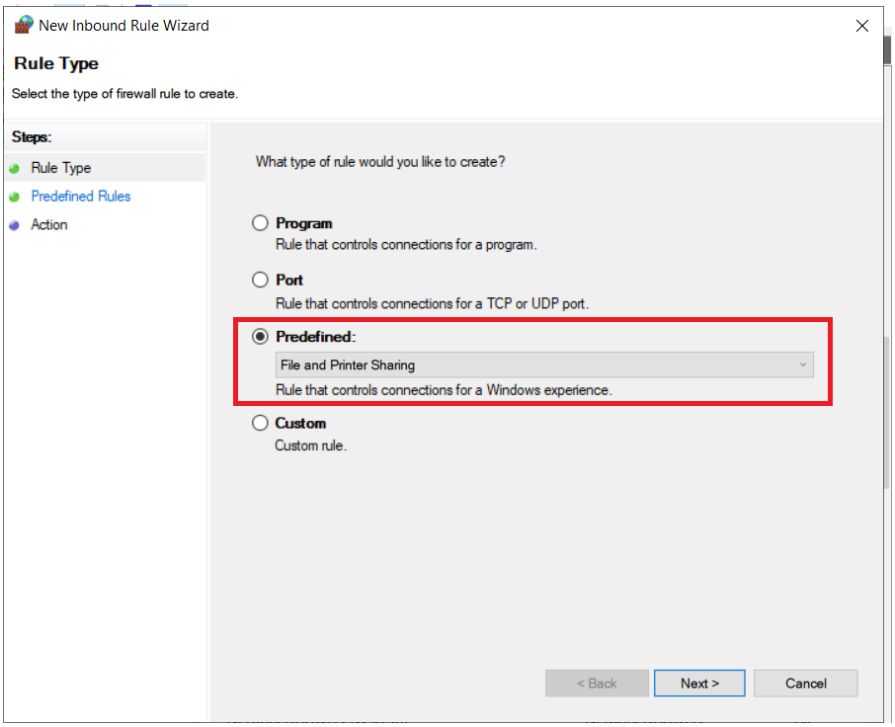
1. On the **Start** menu, search for **Windows Defender Firewall** and open it.



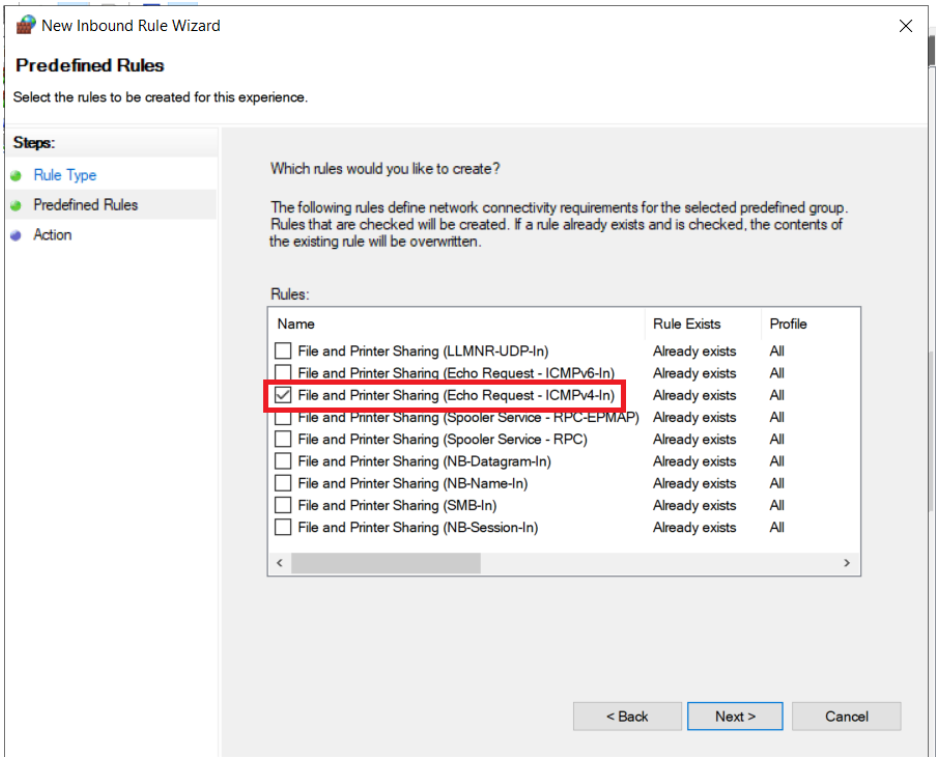
2. Click Advanced settings. click **Inbound Rules** on the left pane and then click on **New Rule** on right pane.



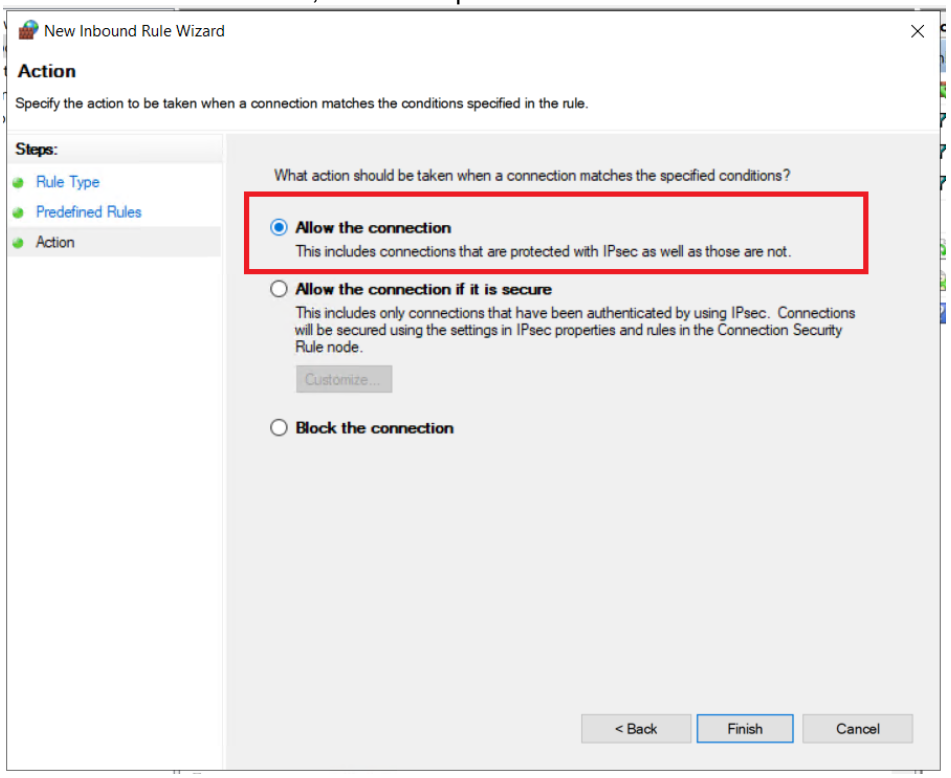
3. In **New Inbound Rule Wizard**, click **Predefined** radio and select the **File and Printer Sharing** from the drop-down. Click Next.



4. Under **Predefined Rules** select **File and Printer Sharing (Echo Request - ICMPv4-In)** checkbox and click **Next**.



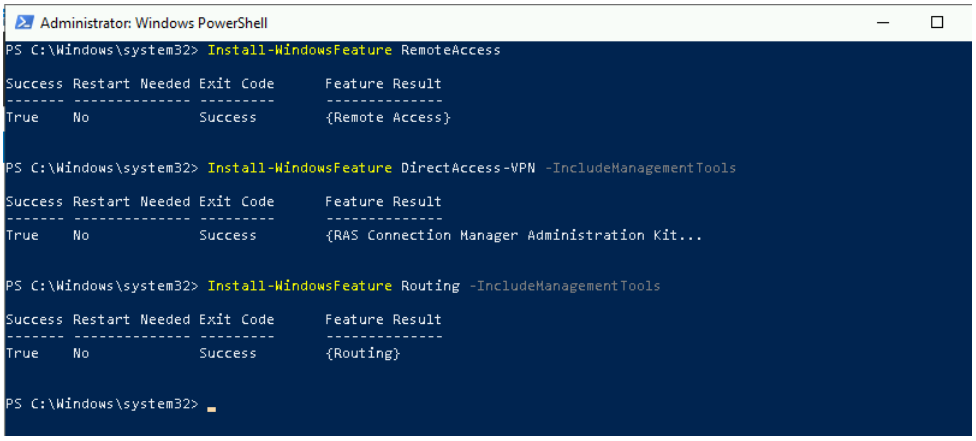
5. Under **Action** select, select the option **Allow the connection** and click **Finish**.



3.15.2.4 Step 3 Install Remote Access Role

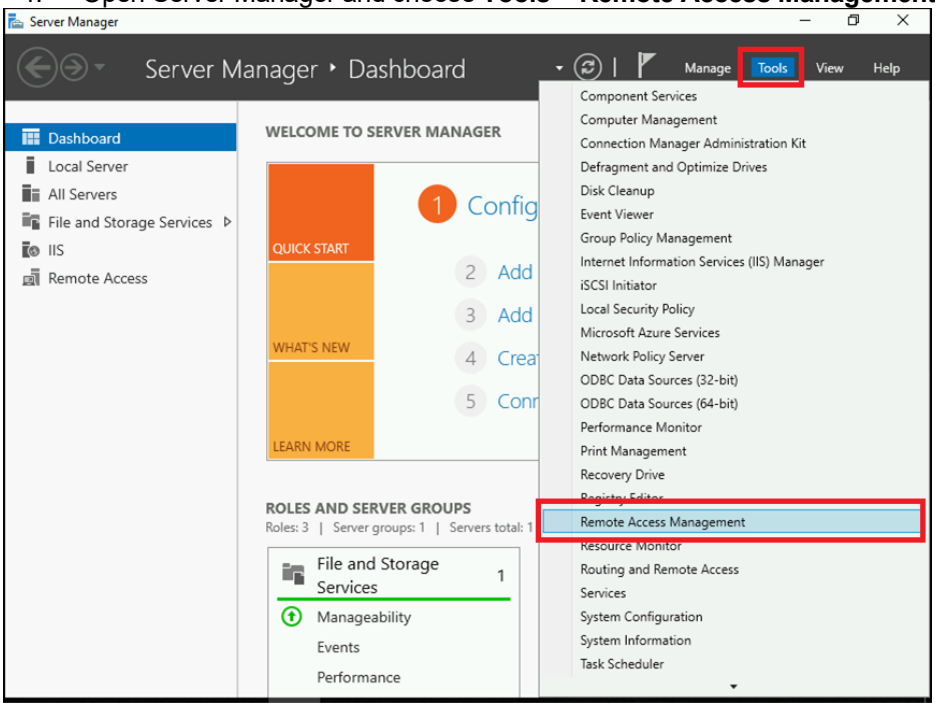
1. Open Powershell again in administrative mode and run the following command to install the Remote Access feature with Direct Access and VPN (RAS) and Routing along with management tools:

   Install-WindowsFeature RemoteAccess
   Install-WindowsFeature DirectAccess-VPN -IncludeManagementTools
   Install-WindowsFeature Routing -IncludeManagementTools

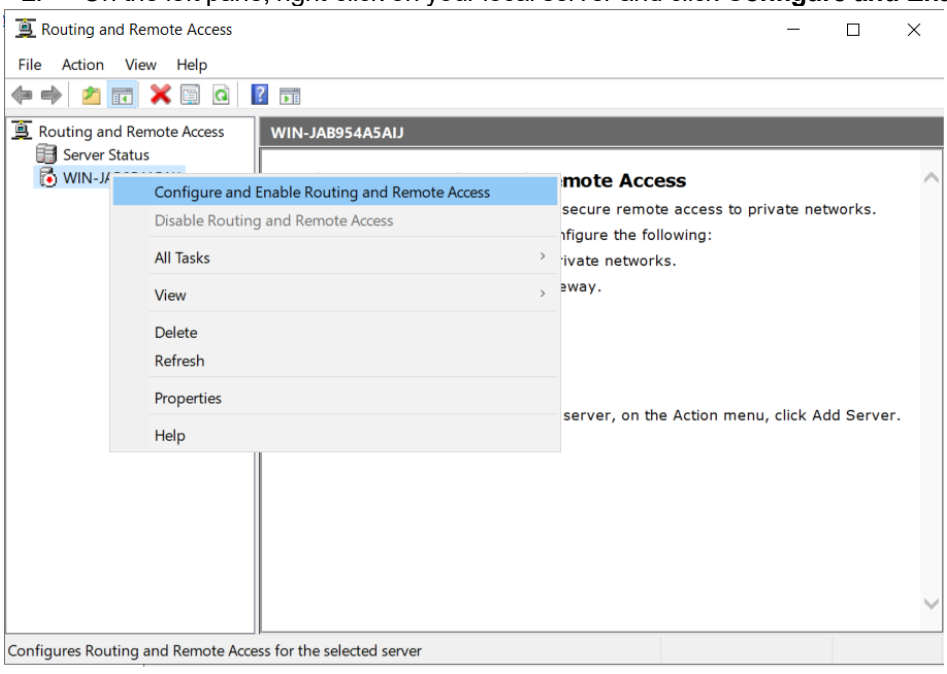


3.15.2.5 Step 4 Configure Routing and Remote Access

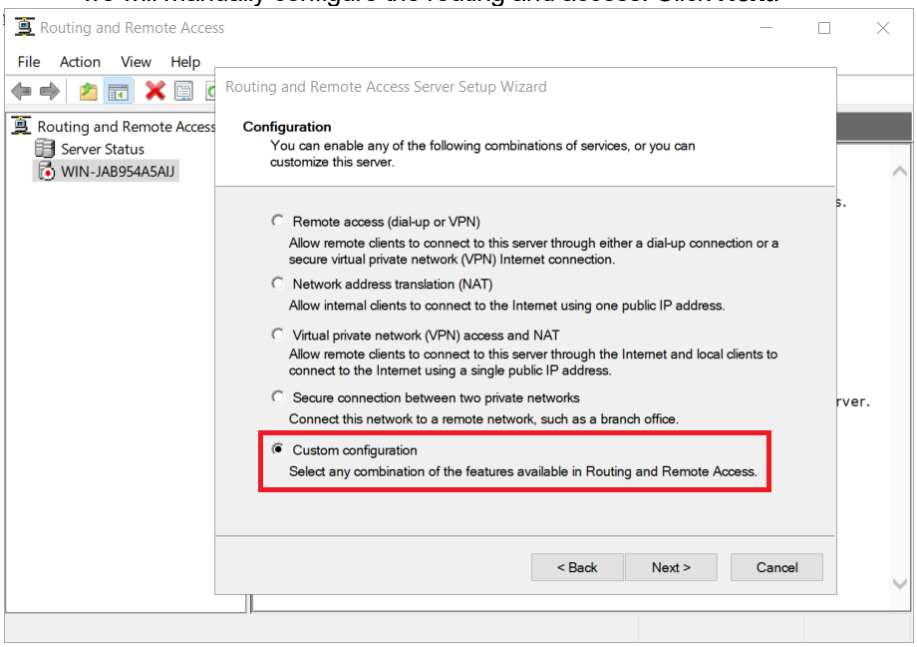
1. Open Server Manager and choose **Tools > Remote Access Management**.



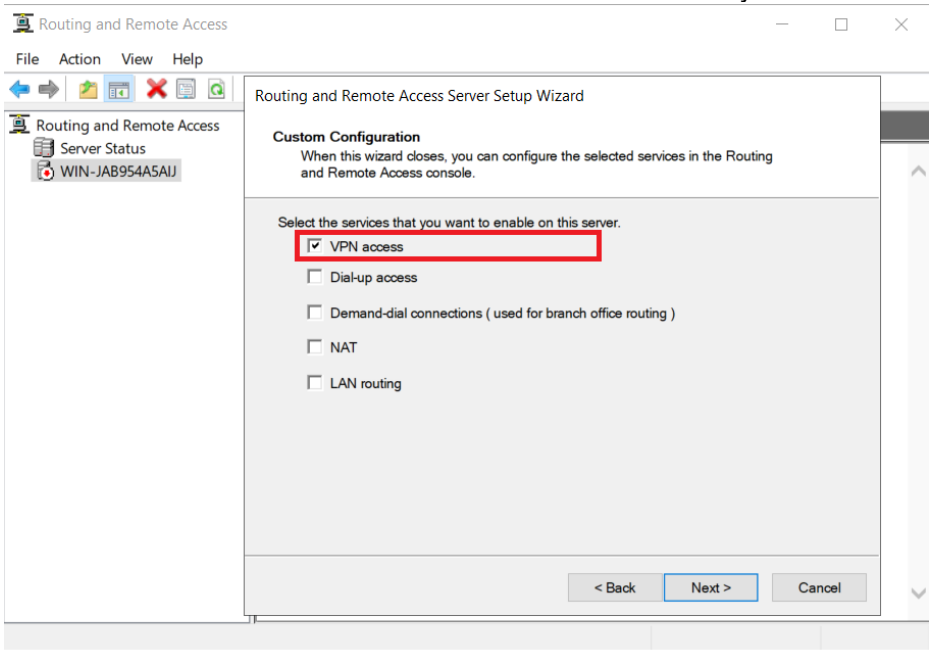
2. On the left pane, right-click on your local server and click **Configure and Enable Routing and Remote Access**.



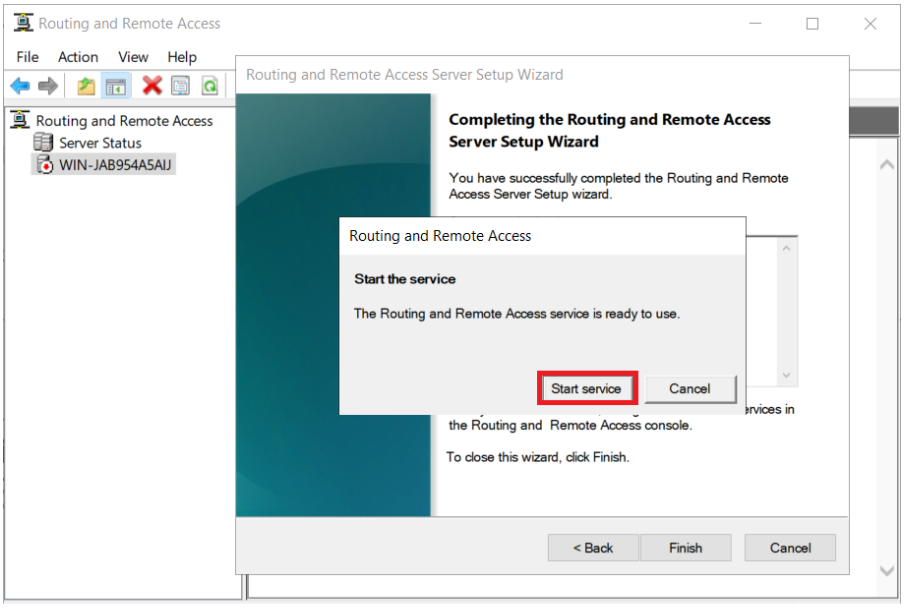
3. In **Configure and Enable Routing and Remote Access Wizard**, select **Custom configuration** radio button as we will manually configure the routing and access. Click **Next**.



4. Select **VPN access** checkbox and click **Next** to see a summary of the selection.

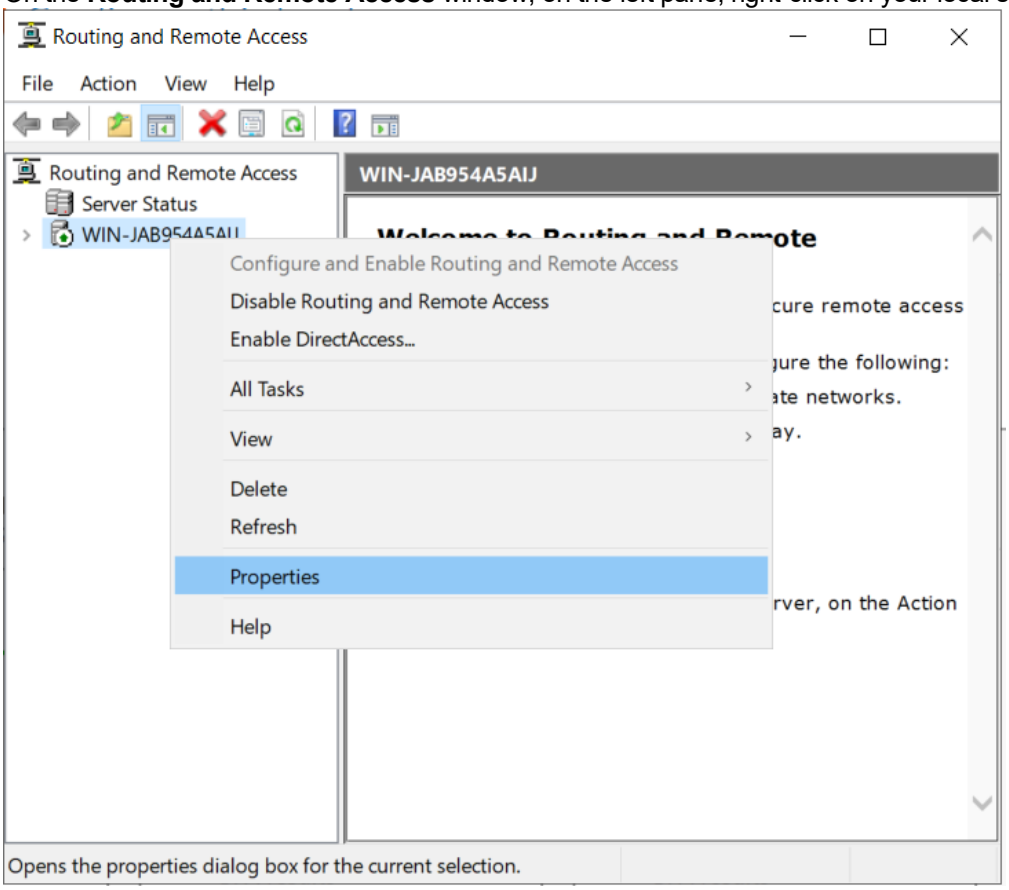


5. Click **Finish**. You will see a prompt to start the **Routing and Remote Access Services**. Click **Start Service**.



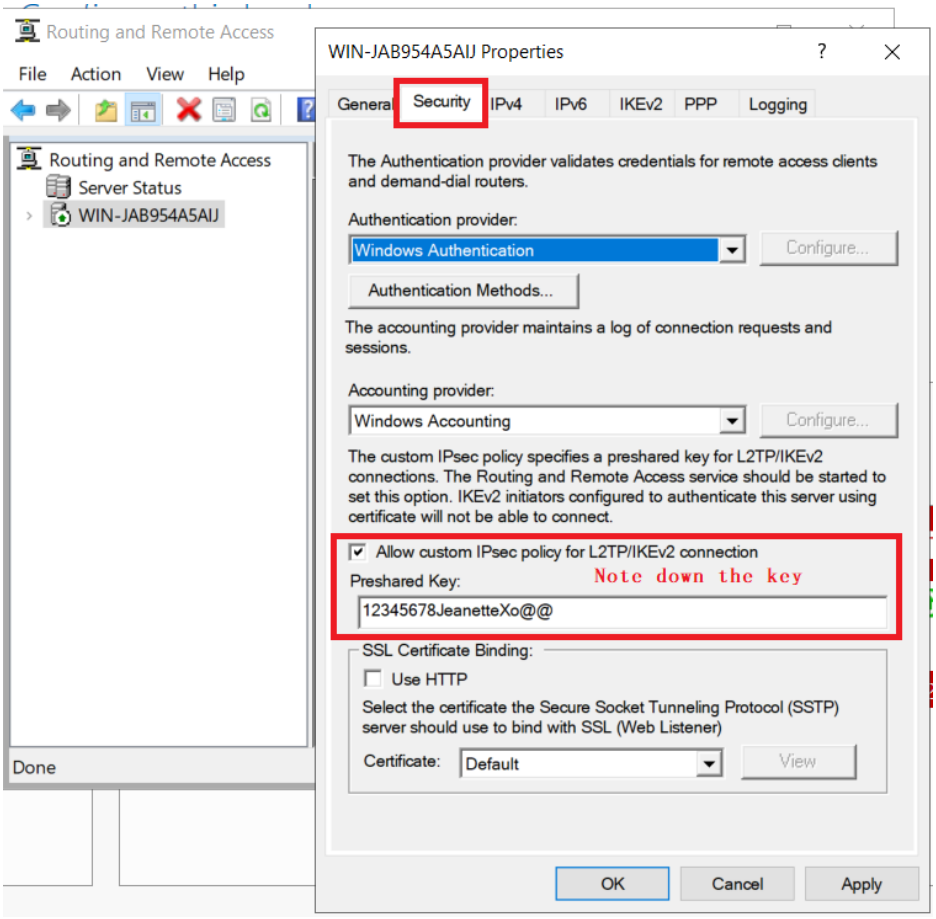
3.15.2.6 Step 5 Configure VPN Properties

On the **Routing and Remote Access** window, on the left pane, right-click on your local server and click **Properties**.



3.15.2.6.1 Configure Pre-shared key

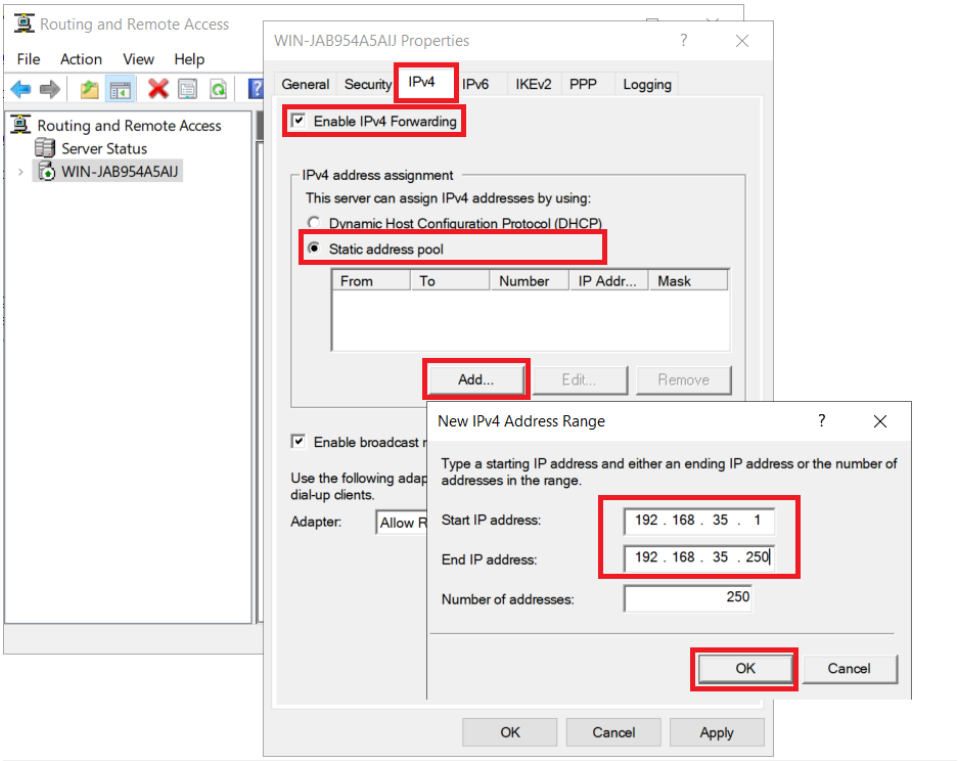
1. Navigate to the security tab and click on **Allow custom IPSec policy for L2TP/IKEv2 connection** and put a Pre-shared key. You can use any tool to generate a random key.
   Ensure the Pre-shared key contains at least 30 characters with numbers, upper and lower case letters (for example: 12345678JeanetteXo@@.)
   After being configured in VPN Server, the key needs to be filled in the VPN configuration interface of XO client (refer to *VPN configuration*). Remember the PSK as we will need to share the PSK with every user who wants to join VPN.



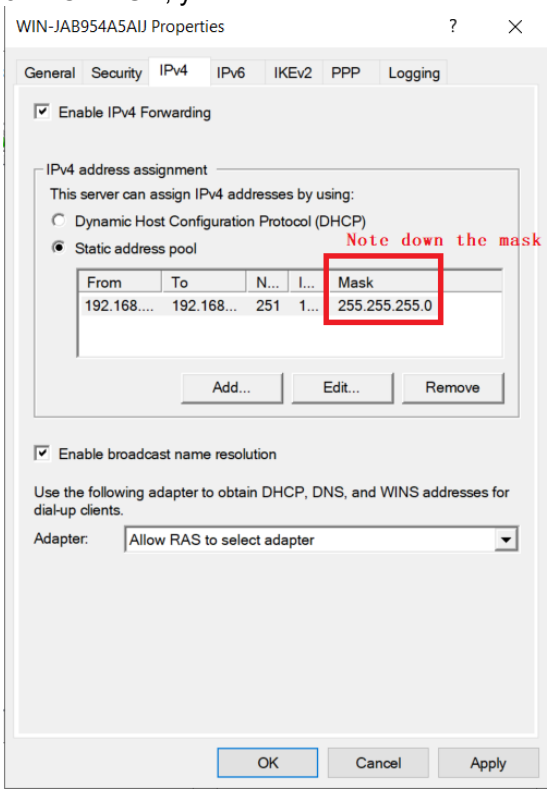
3.15.2.6.2 Configure static address pool

- The addresses pool should not coincide with the network segment of the real network of Windows Server 2019 or the real network of XO NVR devices.
- Most of addresses in the addresses pool are to be assigned to the XO NVR joining the virtual private network. But the VPN server will use one address also, generally the VPN server uses the first address. So please do not assign the first address to any XO NVR when you configure an account for XO NVR on VPN server.
- For example the number of XO NVR devices joining the virtual private network is N, please ensure that the number of addresses in the addresses pool is more than (N + 1).

1. Go to IPv4 tab and under IPv4 address assignment select static address pool.
2. Click **Add** button and you will get a pop up to put IP address ranges. Put the starting address and ending address of the IP address range you want the users to assign to.
   Make sure that XO NVR can access this IPV4 address, otherwise NVR cannot join the VPN. The IPv4 address of Windows Server 2019 on the public network needs to be filled in the VPN configuration interface of XO client later.



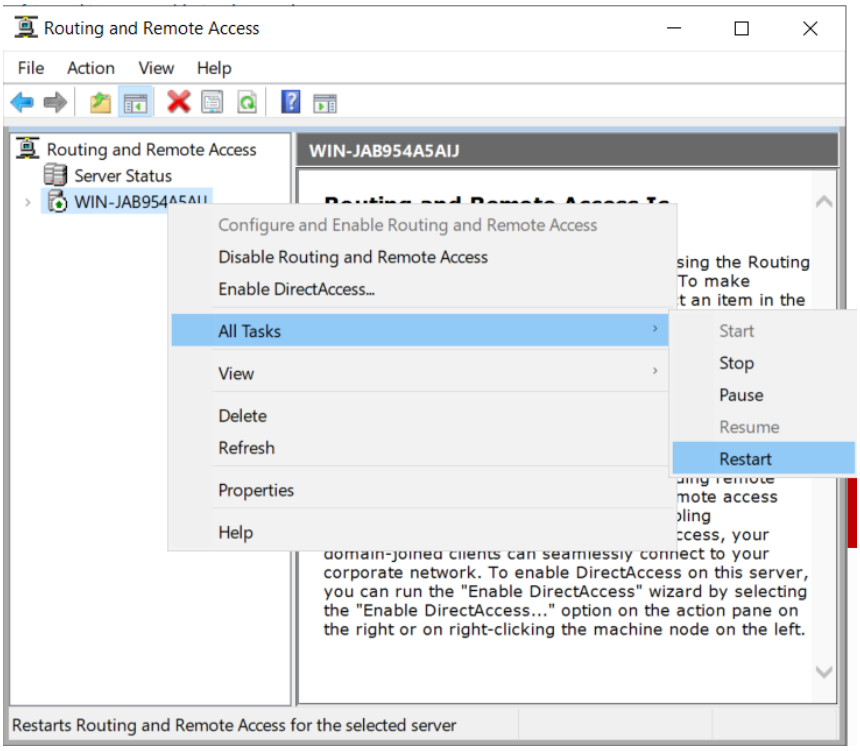
3. Click **OK**, you can see the subnet mask of the VPN. Note down the mask.



4. Click **Apply** button first and then click **OK** button.

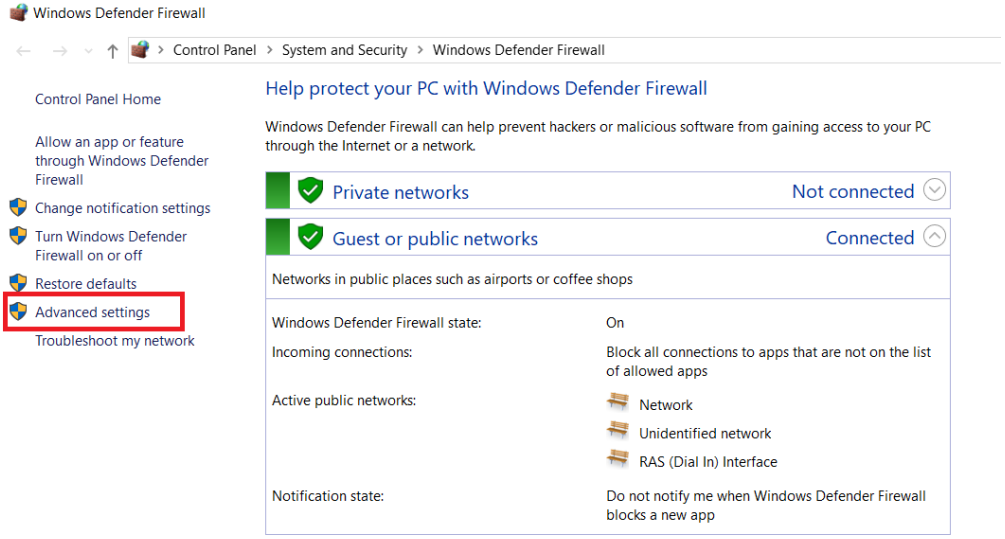
3.15.2.7 Step 6 Restart Routing and Remote Access

1. On the left pane of Routing and Remote Access window, right-click on your local server and click on **Restart** under **All Tasks**.

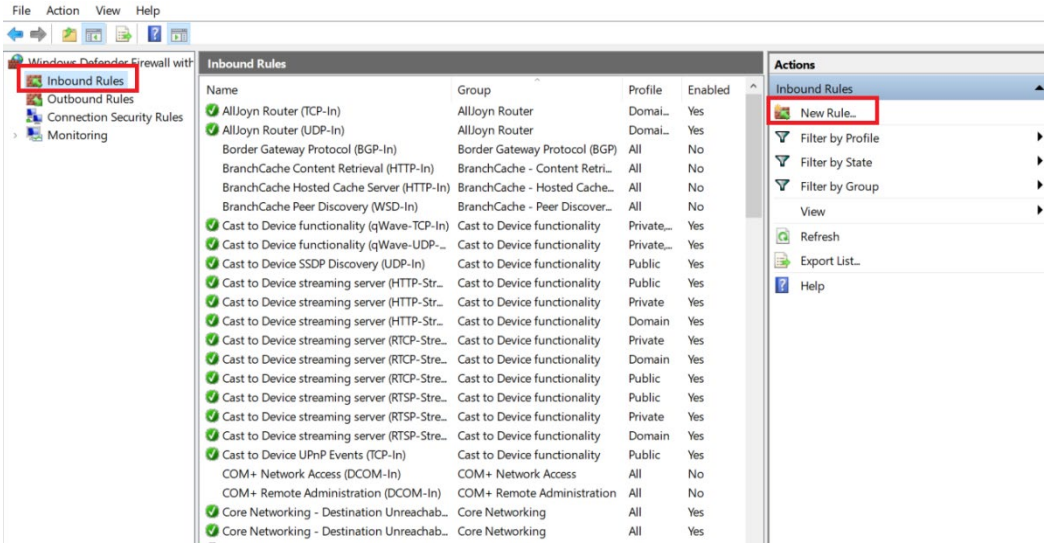


3.15.2.8 Step 7 Configure Windows Firewall to allow Inbound traffic on Routing and Remote Access(L2TP-In)

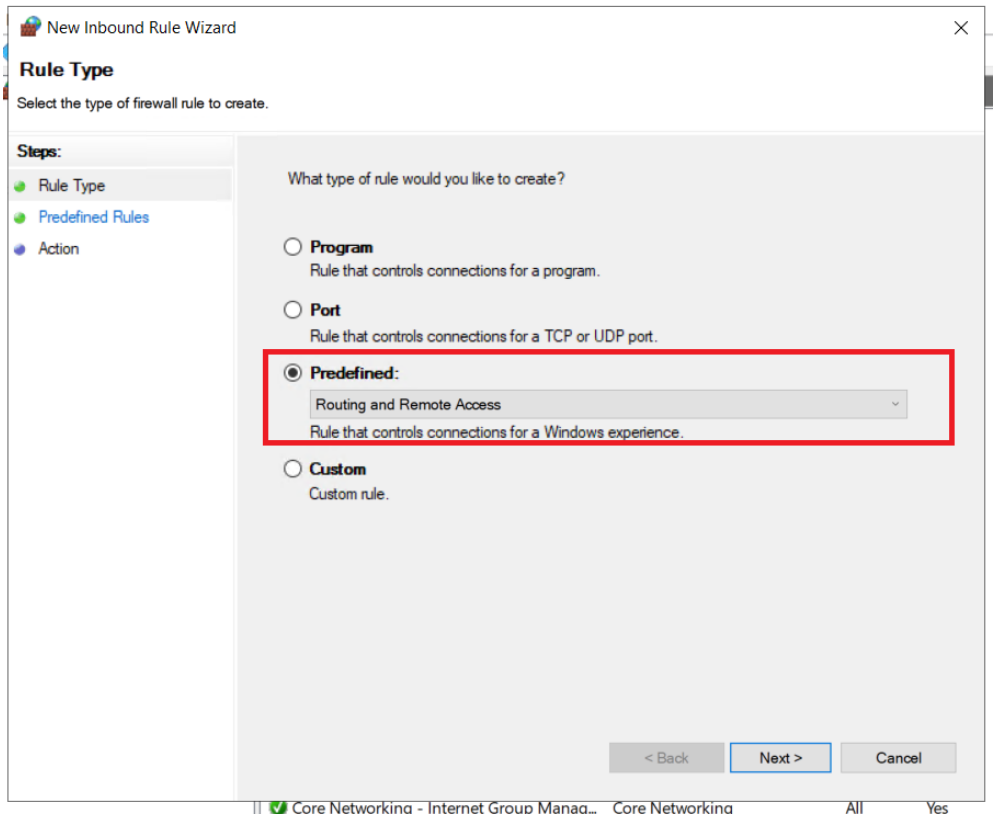
1. On the start menu, search for Windows defender firewall and open it. Click **Advanced settings** on windows defender firewall.



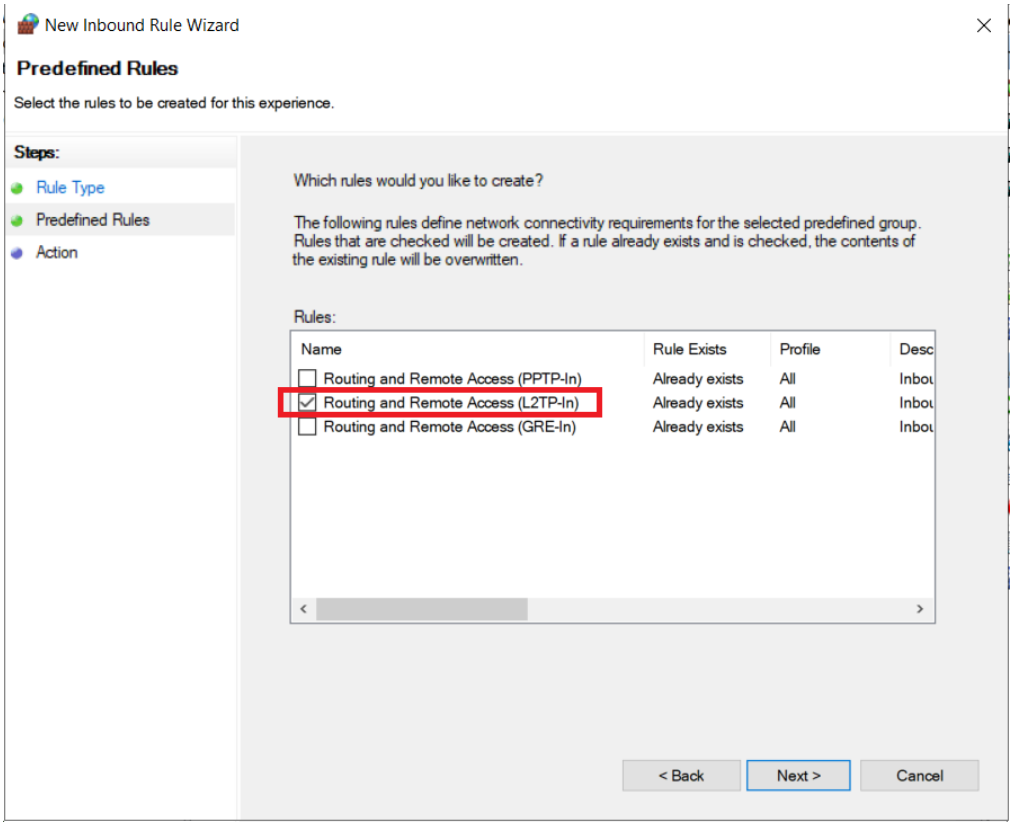
2. Under **Advanced settings**, click **Inbound Rules** on the left pane and then click on **New Rule** on right side pane.



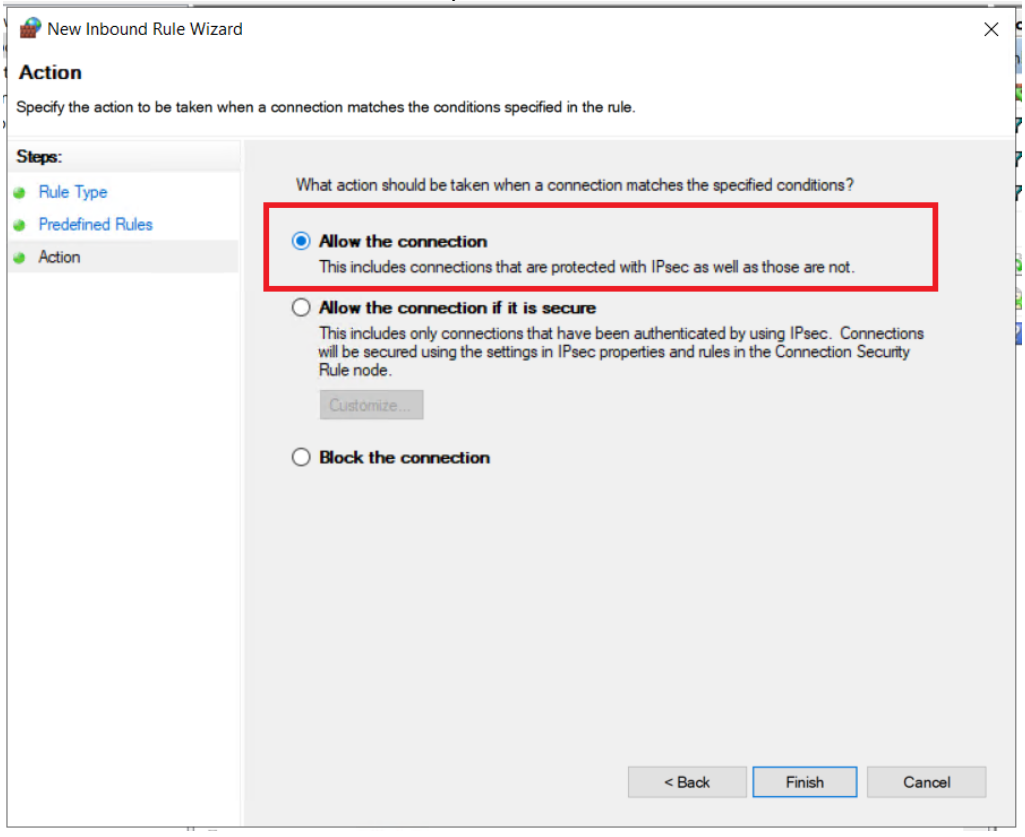
3. In **New Inbound Rule Wizard** click on **Predefined** radio button and select the **Routing and Remote Access** from the drop-down, click **Next**.



4. Under **Predefined Rules** select **Routing and Remote Access(L2TP-In)** checkbox and click **Next**.



5. Under **Action** select, select the option **Allow the connection** and click **Finish**.



3.15.2.9 Step 8 Set advanced setting for VPN to improve security

1. Search for Windows Powershell and open it in Administrative mode. Run the following commands:

```
Set-VpnServerConfiguration -TunnelType L2tp -CustomPolicy -EncryptionMethod AES256
Set-VpnServerConfiguration -TunnelType L2tp -CustomPolicy -IntegrityCheckMethod SHA256
Set-VpnServerConfiguration -TunnelType L2tp -CustomPolicy -DHGroup ECP384

Set-VpnServerConfiguration -TunnelType L2tp -CustomPolicy -CipherTransformConstants AES256
```

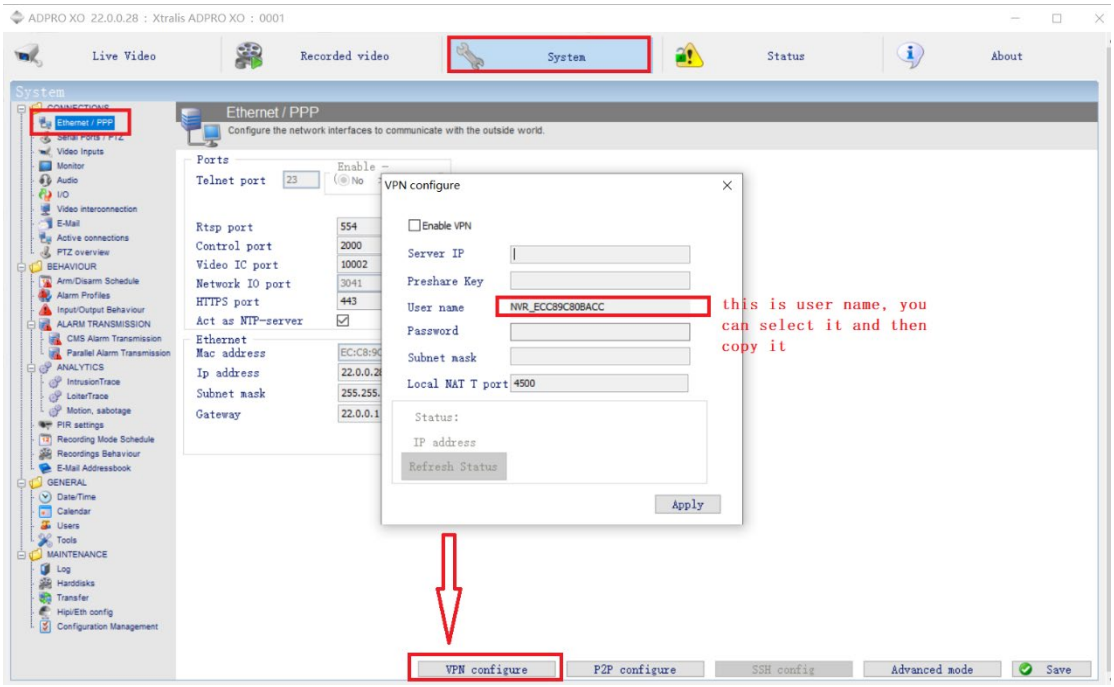
```
Set-VpnServerConfiguration -TunnelType L2tp -CustomPolicy -
AuthenticationTransformConstants SHA256128
Set-VpnServerConfiguration -TunnelType L2tp -CustomPolicy -PfsGroup None
Set-VpnServerConfiguration -SALifeTimeSeconds 3600
```

2. Restart the computer and you have set up L2TP/IPSec VPN on Windows Server 2019 successfully.

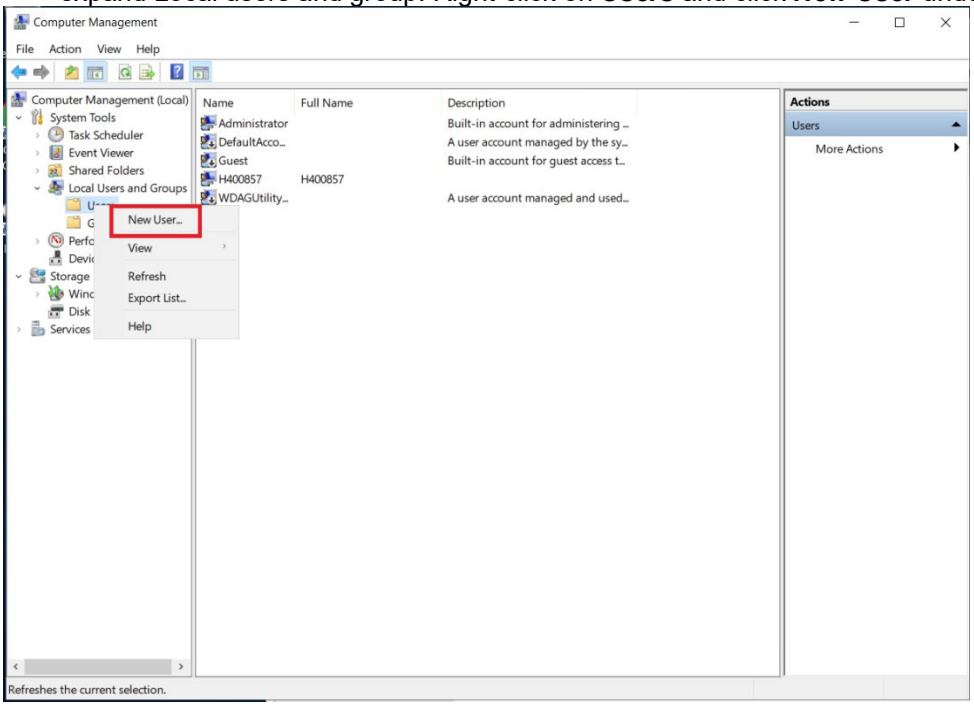
3.15.3 Add an account for XO NVR on Windows Server 2019

Before you configure an account for XO NVR on Windows Server 2019, please make sure you have installed VPN server on the same Windows Server 2019 referring to *Set up a L2TP/IPSec VPN in Windows Server 2019.*

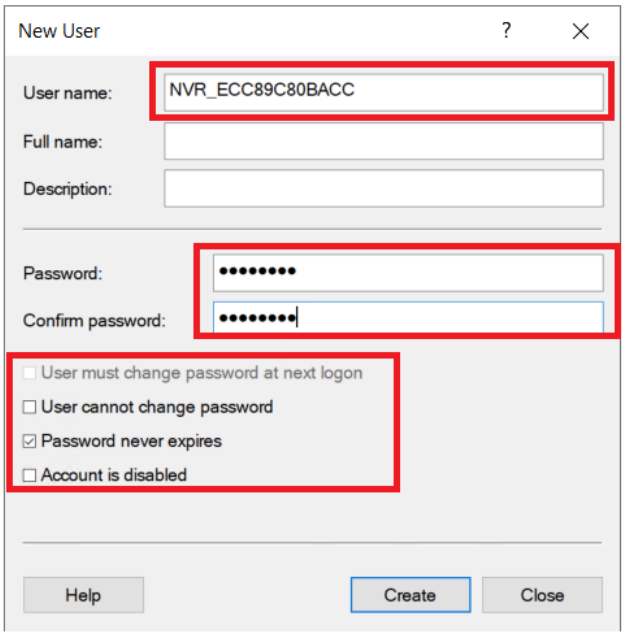
1. Get the username of the XO NVR on the XO client.
   XO NVR has generated a globally unique and unchanging user name. Please log in via XO client, you can get the user name on the VPN configuration interface. Refer to *VPN configuration* for detailed information.



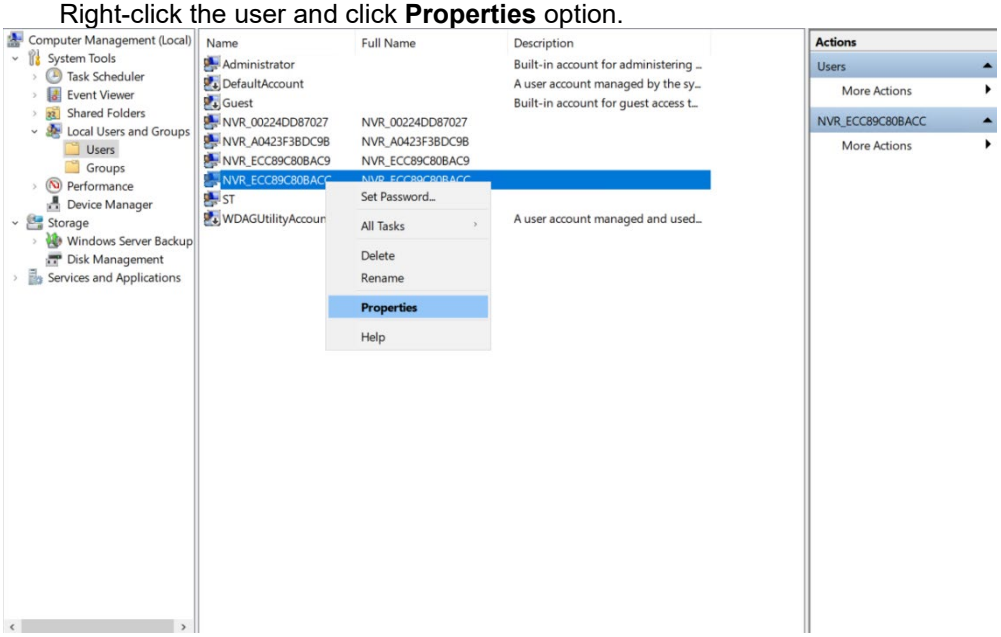
2. Logged in the Windows Server 2019 as an administrative user.
3. Search for Computer Management in the start menu and under **Computer Management** window expand Local users and group. Right-click on ***Users*** and click ***New User*** under ***Local Users and Groups***.



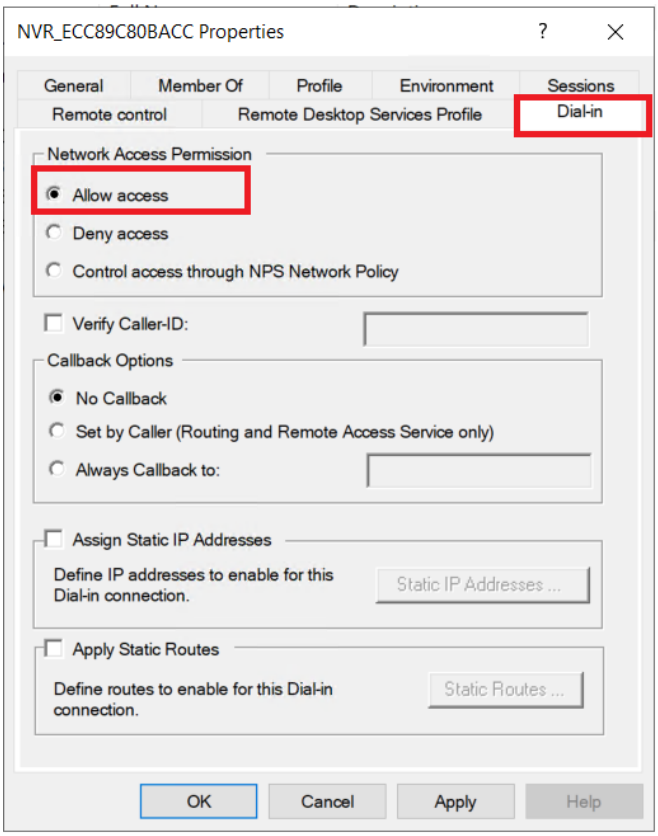
4. On New User prompt, fill in the username of the XO NVR on the XO client in step 1 and set a strong password.
5. Uncheck **User must change the password on next logon** checkbox and check Password never expires checkbox. Please note down the password you type just now, it needs to be filled in the VPN configuration interface on the XO client.
   Ensure that the password contains at least 10 characters with numbers, upper and lower case letters (for example: QWE123456a)



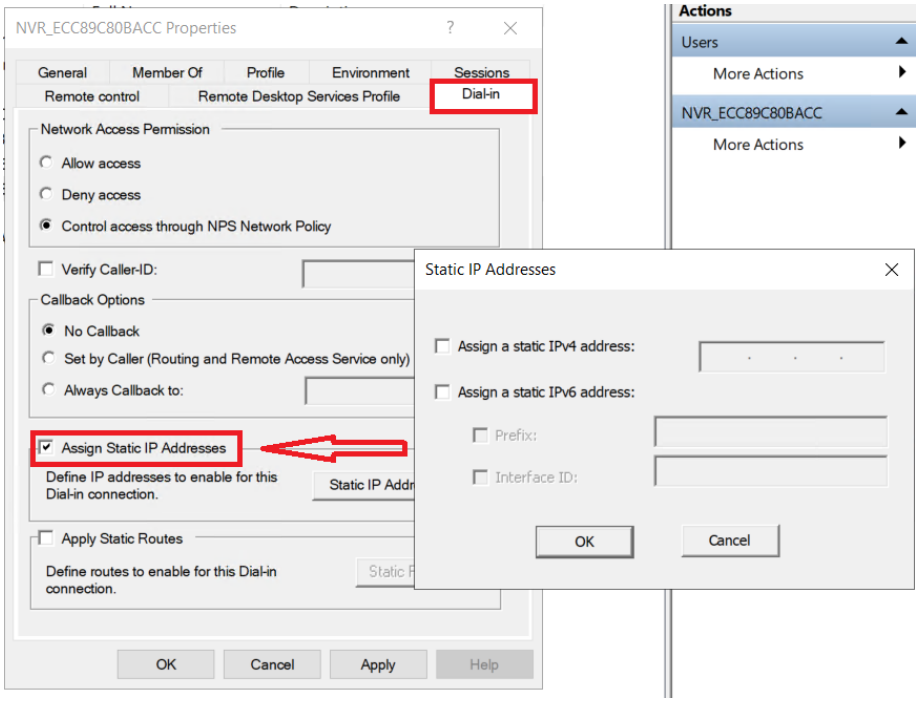
6. Click **Create**.
7. Return to **Computer Management** interface and you can find the newly created user in the list of users. Right-click the user and click **Properties** option.



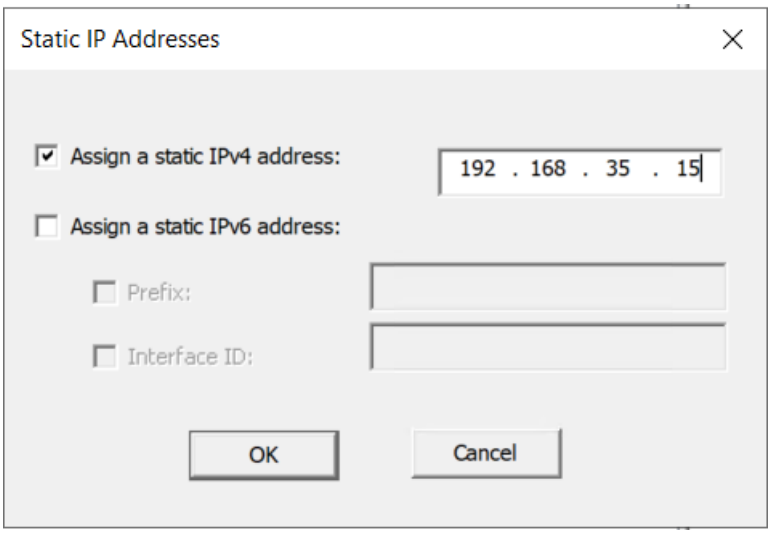
8. On your VPN users properties, navigate to **Dial-in** tab. Select **Allow access** option for Network Access Permissions setting.



9. Check **Assign Static IP Addresses** checkbox to pop *Static IP Addresses* interface.
   Assign a static IPv4 address to the new user to ensure the XO device which generates the user name will be assigned a fixed IP address in the virtual private network.
   Please note that the IP address you assign to the new user belongs to the static addresses pool you configure for VPN server. And please do not assign the first address in the pool to any user, because the first address is reserved for VPN server itself.



10. On **Static IP Addresses** interface, check **Assign a static IPv4 address** checkbox, then fill an IP address.



11. Click **OK** button on **Static IP Addresses** interface to return to VPN users properties, then Click **OK** on VPN users properties to save the properties.

4 Alarm Transmission

4.1 Alarm Transmission Channels

For transmitting alarms to the CMS, the XO device offers the following options:

- **Primary transmission only**: the XO device transmits alarms either via the local network (eth0) or via the dial-up connection (PPP).
  - For transmission over the local network, you can specify up to 5 destination IP addresses. For transmission over the dial-up connection, you can specify up to 5 different phone numbers.
  - However, the system transmits the alarm to only one destination. If the system cannot establish a connection with the first destination, it will try the second, then the third, fourth, and fifth.
  - If the system cannot reach any of the destinations, it activates the system input 0032 – [SYST] – PRIMARY LINE FAULT.
- **Primary and backup (secondary) transmission**: the XO device first tries to transmit the alarms via the primary transmission channel (in this case, the local network). If the system cannot transmit over the primary channel, it switches to the backup (secondary) transmission channel (in this case, the dial-up connection).
  - You can specify up to 5 destinations for both primary and backup channel.
  - However, the system transmits the alarm to only one destination. If the system cannot establish a connection with the first destination, it will try the second, then the third, fourth, and fifth.
  - If the system cannot reach any of the 5 destinations defined for the primary channel, it will switch to the backup channel. Again, it will first try the first destination defined for the backup channel, then the second, and so on.
  - If the system cannot reach any of the destinations, it activates the system inputs 0032 – [SYST] – PRIMARY LINE FAULT and 0033 – [SYST] – BACKUP LINE FAULT.

Note

The XO software uses the terms 'backup' and 'secondary' transmission interchangeably. They mean the same thing.

Besides the primary and backup transmission to the main CMS, the system also offers:

- **Parallel transmission to two more monitoring stations.**
  - Parallel transmission is always via the local network, not via the dial-up connection.
  - The same mechanism as for the primary/backup channel applies: you can define up to 5 destinations per parallel channel, and the system will transmit to one destination only (it will try the first destination, then the second, etc).
  - If the system cannot reach the parallel destinations, it activates the system inputs 0042 – [SYST] – PARTX1 LINE FAULT and/or 0045 – [SYST] – PARTX2 LINE FAULT.
  - The parallel transmission channels are independent. There is no backup parallel channel.
- **Email transmission, for example to use with iTrace.**

Caution!

For each alarm (input), check if the required transmission channels (primary, backup, parallel 1 and 2, email) are enabled in its alarm profile. If the standard alarm profiles do not cover your specific needs, define your own alarm profiles and assign them to the inputs as required.

For setting up the alarm transmission channels, keep the following in mind:

- Alarm reception requires appropriate alarm management software on the destination computer (for example: VCP, EMS, or M3000). For setting up such software, see the documentation of the respective application.
- If you will be using a dial-up connection, connect and set up the modem first. For more information, see PPP Connection (Modem) .

You can find detailed instructions for setting up primary, backup, and parallel transmission in the following sections. For setting up email transmission, see *Email*.

4.2 Life Check (Site Pulse)

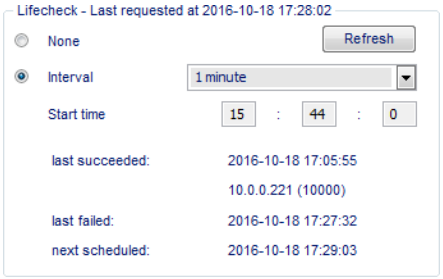
For each transmission channel (primary, backup, and parallel), you can set up a **life check** (also known as Site Pulse or line test) to check the transmission lines at regular intervals. This helps you to identify and correct any communication faults before they become a problem (if the system cannot transmit alarms to the CMS).

The life check on the transmission channels work like the transmission itself: the system sends the life check message on the primary and backup transmission channels to one destination only. If the life check fails on the first primary destination, the system will try the second, the third… destination. If it cannot reach any of the primary destinations, it activates system input 0034 – [SYST] – PRIMARY LIFECHECK. It will then try the first backup destination, then the second, and so on. If it cannot reach any of the backup destinations, it activates system input 0035 – [SYST] – BACKUP LIFECHECK.

For each of the parallel channels independently, the system will try the first destination, then the second… If it cannot reach any of the specified destinations, it activates system input 0044 – [SYST] – PARTX1 LIFECHECK and/or 0047 – [SYST] – PARTX2 LIFECHECK.

If you enable the life check, you can specify the interval for sending the life check messages. The results of the life check appear in the transmission settings window:

- Last succeeded: shows the date (yyyy-mm-dd) and time (hh:mm:ss) on which the system performed the last successful life check; and on which destination.
- Last failed: shows the date (yyyy-mm-dd) and time (hh:mm:ss) on which the system performed the last unsuccessful life check.
- Next scheduled: shows the date (yyyy-mm-dd) and time (hh:mm:ss) on which the system will perform the next life check.



Note

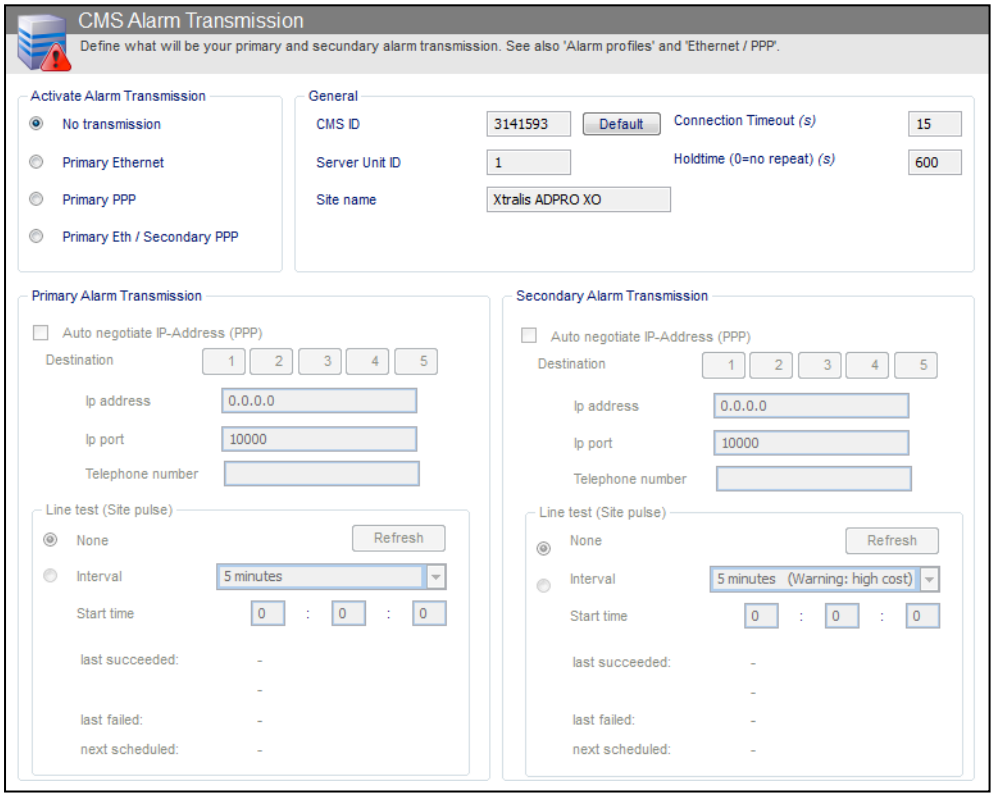
For dial-up transmission (PPP), Honeywell recommends to execute the life check less frequently, because of the connection cost (for example, 1 test a day).

4.3 General Alarm Transmission Settings

The setup below describes the general settings for both the primary and backup transmission channels to the main CMS. This includes identifiers and timeouts, and choosing the desired transmission paths.

To set up the general parameters for alarm transmission, proceed as follows:

1. Choose **System > Behaviour > Alarm transmission > CMS alarm transmission**.



2. Provide the following information:

Item	Description	Default value
General		
CMS ID	This is the alarm sender signature. This number has to match the number programmed in the alarm management software. For a connection to VideoCentral Platinum, the CMS ID has to be the default value. Click **Default** to restore the CMS ID to the default value.	3141593
Server Unit ID	Type the XO device's identification number (1–99999). This number has to be unique for each XO device that sends alarms to the same computer. The server unit ID is included in the name of the subfolders of the default work folder, and the names of the backup files for system license, configurations…. ***Caution!*** After you change the server unit ID, back up your calibration pictures again.	1

Item	Description	Default value
Site name	Type a name for the XO device. You can display the name on the live camera images (layover); it is included in the name of the subfolders of the default work folder; Xchange2 uses it to identify the XO device in its device list. The site name is included in the filename of the calibration pictures. ***Caution!*** After you change the site name, back up your calibration pictures again.	Xtralis ADPRO XO
Connection timeout (s)	Type the delay, in seconds, after which the system automatically disconnects if no more data is exchanged.	15
Hold time (0 = no repeat) (s)	Type the delay, in seconds, before the system retries to connect after a connection error occurs. Enter **0** if you do not want to try again after a connection error. Honeywell recommends that you only do this if you are using a backup connection.	600
Activate Alarm Transmission: select the desired transmission path to the main CMS.		
No transmission	The XO device does not transmit alarms to the main CMS.	
Primary Ethernet	The XO device connects to the main CMS via the local network.	
Primary PPP	The XO device connects to the main CMS via the dial-up connection.	
Primary Eth / Secondary PPP	The XO device uses the local network as the main connection, and the dial-up network as the backup connection.	

3. Depending on the choice you made, continue with the instructions in the following sections for setting up the transmission destinations.

4.4 Primary Alarm Transmission Settings

To set up the primary alarm transmission for the main CMS, proceed as follows:

1. Under **Primary Alarm Transmission**, provide the following information:

Item	Description	Default value
Auto-negotiate IP address (PPP)	This option is only available for the dial-up connection (PPP). Select this checkbox to let the CMS assign IP addresses during the time of the communication. You have to select the checkbox if the CMS uses the VideoCentral Platinum software.	Not selected
Destination 1–5	Here you define up to 5 different computers to receive the alarms. Click the number that you would like to define (1–5), and then provide the information as described below.	–
IP address	Enter the IP address of the destination computer.	0.0.0.0
IP port	Enter the IP port for the alarm transmission.	10000
Telephone number	This option is only available for the dial-up connection (PPP); and you have to set up the connection first. Type the telephone number for the dial-up connection to this IP address. Use only digits; do not use spaces, periods… For example: 056241951	–

Item	Description	Default value
Lifecheck	Select the desired life check for this communication path: • **None**: select this if you do not want to use a life check. • **Interval**: if you want to use a life check, select the interval for sending the life check messages. • **Start time**: if you chose **Interval**, specify the time (in hours, minutes, and seconds) to send the first life check message. The results of the life check appear below. Click **Refresh** to update the test results.	None

2. Click **Save**.
3. Assign suitable alarm profiles for the following events (for details, see *Alarm Input Behaviour*):
   - 0032 – [SYST] – PRIMARY LINE FAULT
   - 0034 – [SYST] – PRIMARY LIFECHECK

4.5 Backup (Secondary) Alarm Transmission Settings

The setup for the backup alarm transmission is identical to that of the primary transmission.

To set up the backup alarm transmission for the main CMS, proceed as follows:

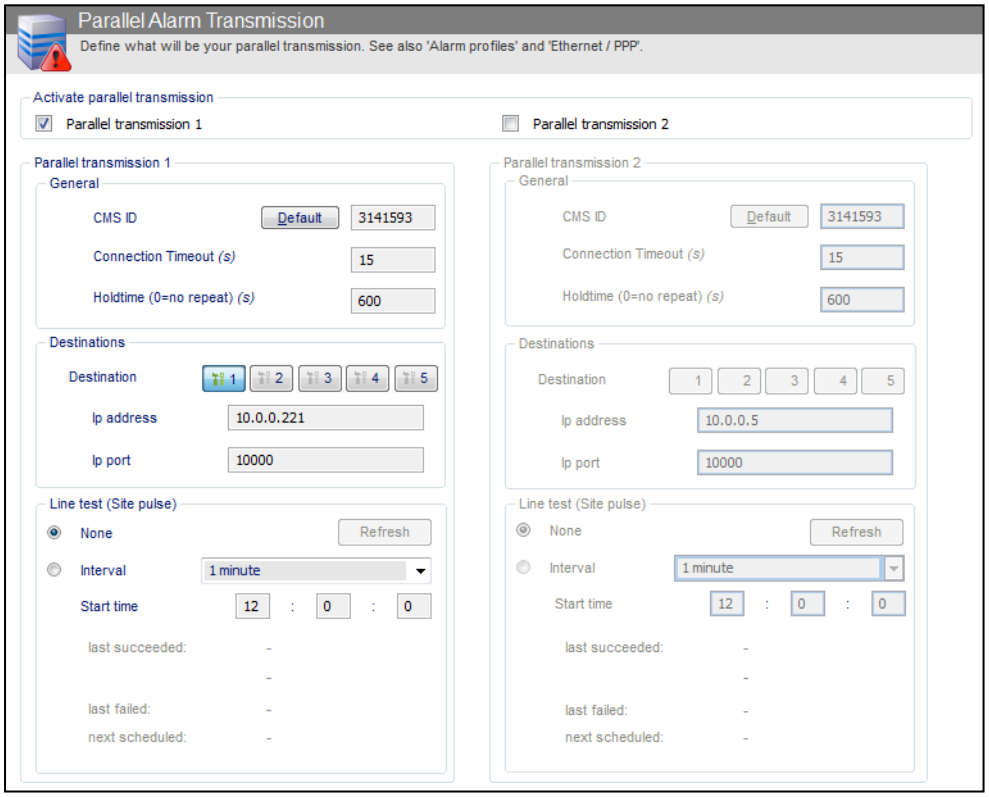
1. Under **Secondary Alarm Transmission**, provide the necessary information.
   For details, see *Primary Alarm Transmission Settings*.
2. Assign suitable alarm profiles for the following events (for details, see *Alarm Input Behaviour*):
   - 0033 – [SYST] – BACKUP LINE FAULT
   - 0035 – [SYST] – BACKUP LIFECHECK

4.6 Parallel Transmission Settings

Besides the primary and backup transmission to the main CMS, you can set up parallel transmission to two more parallel monitoring stations.

To set up parallel transmission, proceed as follows:

1. Choose **System > Behaviour > Alarm transmission > Parallel Alarm Transmission**.



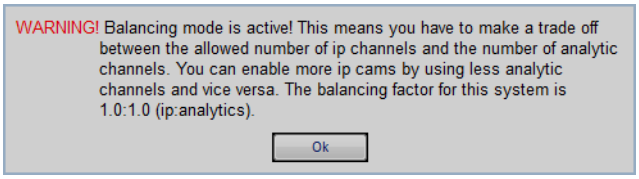
2. To activate parallel transmission, select the checkboxes for **Parallel transmission 1** and/or **2**.
3. Provide the required settings for each parallel transmission channel. Setup is similar to that of the primary transmission:
   - General settings such as identifiers and timeouts: see General Alarm Transmission Settings.
   - Destinations and life check (line test): see Primary Alarm Transmission Settings.
4. Click **Save**.
5. Assign suitable alarm profiles for the following events (for details, see *Alarm Input Behaviour*):
   - 0042 – [SYST] – PARTX1 LINE FAULT (parallel transmission path 1)
   - 0044 – [SYST] – PARTX1 LIFECHECK (parallel transmission path 1)
   - 0045 – [SYST] – PARTX2 LINE FAULT (parallel transmission path 2)
   - 0047 – [SYST] – PARTX2 LIFECHECK (parallel transmission path 2)

5 Using IP Cameras

5.1 Available IP Camera Channels

The number of available IP camera channels on your XO device depends on the device model, the system license, and on the number of installed IP channel licenses.

For the iFT model (not iFT-E), it also depends on the number of analytic channels in use: you trade in one video channel for one analytic channel (balancing mode). The system will display the following reminder when you open the **System** menu on an iFT device:



The eFT Series devices also use the balancing mode.

For each IP camera, you need an IP channel license. You can purchase such licenses in sets, and install them on your XO device using the Xchange2 Tool. You can always purchase extra sets of IP application licenses to add to your XO device, but you can never use more than the maximum allowed channels on your specific model. For more information, see *Licenses*.

When you add an IP camera to your XO device, the camera setup screen displays the number of remaining IP camera channels.

Note

For optimal performance: if you are using 12 (or higher) megapixel (MP) cameras on your XO device, then you can use max. 12 cameras @ 12 MP and max. 12 analytic applications (IntrusionTrace and/or LoiterTrace).

5.2 Prerequisites

Before setting up the camera in the XO client:

- Configure the IP camera network. For more information, see *IP Camera Network*.
- Select IP cameras that are compatible with the XO software. For details, see the following sections in this chapter, and the Supported IP Camera List (26742).
- Set up the IP camera itself: assign an IP address (in the same range as the IP camera network eth1), and set the date and time. You can adjust the time and date manually, synchronise the camera with an NTP protocol, or synchronise the camera with the XO device (in this case, set the camera's NTP port to UDP 123). Honeywell recommends to configure the IP camera using the manufacturer's web interface. Before connecting the camera to the XO device, reset the camera to the default values, except for the IP address (unless you are using the Generic Driver). However, some camera functions may require special settings in the camera web interface (see the Supported IP Camera List (26742)). In this case, a Technician user can connect to a camera's web interface directly from within the XO client and change the settings (from XO version 4.0). For details, see *Remote Access to IP Camera*. If you want to change the IP address only, you can use the IP camera discovery tool (if using the Honeywell or ONVIF driver). For details, see *Changing a Camera's IP Address Using the Discovery Tool*.

Setting up IP cameras in the XO client consists of the following steps:

- Setting up the basic parameters for communication and analytic resolution, and enabling the IP camera. This allows the XO device to establish a connection to the IP camera. For details, see *Enabling IP Cameras* . You can also use the IP camera discovery tool to detect available IP cameras. For details, see *IP Camera Discovery*.

- After enabling the camera: setting up the advanced parameters for live viewing, recording… For details, see *Camera Settings*.

5.3 Selecting Suitable IP Cameras

To select suitable IP cameras for use with your XO device, proceed as follows:

1. Check if the camera is listed in the *Supported IP Camera List* (26742). This document contains the list of supported IP cameras and IP video encoders for FastTrace 2X/2E, iFT Series, eFT Series, and iFT Gateway devices.
   Check the document for restrictions or special settings for using the camera.
2. If the camera is not listed, but the camera is ONVIF compliant, you can try and enable the camera using the ONVIF driver. In this case, check all required functionality carefully.
3. As a last resort, you can try and use the generic IP camera driver to enable the camera. For a list of known URLs that work with the generic IP camera driver, see the *Supported IP Camera List* (26742).



Note

If you want to use IP cameras or video encoders that are not listed in the supported IP camera list, Honeywell does not guarantee that the cameras will function on the XO devices. Honeywell does not guarantee correct operation because cameras may show unexpected behaviour with firmware versions not tested by Honeywell.

Honeywell does not offer any support for untested cameras.

5.4 Analytic Resolution for IP Cameras

The system uses the analytics stream from a camera for:

- the ADPRO analytic applications: IntrusionTrace, LoiterTrace, and Motion/Sabotage.
- camera calibration for the ADPRO analytic applications (3D and bounding boxes)
- the motion and sabotage detection
- postmotion detection
- generating quad images with alarms
- local video output (on a monitor directly connected to the XO device)
- recording, depending on the camera (for details, see the section on the management of IP video streams in the Supported IP Camera List (26742)).

The **default** analytics stream is CIF (352 x 288), or the next available higher resolution with a maximum of 640 x 480, with Qnormal quality, at 5 fps.

As of firmware version XO 4, you have more control over the aspect ratio and quality of the analytics stream:

- By specifying the stream to use for analytics, you can match the aspect ratio to that of the live and recorded views. In some cameras, your choice can be better than the default chosen by the system.
- By selecting a higher compression quality, the system may, in extreme circumstances, give fewer false alarms and more reliable detections because fewer compression artefacts are present. However, it must be stressed that extensive testing shows that the default is typically sufficient, and consumes less bandwidth.
- The resolution of the selected stream does not affect analytics performance.

  When you enable an IP camera, you can select:

- The default analytics stream: CIF/SIF or the next available higher resolution with a maximum of 640 x 480, with Qnormal quality, at 5 fps.
- Or, you can select a specific aspect ratio (4:3, 16:9, or 16:10). If you select an aspect ratio, you can also choose to use a low- or high-resolution image.

- If you choose low resolution (recommended), the system will select the video stream with the selected aspect ratio and the lowest available resolution near to CIF/SIF, with a maximum of 640 x 480, and minimum horizontal resolution of 352 pixels.

  For example: 480 x 360 for 4:3; or 480 x 270 for 16:9.

- If you choose high resolution, the system will select the video stream with the selected aspect ratio and the highest available resolution, but also with a maximum of 640 x 480.

  For example: 640 x 480 for 4:3; or 640 x 360 for 16:9.

If the camera does not supply a video stream that meets your criteria, the system will issue a warning message and automatically revert to the default analytics stream.



Firmware versions below XO 4 always use the default analytics stream.

Selecting a high-resolution analytics stream does not necessarily improve detection, because the analytic engines do not require high-resolution images for reliable detection. They will reduce the high-resolution images to CIF format before processing. Therefore, Honeywell recommends to select a low-resolution stream. However, if you absolutely require a higher resolution for live viewing on a monitor or for recording, then you can select a high-resolution stream. Remember that this may reduce system performance.

Caution!

If you upgrade your device from a version below XO 4, and you change the aspect ratio of the analytics stream for a camera, then **you have to make new calibration images and recalibrate that camera**.

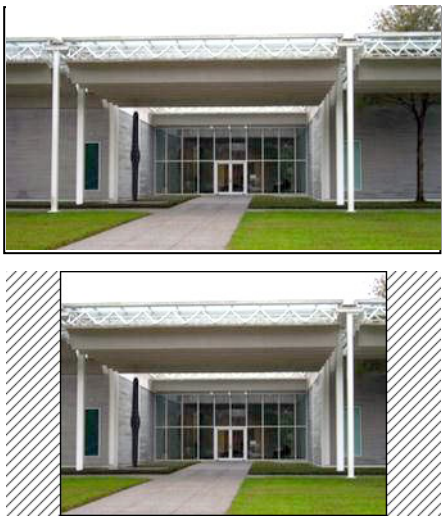
Note

You can only choose the analytics stream aspect ratio and resolution **before you enable** the IP camera. If you want to change the settings, you have to disable the camera first; adjust the settings; and then enable the camera again.

5.5 Streams with Different Aspect Ratios

Ideally, the aspect ratio of the low-resolution analytics stream is identical to the aspect ratio of the high-resolution live/recording streams. However, wide-screen cameras may not offer low-resolution streams with the same aspect ratio.

For example, a camera may offer low-resolution images with aspect ratio 4:3, and high-resolution images with aspect ratio 16:9. Typically, a 4:3 camera image has a narrower field of view than the 16:9 image: the edges are cut off. However, some cameras take the wide image and squeeze it into a narrow image. This results in a full field of view in the 4:3 image, but the image is distorted.

16:9 image	16:9 image
	
4:3 image, cropped: edges are cut off, narrower field of view, but image is not distorted	4:3 image, squeezed: full field of view (no cut-off edges), but distorted image

Both cases have pros and cons, and require careful calibration:

- In a cropped image, the area available for detection is smaller (narrower field of view). However, detection is accurate with careful 3D calibration. Bounding box calibration makes sure that bounding boxes appear correctly on images with all aspect ratios.

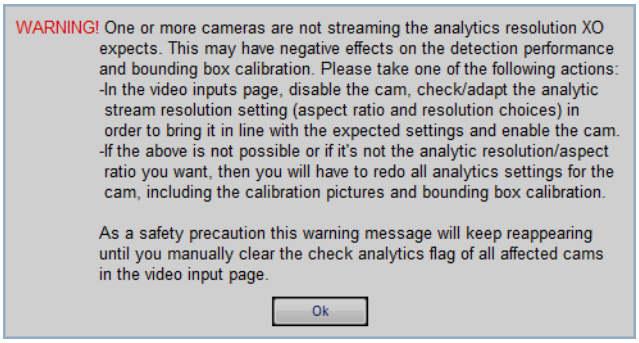
  Keep in mind that, upon an alarm from a PIR detector or from another input, the system produces quad/live alarm images from the cropped stream. When using such cameras, make sure to set up the system (PIR detector FOV, double-knock scenario…) from the analytics stream.

- In a squeezed image, the area available for detection is larger, but the slight distortion of the image will influence the analytics behaviour. Take extra care of 3D and bounding box calibration, and test the detection parameters thoroughly through walk tests.

5.6 Troubleshooting Analytic Resolutions

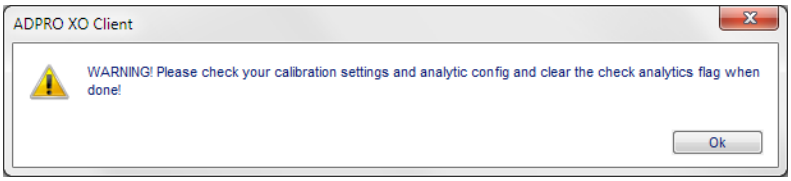
The system performs a number of checks to make sure that your analytics applications work as expected. Issues may occur if there is a mismatch between the analytics stream and the calibration pictures for an IP camera. If the system finds a mismatch, the following warning messages may appear:

- The message One or more cameras are not streaming the analytic resolution XO expects… will appear each time you log on to the XO client, as long as there is a mismatch between the analytics stream and the calibration pictures for at least one IP camera.



- The message Please check your calibration settings… will appear after you disable and then enable a camera

- with a different analytic resolution.



Possible mismatches are:

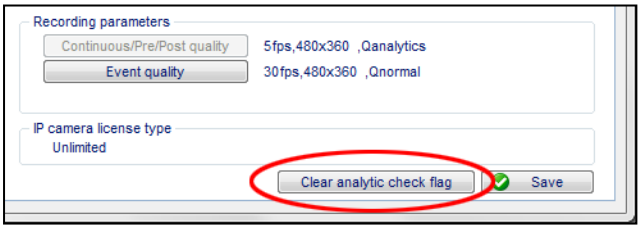
- The aspect ratio of the calibration images is different from the aspect ratio of the analytics stream. This may happen when you had made calibration images before, then changed the analytics stream.

  For example: you had made calibration images when using the default analytics stream, and then disabled and enabled the camera again choosing a 16:9 analytics stream. Or, you switched between corridor and normal modes.

- The aspect ratio of the calibration images and the analytics stream is the same, but the quality is different. For example, you had made calibration images at 480 x 360 (4:3, low resolution), but you have changed the analytics stream to 640 x 480 (4:3, high resolution).

To solve issues with analytic resolutions for a camera, proceed as follows:

1. Open the camera setup window: choose **System** > **Connections** > **Video Inputs**, and then select the desired camera. If there is an issue with the camera, the **Clear analytic check flag** button appears at the bottom of the window.



2. Compare the analytics stream resolution with the calibration pictures resolution:
   - The analytics stream resolution is displayed in the Default analytic resolution box.
   - The calibration pictures resolution is displayed in the calibration window: click Camera calibration and check the resolution under the thumbnails.
3. Proceed as follows:
   - If you do not need to keep the current analytics stream: disable the camera, choose an aspect ratio and quality for the analytics stream that is in line with the existing calibration pictures, and then enable the camera again.
   - If you want to keep the current analytics stream: make new calibration pictures and recalibrate the front and back of the scene. Also perform bounding box calibration, if necessary. For details, see *Camera Calibration*.

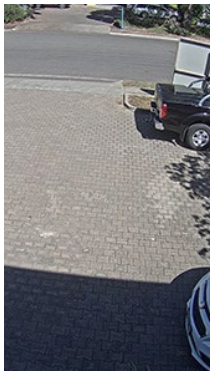
     Check also the analytics application settings (IntrusionTrace, LoiterTrace, and Motion/Sabotage) and perform walk tests to confirm detection.
4. When finished, click the **Clear analytic check flag** button at the bottom of the camera setup window.
5. Click **Save**.

5.7 Using Cameras in Corridor Mode

Software version XO 4.0 and above supports corridor mode (on cameras that support this feature), where the camera image is taller than wide. In hallways and corridors, a larger part of the camera image is useful for analytics when using corridor more. In addition, it reduces the dead zone beneath the camera.



Camera image in normal mode



Camera image in corridor mode, showing more of the foreground

If you have used a camera with analytics in normal mode before, you have to make new calibration pictures and recalibrate the scene when you switch to corridor mode.

Caution!

If you are using analytics in corridor mode, remember that corridor mode affects the maximum horizontal field of view (FOV) because fewer pixels are available horizontally. For details, see the documentation of the analytics application.

To use a camera in corridor mode, proceed as follows:

1. For a camera that is already in use: disable the camera in the XO client.
2. Use the camera's web interface to set the camera in corridor mode. Consult the camera manufacturer's documentation for instructions.
3. Enable the camera.
4. Configure the recording streams (event quality, and continuous/pre/post event quality if available).

Note

When selecting resolutions for a camera in corridor mode, the system displays the available options in the normal way: for example, it will display 640 x 480 (and not 480 x 640). However, the information bar in the **Live Video** window will show the selected resolution in corridor mode: for example, 360 x 480 (and not 480 x 360).

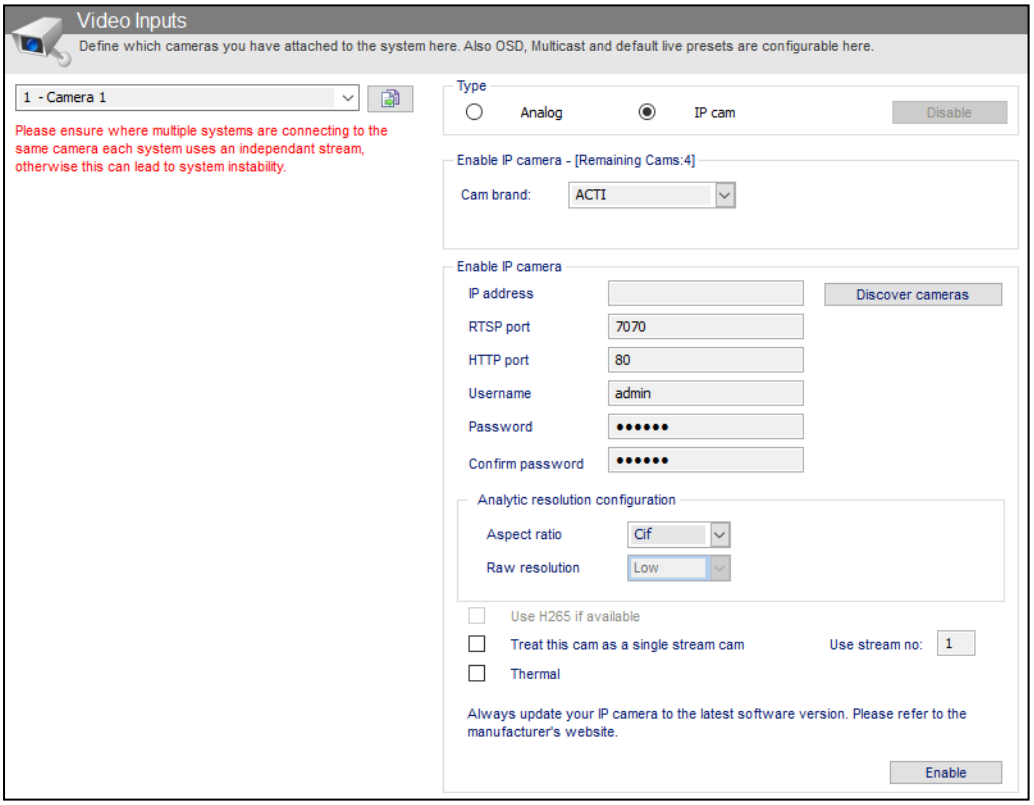
5. Perform 3D calibration: make new calibration pictures, and recalibrate the front and back of the scene.
6. If the camera uses streams in different aspect ratios, also perform bounding box calibration.
7. For analytics (Motion/Sabotage, IntrusionTrace, LoiterTrace…): redraw the detection zones.
8. Check the detection parameters.
9. Redraw mask zones.
10. Perform walk tests to confirm detection.

5.8 Enabling IP Cameras

You can add an IP camera manually if you know its IP address, or you can use the discovery tool to search the network for all IP cameras that the XO device can connect to. You can then add the found IP cameras without entering the IP address yourself. For details, see *IP Camera Discovery*.
The procedure below describes the manual method.

To enable an IP camera manually, proceed as follows:

1. Choose **System** > **Connections** > **Video Inputs**.
2. Choose a free camera number from the list.
   The system indicates camera numbers that are already in use by an asterisk *.
3. Under **Type**, click **IP cam**.



The **Remaining Cams** box displays the number of remaining IP camera channels on the XO device.

4. Provide the following information:

Item	Description
Cam brand	Select the camera's brand driver, the ONVIF driver, or the generic driver. For details on the correct driver, see the *Supported IP Camera List (26742)*. The system automatically fills in a number of settings based on the brand's typical default settings. The following options appear if HONEYWELL or ONVIF PROFILE S driver is selected: • **ONVIF-S**: this version of the driver supports only ONVIF Profile S • **ONVIF-S/ONVIF-T**: this version of the driver supports both ONVIF Profile S and Profile T. **Note** XO 5.0 Client software supports cameras with ONVIF Profile S/T drivers. All the newly approved cameras and future cameras support ONVIF Profile S/T drivers. ONVIF Profile S is supported for backward compatibility. Only the ONVIF Profile S/T drivers support H265, and it is the preferred driver for new cameras. If you select the ONVIF-S/ONVIF-T option, the **Use H265 if available** option is enabled. Less bandwidth is consumed if the camera has H265 module. Check the camera's technical specifications for the correct driver version. • Select Generic Driver 1.0 for a generic-driver camera. Selecting the Decode high-resolution stream checkbox increases the resolution for up to 2 MP. **Note** The XO Client Software supports higher resolution/framerate for the cameras which use generic drivers. Most IP cameras have two streams with one video channel and one analytic channel. Some generic driver cameras have a single stream with 1920 x 1080P resolution. The XO 5.0 Client software has been enhanced to use this single stream as both analytic stream and video stream. For a generic driver camera which has single-stream video input with a frame-rate between 5 and 30 FPS (Frames Per Second), up to 10 FPS can be used as an analytic stream.
Channel selection	Only available for certain drivers. If the driver supports multi-lens or multi-channel devices (such as the Honeywell HQA Performance Series DVRs), the following options may be available: • **Single or IP cam**: select this option for a single-lens or single-channel device (a normal IP camera). • **Multi or HQA**: select this option for a multi-lens or multi-channel device. If you have selected this option, then also select the desired lens or channel that you want to enable.
IP address	Type the camera's IP address.
RTSP port	Type the RTSP communication port number for the camera.
HTTP port	Type the HTTP communication port number for the camera.
Username	Type the username for logging on to the camera.
Password	Type the password for logging on to the camera.
Confirm password	Type the password again.

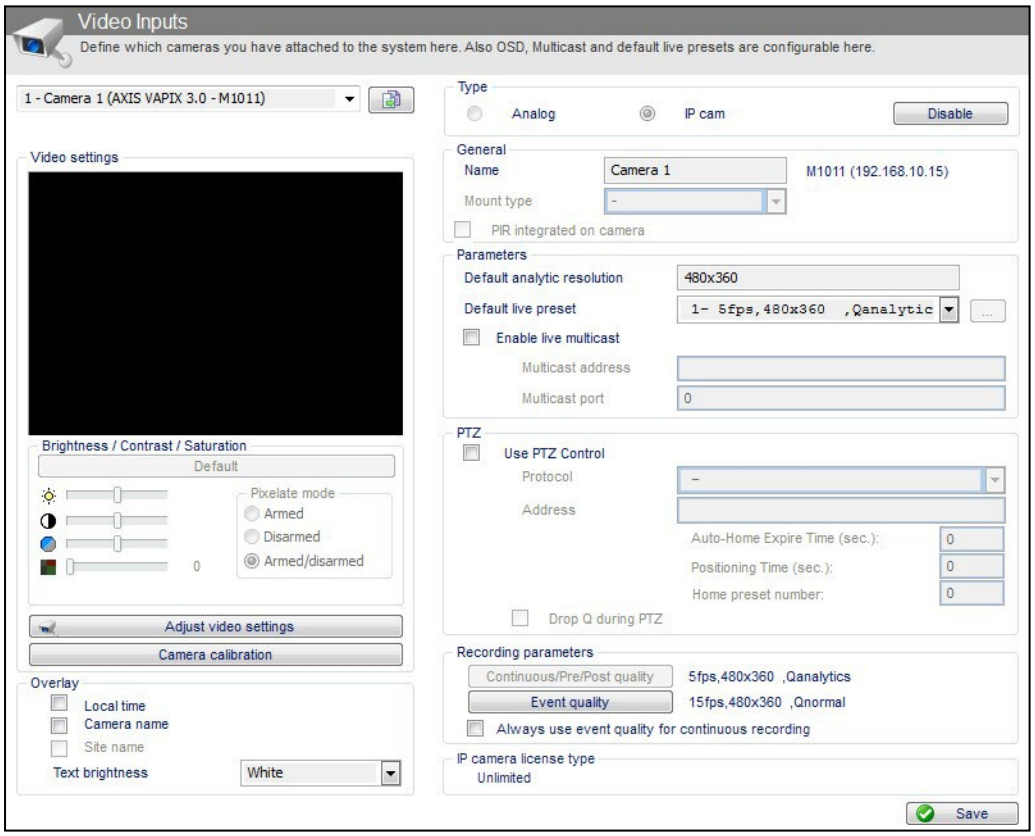
Item	Description
Aspect ratio	Select the desired aspect ratio for the analytics stream. You can choose: • **CIF or SIF**: select one of these options for the default settings. You cannot select a raw resolution with CIF or SIF. • **4:3, 16:9, or 16:10**: select one of these options to match the aspect ratio of the analytics stream with that of the live/recording streams.
Raw resolution	Only available if you use a different aspect ratio than the default CIF/SIF: • **Low** (recommended): the system will select the video stream with the selected aspect ratio and the lowest available resolution near to CIF/SIF, and with a maximum of 640 x 480. • **High**: the system will select the video stream with the selected aspect ratio and the • highest available resolution, with a maximum of 640 x 480.
Use H265 if available	Only available for specific camera drivers: select this checkbox if you want to use H.265 video compression with the camera.
Treat this cam as a single stream cam	You are not allowed to draw any other streams from the IP cameras than those destined for the XO device. If you need to draw other streams from the IP camera for any reason, select the checkbox to use the single stream mode. Using only one stream limits functionality: the XO device will only use the analytics stream.
Use stream no.	For single-stream camera only. Typically, the analytics stream from a camera is stream 1. If the camera uses a different stream, type the stream number here.
Thermal	Select this checkbox to enable the camera as a thermal camera.



Note

As soon as you enable the camera, the settings above are no longer accessible. If you need to change the settings, you have to disable the camera first, change the settings, and then enable the camera again.

5. Click **Enable** to start using the IP camera. The system connects to the camera, and the camera setup window appears:



> **Note**
>
> You can continue working while the system enables the camera in the background. Select the next camera in the camera list.

6. To complete the setup, continue with *Camera Settings*.

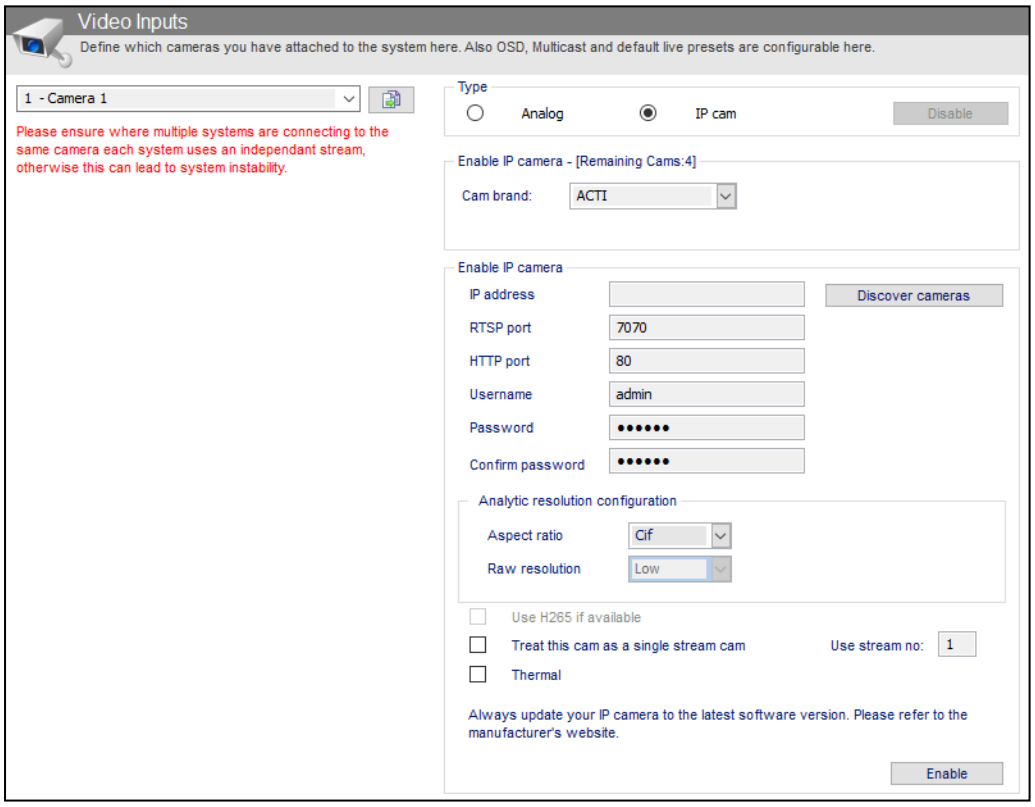
5.9 IP Camera Discovery

The IP camera discovery tool allows you to discover all IP cameras in the network, and to add them easily without entering the IP address manually.

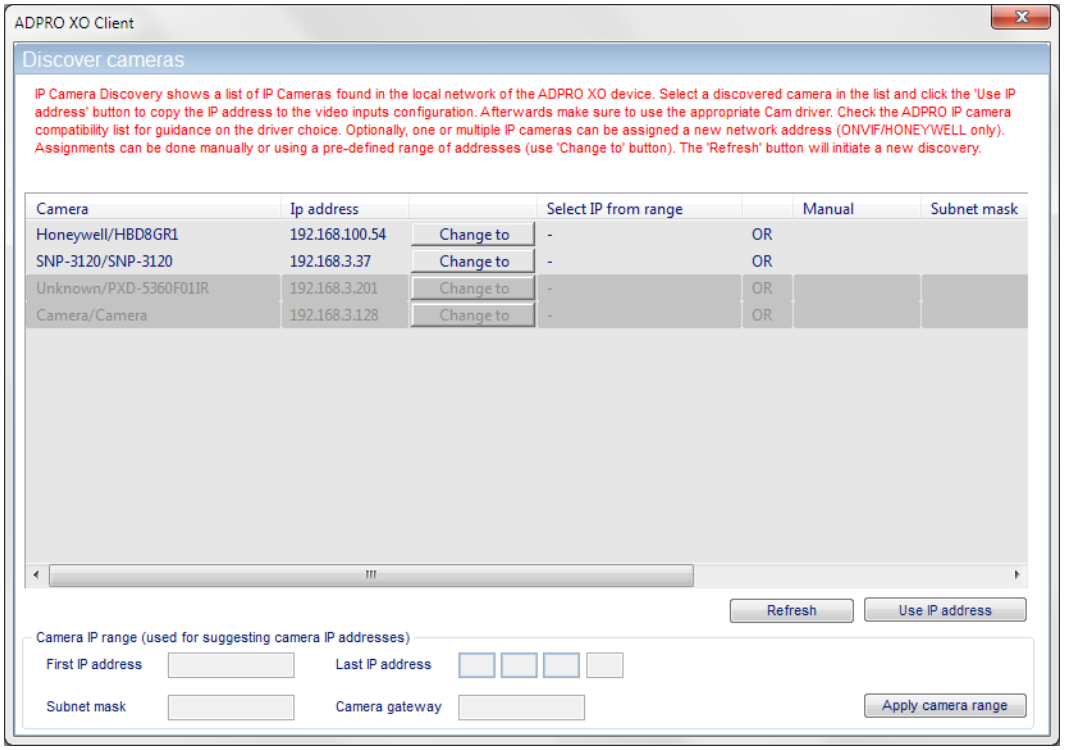
To discover IP cameras, proceed as follows:

1. Choose **System** > **Connections** > **Video Inputs**.
2. Choose a free camera number from the list.
   The system indicates camera numbers that are already in use by an asterisk *.

3. Under **Type**, click **IP cam**.

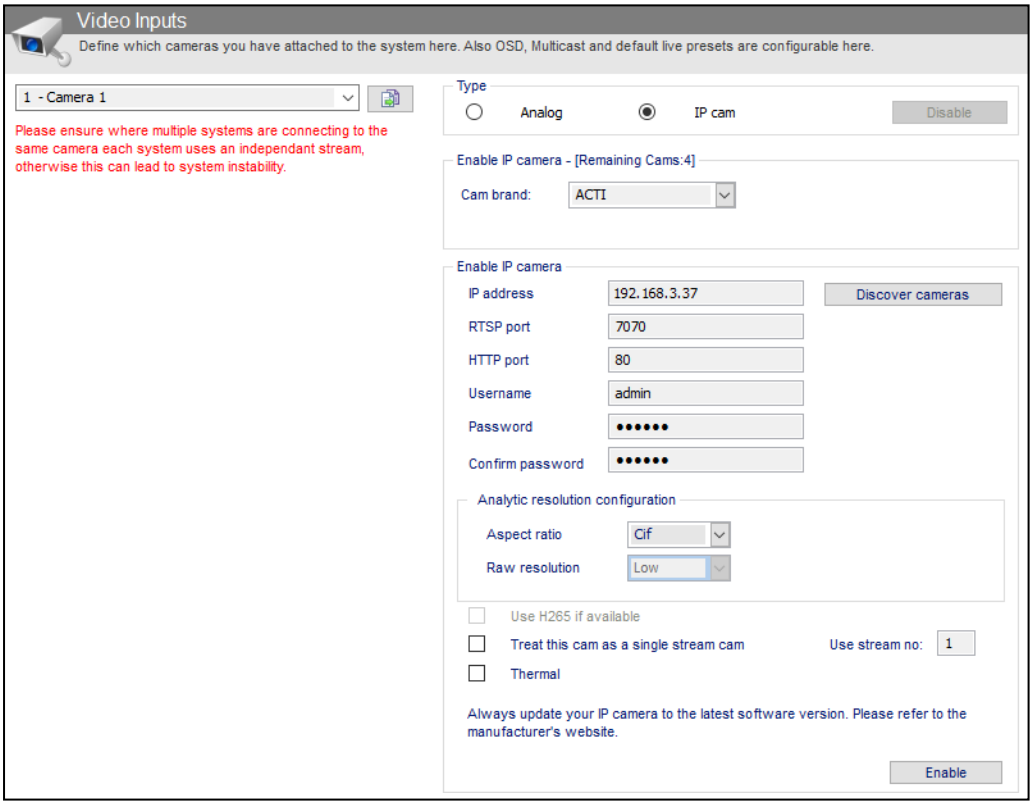


4. Click **Discover cameras** (next to **IP address**). The system starts searching the camera network for IP cameras. When finished, the results appear:



IP cameras that are already enabled on this XO device appear in dark grey; you cannot select or change them. Available cameras appear in light grey.

5. To add an available IP camera to the XO device, click the camera in the list, and then click **Use IP address**. The system returns to the video inputs screen and fills in the camera's IP address:



6. Select the camera brand and fill in all other information as required, and then click **Enable**. For details, see *Enabling IP Cameras*.
7. To complete the setup, continue with *Camera Settings*.

5.10 Changing a Camera's IP Address Using the Discovery Tool

When using the discover tool, you can change the IP address of a discovered camera.

Note

Changing a camera's IP address is only possible for cameras using the Honeywell or ONVIF driver.

The following options exist:

- If you want to change the address of only one camera, you can enter the new IP address manually.
- If you want to change the address of a range of cameras, you can define a range of IP addresses and select the desired address from a list.

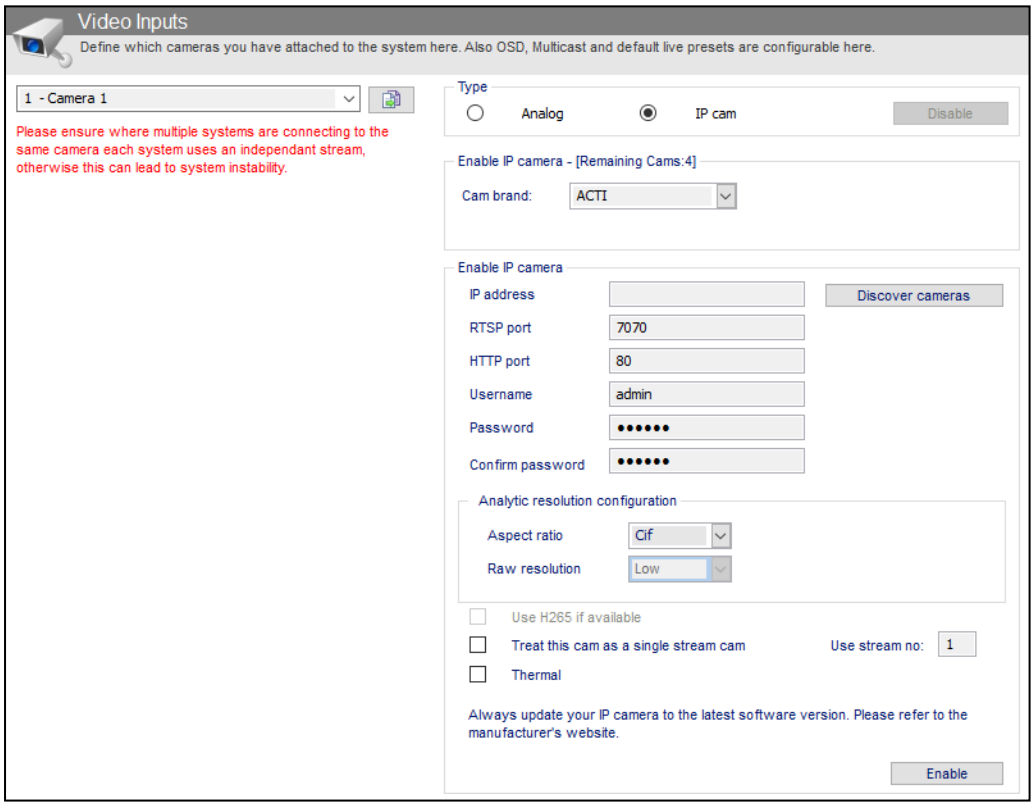
Both methods are described in detail further below.

5.10.1 Changing an IP Address for a Single Camera

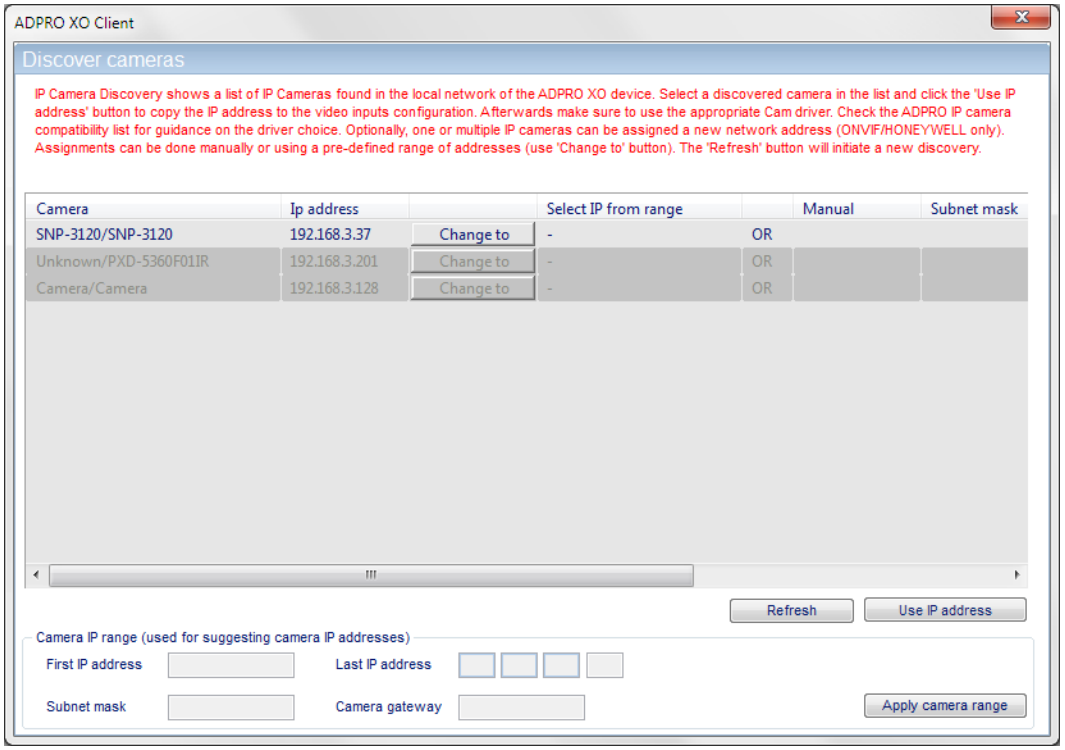
To change a camera's IP address manually using the discovery tool, proceed as follows:

1. Choose **System** > **Connections** > **Video Inputs**.
2. Choose a free camera number from the list. If you want to change the IP address of a currently enabled camera, select the desired camera and disable it.

3. Under **Type**, click **IP cam**.



4. Click **Discover cameras** (next to **IP address**). The system starts searching the network for IP cameras. When finished, the results appear:

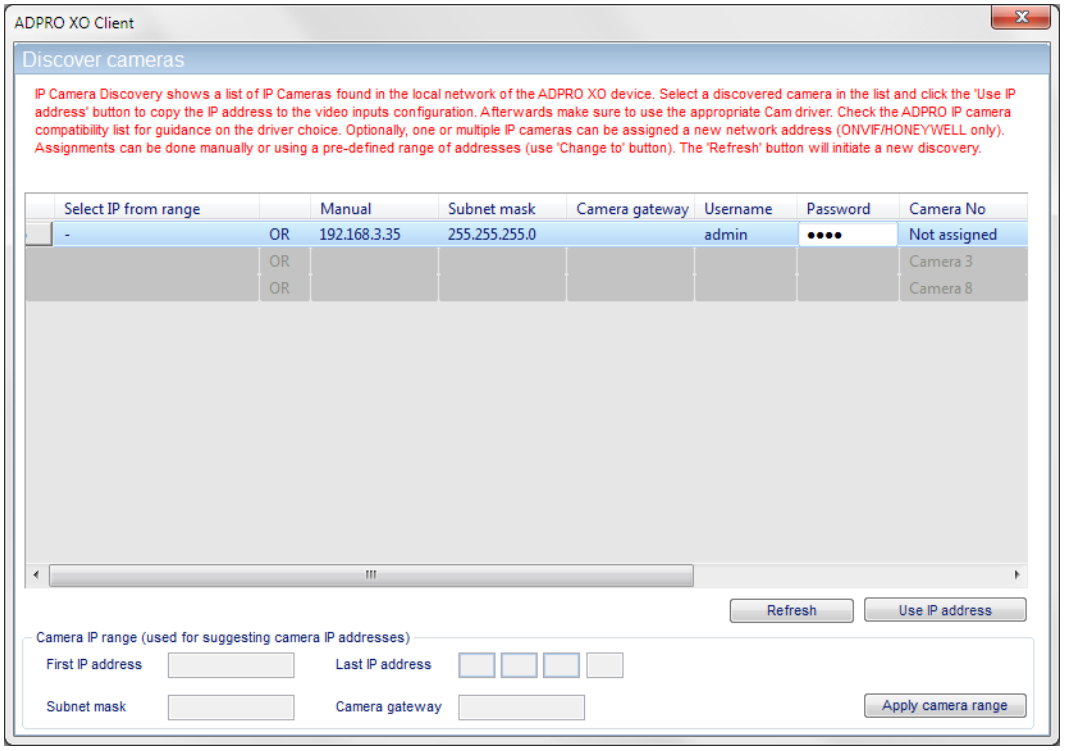


IP cameras that are enabled on this XO device appear in dark grey; you cannot select or change them. Available cameras appear in light grey.

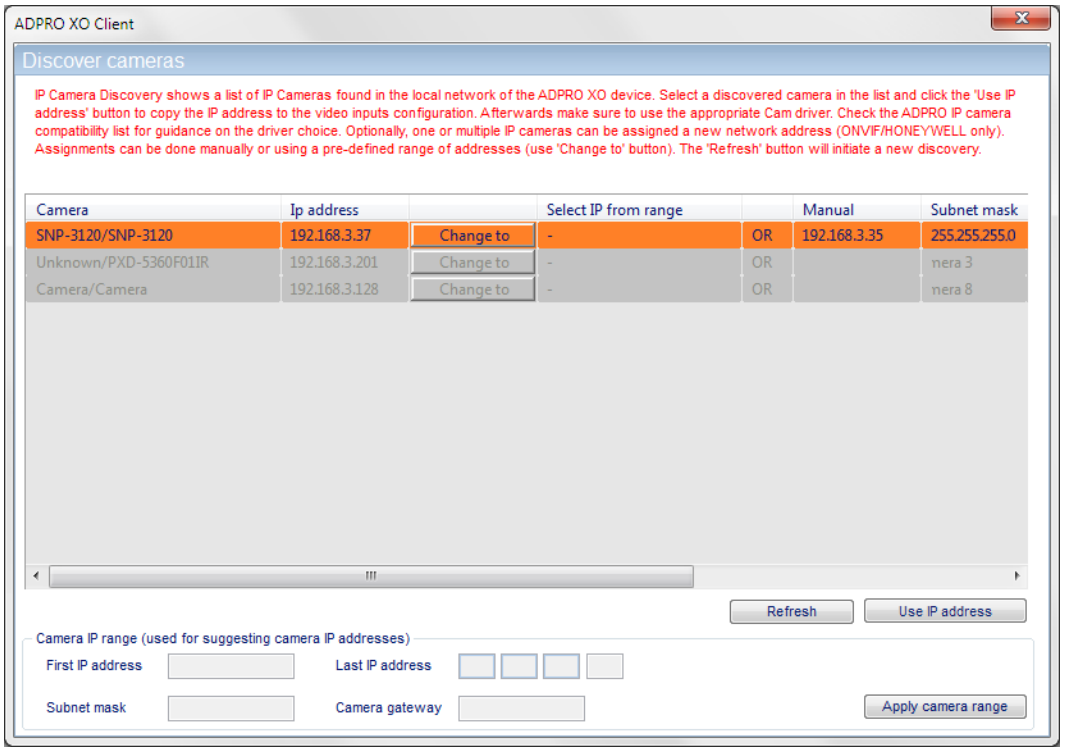
5. In the camera list, provide the following information in the row of the camera that you want to change. Scroll to the right to see more columns.

Item	Description
Manual	Type the new IP address for the camera. Make sure that this IP address is not in use.
Subnet mask	Type the subnet mask for the camera network.
Camera gateway	Optional: type the camera network gateway address.
Username	Type the username for logging on to the camera.
Password	Type the password for logging on to the camera.

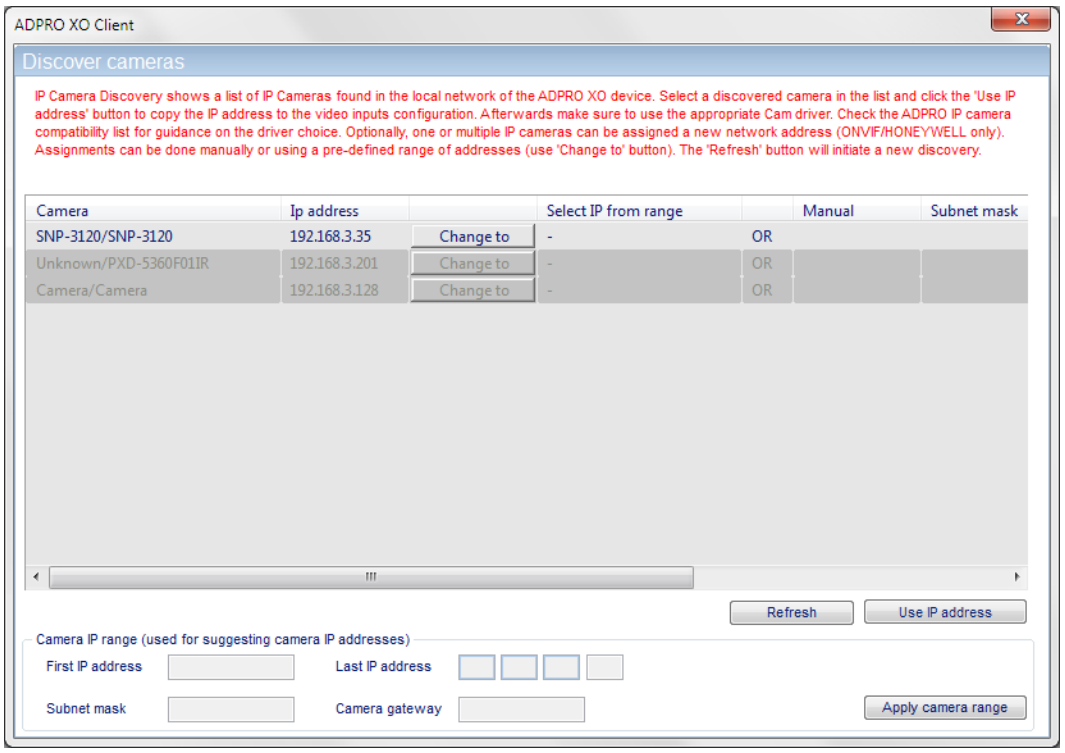
Below is an example of a filled-in screen:



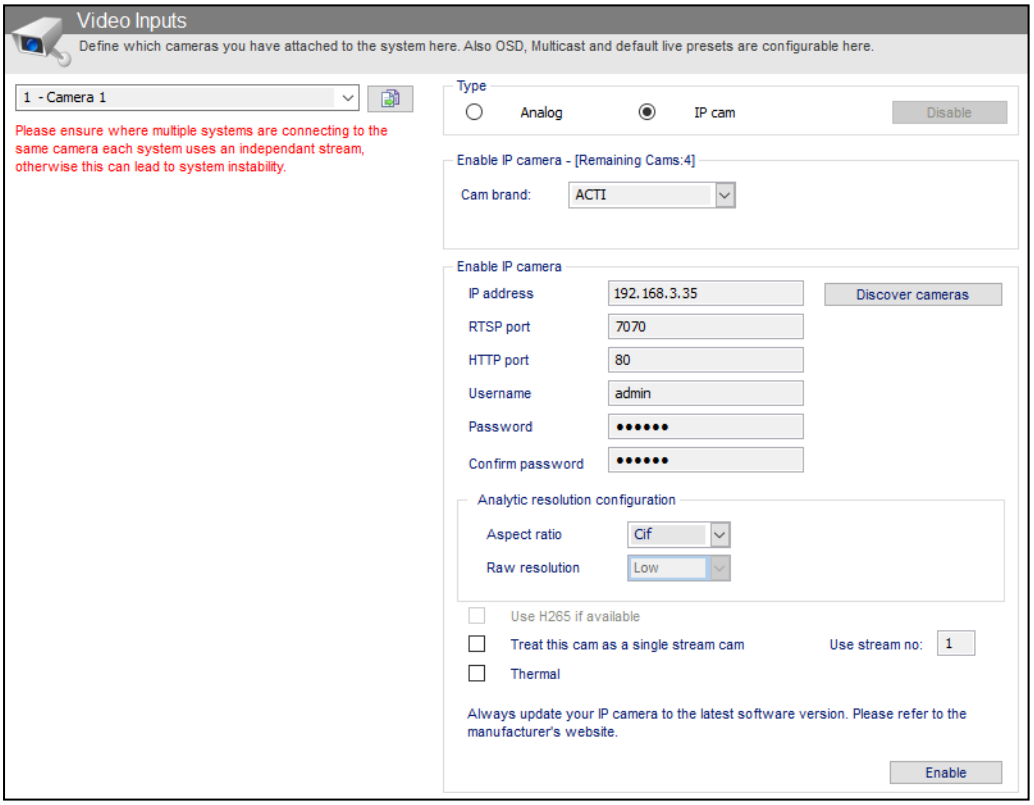
6. Scroll back to the left and click **Change to**. The system will change the camera's IP address. When finished, the following screen appears:



7. To update the camera list and reflect the changes, click **Search**. When finished, the **Ip address** column displays the new IP address:



8. If you want to add the IP camera to the XO device, click the camera in the list, and then click **Use IP address**. The system returns to the video inputs screen and fills in the camera's new IP address:



9. Select the camera driver (**ONVIF Profile S** or **Honeywell**) and fill in all other information as required, and then click **Enable**. For details, see *Enabling IP Cameras*.

> **Note**
>
> Changing a camera's IP address is only possible for cameras using the Honeywell or ONVIF driver.

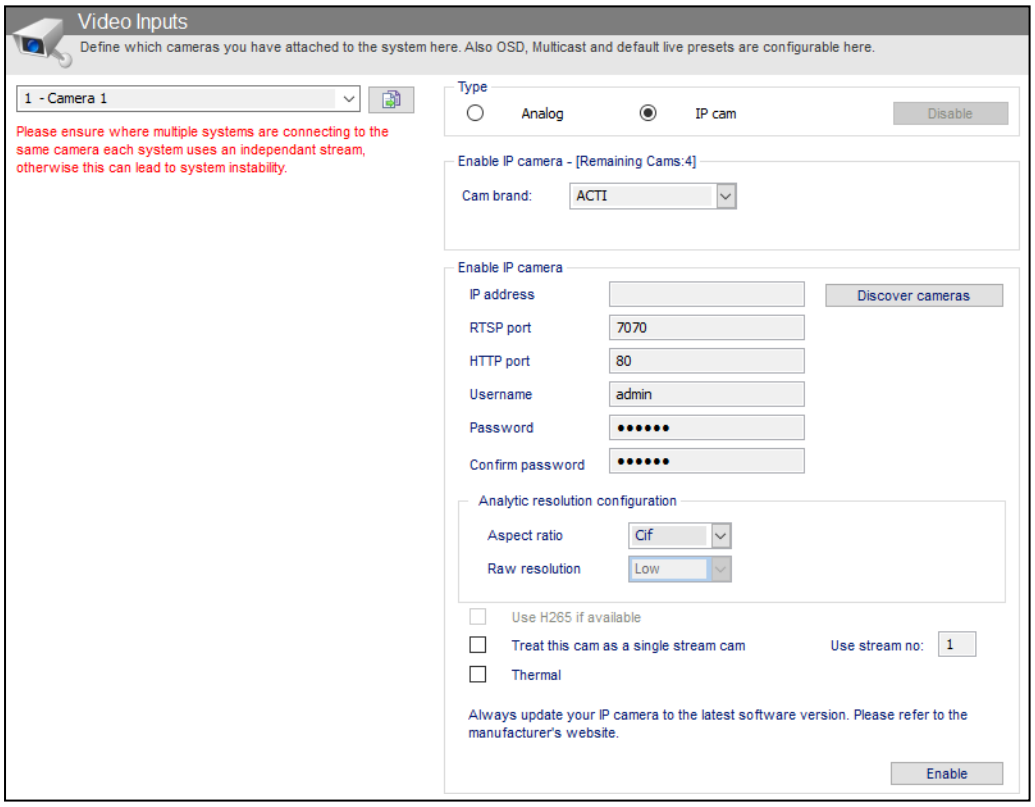
10. To complete the setup, continue with *Camera Settings*.

5.10.2 Changing Multiple IP Addresses Using a Range

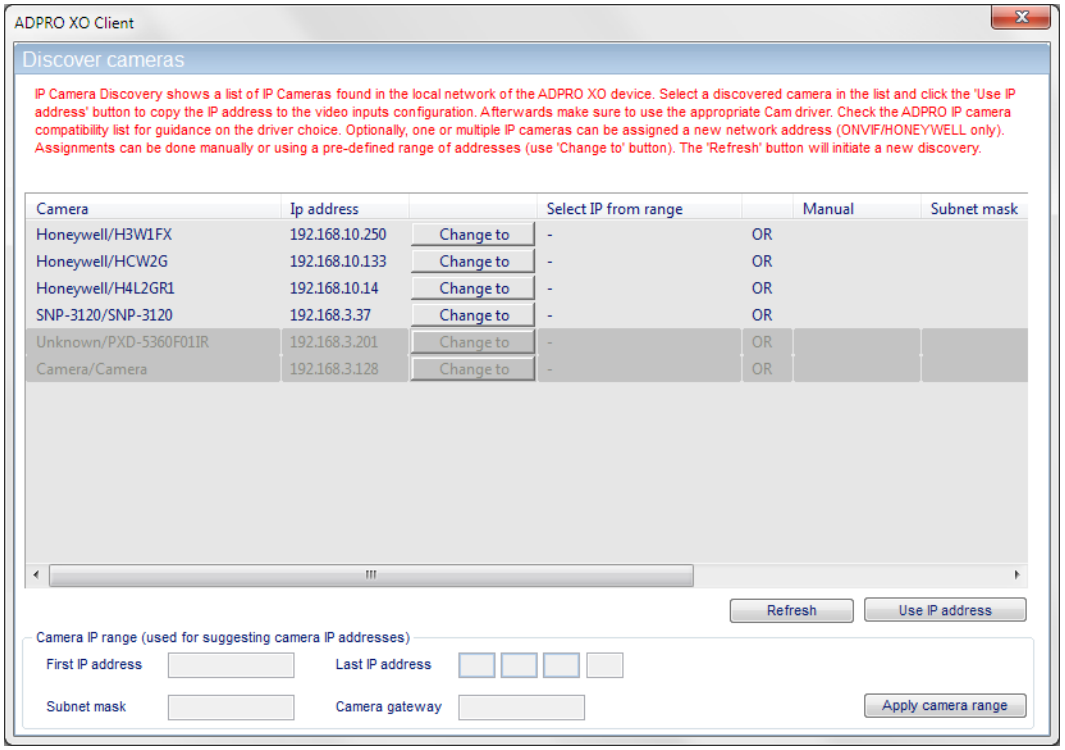
To change a range of camera's IP addresses using the discovery tool, proceed as follows:

1. Choose **System** > **Connections** > **Video Inputs**.
2. Choose a free camera number from the list. If you want to change the IP address of a currently enabled camera, select the desired camera and disable it.

3. Under **Type**, click **IP cam**.



4. Click **Discover cameras** (next to **IP address**). The system starts searching the camera network for IP cameras. When finished, the results appear:

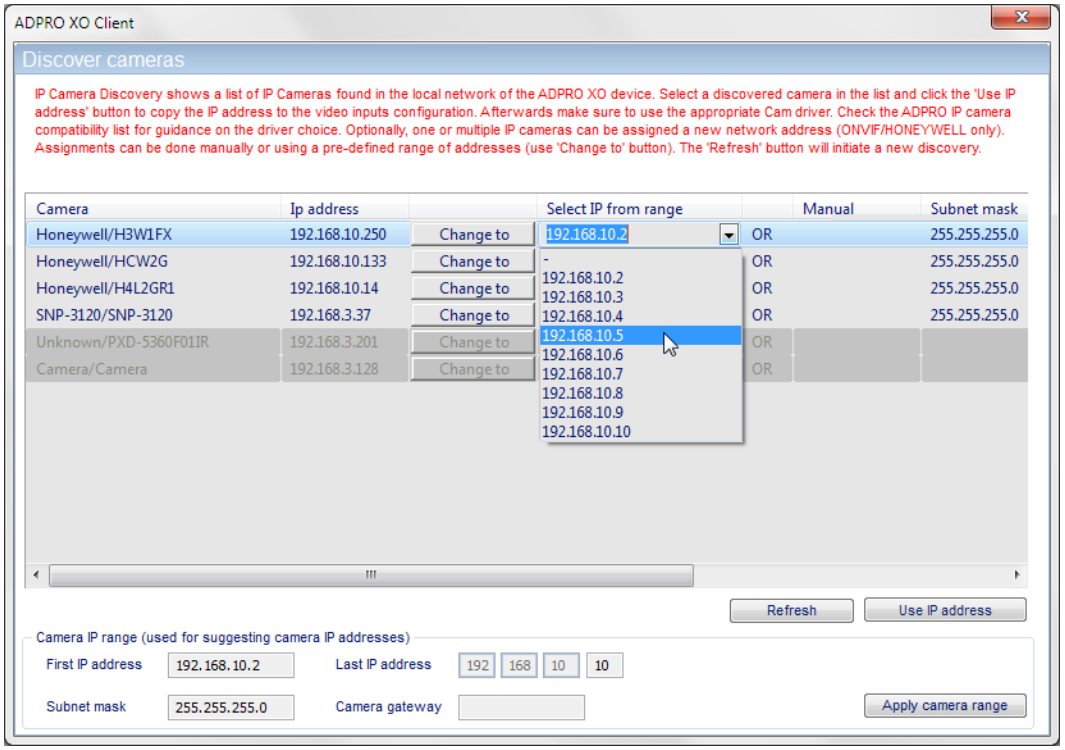


IP cameras that are enabled on this XO device appear in dark grey; you cannot select or change them. Available cameras appear in light grey.

5. If you want to select the new IP address from a range, define the desired IP address range in the boxes under the camera list. Provide the following information:

Item	Description
First IP address	Type the first IP address in the desired range.
Last IP address	Type the last IP address in the desired range. Note that the system automatically copies what you filled in for **First IP address**; and you can only change the last part of the IP address.
Subnet mask	Type the subnet mask of the camera network.
Camera gateway	Optional: type the camera network gateway address.

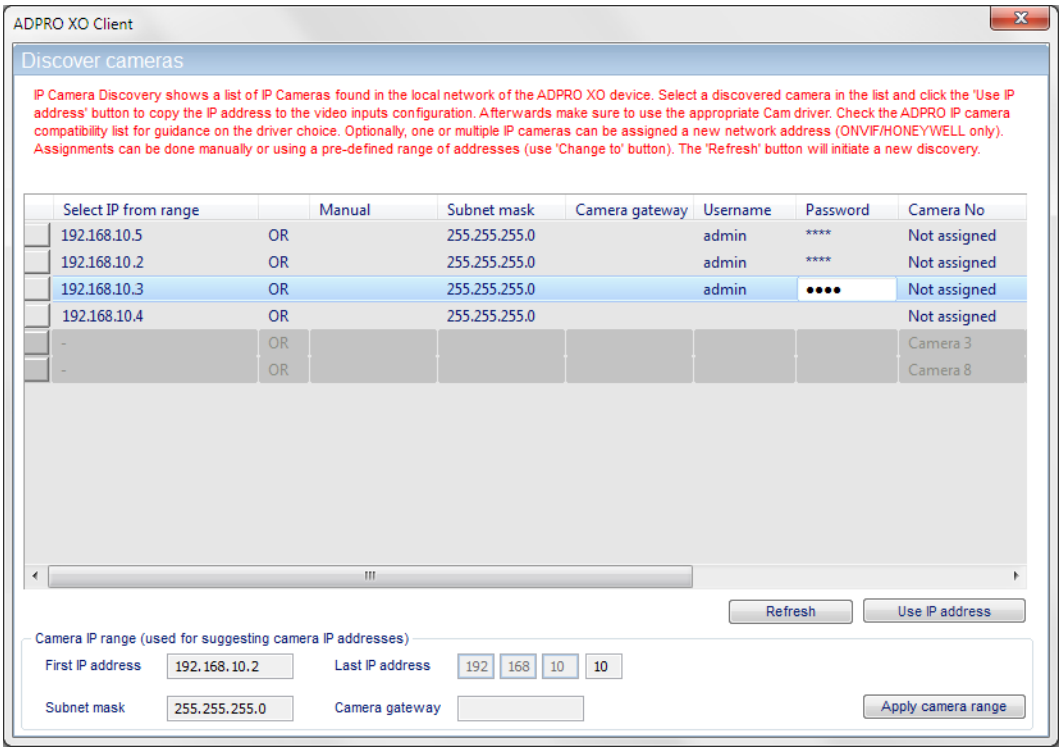
6. To apply the IP address range, click **Apply camera range**.
The system automatically assigns the range of IP addresses for the available cameras, from top to bottom. It also copies the subnet mask and camera gateway (if provided) to the cameras.
7. If you want to change the automatic assignment, select the desired IP address from the list for each camera:



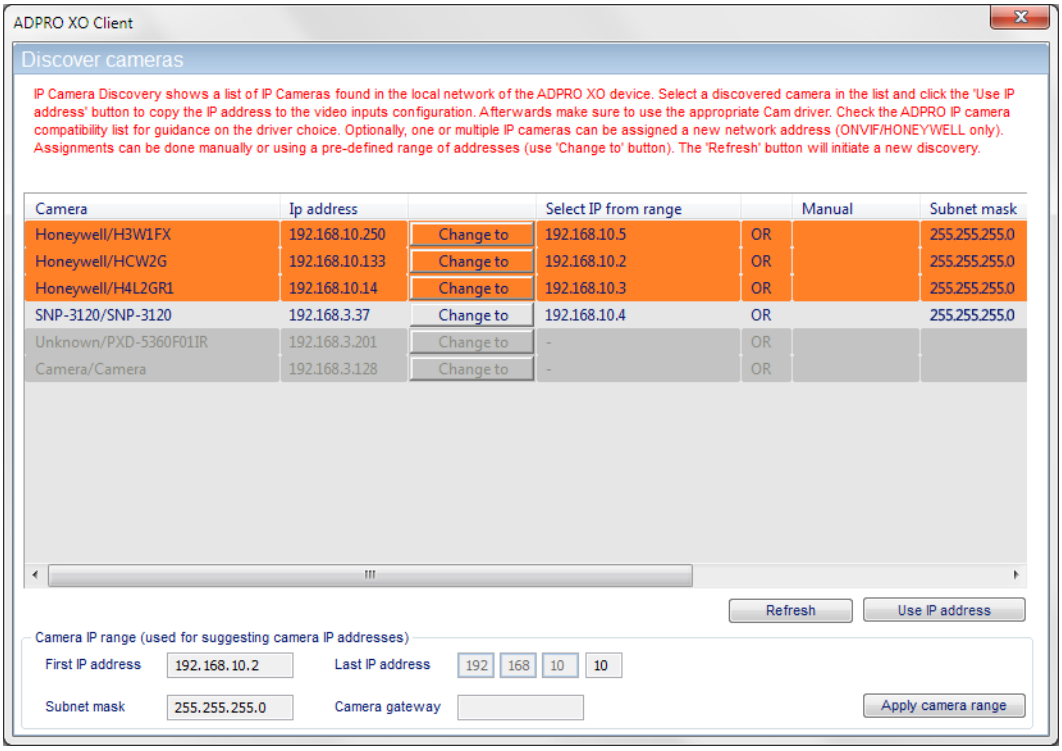
8. In the camera list, provide the following information in the row of each camera that you want to change. Scroll to the right to see more columns:

Item	Description
Username	Type the username for logging on to the camera.
Password	Type the password for logging on to the camera.

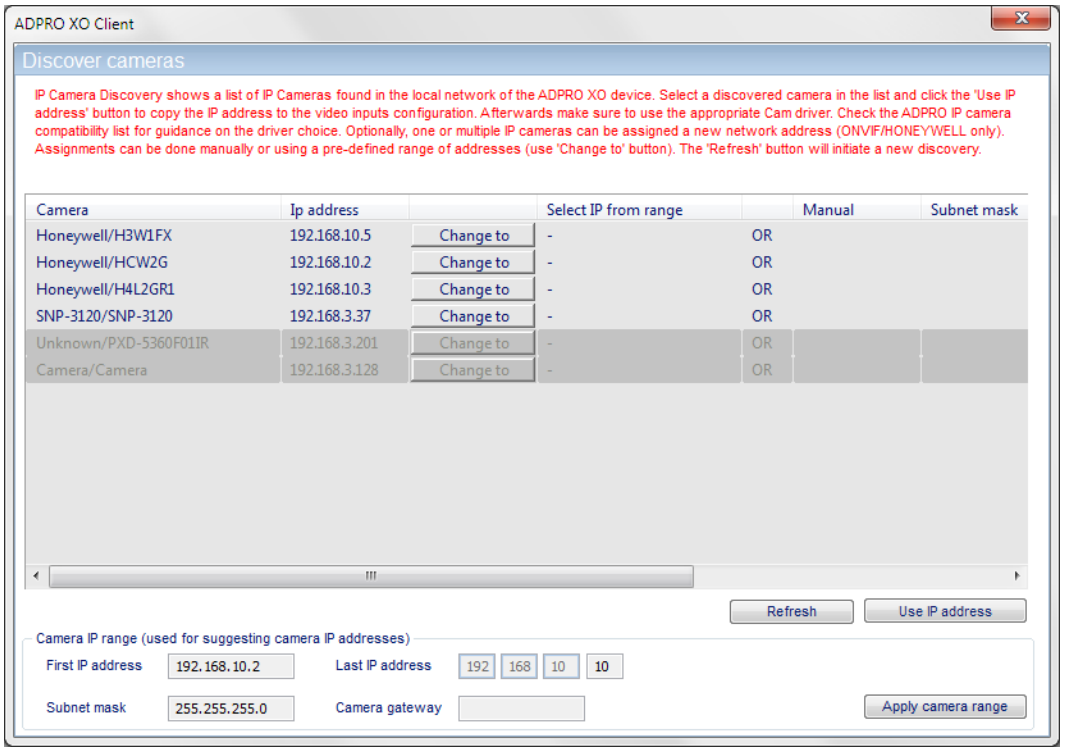
Below is an example of a filled-in screen:



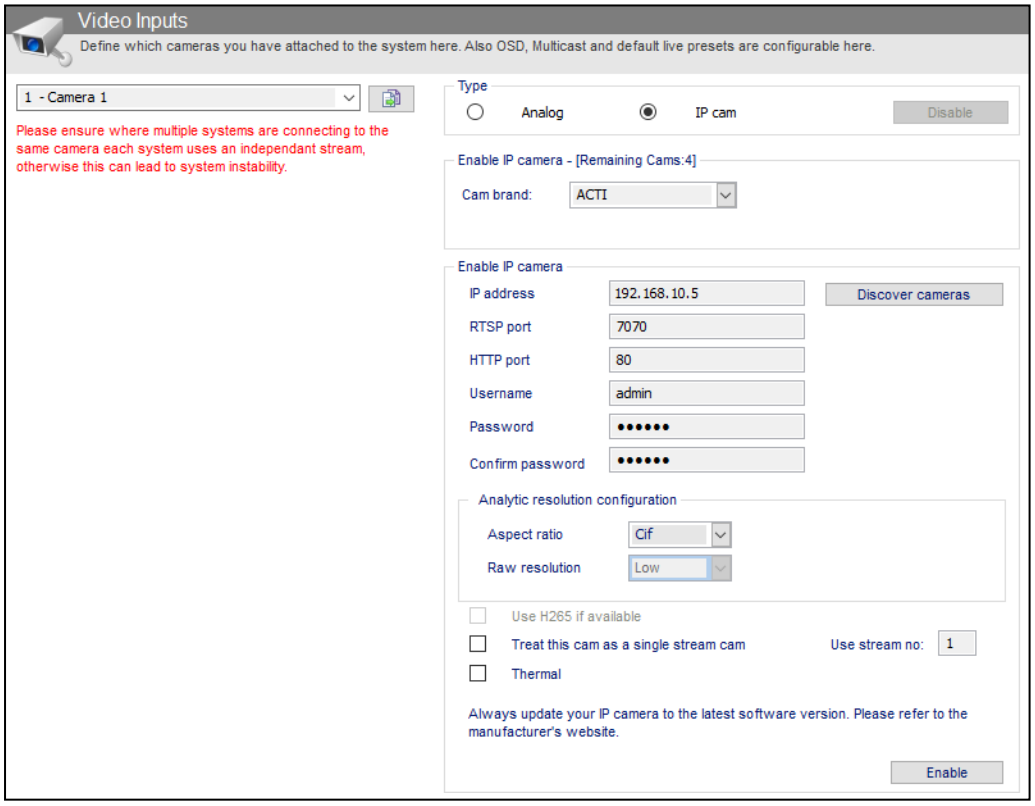
9. Scroll back to the left and click **Change to** for each camera that you want to change. The system will change the cameras' IP addresses. When finished, the following screen appears:



10. To update the camera list and reflect the changes, click **Refresh**. When finished, the **Ip address** column displays the new IP addresses:



11. If you want to add an IP camera to the XO device, click the camera in the list, and then click **Use IP address**. The system returns to the video inputs screen and fills in the camera's new IP address:



12. Select the camera driver (**ONVIF Profile S** or **Honeywell**) and fill in all other information as required, and then click **Enable**. For details, see *Enabling IP Cameras*.

Note

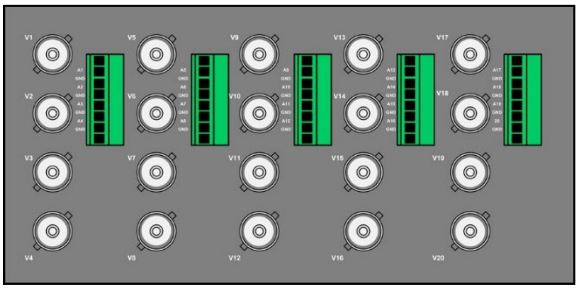
Changing a camera's IP address is only possible for cameras using the Honeywell or ONVIF driver.

13. To complete the setup, continue with *Camera Settings*.

6. Using Analogue Cameras

6.1 Video and Audio Connections

You connect analogue cameras to the BNC connectors at the rear of the FastTrace 2 Series device. The screw terminals allow for connecting analogue audio with the cameras. For more information on the physical connection of analogue audio/video inputs, see the *FastTrace 2 Series Hardware Installation Manual* (21790).



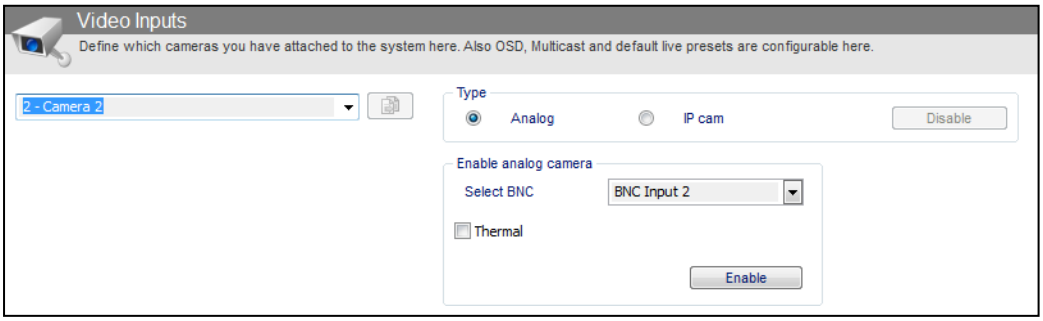
Each camera needs a separate BNC input. Depending on the configuration of your FastTrace 2 Series device, you have 4, 8, 12, 16, or 20 analogue BNC camera inputs available.

Furthermore, the FastTrace 2 Series device requires encoder cards for the analogue channels. These encoder cards come with licenses that enable the analogue channels.

6.2 Enabling Analogue Cameras

To enable an analogue camera, proceed as follows:

1. Choose **System** > **Connections** > **Video inputs**.
2. Choose a free camera number from the list.
   The system indicates camera numbers that are already in use by an asterisk *.
3. Under **Type**, click **Analog**.



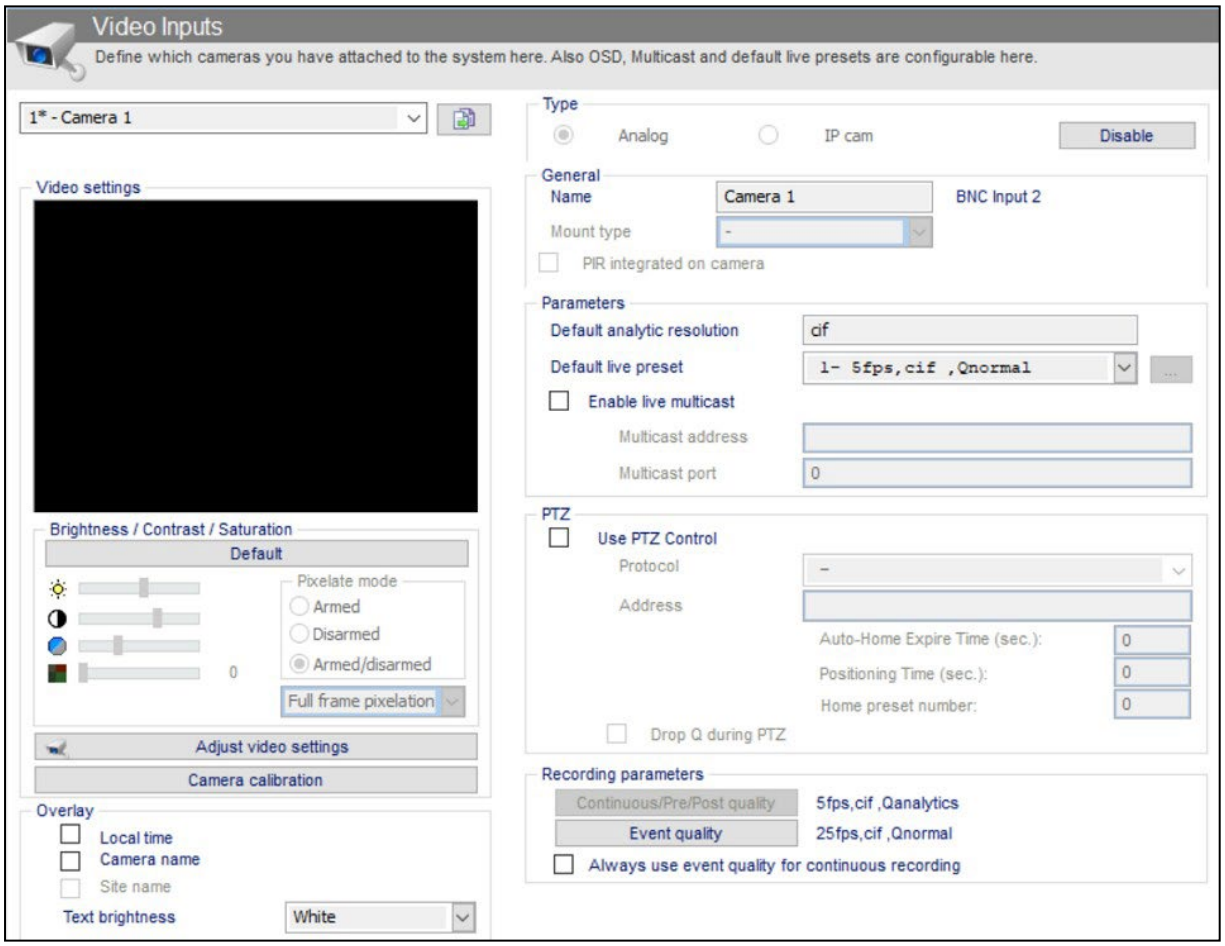
4. Provide the following information:

Item	Description
Select BNC	Select the BNC input to which the camera is connected. The BNC input numbers are indicated on the rear panel of the FastTrace 2 Series device (V1, V2…).
Thermal	Select this checkbox to enable the camera as a thermal camera.

Note

As soon as you enable the camera, the settings above are no longer accessible. If you need to change the settings, you have to disable the camera first, change the settings, and then enable the camera again.

5. Click **Enable** to start using the analogue camera. The system connects to the camera, and the camera setup window appears:



Note

You can continue working while the system enables the camera in the background. Select the next camera in the camera list.

6. To complete the setup, continue with *Camera Settings*.

7 Camera Settings

After enabling the camera, proceed with the following sections to complete the setup.

7.1 General Settings

To specify the general settings for a camera, proceed as follows:

1. Choose **System** > **Connections** > **Video Inputs**, and select the desired camera.
2. Under **General**, provide the following information:

Item	Description
Name	Enter a name for the camera (max. 20 characters). Honeywell recommends to use a meaningful and relevant description.
Mount type	For fisheye cameras only: select how the camera is mounted. This allows the system to correctly identify which part of the fisheye image is the floor and which is the ceiling. The de-warped image will then be the right way up. • **Ceiling**: the fisheye camera is mounted on a ceiling ('looking down'). • **Desktop**: the fisheye camera is mounted on a desktop or floor ('looking up'). • **Wall**: the fisheye camera is mounted on a wall ('looking horizontally'). **Note** For wall mounting, check the camera mounting orientation. If you mount the camera upside down, the dewarped image will be upside down as well.
PIR integrated on camera	This option is only available if the camera has an integrated PIR (for example the Axis M1054). Select the checkbox to enable the integrated PIR. You can then use PIR alarms for this camera.

3. Click **Save**.

7.2 Video Settings

Under **Video Settings**, you can adjust:

- Brightness, contrast, and saturation.
- Pixelation mode: for pixelating video streams to the CMS. For details, see *Pixelation*.

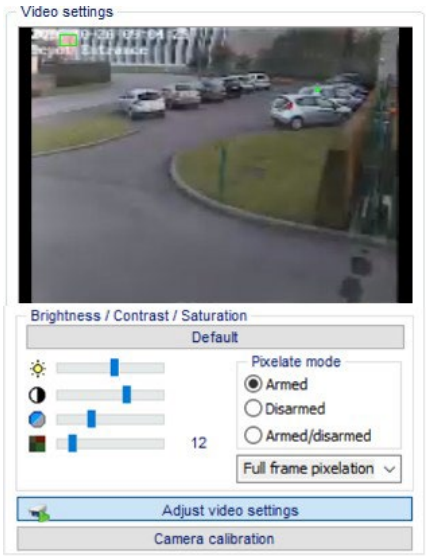
7.2.1 Brightness, Contrast, Saturation

Note

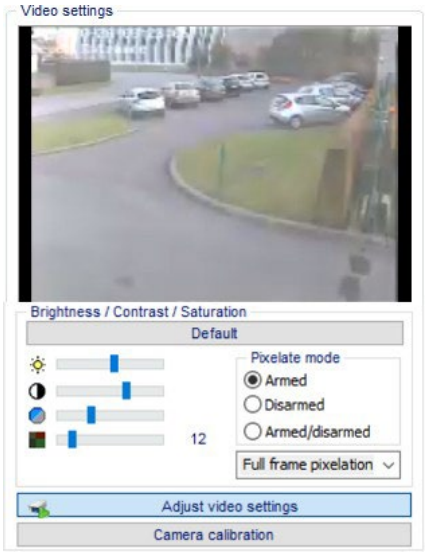
The brightness, contrast, and saturation settings may not work for all IP cameras. In this case, you can try and change the settings using the camera's web interface. Check the *Supported IP Camera List* (26742) for known issues.

To adjust brightness, contrast, and saturation, proceed as follows:

1. Choose **System** > **Connections** > **Video Inputs**, and select the desired camera.
2. Under **Video settings**, click **Adjust video settings**. A live image from the camera appears.



3. Drag the sliders to adjust brightness, contrast and saturation and pixelation level .



4. Click **Default** to restore the default values.

> ***Caution!***
>
> Clicking **Default** will also reset the pixelation level to 0.

5. Click **Save**.

7.2.2 Pixelation

Pixelation allows you to send pixelated video (live, recorded, and quad images) to provide privacy protection when a CMS monitors a site. For each video channel, you can set the pixelation level, and choose to pixelate the image when the system is armed, disarmed, or always.

In the XO client, Administrator users will always see the normal, unpixelated images, regardless of the settings. For other users (Technician or User), you can define which camera images will be pixelated for them. This allows you to provide a pixelated image for one user, but the same, unpixelated image for another. For details, see *Pixelation*.

For example, you set up camera 1 for pixelation, but only in disarmed state. You specify that user A will see pixelated images for camera 1, and user B will see normal images.
In this case: user A will see pixelated images in disarmed state, and normal images in armed state.
User B will always see normal images.

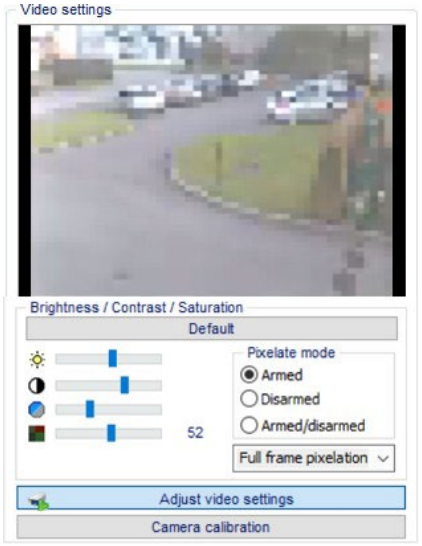
> ***Caution!***
>
> For pixelation to work with the CMS, the SDK for the CMS has to support pixelation (FT2 SDK version 3.03.0004 or above).

To pixelate a video channel, proceed as follows:

1. Choose **System** > **Connections** > **Video Inputs**, and select the desired camera.
2. Under **Video settings**, click **Adjust video settings**. A live image from the camera appears.



3. Drag the bottom slider to adjust the pixelation level. The number at the right-hand side of the slider indicates the pixelation level (0–100). The result is visible in the preview window.



4. Under **Pixelate mode**, select when the system has to apply pixelation:
   - **Armed**: only when the system is armed.
   - **Disarmed**: only when the system is disarmed.
   - **Armed/disarmed**: always.
5. If you want to remove pixelation, drag the slider to the far left (pixelation level = **0**).

> ***Caution!***
> Do **not** click **Default**; this will also reset the brightness/contrast/saturation settings.

6. Click **Save**.

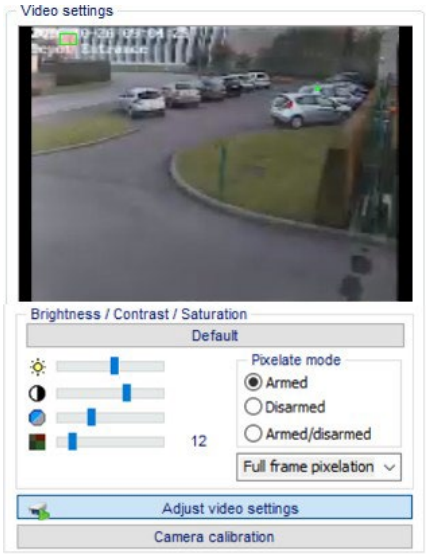
7.2.3 Anonymization

The anonymization feature helps in meeting the European Union standards for GDPR (General Data Protection Regulation) compliance. The objective of this feature is to use the masking techniques which enable hiding the identifiable personal data or personal identity from the video recorded using the video surveillance system. The masking is achieved using pixelation. The XO Client allows you to choose an anonymization type, which can be:

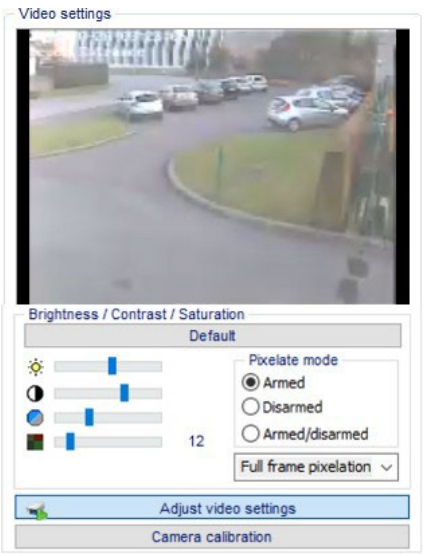
- Full frame pixelation – To pixelate the entire frame
- High Motion Scene – To anonymize moving objects in a high motion scene
- Variable Scene – If the scene contains both stationary and moving people or objects, then select this option to anonymize the objects in the scene.
- Still Scene – To anonymize the objects in a scene where the scene predominantly contains stationary people and objects.

To configure anonymization, proceed as follows:

1. Choose **System** > **Connections** > **Video Inputs**, and select the desired camera.
2. Under **Video settings**, click **Adjust video settings**. A live image from the camera appears.



3. Drag the sliders to adjust brightness, contrast, saturation and pixelation level.



4. Choose a **Pixelate mode**.
5. Choose an anonymization type from the list.

7.3 Camera Calibration

7.3.1 About Camera Calibration

If you are using analytics, you may need to perform the following camera calibrations:

- **3D calibration**: only if you use the ADPRO analytics applications IntrusionTrace (calibration is mandatory) or LoiterTrace (calibration is optional). The 3D calibration of a scene makes sure that the video analytics application knows the size of an object, the distance it travels through the scene, the speed… Correct detection is based on these parameters.
- **Bounding box calibration**: only for IP cameras that use different aspect ratios for the analytics stream and the live/recording stream. Bounding box calibration makes sure that the analytic bounding boxes appear correctly on all streams, regardless of their aspect ratio.

You can find detailed instructions for both calibrations in the following sections.

> ***Caution!***
>
> If you upgrade your device from a version below XO 4, and you change the aspect ratio of the analytics stream for a camera, **you have to make new calibration images and recalibrate that camera**.

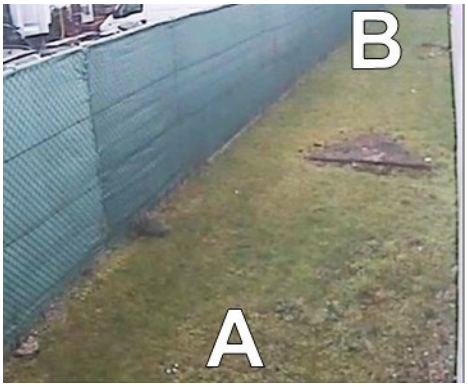
7.3.2 3D Calibration

3D calibration allows analytics applications to identify the size, speed… of detected objects in the camera image. Setup requires two easy steps to mark:

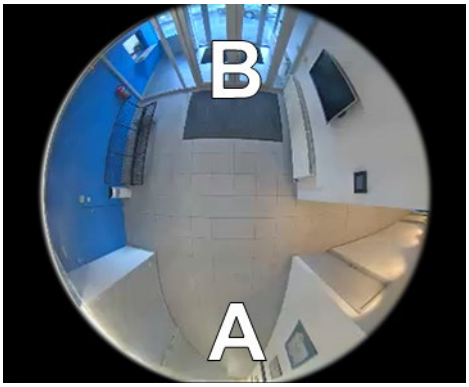
- the height of a known object at the front of the scene
- the height of that same object at the back of the scene.

Typically, you make a snapshot of the scene with a person/object standing at the front of the scene (**A**), at the bottom of the camera image, and another snapshot with the same person/object standing at the back of the scene (**B**), at the top of the camera image.
On a **fisheye** camera, you do the same: you make a snapshot with a person/object at the bottom of the scene (**A**), and another with the same person/object at the top of the scene (**B**). Although the objects will be similar in size at these two extremes, the measurements provide reliable detection across the scene.

Always perform walk tests to confirm detection.



Position of objects for 3D calibration in normal scene



Position of objects for 3D calibration in fisheye scene

You can either use live images, or you can first record images and take snapshots when you play back the footage, so that only one person can calibrate the scene.

You can calibrate a scene in the XO client:

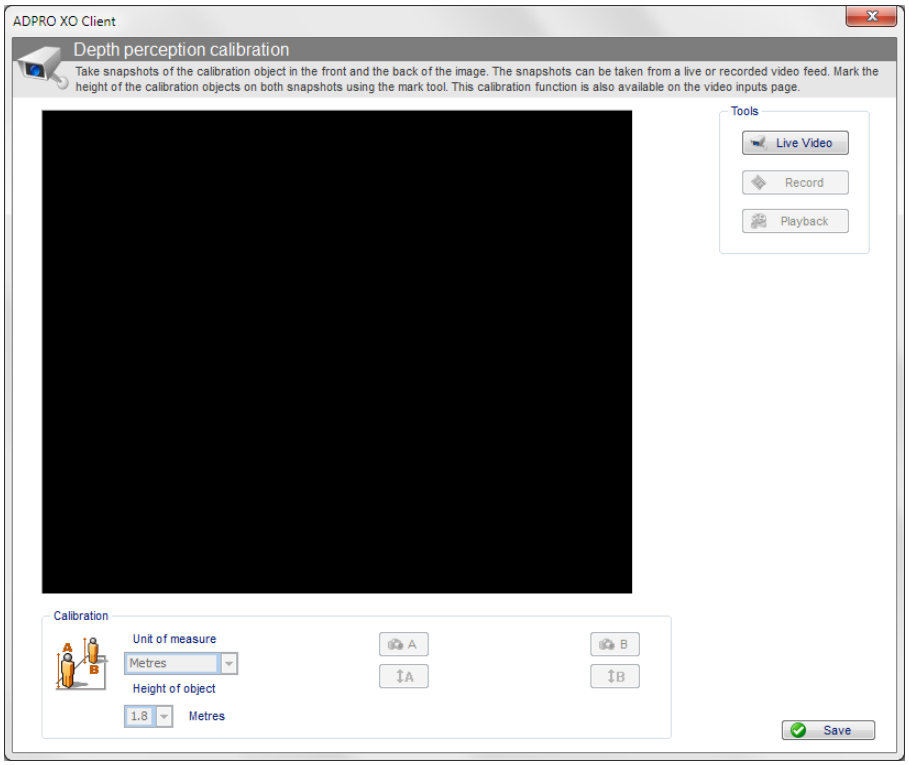
- from the IntrusionTrace configuration window
- from the LoiterTrace configuration window
- or from the video input configuration window.

You need to calibrate a scene only once. The calibration is valid for all analytics applications (IntrusionTrace, LoiterTrace, and Motion/Sabotage). As of XOa 3.02.0017, the system displays thumbnails of the calibration pictures (if available) in the analytics configuration window. As of XO 4.00, the system also displays the resolution of the calibration pictures (= the analytics stream resolution).

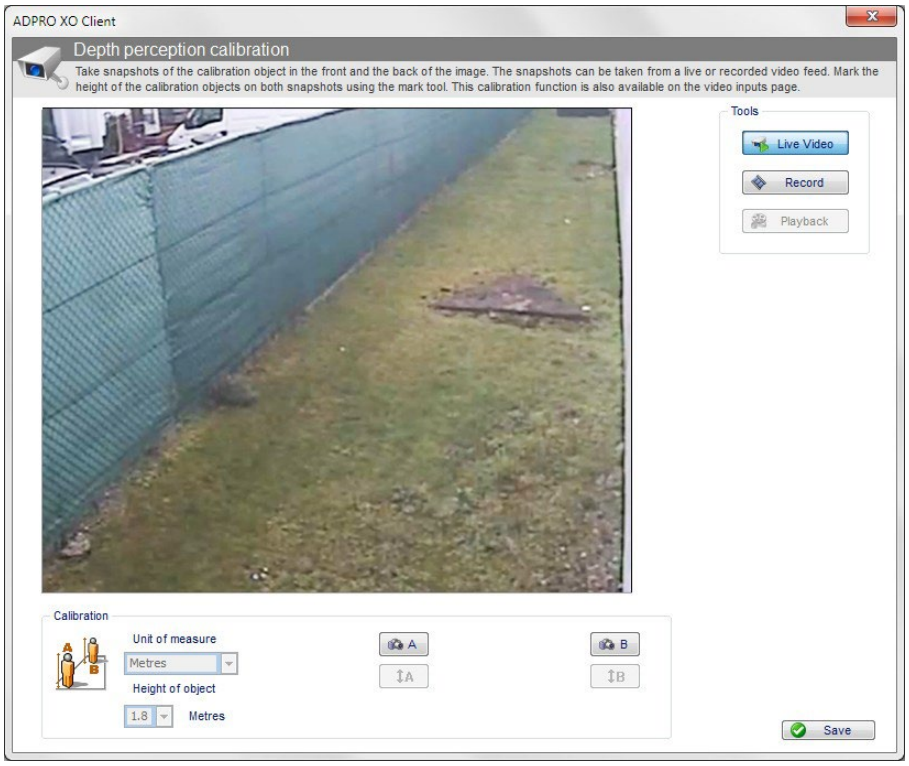
7.3.3 3D Calibration from Live Images

To calibrate a scene from live images, proceed as follows:

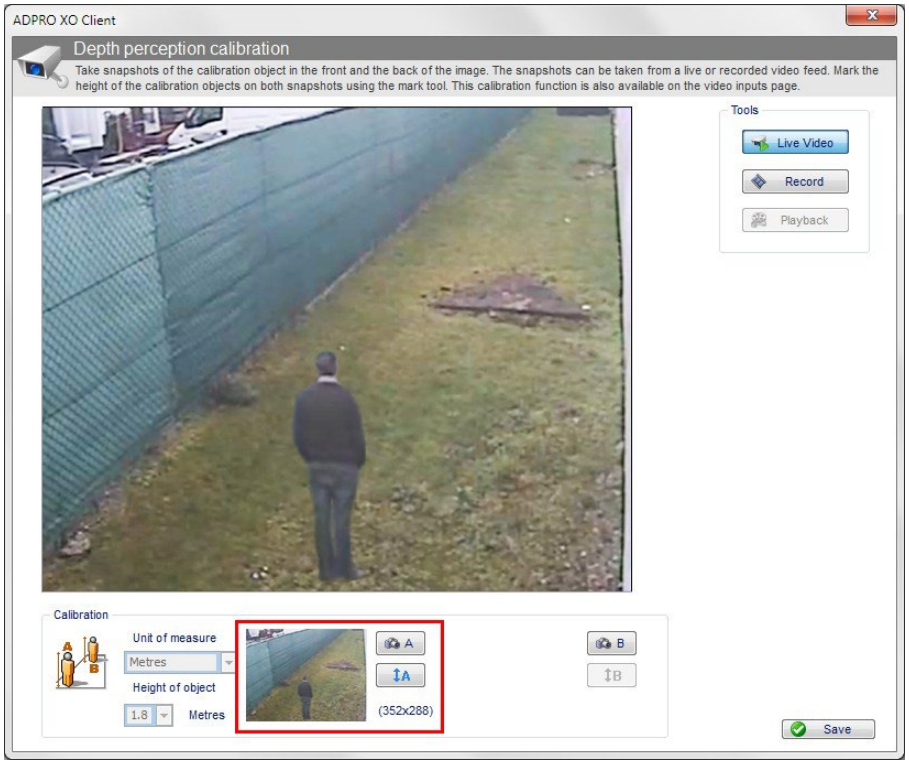
1. Choose **System** > **Connections** > **Video Inputs**, and select the desired camera.
2. Under **Video settings**, click **Camera calibration**.



3. Under **Tools**, click **Live Video**. The live camera image appears.



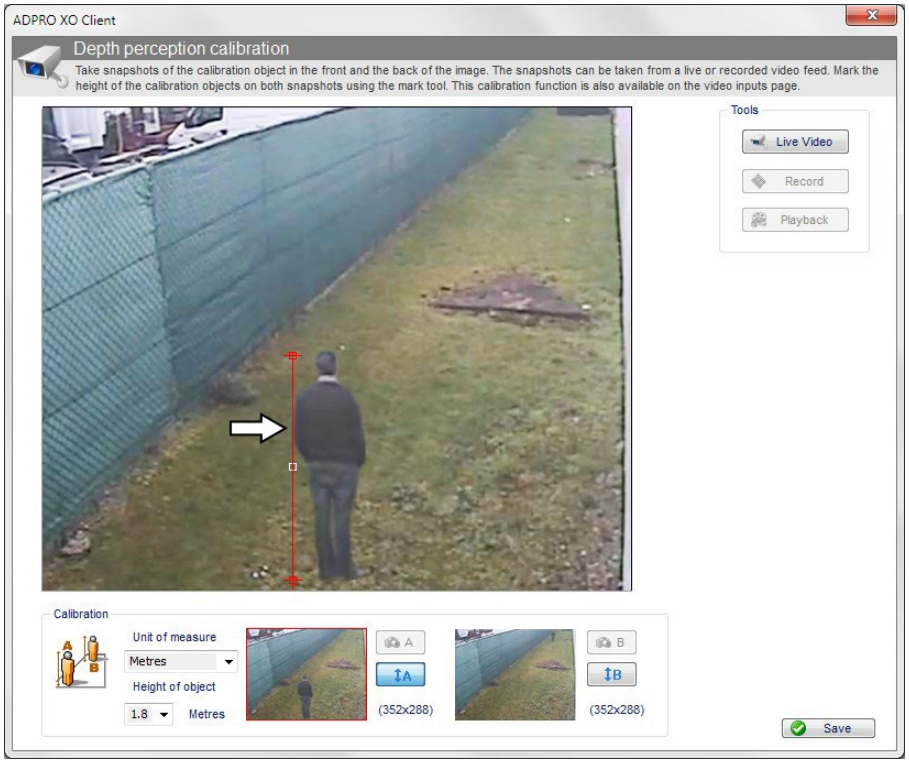
4. When the person/object is standing **at the front** of the scene, click A to make a snapshot. Make sure that the person/object is completely visible (from head to toe). A miniature version of the snapshot appears at the bottom of the screen; the system indicates the image resolution.



5. When the person/object is standing **at the back** of the scene, click B to make a snapshot. Make sure that the person/object is completely visible (from head to toe). A miniature version of the snapshot appears at the bottom of the screen; the system indicates the image resolution.



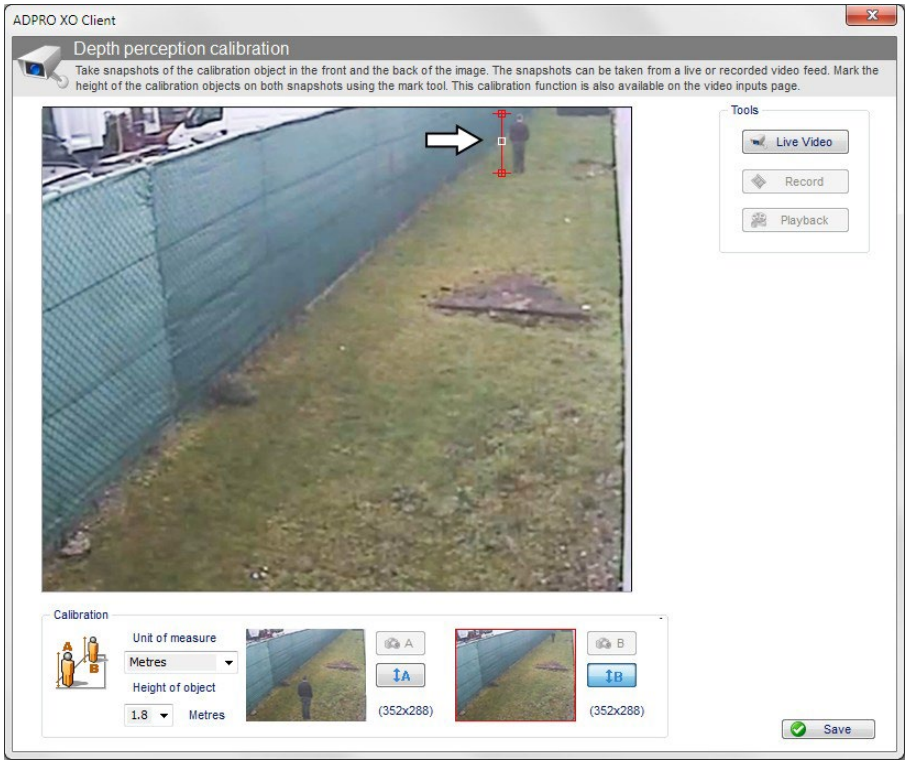
6. To calibrate the front of the scene, you need to draw a marker line with the same height as the object/person in the front: click A. The front snapshot now appears as the camera image.
7. Click the camera image near the top of the person/object, and drag downward to the bottom of the person/object. A vertical, red marker line appears.



Note

If you have calibrated the scene before, the vertical red marker is already visible. You only need to adjust it.

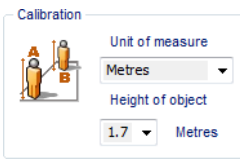
8. Adjust the marker line until it has exactly the same height as the person/object at the front, as follows:
   - To move the position of the marker line in the scene, drag it by its white handle in the middle.
   - To change the height of the marker line, drag the red handles at the top and bottom.
9. Click **Save**. You will now calibrate the back of the scene.
10. To calibrate the back of the scene, click ↕B. The back snapshot now appears as the camera image.
11. Click the camera image near the top of the person/object, and drag downward to the bottom of the person/object. A vertical, red marker line appears.



Note

If you have calibrated the scene before, the vertical red marker is already visible. You only need to adjust it.

12. Adjust the marker line until it has the same height as the person/object at the back.
    Next, you will indicate the height of the person/object.
13. Under **Calibration**, in the **Unit of Measure** list, choose the desired unit of measure (metres, yards, or feet). The unit of measure is valid for the back and front of the scene.
14. In the **Height of object** box, select the height of the person/object. Choose the value that is the closest to the person/object's exact height. The height is valid for the back and front of the scene.

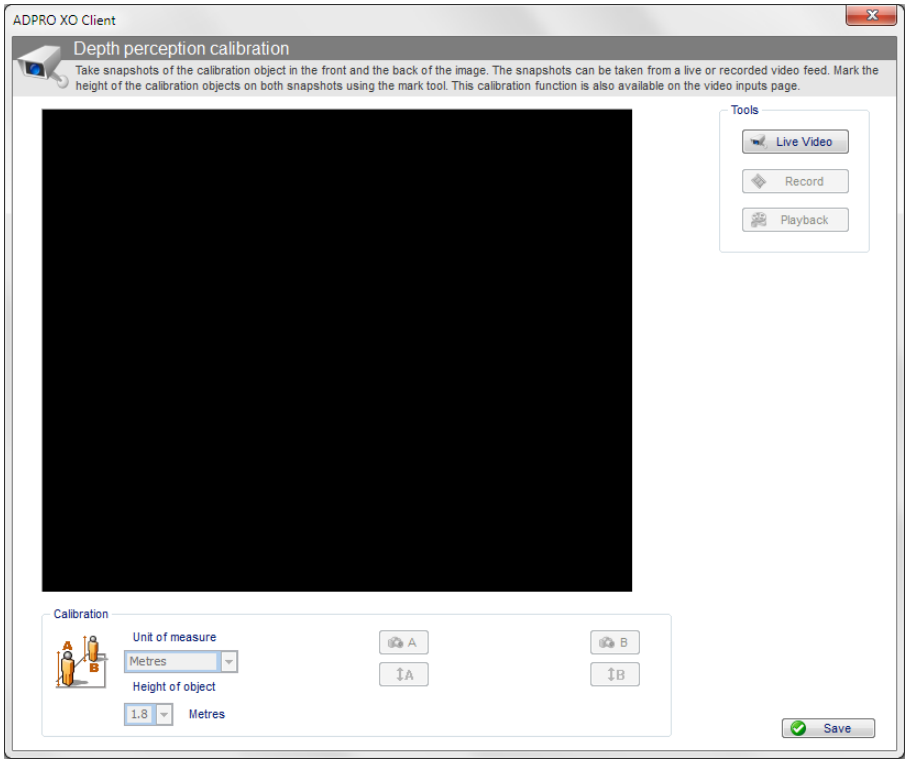


15. Click **Save**, and then close the calibration window.

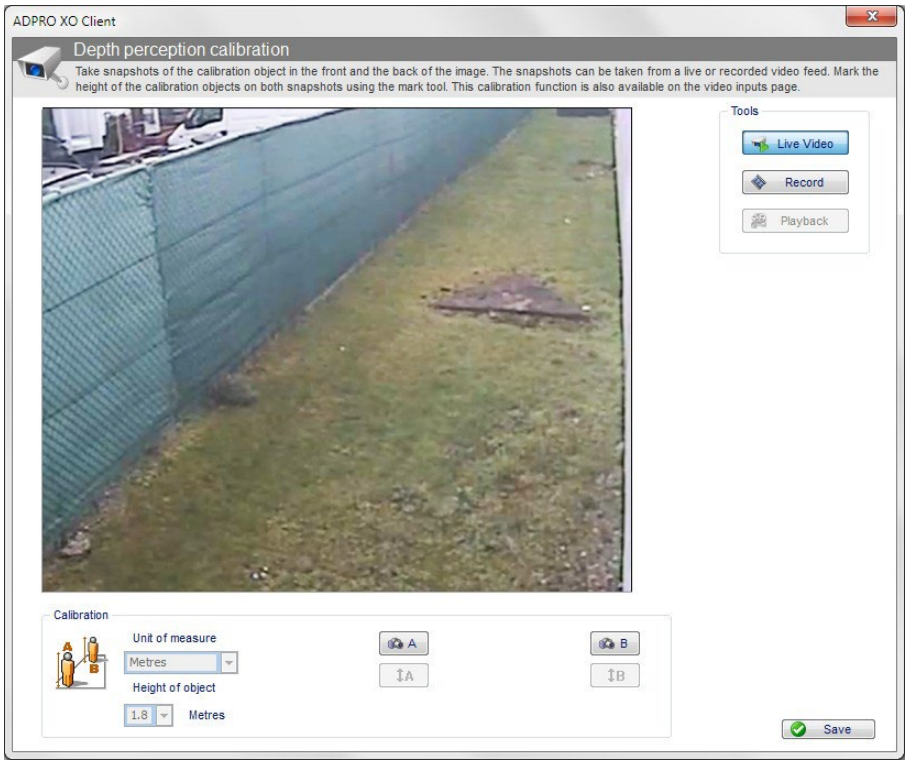
7.3.4 3D Calibration from Recorded Images

To calibrate a scene from recorded images, proceed as follows:

1. Choose **System** > **Connections** > **Video Inputs**, and select the desired camera.
2. Under **Video settings**, click **Camera calibration**.

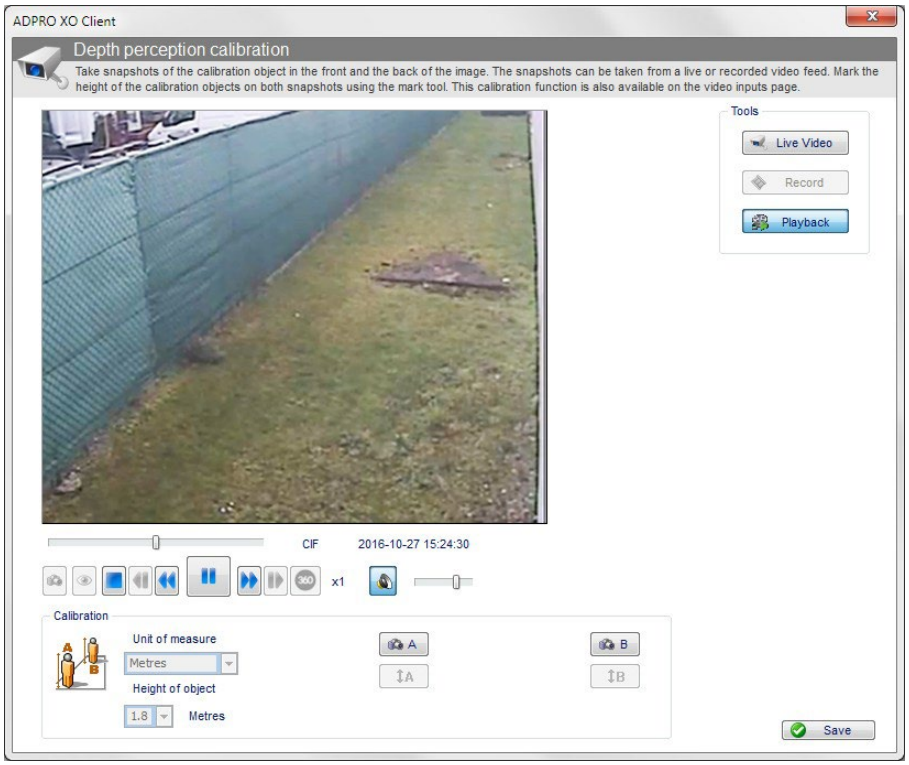


3. Under **Tools**, click **Live Video**. The live camera image appears.



4. Click **Record**. The system starts recording the live images.
5. While recording, make the person/object stand still **at the front** and **at the back** of the scene.
6. When you have the required footage, click **Record** again to stop recording.

7. Click **Playback**. The system starts playing the recorded footage.



8. Making snapshots and calibrating the scene is identical as for live video. For details, see the procedure in *3D Calibration from Live Images*. Start at *step 4*, and continue to the end.

7.3.5 Bounding Box Calibration for Different Aspect Ratios

Bounding box calibration is only required for IP cameras that use different aspect ratios for the analytics stream and the live/recording stream. It makes sure that the analytic bounding boxes appear correctly on all streams, regardless of the aspect ratio.

Correct bounding box calibration depends on the way the camera provides the low-resolution stream (see *Streams with Different Aspect Ratios*):

- To calibrate the bounding boxes for cameras that provide cropped images: see *Normal Bounding Box Calibration*.
- To calibrate the bounding boxes for cameras that provide squeezed images: see *Bounding Box Calibration for Squeezed Images*.

> ***Caution!***
>
> Set up the recording stream resolution (see *Recording Parameters*) **before** you calibrate the bounding boxes.

Bounding box calibration is available in firmware version V2.10 and above. If the analytics and recording streams have the same aspect ratio, then bounding box calibration is not required and the option is unavailable.

7.3.5.1 Normal Bounding Box Calibration

To calibrate the bounding boxes, proceed as follows:

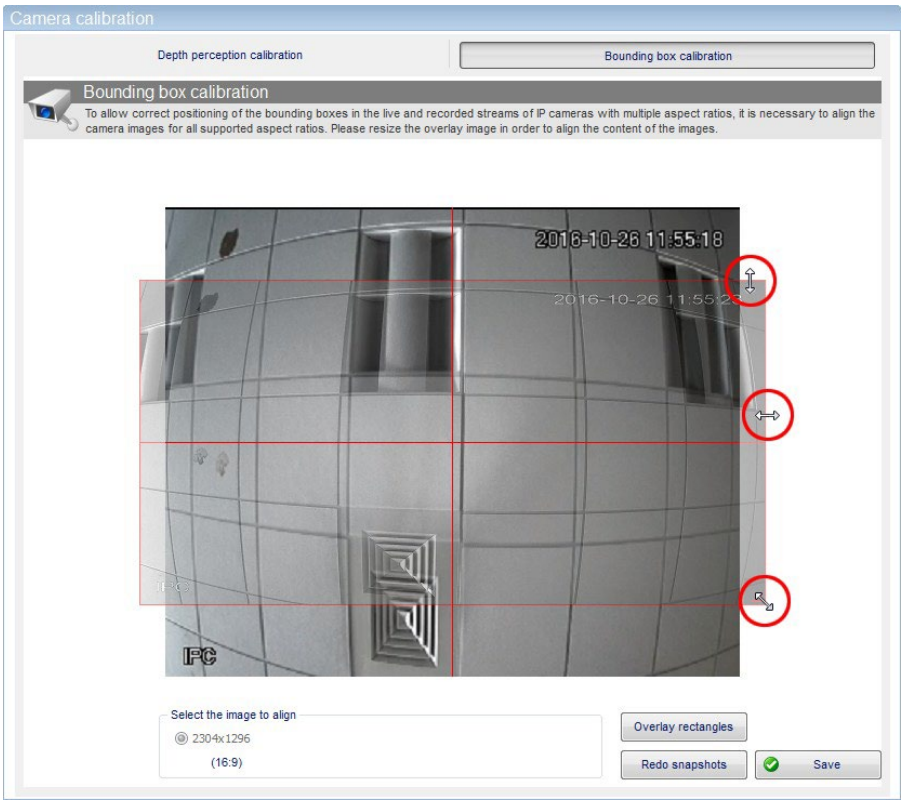
1. Choose **System** > **Connections** > **Video Inputs**, and select the desired camera.
2. Under **Video settings**, click **Camera calibration**.

3. Click the **Bounding box calibration** tab.

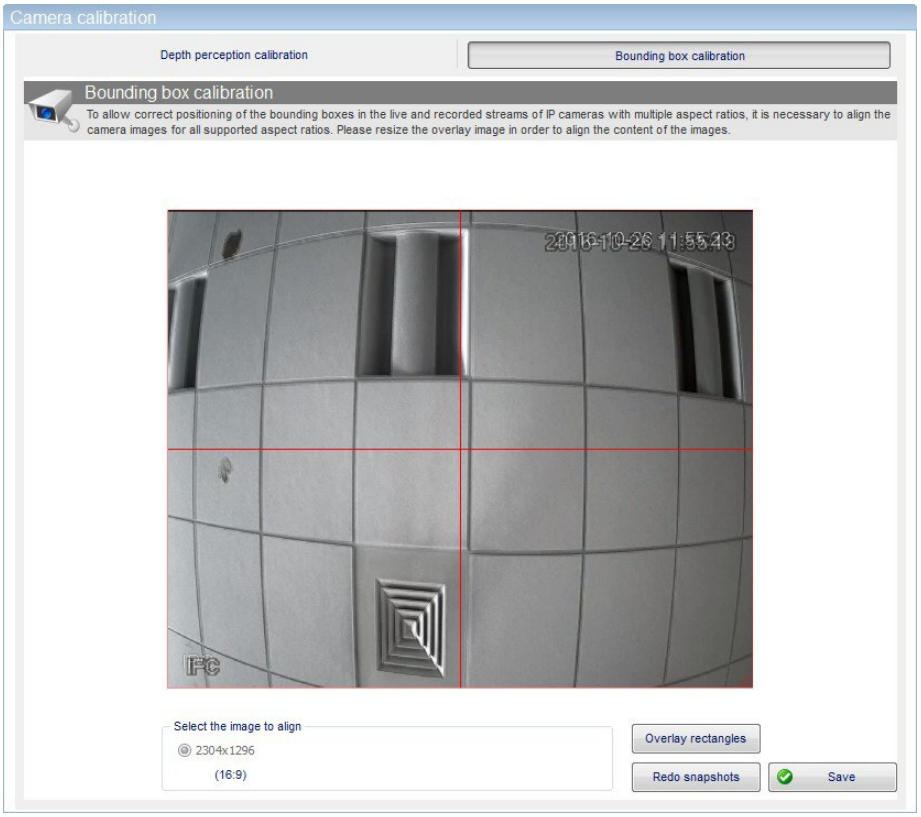


The system takes two snapshots, one at each resolution, and displays them on top of each other.

4. Drag the sides or the corner of the image until both images overlap perfectly.



The result should look like this:



5. Click **Save**, and then close the calibration window.

7.3.5.2 Bounding Box Calibration for Squeezed Images

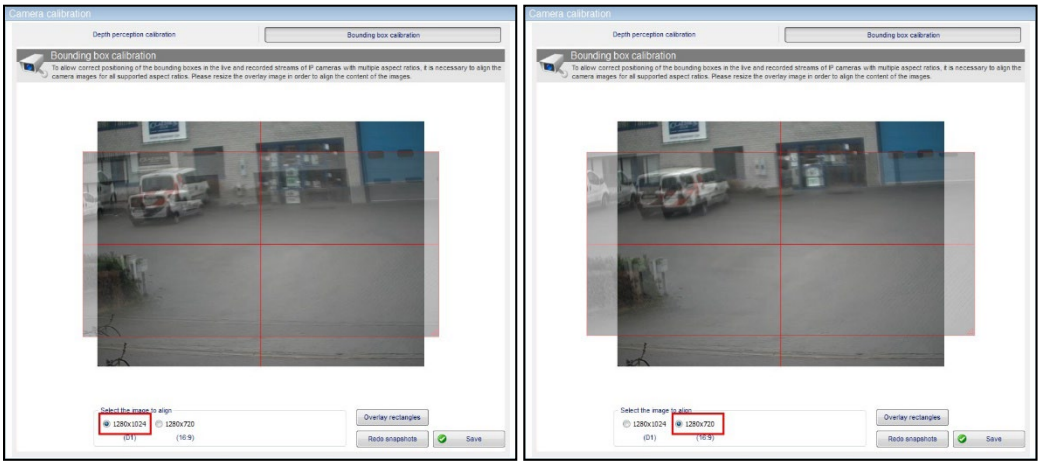
Bounding box calibration for squeezed images is available in firmware version XO 4.0 and above.

To calibrate the bounding boxes for squeezed images, proceed as follows:

1. Choose **System** > **Connections** > **Video Inputs**, and select the desired camera.
2. Under **Video settings**, click **Camera calibration**.
3. Click the **Bounding box calibration** tab. The system takes two snapshots, one at each resolution, and displays them on top of each other.
4. Click **Overlay rectangles**. The system aligns the images automatically.
5. Click **Save**, and then close the calibration window.

7.3.5.3 Bounding Box Calibration for Three-stream Cameras

If your camera provides 3 streams, and you have selected 3 different aspect ratios (for analytics, continuous, and event recording), then you have to perform calibration twice. The **Select the image to align** box will display two resolutions. Select each resolution in turn and perform calibration as required.



7.4 Overlay

> **Note**
>
> The overlay options may not be available, or may not work for all IP cameras. You can try and set the overlay info using the camera's web interface.

In the camera configuration screen, under **Overlay**, you can specify which information you want to appear on top of the camera image in the **Live Video** window.



To specify the overlay texts, proceed as follows:

1. Choose **System** > **Connections** > **Video Inputs**, and select the desired camera.
2. Under **Overlay**, provide the following information:

Item	Description
Local time	Select this checkbox to display the local time on the camera's live image.
Camera name	Select this checkbox to display the camera name on the camera's live image.
Site name	Select this checkbox to display the site name on the camera's live image. The **Site name** option only appears after you select the **Camera name** checkbox.
Text brightness	Select a colour for the text that is displayed on the camera's live image. Select the colour that has the best contrast with the camera image.

3. Click **Save**.

7.5 Live View and Multicast (Parameters)

To specify the network-related settings for live streaming and multicast, proceed as follows:

1. Choose **System** > **Connections** > **Video Inputs**, and select the desired camera.
2. Under **Parameters**, provide the following information:

Item	Description
Default analytic resolution	This box indicates the analytic resolution for the camera, as the system selected when enabling the camera. You cannot change the analytics resolution here. For details, see *Analytic Resolution for IP Cameras*. For analogue cameras, the analytics stream is CIF/SIF @ 5 fps.
Default live preset	Select the default image quality for the live images from the camera. When you add the camera to the **Live Video** window, the system displays the camera images at this selected quality. You can always change the image quality in the **Live Video** window (right-click the camera image). The available options depend on the camera. For IP cameras, the live presets are based on the analytic, continuous, and event streams. If you select the option **Harddisk stream**, the image quality for live images is the same as for continuous recordings (see *Recording Parameters*). This way, only two streams are required. **Note** The XO 5 software supports video rendering up to 6400 x 6400 pixels. For optimal performance: if you are using 12 (or higher) megapixel (MP) cameras on your XO device, then you can use max. 12 cameras @ 12 MP and max. 12 analytic applications (IntrusionTrace and/or LoiterTrace).
...	This button is only available for certain types of cameras. It allows you to define your own quality presets. The XO client comes with 10 predefined quality presets. These presets are valid for all the cameras. However, if the camera functionality allows, you can define your own presets as follows: Click the button to open the list of predefined quality presets. Select a preset that is not in use, and set the following items: • **Fps**: frames per second • **Resolution**: image resolution • **VBR**: click this option to use a variable bitrate. Select the desired quality: **Qlow**, **Qnormal**, or **Qhigh**. • **CBR**: click this option to use a constant bitrate. Type the desired bitrate (in kilobits per second). For more details on VBR and CBR, see *Recording Parameters*.
Enable live multicast	Multicast is the simultaneous supply of information to one or more computers via only one data stream from the source. When multiple computers poll this one stream, the system creates multiple copies, but the initial upload will remain the same. In this way, multicast ensures less data traffic over the network. Select this checkbox if you want to use the multicast protocol.

Item	Description
Multicast address	Enter the IP address to which the XO device has to send the multicast stream. The IP address range assigned for multicasting on the local LAN network is 224.0.0.0 – 239.255.255.255. **Note** Assign a unique multicast address to each camera. Everyone who has subscribed to the multicast, can view the live images on this address, using a web browser or an XO client.
Multicast port	Type the port number for the multicast stream. **Note** Assign a unique multicast port to each camera. The IT Department has to define the multicast port before connecting the XO device to the LAN network.

3. Click **Save**.

7.6 PTZ Control for Analogue Cameras

If you are controlling PTZ on analogue cameras via a **serial port** (USB or MIO card), you will need to perform the following steps in the XO client:

1. Configure the serial port: assign the PTZ protocol to it. If you have analogue PTZ cameras that require different PTZ protocols, you will have to use and set up a separate serial port for each protocol. For details, see *PTZ Control via USB Port/MIO Card*.
2. Enable PTZ on the camera and select the serial port that controls it. For details, see *PTZ Setup*.
3. Define the PTZ parameters such as the PTZ address and timeouts. For details, see *PTZ Setup*. If you are

controlling PTZ via the **DTC card**, you will need to perform the following steps in the XO client:

1. Enable PTZ on the camera and select the DTC protocol to control it. For details, see *PTZ Setup* .
2. Define the PTZ parameters such as timeouts. For details, see *PTZ Setup*.

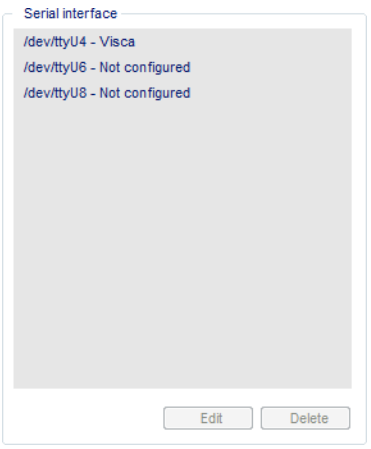
You may have to update the DTC card software, if a new version is available. For details, see *PTZ Control via DTC Card*.

7.6.1 PTZ Control via USB Port/MIO Card

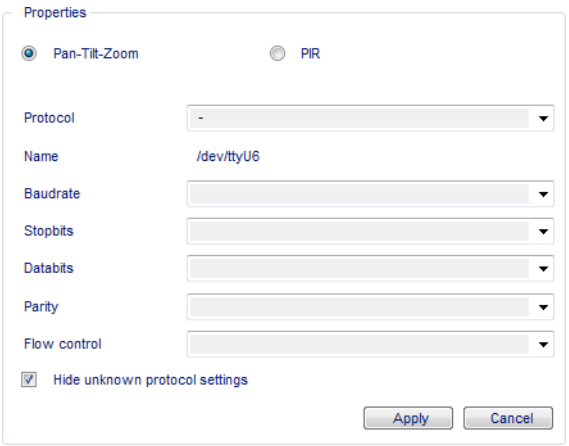
If you control the analogue PTZ cameras via USB port or MIO card, you have to assign the required PTZ protocol to the serial port (USB or MIO card) in the XO client. You can assign one PTZ protocol to only one serial port; you cannot use multiple serial ports with the same PTZ protocol. If you have PTZ cameras using different PTZ protocols, you need to set up a different serial port for each PTZ protocol.

To set up the connection for PTZ control via USB port or MIO card, proceed as follows:

1. Choose **System** > **Connections** > **Serial Ports / PTZ**.



2. Select the correct port in the list:
   - For a connection via the first MIO card, select **/dev/ttyU6**.
   - For a connection via the second MIO card, select **/dev/ttyU8**.
   - For a connection via a USB converter, see the *FastTrace 2 Series Hardware Installation Manual* (21790) for the correct port number on the motherboard.
3. Click **Edit**.



4. Choose the correct option: **Pan-Tilt-Zoom**.
5. In the **Protocol** list, select the required protocol, depending on the camera type.
   The system automatically fills in the other parameters with default values for the selected protocol. The default values are suitable for most cases.
6. If you need to modify the default settings, clear the **Hide unknown protocol settings** checkbox, and then enter baud rate, stop bits, data bits, parity, and flow control according to the camera specifications.
7. Click **Apply**, and then click **Save**.

7.6.2 USB Port/MIO Card Supported PTZ Protocols

The XO software supports the following PTZ protocols via USB port/MIO card:

- 360 Vision / Vantage Juno / VT Fastrax-P / Xeno Neodome
- Amux IEC
- Baxall ZMX
- Baxall ZTX
- BBV
- Burle/Philips/Bosch
- COHU
- Conway
- CS Lilin
- CS Lilin 2
- Dennard 2050
- Diamond
- Digital Sprite
- Elbex
- Ernitec
- GPS
- Grundig
- Harris
- JVC
- Kalatel
- Mark Mercer
- Molynx
- Molynx Variable Speed
- Pacom
- Panasonic (Conventional)
- Panasonic (New)
- Pelco D
- Pelco D (no zoom speed)
- Pelco P
- Samsung
- Sensormatic
- Sensormatic Controller
- Sensormatic Speeddome VII
- Siemens
- Synectics
- TEB
- TEB (rail)
- Unidex
- VCL
- Vicon
- Video Switch
- Visca
- Vista PowerDome

7.6.3 PTZ Control via DTC Card

Some analogue PTZ cameras can send the PTZ signal through the coax cable (down-the-coax PTZ control), so that no extra wiring is required. If you want to use this, you need to have your FastTrace 2 Series device equipped with a DTC card. In the camera setup window, you select the DTC protocol in the camera setup. For an overview of available DTC protocols, see *DTC Supported PTZ Protocols*.

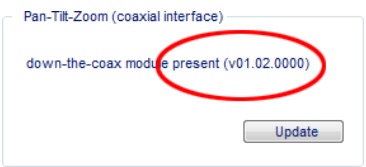
Note

If you need a DTC card in a FastTrace 2 Series device, you can have maximum 16 analogue channels. In a device with 20 analogue channels, channels 17–20 will be physically removed. The DTC card is built in at the factory; you cannot order it separately.

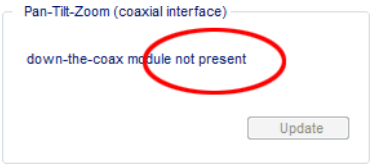
The DTC card requires software. You can retrieve the current software version of the DTC card in the XO client software, and update the software if required.

To retrieve the DTC card's software version, proceed as follows:

1. Choose **System** > **Connections** > **Serial Ports / PTZ**.
   — If the system contains a DTC card, the screen indicates the card's current software version.

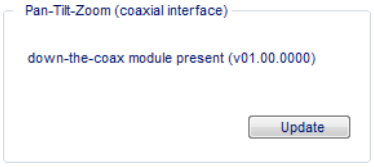


— If the system does not contain a DTC card, the screen indicates that the DTC module is not present.

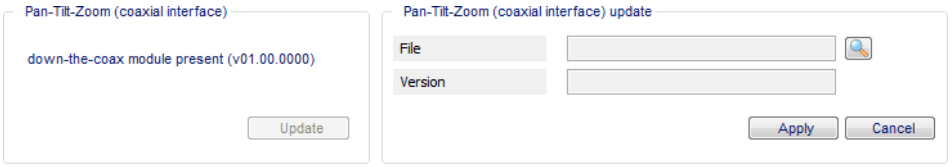


To update the DTC card software, proceed as follows:

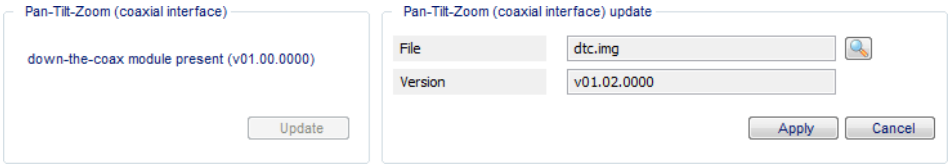
1. Choose **System** > **Connections** > **Serial Ports / PTZ**. The **Pan-Tilt-Zoom** box indicates the current software version (v01.00.0000 in the example below).



2. Click **Update**.



3. Click  and select the **dtc.img** file with the latest software. The **Version** box indicates the new software version (v01.02.000 in the example below).



4. Click **Apply**.
5. Click **Save**.

7.6.4 DTC Supported PTZ Protocols

The DTC card supports the following PTZ protocols:

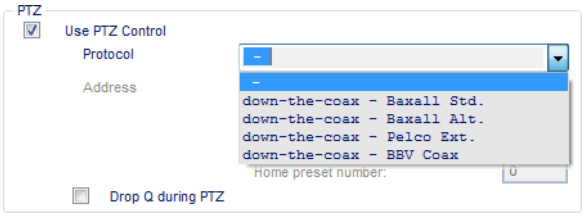
- Down-the-Coax (Pelco Ext.)
- Down-the-Coax (Baxall Std.)
- Down-the-Coax (Baxall Alt.)
- Down-the-Coax (BBV coax).

7.7 PTZ Setup

To set up pan-tilt-zoom (for PTZ cameras only), proceed as follows:

1. Choose **System** > **Connections** > **Video Inputs**, and select the desired camera.
2. Under **PTZ**, provide the following information:

Item	Description
Use PTZ Control	Select the checkbox to enable the PTZ functions of the PTZ camera.

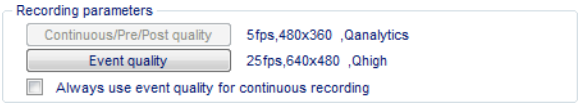
Item	Description
Protocol	For analogue cameras only. (For IP cameras, the driver handles PTZ commands.) Select the PTZ protocol for the camera: • If you control PTZ via USB or MIO card, select the correct port. You have to set up the serial port for PTZ control first. For more information, see *PTZ Control via USB Port/MIO Card*. • I If you are using a DTC module, select the correct PTZ protocol from the list:  For more information on the DTC module, see *PTZ Control via DTC Card* .
Address	For analogue cameras via serial port only: enter the correct PTZ address for the camera you have installed. For more information, see the camera manufacturer's documentation. **Note** • When using the Pelco Spectra Cam 4, the PTZ address has an offset of 1 in the XO client. • When using the JVC protocol, the PTZ address has an offset of +1 in the XO client. **Example**: When using a JVC protocol with address 1 in the XO client, the PTZ address of the camera is 2.
Auto-Home Expire Time (sec.)	Enter the time, in seconds, before the camera automatically moves back to its home position after a PTZ action. The minimum time is 10 seconds. Set to **0** if you want to disable the auto-home feature (keep the camera at the PTZ position). **Note** If you are using the **Auto-Home Expire Time** (value different from 0), the system suppresses analytics detection during PTZ movement. The analytics detection resumes when the camera has returned to the home position.
Positioning Time (sec.)	Enter the time, in seconds, to allow the camera to move to a preset position. The system takes the positioning time into account if you let the PTZ camera move to a preset position when an input is triggered. The system then delays the alarm message of that input until the positioning time has expired. This makes sure that the camera is in position and has stopped moving, so that quad images are sharp. If the camera is still moving when the system creates the quad images, the quad images will be blurry.
Home preset number	Only for IP cameras. Leave this setting at the default value (= **0**). In the exceptional case of an IP camera that does not support a PTZ home position, you can specify a specific preset number that will server as the 'home' position for such a camera.
Drop Q during PTZ	For analogue cameras only: select this checkbox if you want to lower the image quality during PTZ movements. This setting has no effect on IP cameras.

3. Click **Save**.

7.8 Recording Parameters

Under **Recording parameters** you define the image quality for continuous and/or event recording. The available options and values depend on the camera type. For details on IP cameras, see the *Supported IP Camera List* (26742).

If you have selected **Treat this cam as a single stream cam** (IP cameras only) when enabling the camera, then the recording settings are unavailable: recording always occurs at the same quality as live viewing (see *Live View and Multicast (Parameters)*).

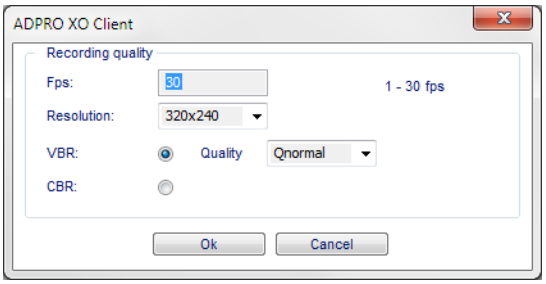


To specify the recording parameters, proceed as follows:

1. Choose **System** > **Connections** > **Video Inputs**, and select the desired camera.
2. Under **Recording parameters**, provide the following information (if available):

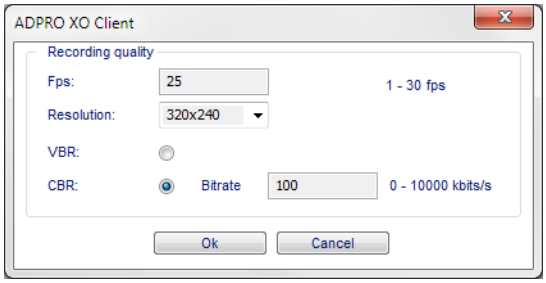
Item	Description
Continuous/Pre/Post quality	Only available for specific cameras: click to specify the image quality that you want for continuous recording and for pre and post event recording. See further below for details.
Event quality	Click to specify the image quality that you want for event recording. See further below for details.
Always use event quality for continuous recording	Only available for specific IP and analogue cameras: select this checkbox to use the event recording quality for continuous recording (instead of the analytics quality).

The quality settings for continuous and event recording are similar:



3. For the recording settings, provide the following information:

Item	Description
Fps	Type the desired number of frames per second. The available range is indicated on the right side of the box.

Item	Description
Resolution	Select the desired image size: available as **cif**, **qcif**… or in pixels (width x height). ***Caution!*** If you select an image size that has a different aspect ratio than the analytics stream (as shown in the **Default analytic resolution** box in the camera setup window), you have to calibrate the bounding boxes. For details, see *Bounding Box Calibration for Different Aspect Ratios*. The XO 5 software supports video rendering up to 6400 x 6400 pixels. For optimal performance: if you are using 12 (or higher) megapixel (MP) cameras on your XO device, then you can use max. 12 cameras @ 12 MP and max. 12 analytic applications (IntrusionTrace and/or LoiterTrace).
VBR	Select this option to use a variable bitrate for a constant image quality. Select the desired quality: • Qlow: low image quality • Qnormal: normal image quality • Qhigh: high image quality. With a variable bitrate, the bitrate changes with scene content. The bitrate will be higher for scenes with a lot of motion, and lower for scenes with less motion. This setting is suitable if you need high-quality images when there is motion in the scene. Keep in mind that the available bandwidth has to be sufficient to accommodate high throughputs. The recommended setting is VBR at normal image quality.
CBR	Select this option to use a constant bitrate with a variable image quality. Type the desired bitrate, in kbps (kilobits per second), in the **Bitrate** box. The available range depends on the camera, and is indicated on the right side of the box.  With a constant bitrate, the image quality and/or frame rate will decrease for scenes with a lot of motion, if the required bitrate exceeds the set bitrate. The higher the bitrate value, the higher the image quality and frame rate can be, but also the higher the consumed bandwidth. This setting is suitable if the available bandwidth is limited.

4. Click **OK** to close the recording quality window.
5. Click **Save**.

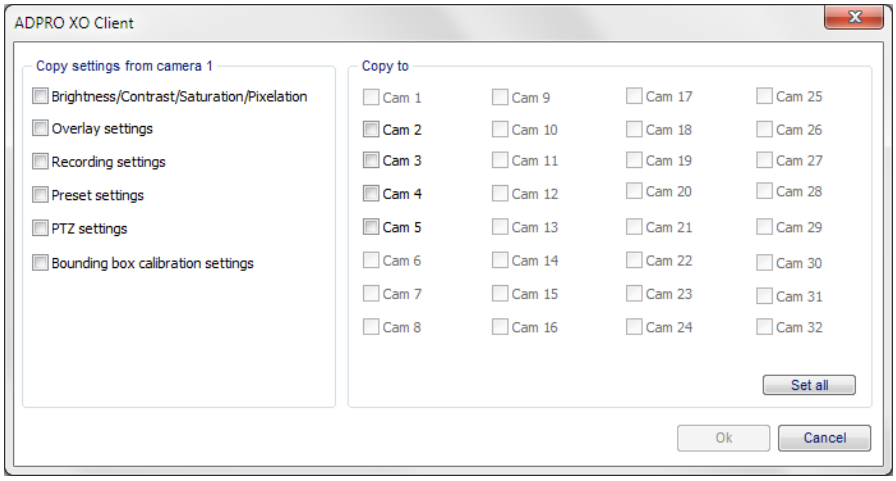
7.9 Copying Camera Settings

If you have several (nearly) identical cameras connected to your XO device, you can set up one camera and then copy its settings to the other cameras. You need to enable all the required cameras first.

Caution!
- You can copy the settings for recording, PTZ, and live preview only to compatible cameras.
- You can copy the settings for the bounding box calibration only to identical cameras.

To copy settings to other cameras, proceed as follows:

1. Choose **System** > **Connections** > **Video Inputs**, and select the camera from which you want to copy the settings.
2. Click the button (on the right-hand side of the camera list).



3. Under **Copy settings from camera x**, select the settings that you want to copy to the other cameras:

Item	Description
Brightness / Contrast / Saturation / Pixelation	Settings for brightness, contrast, saturation, and pixelation. Check these settings for each camera after copying, and adjust as needed.
Overlay settings	Information to display on the camera image (date and time, camera name…).
Recording settings	Image quality settings for continuous and event recording.
Preset settings	Default image quality setting for live viewing.
PTZ settings	PTZ settings (protocol, address, positioning times…).
Bounding box calibration settings	Bounding box calibration settings for IP cameras with multiple aspect ratios. To make sure that bounding boxes function properly, check the calibration for each camera after copying, and adjust as needed.

4. Under **Copy to**, select all the cameras to which you want to copy the selected settings. If you want to copy the selected settings to all other cameras, click **Set all**.
5. Click **OK**.

7.10 Disabling Cameras

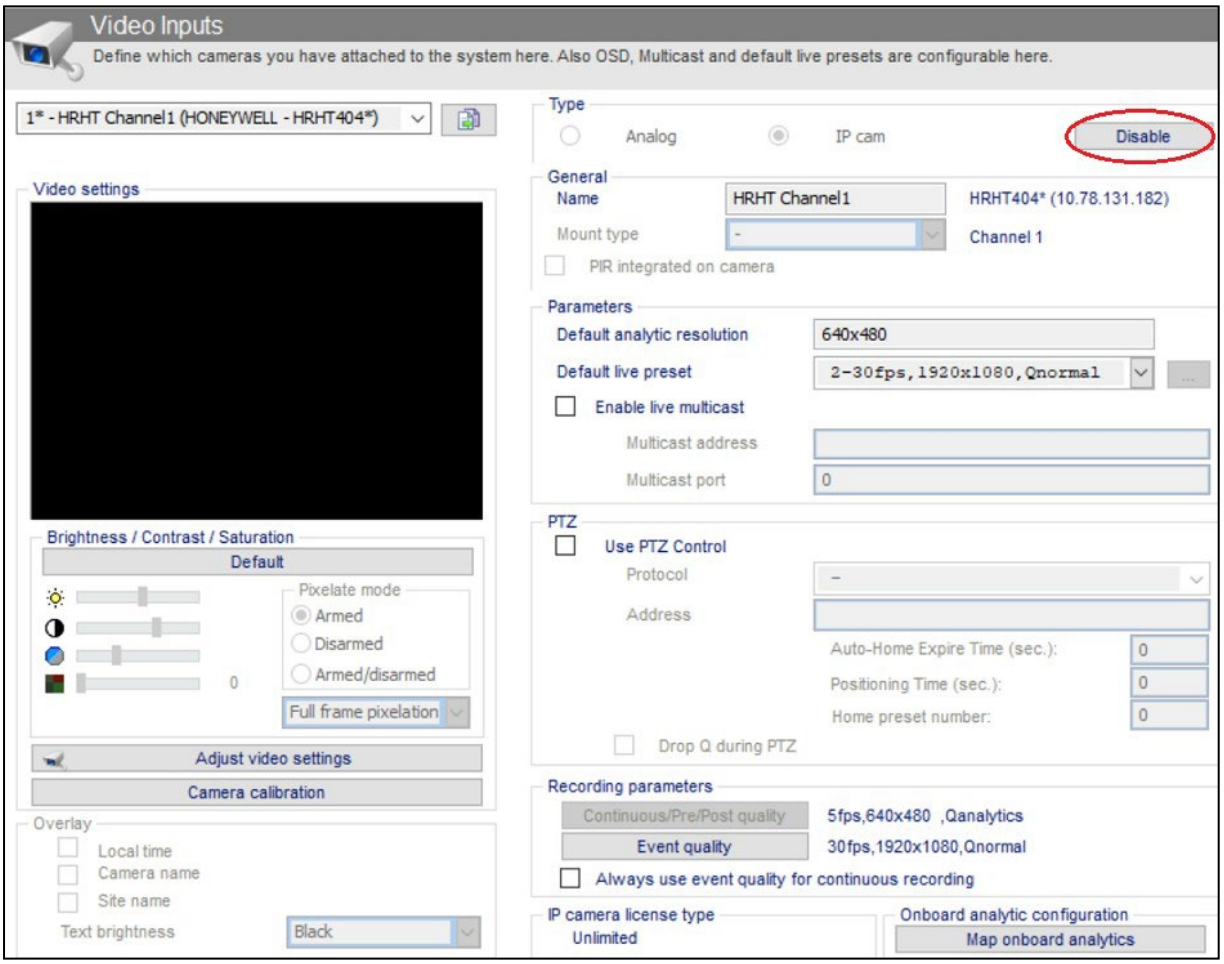
You can temporarily disable a camera, for example to prevent false alarms during maintenance.
The system remembers the camera settings, and will restore them automatically when you enable the camera again. It will also automatically reassign any analytics application licenses (if still available) and analytics configuration that was applied to the camera.

> ***Caution!***
>
> Before re-enabling analogue cameras, make sure to select the correct BNC input.

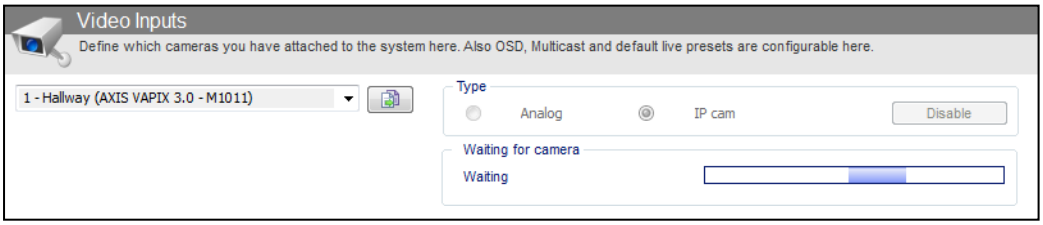
To disable a camera, proceed as follows:

1. Choose **System** > **Connections** > **Video Inputs**, and select the desired camera.

2. Click **Disable**.



The following screen appears while the system disables the camera:



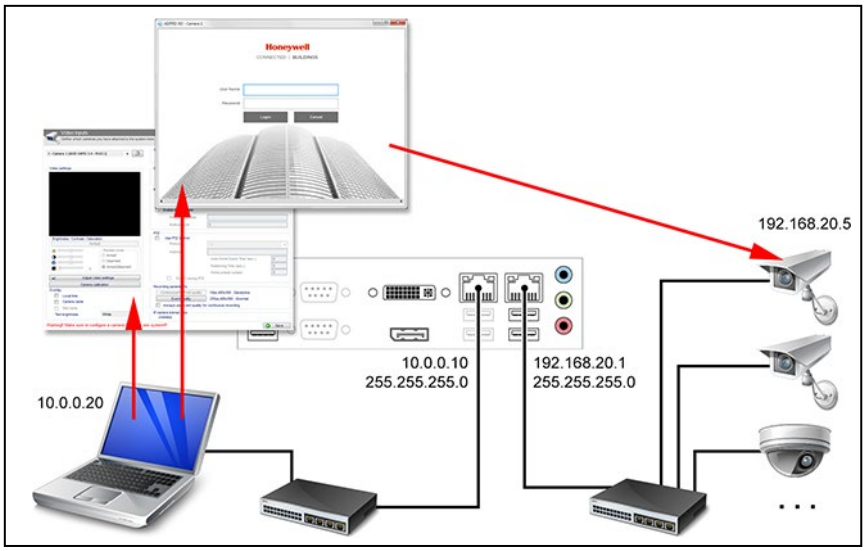
Note

You can continue working while the system enables the camera in the background. Select the next camera in the camera list.

3. When finished, click **Save**.

7.11 Remote Access to IP Camera

The device network (eth0) and the camera network (eth1) are separate networks. To use the client, your PC needs to be in the eth0 network. If you want to access an IP camera's web interface for configuring the camera from that same PC, you need to change your PC's IP address and set it in the eth1 network. However, with firmware version XO 4.0 and above, this is no longer necessary. A Technician user can connect to an IP camera's web interface from within the XO client. The system opens a special browser window; running simultaneously with the XO client.



You can access all configured IP cameras on the XO device, even if they have been disabled in the XO client.

The following restrictions apply:

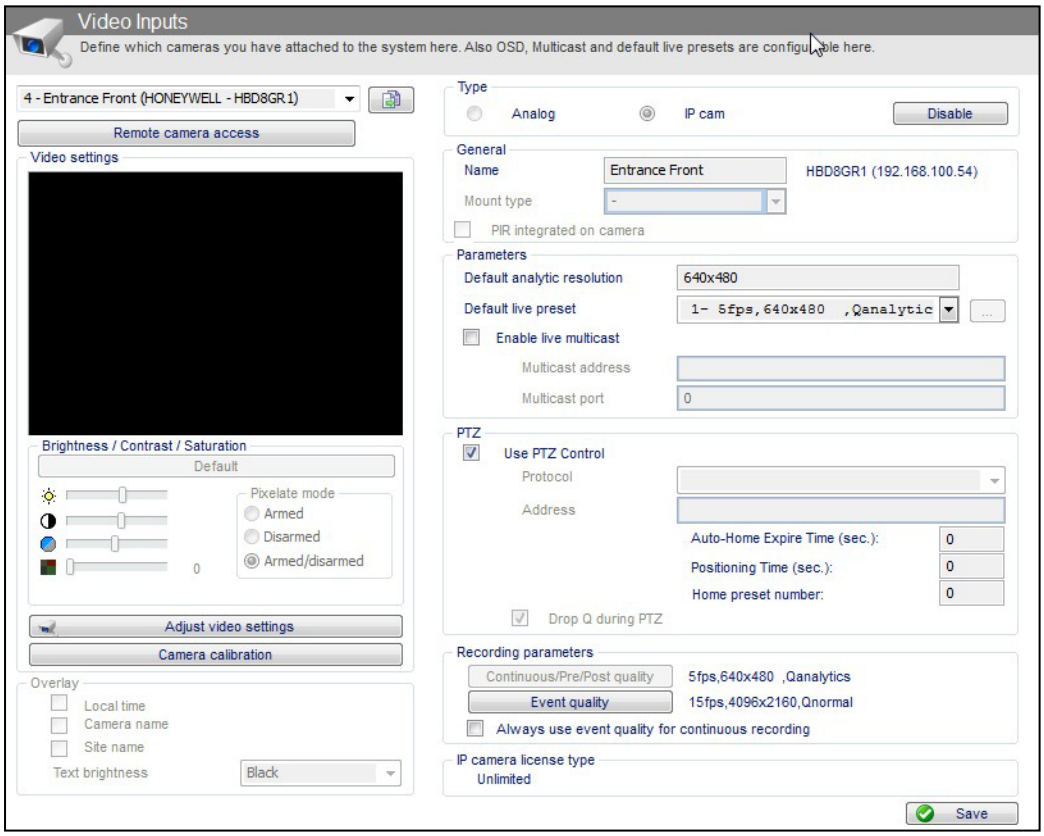
- The IP camera must have been enabled at least once on the XO device before remote access is available.
- Remote access is not available for IP cameras using the generic driver.
- Remote access is disabled when the Technician grant is disabled.
- Remote access is disabled when the Technician user closes the client.
- If the client stays open, remote access is disabled 4 hours after the Technician has opened the special browser window. If the Technician opens multiple windows, remote access is disabled 4 hours after the last window was opened.

While remote camera access is enabled, system input 0091 – [SYST] – TUNNEL IP CAM is active.

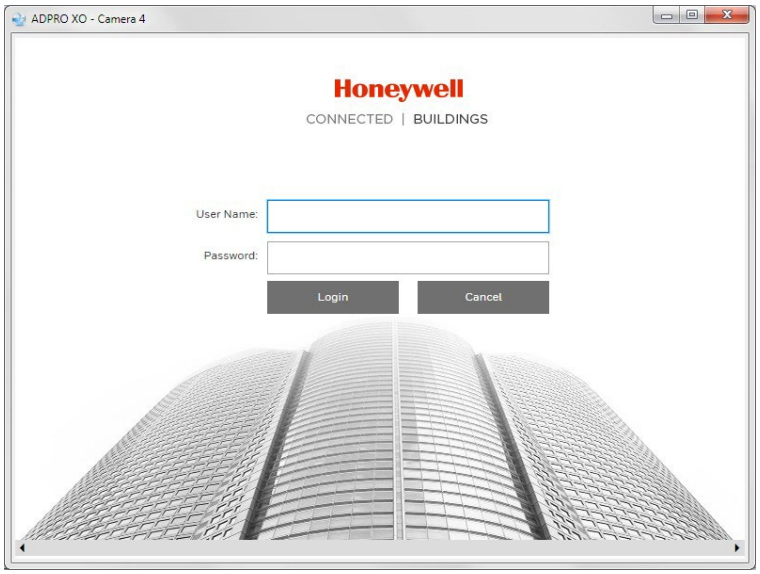
To access an IP camera's web interface, proceed as follows:

1. Open the XO client, and log on as Technician.
2. Choose **System** > **Connections** > **Video Inputs**.

3. Select the desired IP camera from the list.



4. Click **Remote camera access** (just below the camera list). The system opens a separate window with access to the camera web interface. The example below is for a Honeywell camera.



5. Log on to the camera web interface and change any settings as required.
6. Test if the camera and any analytics running on it still function as desired.
7. Log off and close the window when finished.

8 Audio

8.1 About Audio

8.1.1 Audio Input

If you want to use audio from a camera, you have to enable the camera's audio input in the XO client so that the system can **record sound** together with the video. You can then **listen to the sound during playback** of the recorded footage.

Furthermore, you can separately enable audio input for the **live view**, so that you can **listen to sound** from the site **while watching live images**. If you are live viewing more than one camera simultaneously (matrix view), the sound you hear is from the camera that is currently selected in the matrix.

You can also use IP audio devices that provide audio in (for example the Axis horn speaker that has a built-in microphone). You configure these devices just like an IP camera. An IP audio device occupies an IP channel.

Note

- If the connection bandwidth is low, Honeywell recommends to disable live audio streaming.
- Audio in is unbalanced audio.
- Enabling/disabling audio inputs for recording requires a system restart.

8.1.2 Audio Output – Talkback

Talkback to the site works via the **Live Video** window. You select a camera, and then use the microphone (typically connected to the client PC) to talk to the site via the speaker that is associated with that camera. If you are using multiple speakers (via VM22A or VM22E audio switchers), or audio out over IP (speaker built in or connected to IP camera), you have to associate the cameras with the desired speaker or speakers.

8.1.3 Full Duplex Mode

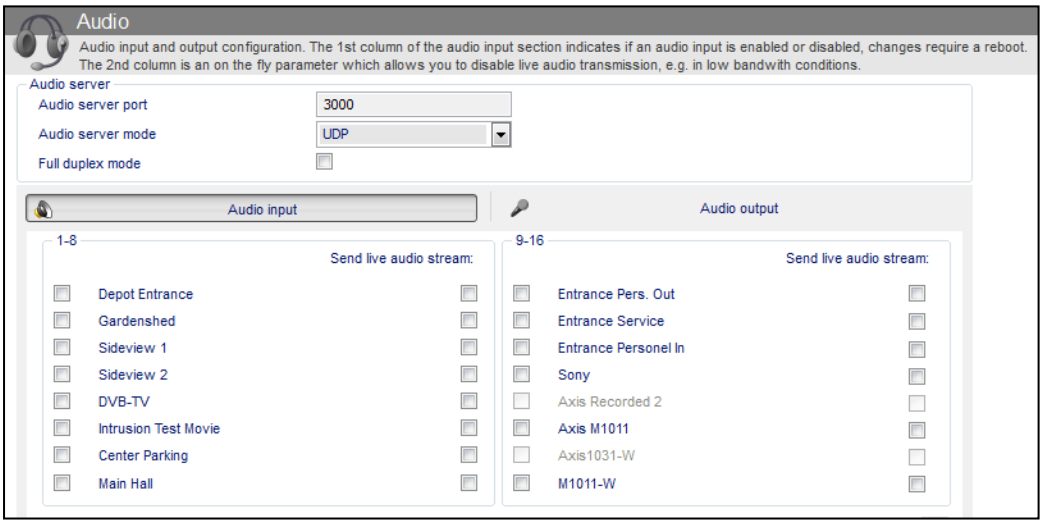
Normally, audio transmission is one way only: you can either listen to incoming audio, or speak to the site, but not both at the same time.

You can enable full duplex mode to allow simultaneous communication in both directions (talk and listen – not recommended).

8.2 Audio Communication Setup

To specify the general communication settings for audio, proceed as follows:

1. Choose **System** > **Connections** > **Audio**.



2. Under **Audio server**, provide the following information:

Item	Description	Default value
Audio server port	Type the port number for transmitting audio from the client to the XO device. In a network with multiple XO devices, and if you need to access the devices from an external network (for example, a CMS via router/firewall), you have to specify a **unique audio server port number** for each device. For example: 3000 for the first device, 3001 for the second… **Do not use** port numbers **3040** and **3041**: these port numbers are reserved for NetFinder and network I/O protocols.	3000
Audio server mode	Select the desired protocol (UDP or TCP) for transmitting audio.	UDP
Full duplex mode	Select this checkbox if you want to allow simultaneous communication in both directions (talk and listen – not recommended).	Off

3. Click **Save**.

Next, you can set up audio inputs and outputs.

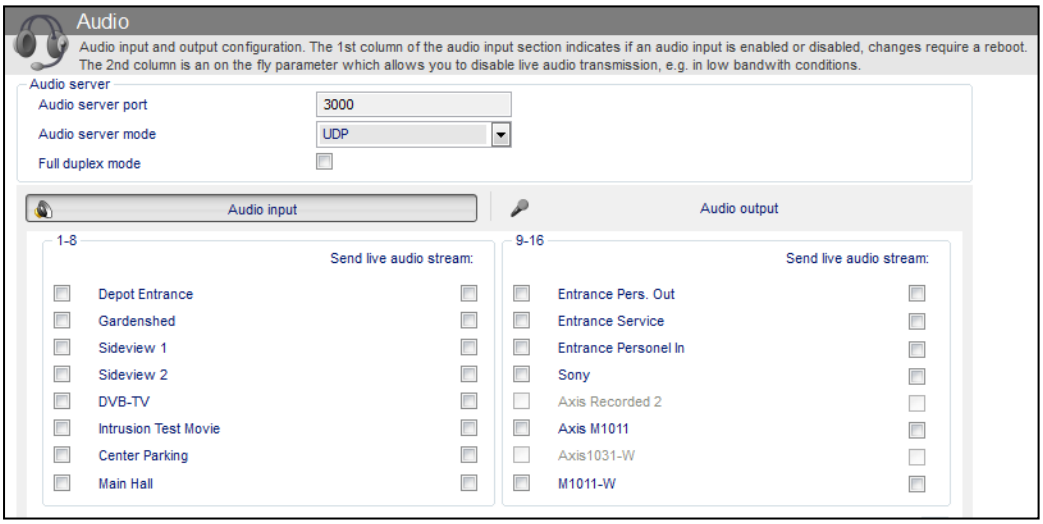
Note

If you switch full duplex mode on or off, you need to click a different camera in the live view for the change to take effect.

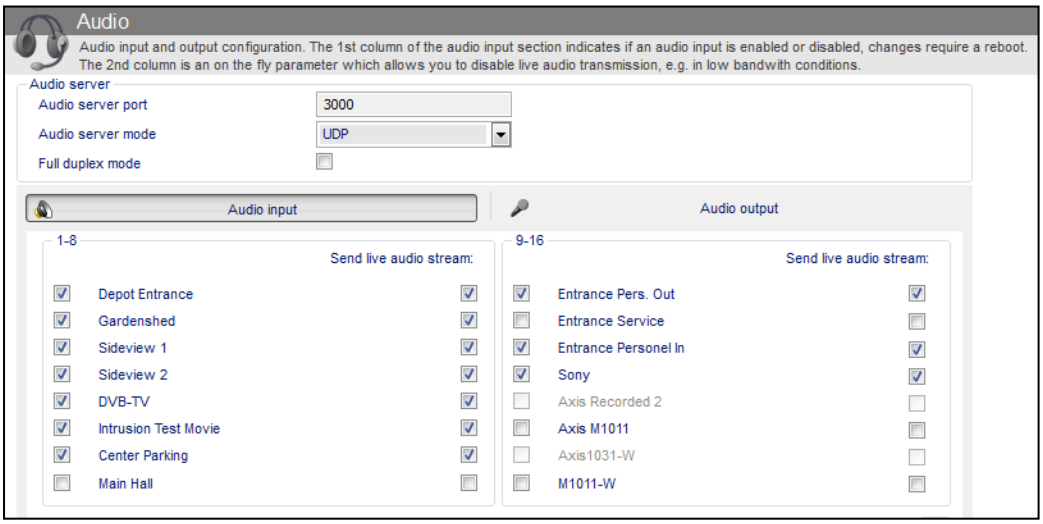
8.3 Setting up Audio Inputs

To set up audio inputs for recording or live listening, proceed as follows:

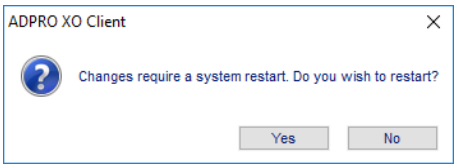
1. Choose **System** > **Connections** > **Audio**.



2. To record audio from a camera: under **Audio input**, select the checkbox on the left side of the camera name.
3. To enable audio in the live view for a camera, also select the camera's checkbox in the **Send live audio stream** column.



4. Click **Save**. If you have enabled/disabled audio inputs, the system needs to restart:



5. Click **Yes**. The following warning appears:



6. Click **OK** to confirm. The XO device restarts. If you have selected audio inputs for cameras that do not support audio, the system will automatically deselect those cameras.

8.4 Setting up Audio Outputs

If you are using multiple speakers (via VM22A or VM22E audio switchers), or audio out over IP (speaker built in or connected to IP camera), you have to associate the cameras with the desired speaker or speakers. With audio switchers, you also need to specify the switcher type in the MIO card setup.

You can test the audio output by playing a sound clip.

8.4.1 Specifying the Audio Switcher Type

You only need to execute this procedure if you are using audio switchers (VM22A or VM22E).

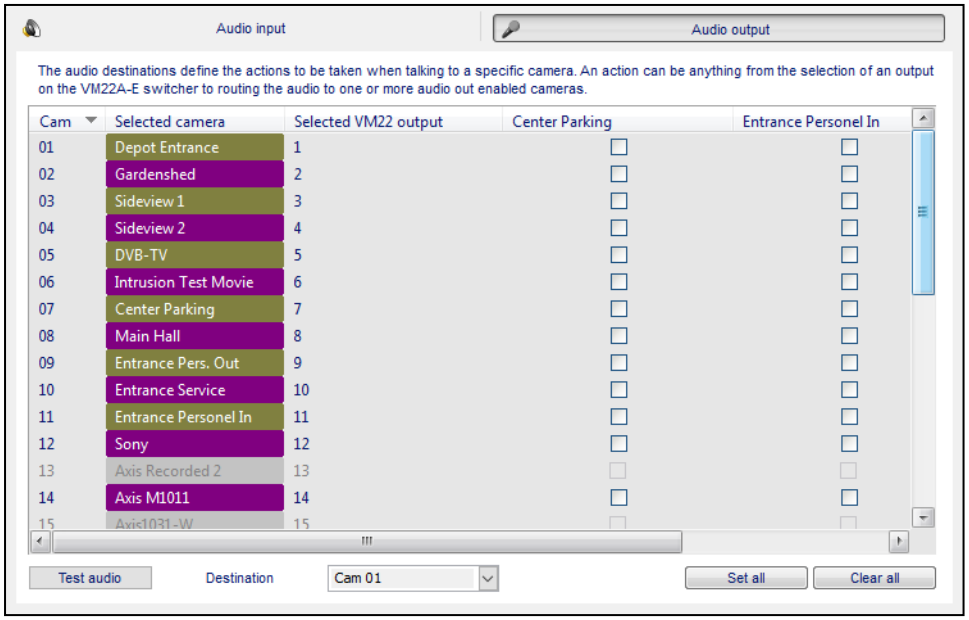
To specify the audio switcher type, proceed as follows:

1. Choose **System** > **Connections** > **I/O**.
2. Under **On the box I/O**, click the first line in the list, and then click **Configuration**.
3. Under **Audio switcher type**, click the correct switcher type: **VM22A** or **VM22E**.
4. Click **OK**.
5. Click **Save**.

8.4.2 Associating Cameras with Audio Outputs

To associate cameras with the desired audio outputs, proceed as follows:

1. Choose **System** > **Connections** > **Audio**.
2. Click the **Audio output** tab.

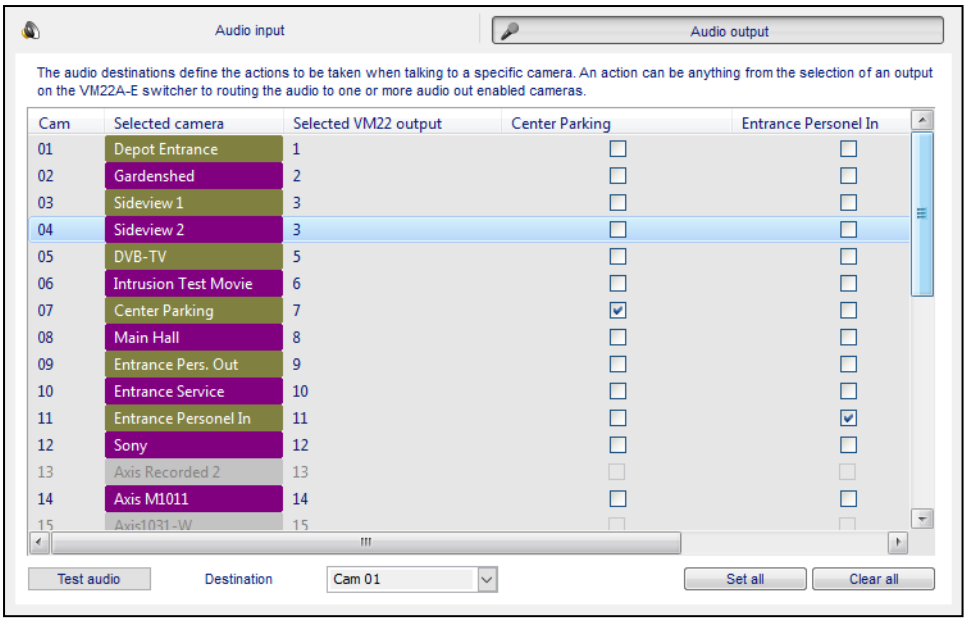


The screen displays the following information:

Item	Description
Cam	Camera number
Selected camera	Camera name

Item	Description
Selected VM22 output	The number of the audio output on the VM22A/VM22E audio switcher. By default, the system associates each camera to the audio output with the matching number (camera 1 to output 1, camera 2 to output 2…). If you are not using audio switchers, you can leave the settings as they are.
Cameraname	The system displays a column for each IP camera that supports audio out over IP. The camera name appears as the column title. The example above shows columns for the cameras named **Center Parking** and **Entrance Personel In**.

3. To associate a camera with a VM22 output, click in the **Selected VM22 output** column and type the number of the desired audio output. For the numbering of the audio outputs, see the *VM22A Audio Switcher – Installation and User Manual*, or the *VM22E Audio Switcher Technical Manual* (29541).
4. To associate a camera with the speaker built in or connected to an IP camera, click the corresponding checkbox in the column for the desired IP camera.
   Use the **Set all**/**Clear all** buttons to select/clear all checkboxes at once.



   The example above shows:

   - Cameras 03 and 04 are both associated with VM22 output 3.
   - Cameras 07 (Center Parking) and 11 (Entrance Personel In) are associated with their own audio outputs.

5. Click **Save**.
6. To test audio out, select the desired camera number in the **Destination** box, and then click **Test audio**. The system will play a sound clip.

8.5 Using IP Audio Devices

There are several IP audio devices that you can use for audio in/out, such as the Axis Network Horn Speaker (C3003-E) and the Axis P8221 I/O Audio Module. For details on the supported features of the IP audio devices, see the *Supported IP Camera List* (26742).

You manage an IP audio device on the XO device as if it were an IP camera with audio in and audio out capabilities:

- You connect the IP audio device to the IP camera network, and enable it in the XO client as an IP camera. The audio device occupies one IP channel. As there is no video from the device, the system will display a speaker icon in the live/recorded video windows.
- You enable audio in and audio out just like for an IP camera.

- You select it for talkback in the Live Video window just like a camera with audio out.
- You can set up recording for the device. When you play back the recording, the system will display a speaker icon instead of video, but you will hear the recorded sound (audio in from the built-in microphone and audio out from talkback).

9 Recording Behaviour

9.1 Setting up Recordings

You can automatically record the images from each connected camera. The system stores the recordings on the XO device's hard disk(s). You can play back the recordings in the **Recorded video** window. The system can automatically clean up old recordings, to comply with local regulations and to prevent that the system runs out of disk space.

You set up recording conditions to define:

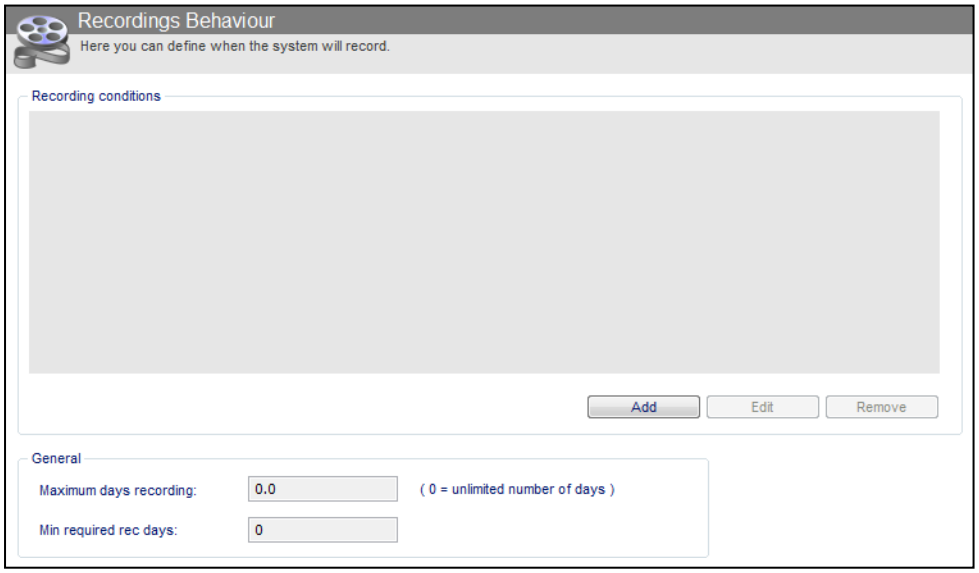
- A descriptive name for the recording.
- The cameras from which you want to record; and any desired camera actions: activating an output, moving to PTZ preset positions (typically for recording on event).
- When you want to record:
  - Dates, days of the week, holidays.
  - Time: time zones in the selected days.
- What you want to record:
  - Everything = continuous recording
  - Events only: which events, how long to record before/during/after.
    For event recording, you can choose to lock the recordings, so that the system does not erase them automatically during clean-up.

You can set up as many recording conditions as needed. Each step is described in detail in the following sections.

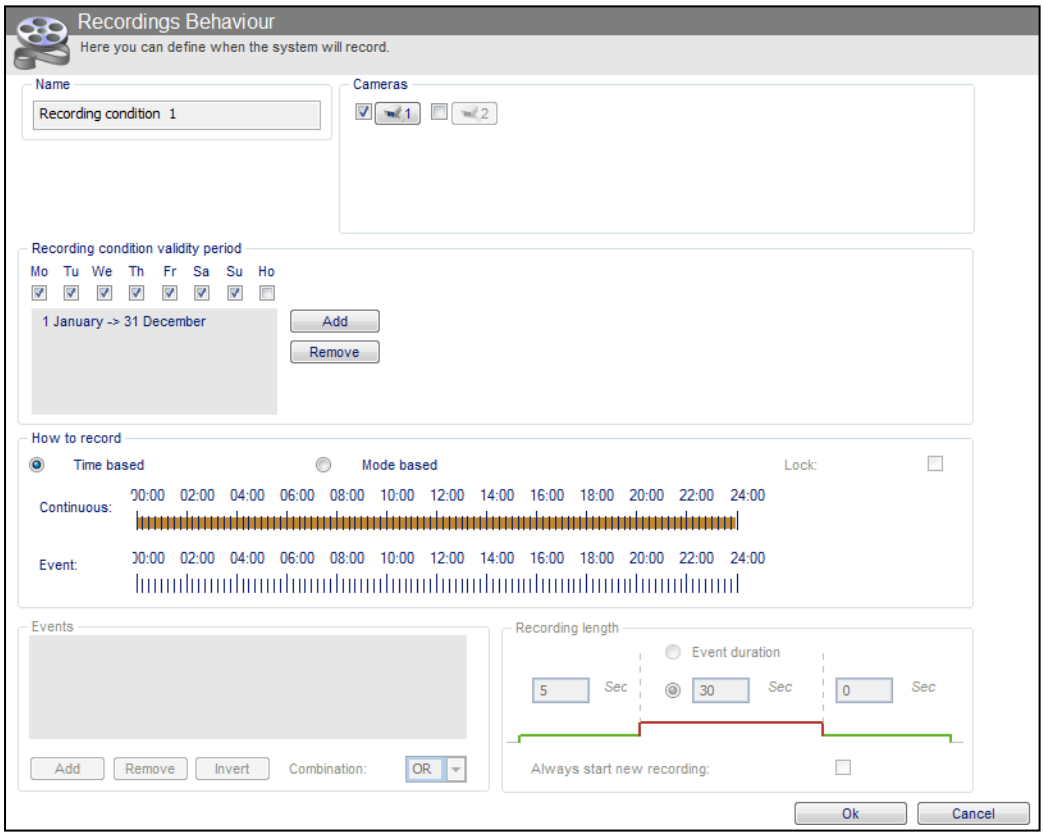
9.2 Creating Recording Conditions

To create a recording condition, proceed as follows:

1. Choose **System** > **Behaviour** > **Recordings Behaviour**.



2. Click **Add**.



3. In the **Name** box, type a suitable name for the recording (max. 20 characters).
4. Under **Cameras**, select the cameras that you want to record from. You can select multiple cameras if necessary. The screen only displays the active cameras.

Next, you can specify the camera actions for the recording.

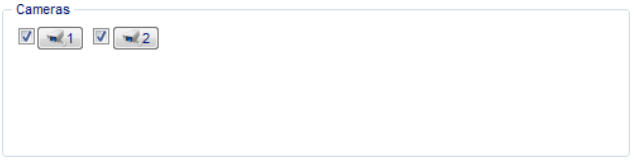
9.3 Recording-Controlled Camera Actions

The recording controlled camera actions include:

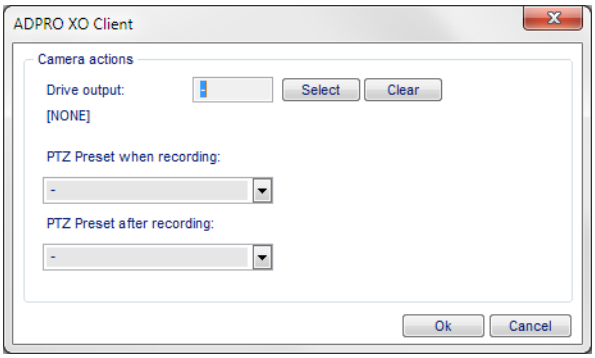
- Moving PTZ cameras to preset positions during and after recording. You have to set up the PTZ preset positions first. For instructions, see *Managing PTZ Preset Positions*.
- Activating an output when the recording starts. You can activate one output per recording condition. You have to set up the desired output first. For instructions, see *Recording-Controlled Outputs*.

To set recording-controlled camera actions, proceed as follows:

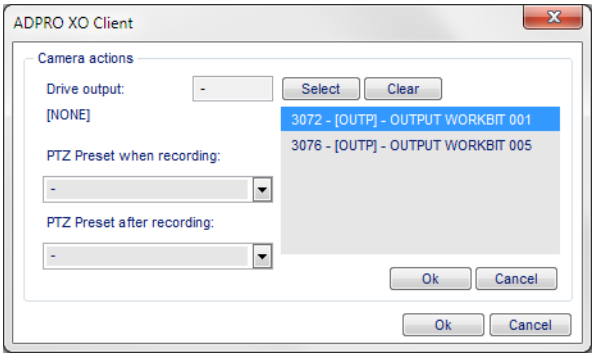
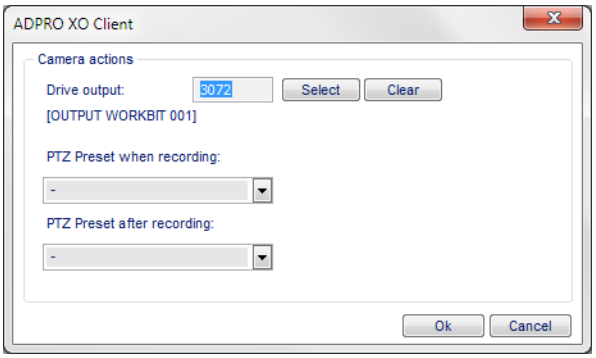
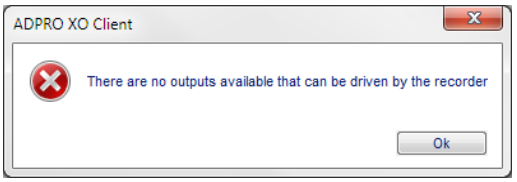
1. Make sure that you have selected at least one camera for recording.



2. Click the camera number. The following screen appears:



3. Provide the following information for the selected camera:

Item	Description
Drive output	If you want the recording on this camera to activate an output, click **Select**, and then click the desired output in the list that appears.  Click **OK** to confirm.  You have to set up the recording-controlled output first. If you did not set up any outputs first, the following error message appears:  For setting up recording-controlled outputs, see *Recording-Controlled Outputs*.
PTZ Preset when recording	For PTZ cameras only: if you want to move the camera to a specific PTZ position during the recording, select the desired PTZ preset position.
PTZ Preset after recording	For PTZ cameras only: if you want to move the camera to a specific PTZ position after the recording, select the desired PTZ preset position.

4. Click **OK** to close the camera actions window.

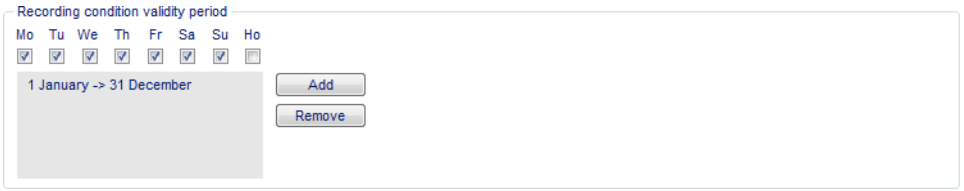
5. Repeat for other cameras.

Next, you will set up the active period (date, days of the week, holidays) for the recording.

9.4 Setting up the Active Periods

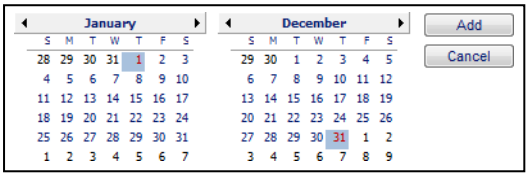
9.4.1 Dates and Days of the Week

By default, the recording is active during the full year (January 1st to December 31), and on all days of the week except on the holidays as defined in the calendar. For the list of holidays, see *Calendar*.

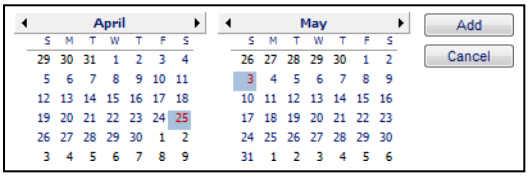


To set up the active period or periods for the recording, you will work in the **Recording condition validity period** section. Proceed as follows:

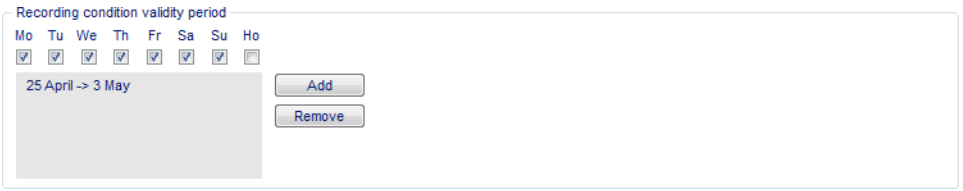
1. If you want to record in specific periods of the year, first delete the existing period for the whole year: click **1 January -> 31 December**, and then click **Remove**.
2. Click **Add**. The following section appears:



3. Select the start date on the left, and the end date on the right.



4. Click **Add**. The selected period appears in the list.



5. Repeat to add more periods in the year.

   Select the checkboxes for each day of the week that you want to record in the specified periods of the year: **Mo–Su** for Monday–Sunday, and **Ho** for the holidays.
   Clear the checkboxes for the days you do not want to record.
   Remember that the days are valid for all the periods in this recording. If you need different days in different periods, then set up different recordings.

Next, you will specify the active time zones within the selected periods and days.

9.4.2 Time in the Days: Time-Based and Mode-Based Recording

For defining the active time zones in the days for recording, you have the following options:

- If the required time zones for recording are the same for all days, you use time-based recording. In the recording condition, you only need to indicate the required time zones on a time bar.
- If you want to set up different time zones on different days, you use mode-based recording. You can define up to 4 different recording modes. You can activate modes using an automated schedule, or using a switch. For instructions on setting up recording modes, see *Recording Modes*.

  In the recording condition, you only need to select the modes in which you want to record.

You specify whether to use time-based or mode-based recording together with continuous or event recording. Details are in the following sections.

9.5 Continuous Recording

9.5.1 Definition

With continuous recording, you record everything from the selected cameras, on the selected dates/days, and:

- during the selected time zones (for time-based recording).
- in the selected recording modes (for mode-based recording). Both methods are described in detail in the following sections.

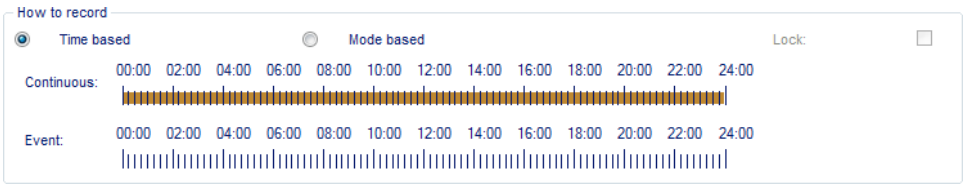
Note

- Although you can combine continuous recording with event recording in one recording condition, Honeywell recommends to create separate recording conditions for continuous and event recording.
- You cannot lock continuous recordings.

9.5.2 Time-Based Continuous Recording

To set up time-based continuous recording, proceed as follows:

1. Under **How to record**, click **Time based** to activate the recording in function of a time schedule.

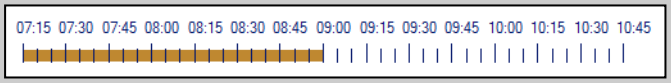


   You will indicate the desired time zones in the **Continuous** time bar. By default, the **Continuous** time bar is completely selected (coloured). Remember that the time zones are the same for all the selected dates/days in the recording.

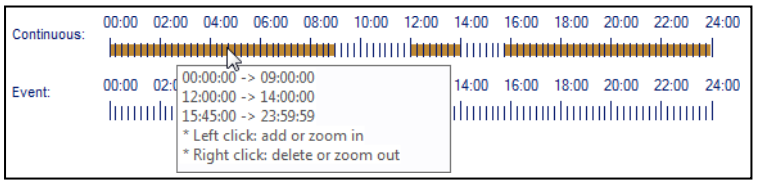
2. To define separate time zones, you need to clear the existing time zone first: right-click anywhere in the **Continuous** time bar. Next, you will define the active time zones.
3. Drag the mouse over the desired time zones in the **Continuous** time bar. The selected period colours orange. You can add maximum 8 different time zones in the time bar.



4. To remove a time zone, right-click it.

> **Note**
>
> To make accurate selections, you can zoom in (up to the minute): move the mouse pointer just above the coloured time bar. The pointer changes into a magnifying glass. Drag the mouse over the part that you want to zoom in on. A blue line appears while dragging.
>
> 
>
>
> 
>
>
> To zoom out again to the full day, right-click just above the time bar.

5. To see the details of the selected time zones, position the mouse cursor over the time bar. The system displays the start and end times of each zone.

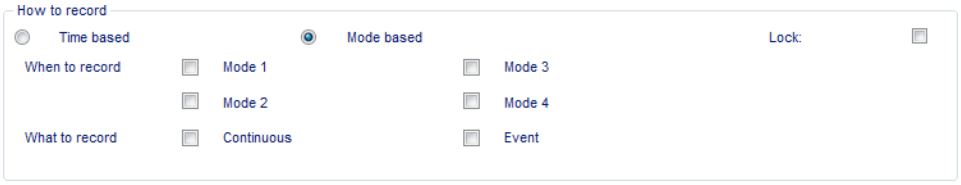


6. When finished, click **OK**.
7. Click **Save**.

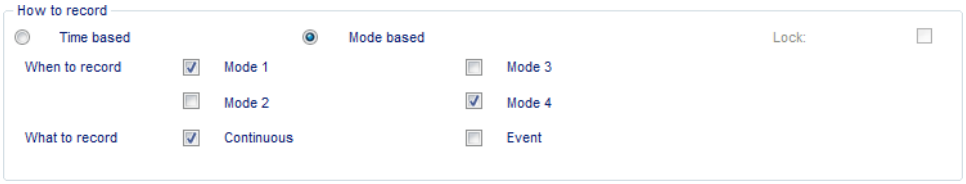
9.5.3 Mode-Based Continuous Recording

To set up mode-based continuous recording, proceed as follows:

1. Under **How to record**, click **Mode based** to activate the recording in function of the recording mode.



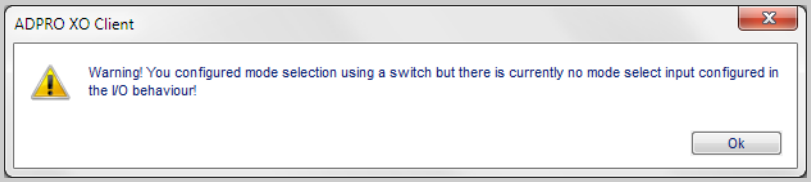
2. Next to **When to record**, select the modes when you want to record.
3. Next to **What to record**, select the **Continuous** checkbox.



4. Next to **What to record**, clear the **Event** checkbox (to prevent conflicts).
5. Click **OK**.

Note

If you use a switch to change recording modes, the following warning will appear if you did not yet defined an input for switching:



To set up an input for switching recording modes, see *Recording Mode with Manual Selection*.

6. Click **Save**.

9.6 Recording on Event

9.6.1 Definition

With recording on event, you start a recording based on an event (input), on the selected dates/days, and:

- during the selected time zones (for time-based recording).
- in the selected recording modes (for mode-based recording).

Both methods are described in detail in the following sections.
You define which inputs trigger the recording, and how long to record before/during/after the event. If the events follow each other so quickly that the recordings overlap, the system will merge multiple recordings into one recording.

Note

- Although you can combine continuous recording with event recording in one recording condition, Honeywell recommends to create separate recording conditions for continuous and event recording.
- If recordings with different quality settings overlap, the system applies the highest quality and image rate.
- The system can record maximum 16 000 events a day (the counter is reset at night). If more events occur on the same day (overflow), the system will automatically switch to continuous recording for all cameras. These recordings will have CIF/SIF or nearest resolution, 25 fps, and quality 75 (level of compression). Overlapping recordings appear in blue on the timeline of the Recorded video window.
- With the TRANSMITTER system license, the recording on event is fixed to 5 seconds on pre-recording, 10 seconds on event recording, and no post-recording.

Furthermore, you can choose to lock the recordings, so that the system does not erase them automatically during clean-up. Locked recordings activate system input 0049 – [SYST] – LOCKED RECORDER (by default linked to the alarm profile NORMAL EVENT).

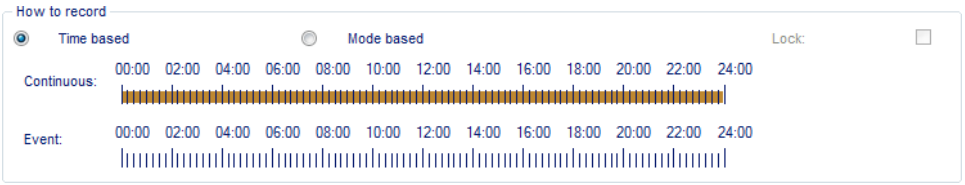
Caution!

The XO device cannot delete locked recordings. When it encounters a locked recording during automatic clean-up (for example after 30 days), the XO device **stops cleaning up**. When the device runs out of storage space, it also **stops recording**. For more information on handling locked recordings, see *Locked Recordings*.

9.6.2 Time-Based Recording on Event

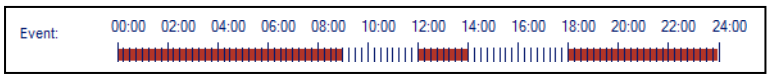
To set up time-based recording on event, proceed as follows:

1. Under **How to record**, click **Time based** to activate the recording in function of a time schedule.

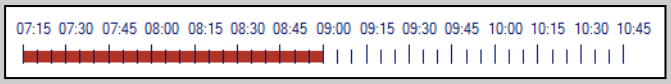


   You will indicate the desired time zones in the **Event** time bar. By default, the **Event** time bar is empty. Remember that the time zones are the same for all the selected dates/days in the recording.

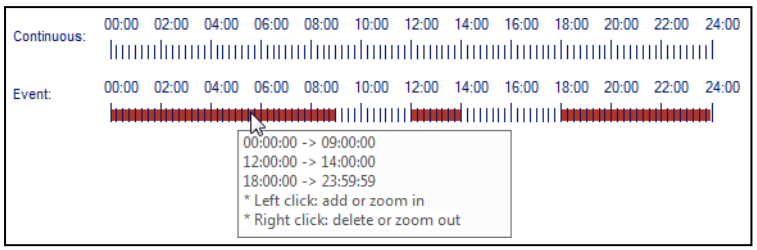
2. First, to prevent conflicts, clear the time bar for **Continuous** recording: right-click anywhere in the **Continuous** time bar. Next, you will define the active time zones for event recording.
3. Drag the mouse over the desired time zones in the **Event** time bar. The selected period colours red. You can add maximum 8 different time zones in the time bar.



4. To remove a time zone, right-click it.

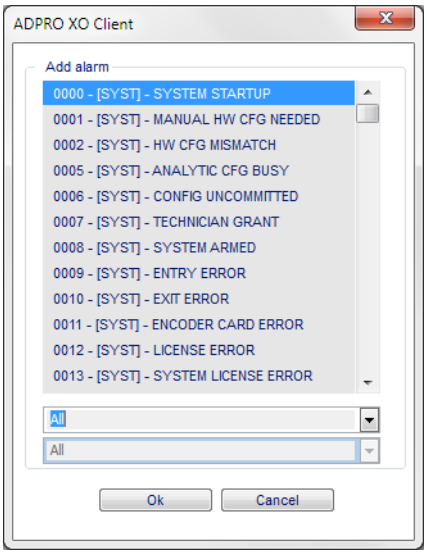
> **Note**
>
> To make accurate selections, you can zoom in (up to the minute): move the mouse pointer just above the coloured time bar. The pointer changes into a magnifying glass. Drag the mouse over the part that you want to zoom in on. A blue line appears while dragging.
>
> 
>
>
> 
>
>
> To zoom out again to the full day, right-click just above the time bar.

5. To see the details of the selected time zones, position the mouse cursor over the time bar. The system displays the start and end times of each zone.



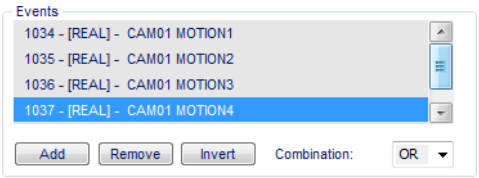
   Next, you will set up the events (inputs) that trigger the recording.

6. Under **Events**, click **Add**. The following window appears:

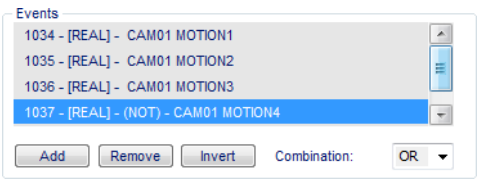


Use the filters below the list to reduce the list. If you filter on camera inputs, you can filter further on camera number.

7. Select the desired input, and then click **OK**. You can select multiple inputs as follows:
   - To select multiple non-consecutive inputs in the list, Ctrl+click each input.
   - To select multiple consecutive inputs in the list, click the first input, and then Shift+click the last input. The selected inputs appear in the Events list.



8. To invert an input (record when the input is inactive, stop recording when the input is active), select the input in the list, and then click **Invert**. The indication **(NOT)** appears in front of the input name in the **Events** list.



9. If you trigger on more than one input, select the correct operator in the **Combination** box:
   - AND: to record only if ALL the selected inputs are active.
   - OR: to record if at least one of the inputs is active. The first input that becomes active will trigger the recording.

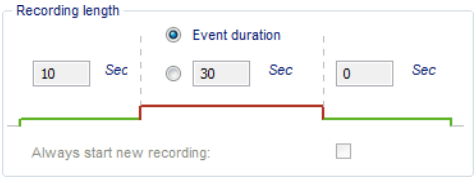
   Next, you will set the length of the recording.

10. Under **Recording length**, set up the length of the recording as follows:

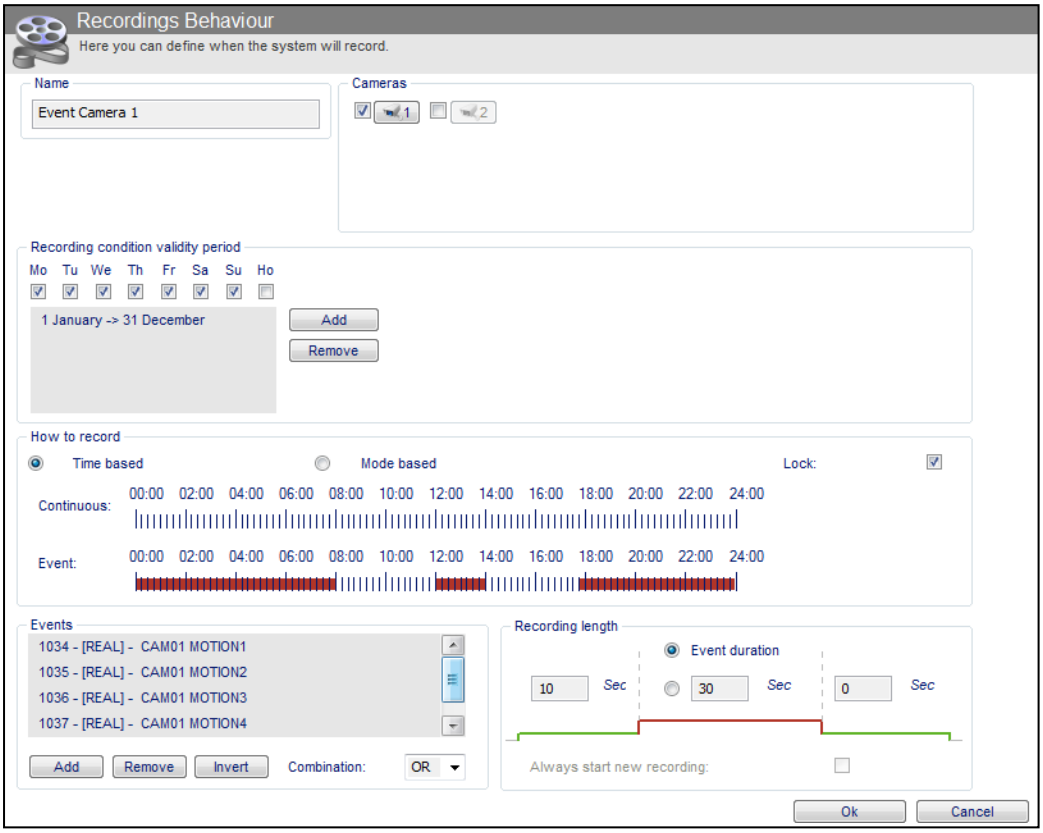
Item	Description
Pre event recording (left)	Click in the box on the left, and type the number of seconds that you want to record before the event. The maximum is 3600 s (= 1 hour).

Item	Description
Event recording (middle)	• To record as long as the event lasts (as long as the input is active), select **Event duration**. • To record a fixed number of seconds, select the option below. In the box, type the number of seconds that you want to record.
Post event recording (right)	Click in the box on the right, and type the number of seconds that you want to record after the event. The maximum is 3600 s (= 1 hour).

The example below uses 10 seconds pre event recording, recording while the event lasts, and no post event recording (0 seconds).



11. If you want to lock the recordings (so that the system cannot delete them automatically), select the **Lock** checkbox.

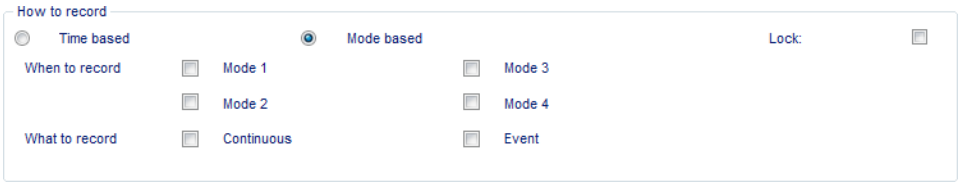


12. Click **OK**.
13. Click **Save**.

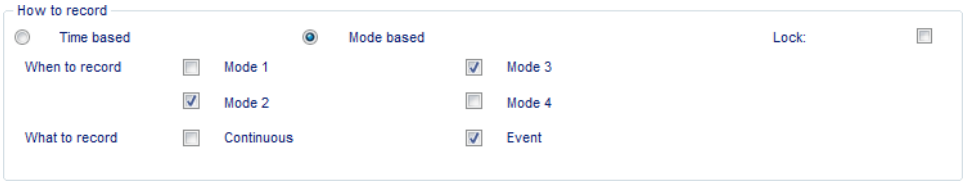
9.6.3 Mode-Based Recording on Event

To set up mode-based recording on event, proceed as follows:

1. Under **How to record**, click **Mode based** to activate the recording in function of the recording mode.

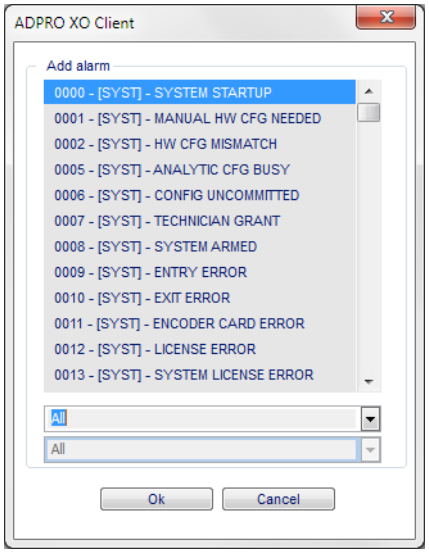


2. Next to **When to record**, select the modes when you want to record.
3. Next to **What to record**, clear the **Continuous** checkbox (to prevent conflicts).
4. Next to **What to record**, select the **Event** checkbox.



Next, you will set up the events (inputs) that trigger the recording.

5. Under **Events**, click **Add**. The following window appears:

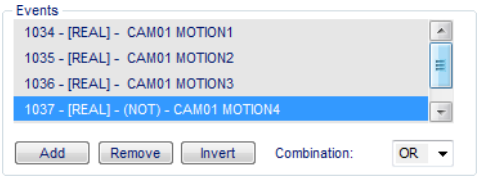


Use the filters below the list to reduce the list. If you filter on camera inputs, you can filter further on camera number.

6. Select the desired input, and then click **OK**. You can select multiple inputs as follows:
   - To select multiple non-consecutive inputs in the list, Ctrl+click each input.
   - To select multiple consecutive inputs in the list, click the first input, and then Shift+click the last input. The selected inputs appear in the **Events** list.



7. To invert an input (record when the input is inactive, stop recording when the input is active), select the input in the list, and then click **Invert**. The indication **(NOT)** appears in front of the input name in the **Events** list.



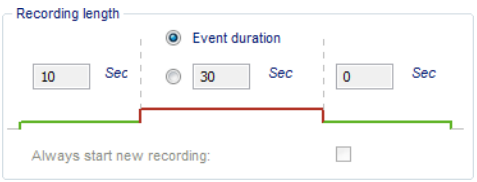
8. If you trigger on more than one input, select the correct operator in the **Combination** box:
   - AND: to record only if ALL the selected inputs are active.
   - OR: to record if at least one of the inputs is active. The first input that becomes active will trigger the recording.

   Next, you will set the length of the recording.

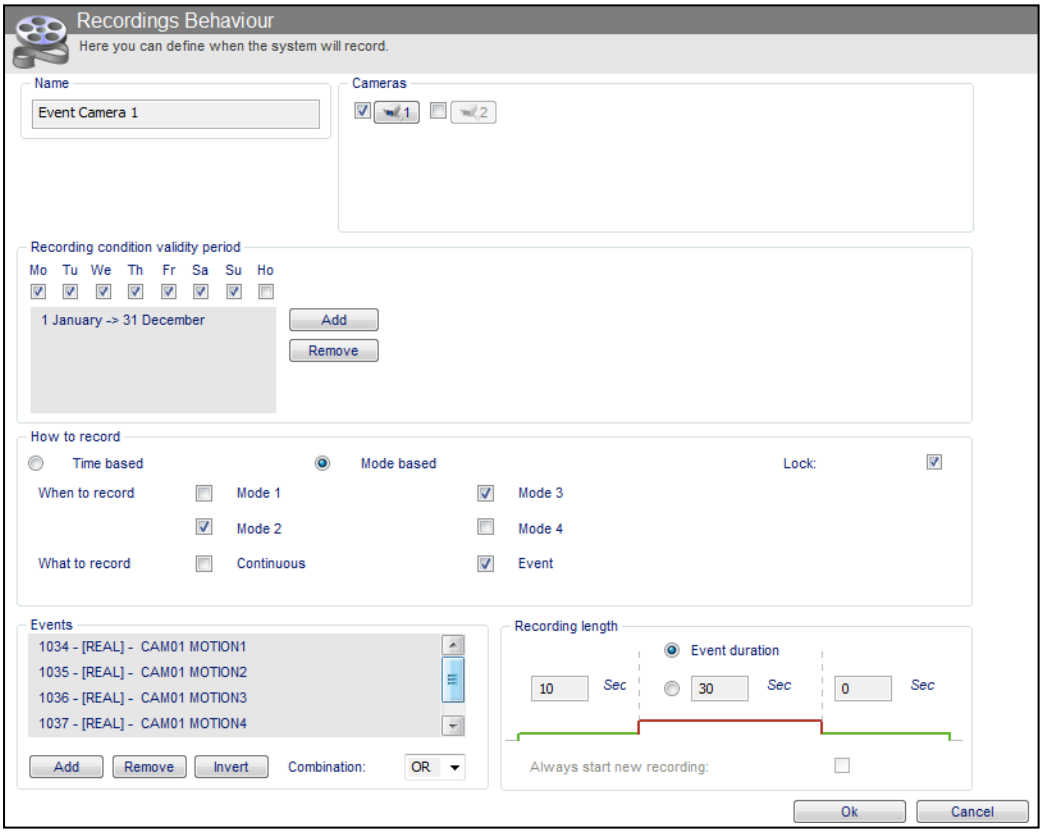
9. Under **Recording length**, set up the length of the recording as follows:

Item	Description
Pre event recording (left)	Click in the box on the left, and type the number of seconds that you want to record before the event. The maximum is 3600 s (= 1 hour).
Event recording (middle)	ı To record as long as the event lasts (as long as the input is active), select **Event duration**. ı To record a fixed number of seconds, select the option below. In the box, type the number of seconds that you want to record.
Post event recording (right)	Click in the box on the right, and type the number of seconds that you want to record after the event. The maximum is 3600 s (= 1 hour).

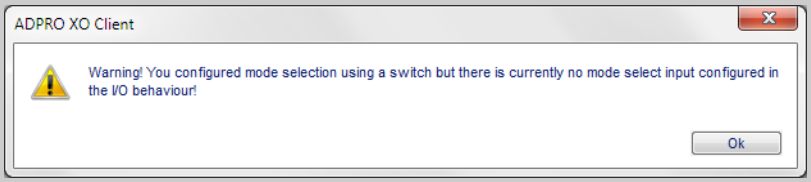
The example below uses 10 seconds pre event recording, recording while the event lasts, and no post event recording (0 seconds).



10. If you want to lock the recordings (so that the system cannot delete them automatically), select the **Lock** checkbox.



11. Click **OK**.

> **Note**
>
> If you use a switch to change recording modes, the following warning will appear if you did not yet defined an input for switching:
>
> 
>
>
> To set up an input for switching recording modes, see *Recording Mode with Manual Selection*.

12. Click **Save**.

9.7 Changing or Deleting Recording Conditions

To change or delete an existing recording condition, proceed as follows:

1. Choose **System** > **Behaviour** > **Recordings Behaviour**.
2. Select the desired recording condition in the list.
3. Proceed as follows:
   - To edit the recording condition, click Edit. Change the settings as desired, and then click OK.
   - To delete the recording condition, click Remove.
4. Click **Save**.

9.8 Automatically Erasing Old Video Recordings

Local legal requirements (variable and depending on state and region) may demand that the XO device can only store recordings for a limited time. When that time has passed, the system must erase the recordings.
You can let the system automatically clean up recordings that are older than a defined number of days.

Likewise, you can let the system keep a minimum number of days of recordings (available from version XO 4.00). The system will calculate if there is sufficient space on the hard disks in the XO device, and it will activate system input 0050 – [SYST] – STORAGE INSUFFICIENT if this is not the case. The system calculates the required space based on the past recordings, as follows:

- The system requires at least 24 hours of recordings to be able to estimate the required space. It will not activate the alarm if there are less than 24 hours of recordings. The more hours of recordings available, the more accurate the estimation will be.
- The system will activate the alarm if the recording disks are not full yet, but the system estimates that there is not enough free disk space for the required number of days.
- The system will activate the alarm if the recording disks are full and there are less than the required number of days of recordings on the disks. In this case, the system will also activate system input 0015 – [SYST] – HARDDISK FULL.

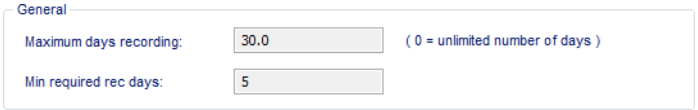
You can see how many days the system estimates that it can record in the **Harddisks** screen (**System** > **Maintenance** > **Harddisks**), in the **Estimated days, based on past recordings** box. For tips on adjusting your settings for the required number of recording days, see *Calculating the Write Speed*.

Caution!

- If you do not erase any recordings, or if you set the minimum days of recording too high (and ignore the STORAGE INSUFFICIENT message), the XO device will eventually run out of storage space. It will activate the system input 0015 – [SYST] – HARDDISK FULL, and it will stop recording.
- The XO device cannot automatically erase recordings on event that are locked. You have to unlock these recordings manually, so that the XO device can erase them. If not, the XO device stops erasing when it encounters the first locked recording during clean-up. When the device runs out of storage space, it will stop recording. For more information, see *Locked Recordings*.
- If you change the maximum number of recording days, remember that the system will delete recordings older than the maximum number of recording days. Back up the recordings first if necessary. For instructions, see Downloading and Storing Selected Video Recordings.

To automatically erase recordings, proceed as follows:

1. Choose **System** > **Behaviour** > **Recordings Behaviour**.
2. In the **Maximum days recording** box, type the number of days that you want to keep recordings. The system will delete any recordings older than that number of days.
   If you do not want to erase any recordings, type **0**.
3. In the **Min required rec days** box, type the minimum number of days that you want to keep recordings.
   If you do not want to use this feature, type **0**.
   The minimum number of days must be lower than the maximum number of days.



4. Click **Save**.

9.9 Recording Modes

9.9.1 About Recording Modes

The system can operate in up to 4 different recording modes. In each mode, the video recorder can behave differently. For example, you can record continuously in one mode, and record only on specific events in another mode. There are several ways to switch from one recording mode to another:

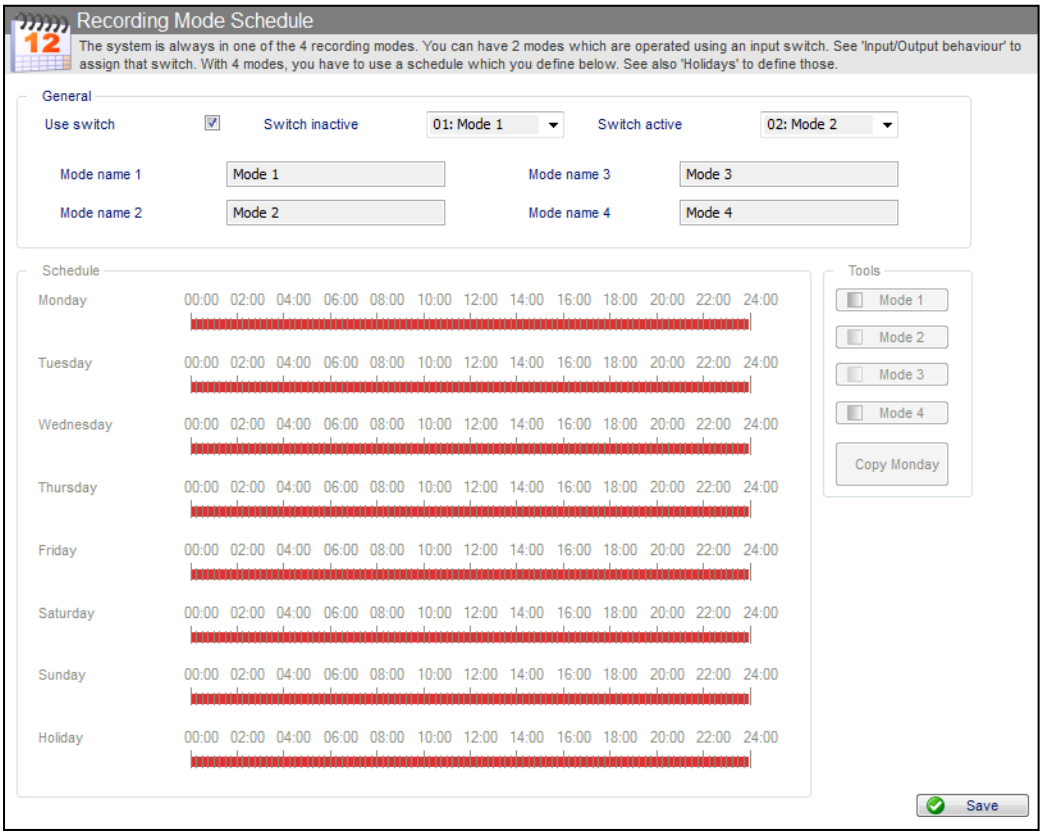
- Automatically, according to a time schedule. See *Recording Mode with Time Schedule*.
- Manually, using an input as a switch. See *Recording Mode with Manual Selection*.
- It is also possible to change the recording mode using third-party software. For more information, see the documentation of the ADPRO XO Software Development Kit (SDK).

9.9.2 Recording Mode with Time Schedule

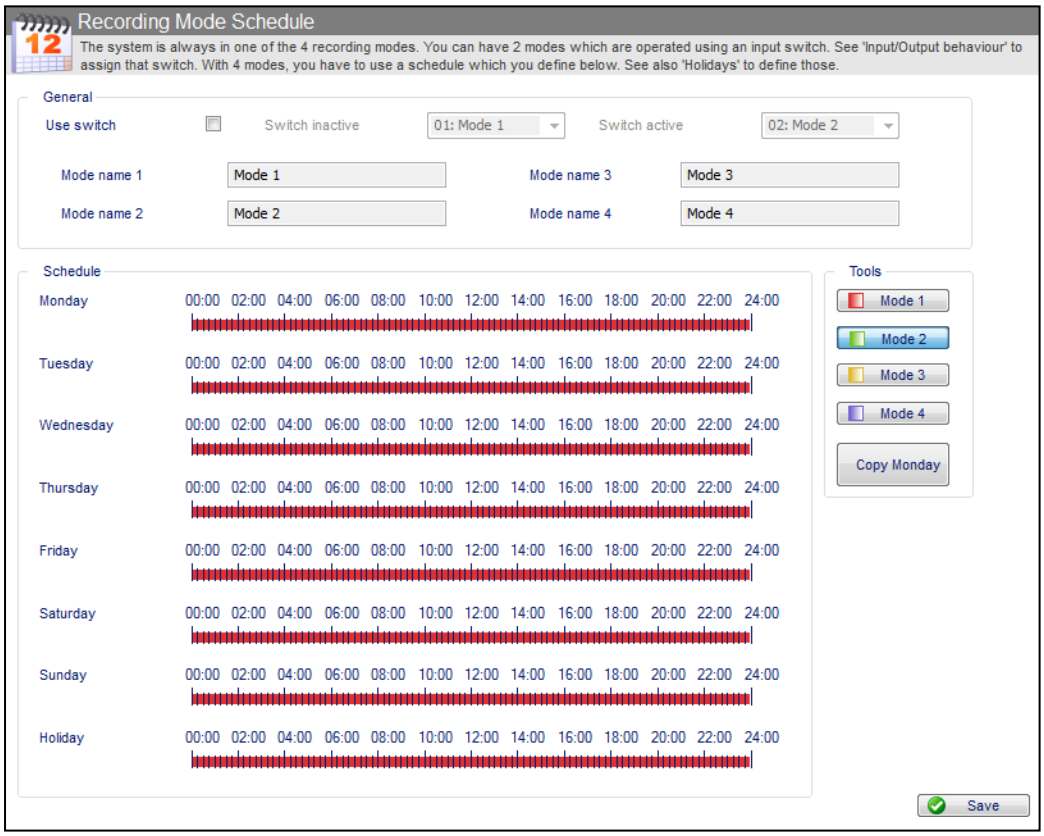
With a time schedule, you can automatically switch between up to 4 recording modes. You define which mode is active when. Only one mode can be active simultaneously. You can set up an individual schedule for each day of the week (Monday–Sunday), and for holidays. To define the holidays, see *Calendar*.

To set up automatic switching between recording modes, proceed as follows:

1. Choose **System** > **Behaviour** > **Recording Mode Schedule**.



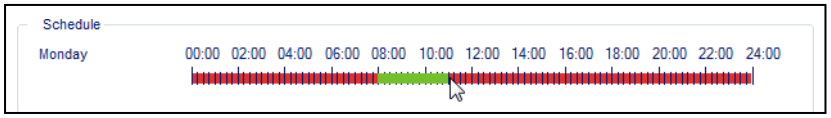
2. Clear the **Use switch** checkbox.



3. In the **Mode name 1** to **Mode name 4** boxes, type a meaningful name for each of the recording modes. You can use up to 20 characters. An example:
   - Mode 1 = NIGHT
   - Mode 2 = DAY
   - Mode 3 = HOLIDAY
   - Mode 4 = SPECIAL.

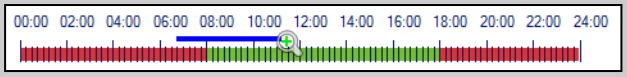
   Under **Schedule**, a time bar is visible for each day (Monday–Sunday), and one for holidays. By default, the system operates in mode 1 during the whole schedule: all time bars are red.

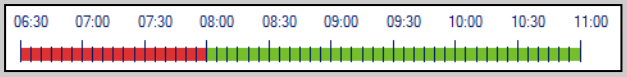
4. Under **Tools**, click the desired mode button (**Mode 1**–**Mode 4**), and then drag the mouse over the day and time when the mode has to be active. Where you drag, the time bar changes to the colour of the selected mode.



Note

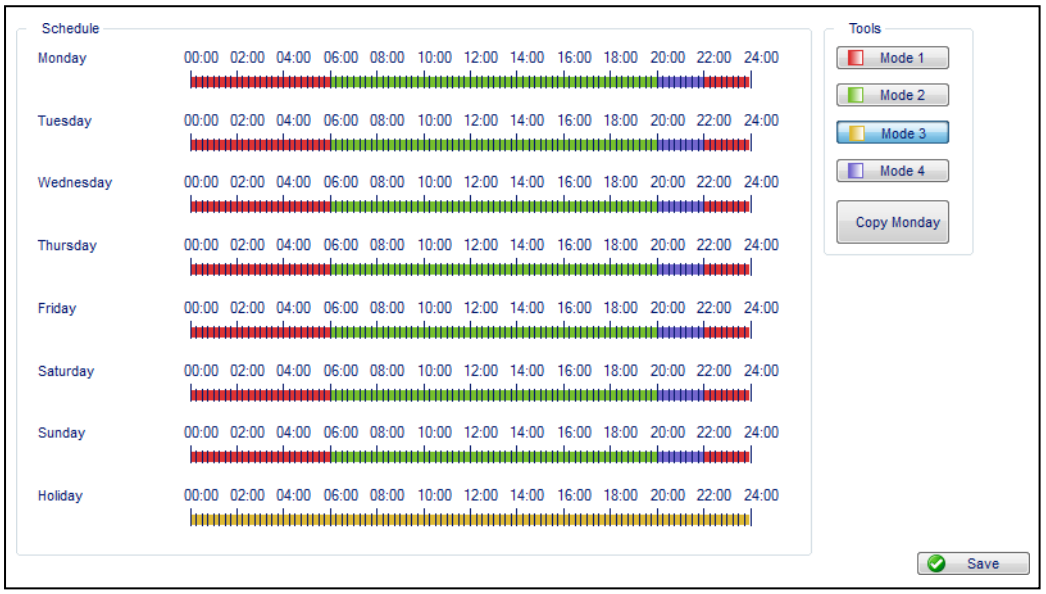
To make accurate selections, you can zoom in on a part of the day: move the mouse pointer just above the coloured time bar. The pointer changes into a magnifying glass. Drag the mouse over the part that you want to zoom in on. A blue line appears while dragging.





To zoom out again to the full day, right-click just above the time bar.

5. If you have a repeating schedule, you can copy the schedule from Monday to all other days (including holidays): click **Copy Monday**, and then click **Yes** to confirm.
6. Adjust until you have the correct schedule for each day.



7. Click **Save**.

The system now switches automatically from one mode to another according to the schedule.

9.9.3 Recording Mode with Manual Selection

If you use manual selection, you can manually switch between 2 recording modes. You name the modes, and set up the input that serves as a switch. You can use only one input for switching recording modes. The following input types are suitable for switching recording modes:

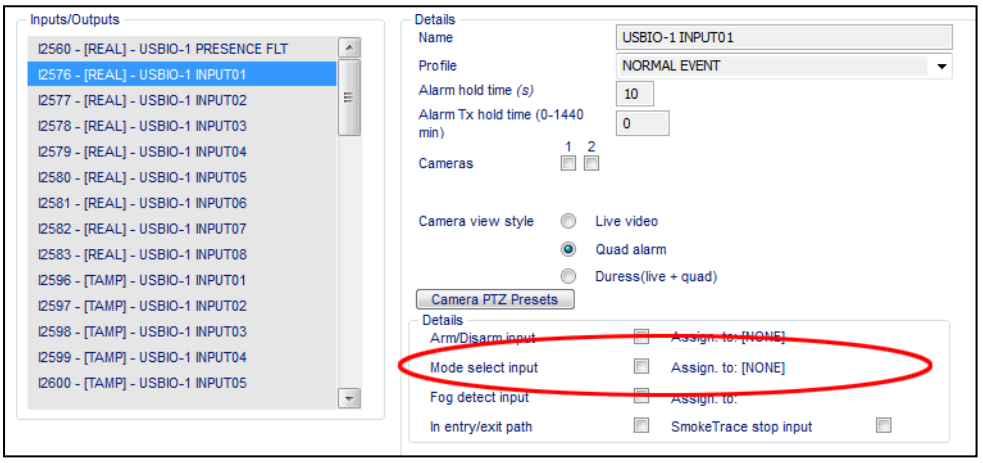
- The inputs on the MIO/EIO cards or on the Net I/O units.
- The virtual inputs from an S3100 panel.
- Input workbits.

Note

If you use manual selection (switch), you can use **only two** recording modes. If you need more recording modes, you have to use the time schedule instead.

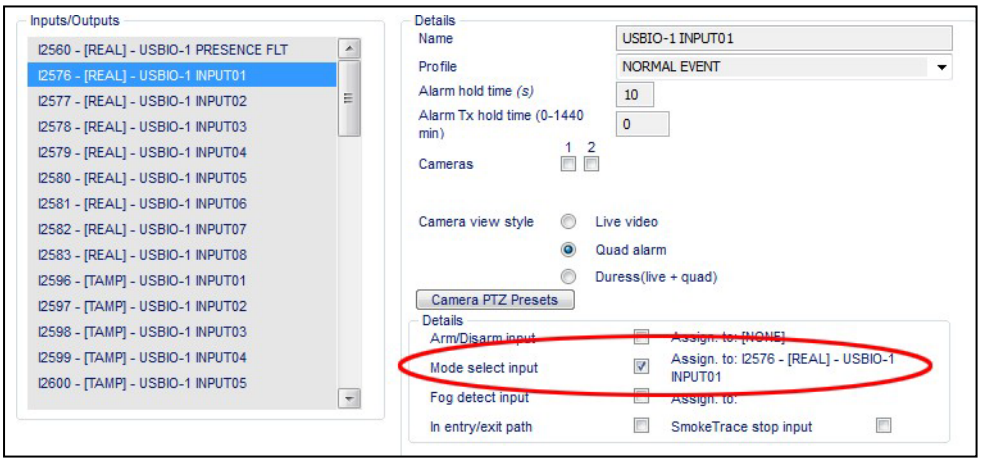
To set up manual switching between two recording modes, proceed as follows:

1. First, you will set up the input that serves as a switch: choose **System** > **Behaviour** > **Input/Output Behaviour**.
2. Select the desired input in the **Inputs/Outputs** list.
   The system displays the number and name of the input that is currently assigned for switching at the right side of the **Mode select input** checkbox. If no input is assigned, it displays NONE:



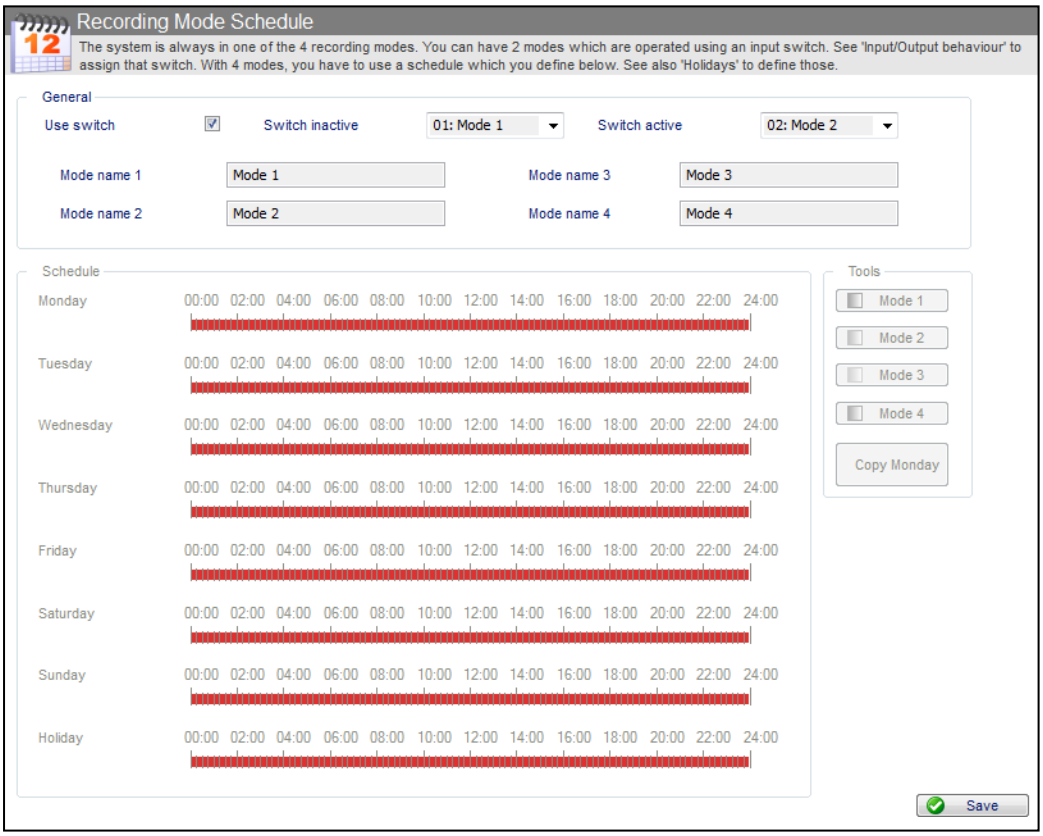
> ***Caution!***
>
> There can only be one input for switching modes. If there already is an input assigned, and you assign to a new input, then the system automatically clears the **Mode select input** checkbox of the previously assigned input.

3. To use the selected input for switching recording modes, select the **Mode select input** checkbox. The input number and name appear to the right of the checkbox.



4. Modify any other settings as necessary. For details on setting up inputs, see *Alarm Input Behaviour* .
5. Click **Save**.

6. Now you will set up the recording modes: choose **System** > **Behaviour** > **Recording Mode Schedule**.



7. Make sure that the **Use switch** checkbox is selected.
8. In the **Switch inactive** box, select the recording mode that you want to use when the switch is inactive.
9. In the **Switch active** box, select the recording mode that you want to use when the switch is active.
10. In the **Mode name** boxes for the two selected modes, type a meaningful name for the modes. You can use up to 20 characters. An example:
    - Mode 1 = DAY
    - Mode 2 = NIGHT
11. Click **Save**.

The system now switches between two modes according to the input.

10 Watching Live Images

You can watch live images:

- In the Live Video screen. For details, see the following sections.
- On an external monitor. For details, see *Watching Live Images on a Monitor*.
- Via a web browser. For details, see *Watching Live Images via a Web Browser*.

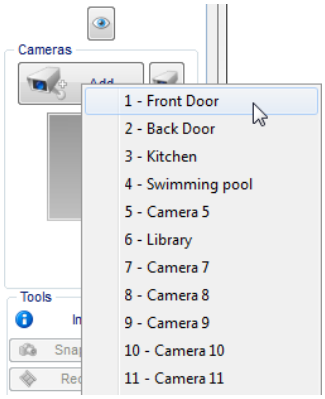
10.1 Watching Live Images in the Live Video Screen

The **Live Video** screen allows you to watch live camera images in a matrix view. The matrix view accommodates up to 32 cameras. From the **Live Video** screen you can:

- enlarge one camera image in the matrix to full screen
- change the live view image resolution
- de-warp 360° camera images: see *360° Camera Images*
- display analytic bounding boxes: see *Rendering Analytic Bounding Boxes*
- display camera information
- activate outputs
- take snapshots
- record video to your PC's hard disk (local recording)
- listen to audio from a camera (if enabled) I talk back to the site using a microphone I use the PTZ controls.

To watch live images from the **Live Video** screen, proceed as follows:

1. In the top menu, click **Live Video**.
2. To add a camera to the live view: under **Cameras**, click **Add**, and then click the camera that you want to display.

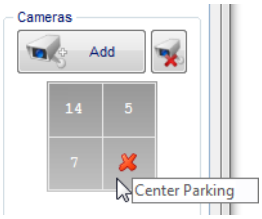


3. Repeat to add more cameras. The system automatically adjusts the live view grid to accommodate for more cameras.

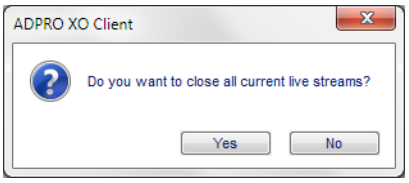


The grey box under **Cameras** displays the selected camera numbers.

4. To remove cameras from the live view, proceed as follows:
   - To remove one camera: under Cameras, click the camera number in the grey box.



   - To close all live streams (= remove all camera images from the **Live Video** screen): under **Cameras**, click the  button, and then click **Yes** to confirm when the message below appears.



Note

If you want the system to remember the last used camera matrix in the live view, then set the **Save live view** option in the settings of the **Login** window to **Yes**. If you set it to **No**, the live view window is empty when you start the client, and you have to select the cameras for the live view matrix each time you start the client. For instructions, see *Launching the XO Client*.

10.2 Full Screen View

Double-click a camera image in the matrix to display it at full screen. Double-click again to return to the matrix view.



10.3 Changing the Image Quality (Resolution)

You define the default image quality for the live view in the camera setup window (**Video Inputs**). To adjust the quality of the image temporarily in the **Live Video** screen, right-click the camera image and select one of the options.

Note

The available options depend on the camera type.



Furthermore, live streaming for **analogue cameras** has certain limitations. For DS42xx A/V cards, the limitations are set per camera. If you set recording quality to 4CIF/4SIF, the maximum quality for live viewing is CIF/SIF or QCIF/QSIF. If you set recording quality to 2CIF/2SIF, only CIF/SIF, QCIF/QSIF and 2CIF/2SIF are available for live viewing. In all these cases, the maximum frame rate is 25 fps.

10.4 Info Display

Under **Tools**, click **Info** to display the camera information under each camera image:



The system displays the following information:

Item	Description
	Video streaming status: (green) = video is streaming on this live stream slot (either from camera or NO VIDEO) (red) = no video is streaming (free live stream slot, no camera is assigned).
Hallway	Camera name
480x360	Image size (CIF, 2CIF… or in pixels)
30 Fps	Number of frames per second
V:8.76 kB/s	Video stream transfer speed in kilobyte per second
A:9.74 kB/s	Audio stream transfer speed in kilobyte per second
	Local recording (on hard disk of your PC; for more information, see *Local Video Recordings*): (blue) = recording locally (grey) = not recording locally.
	Live sound is active. = live sound active = live sound not active.
R	Recording (on the hard disk of the XO device): (blue) = recording (grey) = not recording.
T	Tamper detection. A tamper event occurred on the camera, or no video (for example: BNC not connected for analogue camera). (yellow) = tampering detected (grey) = no tampering detected.
M	Motion detection: (green) = motion detected (grey) = no motion detected.

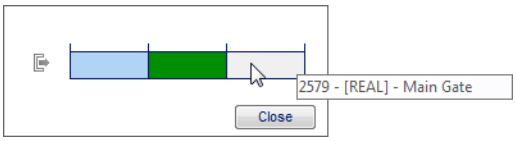
10.5 Activating Outputs

You can manually activate outputs via the live view of a camera. You need to configure such outputs in **Input/Output Behaviour** first (see *Setting up Outputs for Manual Operation*). The button then becomes available under **Tools** when you click the camera image in the live view:

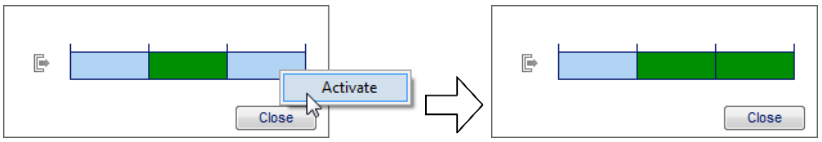


To activate/deactivate an output from the **Live Video** window, proceed as follows:

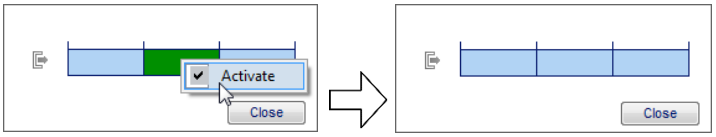
1. In the **Live Video** window, click the camera image to which the output is associated.
2. Under **Tools**, click the button. A popup window appears with a status bar for the outputs on the selected camera. Idle outputs are blue, active outputs are green. When you place the mouse cursor over an output, the system displays the output number and name.



3. To activate an output, right-click the desired output in the status bar, and then click **Activate**. The output bar colours green.



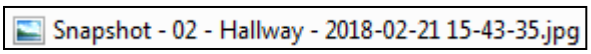
4. To deactivate an output, right-click the desired output in the status bar, and then click **Activate**. The output bar colours blue.



5. Click **Close**.

10.6 Taking Snapshots

You can take a snapshot of the live video streams, either of one selected camera only, or of all the cameras in the live view. By default, the system saves the snapshots in .jpg format in the work folder, in the subfolder for this XO device. If the subfolder does not exist yet, the system will create it. You can specify any other folder if you wish. The snapshot's filename contains the camera number and name, followed by a date stamp in the format *year-month-day hours-minutes-seconds*.



You can also immediately print the snapshot(s).

To take a snapshot of the live view, proceed as follows:

1. You have the following options:
   - To take a snapshot of only one camera image, click the desired image in the matrix (a thin red border appears around the selected image), and then click **Snapshot**.

— To take a snapshot of all cameras in the live view, click **All**. The following screen appears:

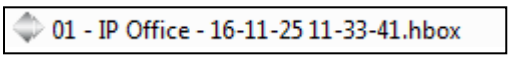


2. Proceed as follows:

Button	Description
	Click the arrow buttons to navigate to the different snapshots. These buttons are only available if you have taken a snapshot of all cameras in the live view.
	Save the snapshot that is currently displayed.
	Save all snapshots. This button is only available if you have taken a snapshot of all cameras in the live view.
	Print the snapshot that is currently displayed to a printer of your choice.
	Print all snapshots to a printer of your choice. This button is only available if you have taken a snapshot of all cameras in the live view.

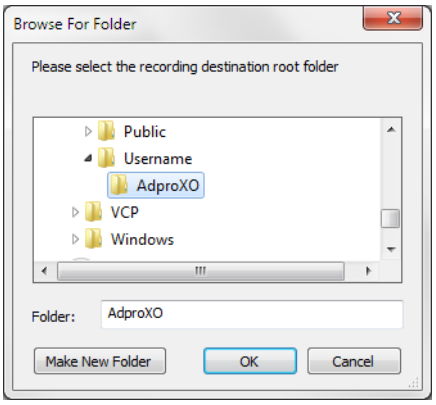
10.7 Local Video Recordings

Besides the automatic recordings as defined in the recording conditions, you can start recording manually from the live view, either for one selected camera only, or for all the cameras in the live view. The system stores these recordings on the hard disk of your PC (instead of the XO device's hard disk). By default, the system saves the recordings in .hbox format in the work folder, in the subfolder for this XO device. If the subfolder does not exist yet, the system will create it. You can specify any other folder you wish, and the system will automatically create a subfolder in it. The recording's filename name contains the camera number and name, followed by a date stamp in the format *year-month-day hours-minutes-seconds*.



To record the live images to your local hard disk, proceed as follows:

1. To record from only one camera, click the desired camera image, and then click **Record**. Alternatively, to record from all cameras in the live view, click **All**. The following screen appears:



2. Select a different folder if desired, and then click **OK**. Remember that the system stores the recording in a subfolder of the indicated folder; you do not have to select or create the subfolder itself.
   The system starts recording. The local recording icons in the information bar turn blue for the selected cameras.
3. To stop recording, click **Record/All** again. The local recording icons turn grey.

10.8 Audio, Listening

You can listen to audio from an audio-enabled camera in the live stream. You can listen to only one camera at once.

To listen to audio from a camera in the live view, proceed as follows:

1. Click the desired camera in the live view. A thin red border appears around the selected camera image. The system plays the sound from the selected camera.
2. To mute the sound: under **Audio**, click . The button changes appearance to indicate that sound is muted: .
3. To unmute the sound, click .
4. To adjust the volume, drag the slider under the button.



Note

If the audio button is unavailable , the camera does not support audio, or the camera's audio settings are incorrect. The **Send live audio stream** checkbox has to be selected for the camera. For more information, see *Audio Input*.

10.9 Audio, Talkback

If you connect a microphone or headset to the client PC, you can use it to talk to the person on site via a loudspeaker (audio output) associated with the camera.

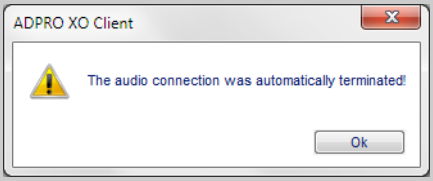
To talk back to a person on the monitored site, proceed as follows:

1. In the **Live Video** window, click the desired camera view. A thin red border appears around the selected camera image.
2. Under **Audio**, use the microphone button as follows:
   - If full duplex mode is off (default), click and hold the microphone button . The button changes colour .
     Talk through the microphone that is connected to the MIC input of the client PC. When finished, release the microphone button.
   - If full duplex mode is on, click the microphone button  once. The button changes colour .
     Talk through the microphone.
     When finished, click the microphone button again.
   - To adjust the input volume, use the volume slider under the  button.



Note

If you do not click the microphone button to stop talkback in full duplex mode, the system automatically terminates the audio out connection after 10 minutes. The following message appears:



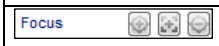
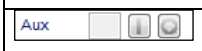
Click **OK** to close the message box.

10.10 PTZ Control

10.10.1 Using PTZ Functions

Under **PTZ**, you can find the PTZ controls for PTZ-enabled cameras.

Item	Description
	Use the arrows to move the camera to the left or right, and up or down. Use the home button  in the middle to move the camera to the home position (= start position). For information on the  button, see below.

Item	Description
	Click the button to enable digital zoom. The button turns red  when digital zoom is active. Click the button again to disable digital zoom. • To zoom in: position the mouse over the area where you want to zoom in, and then press and hold the mouse button. When zoomed in, the text **Digital Zoom** appears (in green) on the image.  • To zoom out: press and hold the Shift key and the mouse button.
	Use this slider to adjust the moving speed of the PTZ camera (if the camera supports this function).
	Press and hold the buttons to zoom in or out on the centre of the camera image.
	Adjust focus (only available if the camera supports the function). Click the middle button to manually adjust the focus. Use the + and – buttons to adjust.
	Adjust iris (only available if the camera supports the function). Click the buttons to manually adjust the iris (open/close).
	Wash/wipe (only available if the camera supports the function). Click to wash and/or wipe the lens of the outdoor camera.
	Manage and use PTZ preset positions. For more information, see *Managing PTZ Preset Positions*.
	(Infra-red) LEDs on the camera (only available if the camera supports the function). Click to switch the LEDs on or off. ***Caution!*** If you are running video analytic applications on the camera, Honeywell strongly recommends to disable the IR LEDs, because they may attract insects to the camera lens and interfere with detection by the analytic applications. Use separate IR illuminators if necessary. For details on (IR) illumination with video analytics, see the *IntrusionTrace Design Guide* (21814).
	Auxiliary functions: type the auxiliary function number (1–255) in the box, and then click the buttons to enable or disable the selected auxiliary function on the camera. Auxiliary camera functions vary depending on the camera model. For more information, consult the documentation of the camera. The XO software may not support all available functions.

Instead of the buttons on the screen, you can also use these keys on the keyboard for PTZ control:

- Arrow keys (up, down, left, right)
- Home = Zoom in
- Page Up = Zoom out

- End = Focus near
- Page down = Focus far.

Furthermore, on-screen PTZ is available. Move the mouse cursor to the edge of the image and it will transform into a white arrow. Press and hold the mouse button to move the camera in the direction of the arrow.



10.10.2 Managing PTZ Preset Positions

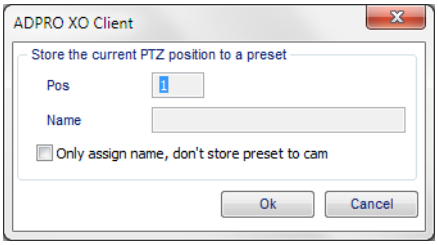
You can create, change, delete, or move the camera to PTZ preset positions from the **Live Video** window, using the **Preset** buttons.



10.10.2.1 Creating PTZ Preset Positions

To create a preset position, proceed as follows:

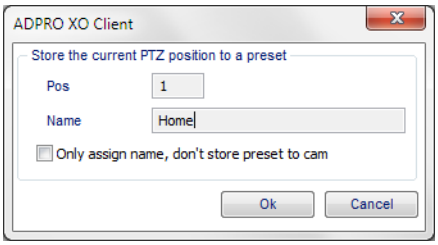
1. In the **Live Video** window, click the desired camera image. A thin red border appears around the selected camera image.
2. Use the PTZ controls to move the camera to the desired position.
3. To save the current position to a preset: next to **Preset**, click the  button.



4. In the **Pos** box, type a number (1–255) for the preset position. For the home position, type **1**.

> ***Caution!***
>
> If you type the number of a preset that already exists, its name automatically appears in the **Name** box. To keep the existing preset and define a new one, type a different number and check that the **Name** box remains empty. If you continue with this number, you will overwrite the existing preset.

5. In the **Name** box, type a name for the preset position.

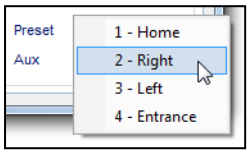


6. Make sure that the **Only assign name…** checkbox is cleared.
(If the checkbox is selected, the system will store the name, but not store the camera position. For more information, see *Renaming a Preset Position*.)
7. Click **OK**.
8. Repeat for other preset positions.

10.10.2.2 Moving the Camera to a Preset Position

To move the camera to a preset position, proceed as follows:

1. In the **Live Video** window, click the desired camera image. A thin red border appears around the selected camera image.
2. Next to **Preset**, click the button, and then click the desired position in the list.



10.10.2.3 Adjusting the Position of a PTZ Preset Position

To adjust the position of a preset position, proceed as follows:

1. In the **Live Video** window, click the desired camera image. A thin red border appears around the selected camera image.
2. Use the PTZ controls to move the camera to the new desired position.
3. Next to **Preset**, click the button.
4. In the **Pos** box, type the number of the preset position that you want to change. The name appears automatically.
5. Click **OK**.

10.10.2.4 Renaming a Preset Position

To change only the name of a preset position without changing its position, proceed as follows:

1. In the **Live Video** window, click the desired camera image. A thin red border appears around the selected camera image.
2. Next to **Preset**, click the button.
3. In the **Pos** box, type the number of the preset position that you want to change. The name appears automatically.
4. In the **Name** box, type the new name.
5. Select the **Only assign name, don't store preset to cam** checkbox.
6. Click **OK**.

10.10.2.5 Deleting a Preset Position

To delete a preset position, proceed as follows:

1. In the **Live Video** window, click the desired camera image. A thin red border appears around the selected camera image.
2. Next to **Preset**, click the button.



3. Click the desired preset position in the list, and then click **Delete**.



4. Click **Close**.

10.11 Watching Live Images on a Monitor

10.11.1 About Using a Monitor

You can connect a monitor directly to the XO device, and use it for:

- Live viewing in a matrix view
- Consulting basic system information in the XO welcome screen
- Accessing the XO Installer menu for advanced hardware setup. For more information, see the Hardware Installation Manual of your XO device (FastTrace 2 Series: 21790; iFT Series: 27817; eFT Series:35450).

If you use a monitor for live viewing instead of the **Live Video** screen in the XO client, the following restrictions apply:

- You can view maximum 16 camera images.
- The image resolution is equal to the analytics stream resolution.
- You cannot display analytics bounding boxes.
- The controls (tools, audio, PTZ) are not available.
- You cannot de-warp 360° camera images.
- For the iFT model with 32 IP video channels: for optimal performance, disable the monitor output if you are using more than 16 IP channels on your iFT device. This restriction does not apply to the iFT-E model.

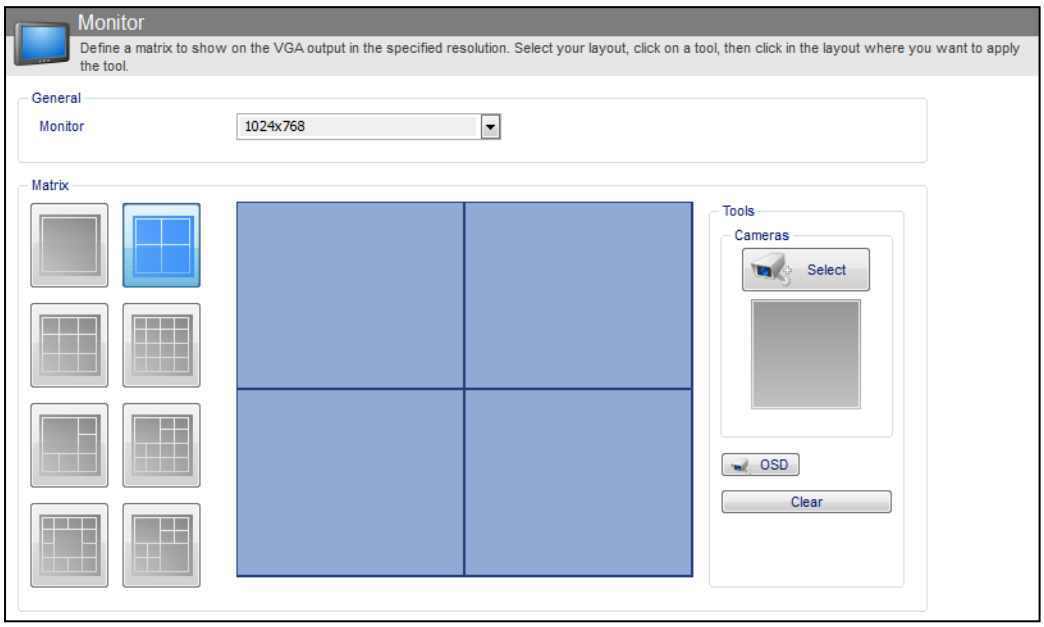
Note

If you want to view more than 16 cameras on a monitor, or if you want to combine camera images from different XO devices in one matrix view, then use the Video Manager tool instead.

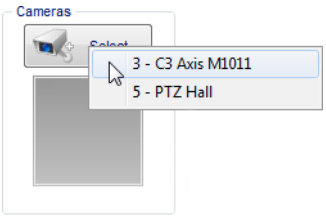
10.11.2 Setting up a Monitor

To set up a monitor for live viewing, proceed as follows:

1. Choose **System** > **Connections** > **Monitor**.
2. In the **Monitor** box, select the monitor's resolution.
3. Under **Matrix**, click the desired matrix layout.



4. Add camera images to the matrix as follows: click **Select**, and then click the desired camera in the list. The selected camera number appears in the grey box.

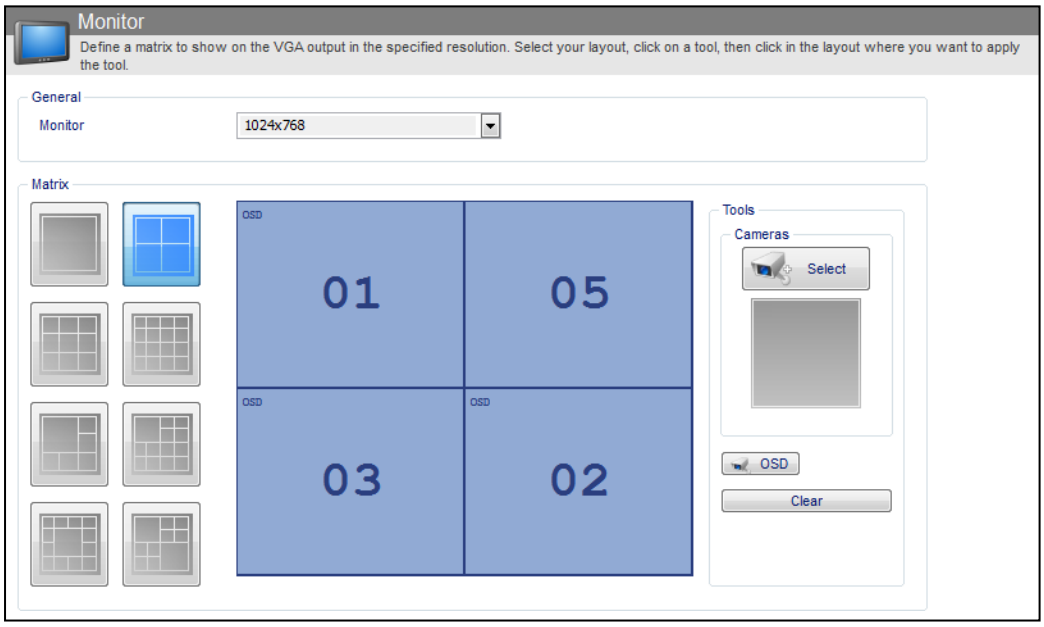


5. Click the matrix cell where you want the camera image to appear. The camera number appears in the matrix cell.

> **Note**
>
> You can assign a camera image to only one matrix cell.

6. To replace the existing camera image in a matrix cell, click **Select**, select a different camera, and then click the matrix cell.
7. To display the camera name on the matrix cell, click **OSD**, and then click each matrix cell where you want the camera name to appear. The 'OSD' indicator appears in the top left corner of the matrix cell. Click again to remove.
8. To remove camera images from the matrix, proceed as follows:
   - To remove one camera image, right-click the matrix cell.
   - To remove all camera images, click **Clear**.

The example below shows a monitor setup with 4 cameras:



9. Click **Save**. The camera images now appear on the monitor.

Note

If the camera images do not appear on the monitor after you click **Save**, switch the monitor off and on again. You can setup a second monitor for eFT devices. A single camera can be viewed in full screen mode at 1080P (1920x1080) resolution.

10.11.3 Disabling the Monitor

To disable the monitor matrix view, proceed as follows:

1. Choose **System** > **Connections** > **Monitor**.
2. In the **Monitor** box, select **Disabled**.
3. Click **Save**.

10.11.4 Switching Between Matrix View and Welcome Screen

You can easily switch between the matrix view and the welcome screen if you have a keyboard attached to the XO device:

- To switch to the welcome screen, press Ctrl+Alt+F1.
- To switch to the matrix view, press Ctrl+Alt+F7.

```
ADPRO XO 04.03.0006
Ip          : 10.0.0.10
Subnet :  255.255.255.0
Gateway:  10.0.0.1

Port [HTTP]:  80
Port [CTRL]:  2000
Port [RTSP]:  554
```

The welcome screen displays the following information:

- XO device (server) software version
- IP address, subnet mask, and gateway
- HTTP, control, and RTSP port numbers.

10.12 Watching Live Images via a Web Browser

> ***Caution!***
> Watching live images via web browser is possible only if the technical grant is left active which is not recommended.

You can watch live images directly in a web browser by entering a URL. To connect to the XO device and watch live images, you need to provide the following information and options in the URL:

- The IP address of the XO device
- The camera(s) that you want to display, using the autostartmask value (see further below)
- A valid username and password for connecting to the XO device using the &username and &password strings
- Optional: connection over UDP (not TCP) using the &notcp string
- Optional: displaying only the camera images and hiding the XO client user interface (controls), using the &nogui string.

An example: to display the live image of camera 1 on an XO device with IP address 10.0.0.10, connecting with the standard Administrator user (username = 0 and password = 666777), over UDP, and while hiding the controls, enter the following URL in the browser:

http://10.0.0.10/index.php?autostartmask=1&username=0&password=666777&notcp&nogui

Another example, showing camera images 1, 2, and 5, over TCP, and showing the user interface controls:

http://10.0.0.10/index.php?autostartmask=19&username=0&password=666777

The autostartmask value is a decimal value converted from the binary camera mask.
The binary camera mask is a string of 0s and 1s. There is a digit for each camera, counting from right to left. The first digit from the right represents camera 1; the second digit from the right represents camera 2; and so on.
A 0 means the camera image is not displayed, a 1 means the camera image is displayed.
To find the autostartmask value, you convert the binary string to a decimal value. There are several conversion tools available freely on the internet.

A few examples:
To display camera 1, the binary string = 1. This converts to decimal value = 1.
To display camera 2, the binary string = 10. This converts to decimal value = 2.
To display camera 5, the binary string = 10000. This converts to decimal value = 16.
To display both camera 1 and 5, the binary string = 10001. This converts to decimal value = 17.
To display camera 1, 2, and 5, the binary string = 10011. This converts to decimal value = 19.

For your convenience, the autostartmask values for each individual camera are listed in the table below:

Cam #	Value	Cam #	Value	Cam #	Value	Cam #	Value
1	1	**9**	256	**17**	65 536	**25**	16 777 216
2	2	**10**	512	**18**	131 072	**26**	33 554 432
3	4	**11**	1 024	**19**	262 144	**27**	67 108 864
4	8	**12**	2 048	**20**	524 288	**28**	134 217 728
5	16	**13**	4 096	**21**	1 048 576	**29**	268 435 456

Cam #	Value	Cam #	Value	Cam #	Value	Cam #	Value
6	32	**14**	8 192	**22**	2 097 152	**30**	536 870 912
7	64	**15**	16 384	**23**	4 194 304	**31**	1 073 741 824
8	128	**16**	32 768	**24**	8 388 608	**32**	2 147 483 648

Although the autostartmask values are indicated with spaces for ease of reading, you have to type them without spaces in the URL.

Note

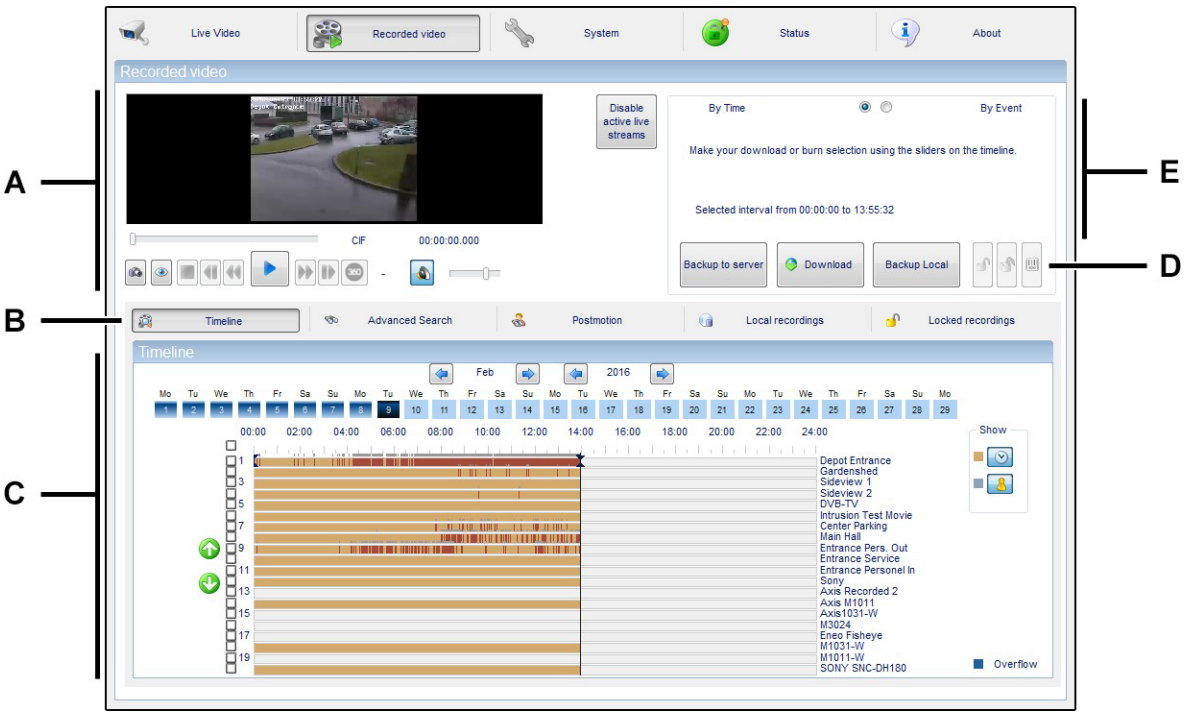
You may need to install the XO client before being able to view live images.

11 Recorded Video

11.1 About Recorded Video

The **Recorded Video** screens allow you to play back or back up the recordings on the XO device's hard disk(s).

In the top menu, click **Recorded video**. By default, the **Timeline** tab opens.



The **Recorded Video** screen contains the following elements:

A	A preview screen with controls for playback.
B	Tabs with different functions in the **Recorded Video** screen.
C	The content of this part of the screen depends on the selected tab. The example above shows the **Timeline** tab with individual timelines for each video channel.
D	Buttons for backing up and unlocking recordings. The available buttons depend on the selected tab.
E	The content of this part of the screen depends on the selected tab. The example above shows options to search recordings by time or event, and a result list below. • When searching by time, this area displays the start and end time of the selected interval. • When searching by event, this area displays a list of found event recordings.

11.2 Searching Recordings on the Timeline

11.2.1 Timeline Overview

The **Timeline** tab contains individual timelines for each video channel, with a calendar on top. The colours of the days in the calendar indicate if there are recordings on that day.

Colour	Description
(grey)	Day without recordings. There were either no recordings made on that day, or the system has already cleaned up the recordings on that day, according to the **Maximum days recording** setting.
(red)	Earliest day with recordings; the system is cleaning up recordings on this day, according to the **Maximum days recording** setting.
(blue)	Day with recordings.
(dark blue)	Currently selected day with recordings. The recordings of this day appear in the camera timelines under the calendar.
(light blue)	Day in the future. No recordings yet.

The camera number appears on the left-hand side of the timeline, the camera name on the right-hand side. The camera name only appears for enabled cameras.
If the system contains more cameras than can fit on the screen, use the arrow buttons and at the left to scroll down/up to see more timelines: click to move one camera up/down; click and hold to scroll continuously.

The colours on the timeline indicate the type of recording.

Colour	Description
(orange)	Continuous recording.
(red)	Recording on event. If you zoom in (drag the mouse on the time indication line) on an event recording, you will see that it consists of the following parts: • Grey areas indicating pre and post event recording. • A red vertical bar indicating the time when the input that triggered the recording, was activated. 
(light grey)	Period without recordings for this video channel.

Under **Show**, on the right-hand side, you can choose to display or hide the recording types on the timeline.

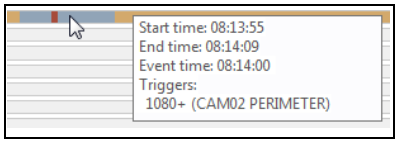
Button	Description
	Click the button to show/hide continuous recordings on the timeline.
	Click the button to show/hide event recordings on the timeline. If you only display event recordings, you can quickly jump from one recording to the next/previous using the and buttons that appear to the left and right side of the timelines.

If you change the display options during playback, playback stops.

Note

The XO device can record maximum 16 000 events per day (the counter is reset at night). If more events occur on the same day (= overflow), the XO device switches automatically to continuous recording for all cameras. This is indicated in blue bars on the timeline. You cannot hide overflowing recordings.

Hover your mouse over a recording in the timeline to see its details:

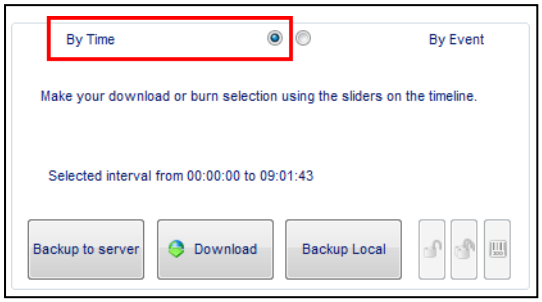


- Start and end time of the recording.
- Event time (only for event recordings)
- Trigger that activated the event (only for event recordings).

11.2.2 Selecting a Timeframe on the Timeline

To select a specific timeframe on the timeline, proceed as follows:

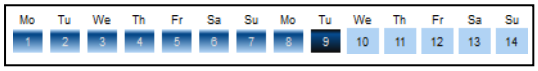
1. In the top menu, click **Recorded video**, and then click the **Timeline** tab.
2. In the top right, click **By Time**.



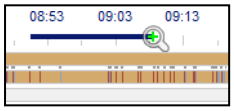
3. Click the arrow buttons to select the desired month and year.



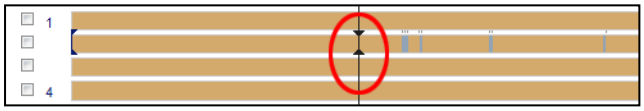
4. Click the desired day. You can only click days that contain recordings; so you cannot click grey and light blue days. The day in dark blue is the currently selected day. The recordings of that day appear in the timeline.



5. By default the time indication is shown with a 30-minute interval. To zoom in, drag the mouse on the time indication line. The pointer changes into a magnifying glass while dragging. A black marker appears to indicate the selected time. To zoom out again, right-click the time indication line.

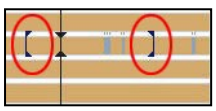


6. Click in the timeline of the desired camera. A black vertical marker appears where you clicked.

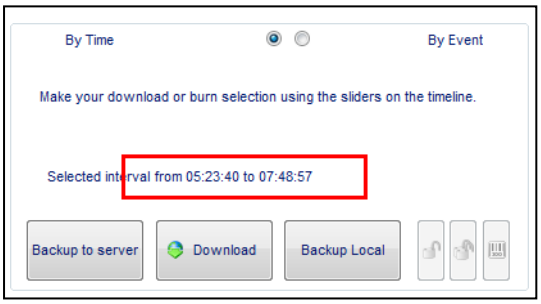


The preview window (top left) displays the still image of the selected camera at the selected date and time.

7. To change the selected time, drag the vertical marker to the desired position. Zoom in on the timeline if necessary.
8. To select a specific interval, drag the black delimiters on the selected timeline to the desired start and end time.



The box at the top right of the screen indicates the exact start and end time of the selected interval:



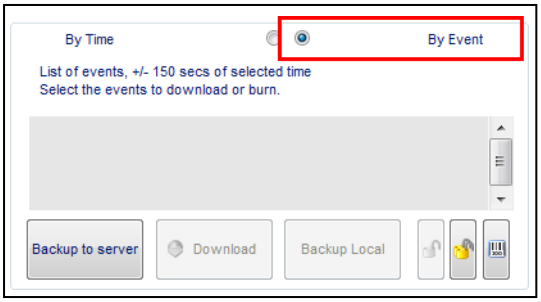
9. You can now watch and/or download this footage:
   - To play the selected video, click the button. Playback starts at the vertical marker in the timeline.
   - To download the selected video, click **Download**.

11.2.3 Searching Event Recordings on the Timeline

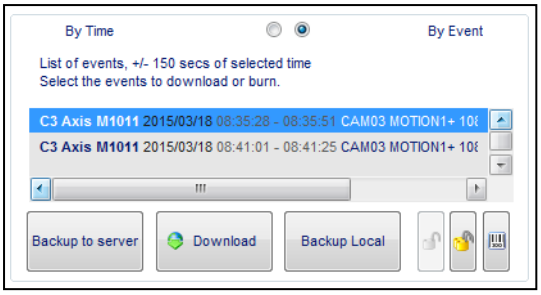
When you search by event, the system will select the events that happened 150 seconds before or after a selected time on the timeline, for a selected camera.

To select event recordings on the timeline, proceed as follows:

1. In the top menu, click **Recorded video**, and then click the **Timeline** tab.
2. In the top right, click **By Event**.



3. Click in the timeline of the desired camera, at the desired time.
   The result list displays the event recordings that happened 150 seconds before and after the selected point in time. If there are no event recordings in that 150-second timeframe, the result list will be empty.



4. You can now watch and/or download this footage:
   - To play a specific recording, double-click it in the result list.
   - To download a recording, click it in the result list, and then click **Download**.

11.2.4 Playing the Selected Footage

When you have selected a timeframe or a video recording, you can play it using the controls under the preview window. Playback starts at the vertical marker in the timeline.



Note

The video player plays what is shown on the timeline. If you display only event recordings, the player skips the 'empty' time slots in between event recordings.

Use the control buttons as follows:

Button	Description
	Click to choose the options for rendering analytic bounding boxes. For details, see *Rendering Analytic Bounding Boxes*.
	Click to take a snapshot.
	Click to stop playback. The image will freeze at the time reached in the playback.
	Click to fast forward/backward.
	Click to start playback.
	Click to pause playback. Click the  button to resume.
	Click to de-warp images from a 360° panoramic camera. For more information, see *360° Camera Images*.
	Click to mute/unmute the sound. To adjust the volume level, drag the slider on the right-hand side of the button. Audio is only available if you have enabled audio for the camera.

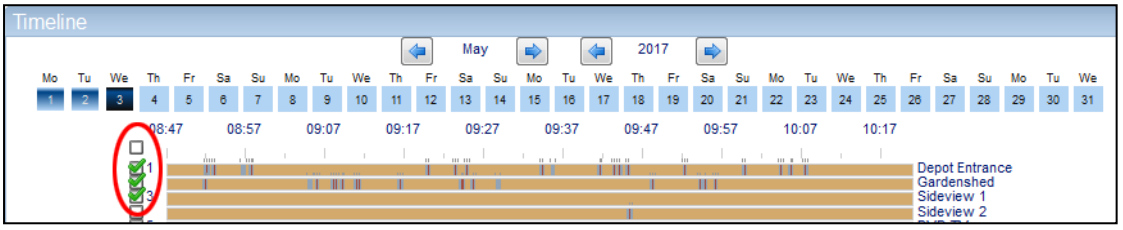
To see the recorded video at full screen, double-click the video player image. Double-click again to return to the normal preview window.

11.2.5 Synchronised Playback

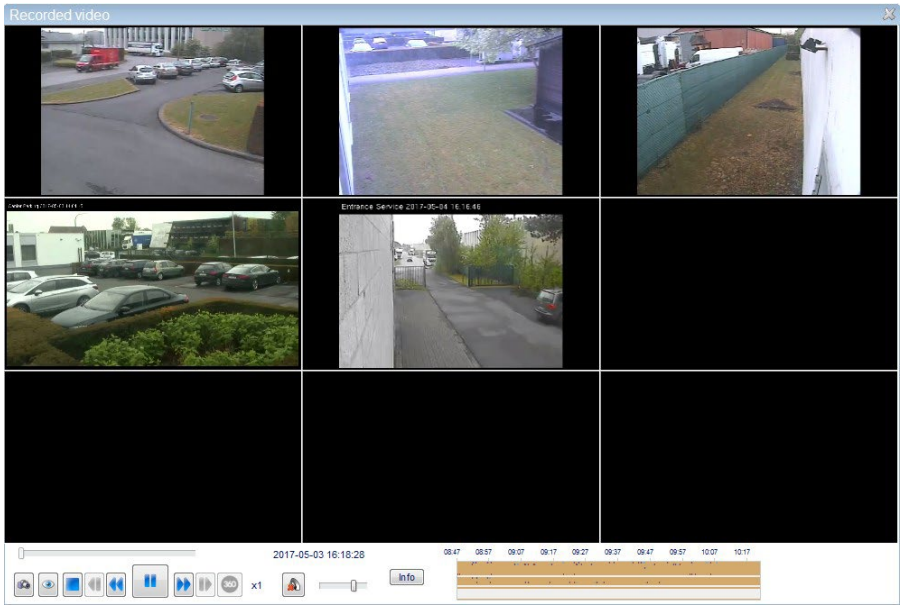
You can watch recorded video of multiple cameras simultaneously (with images of identical time settings).

To synchronised playback, proceed as follows:

1. On the **Timeline** tab, select the checkboxes of the cameras that you want to include in the synchronised playback. To select all cameras, select the checkbox at the top.



2. To set the timeframe, click in any of the selected camera timelines and adjust as required.
3. Click . The system opens a matrix view with the selected camera images.



Synchronised playback offers similar tools as single playback, except that:

- Sound is only available for one video channel at a time: click the camera image for which you want to play the sound.
- You can click the **Info** button to display the camera name and image resolution below the camera images.

4. To view one of the camera images at full screen, double-click it. Double-click it again to return to multiple playback.

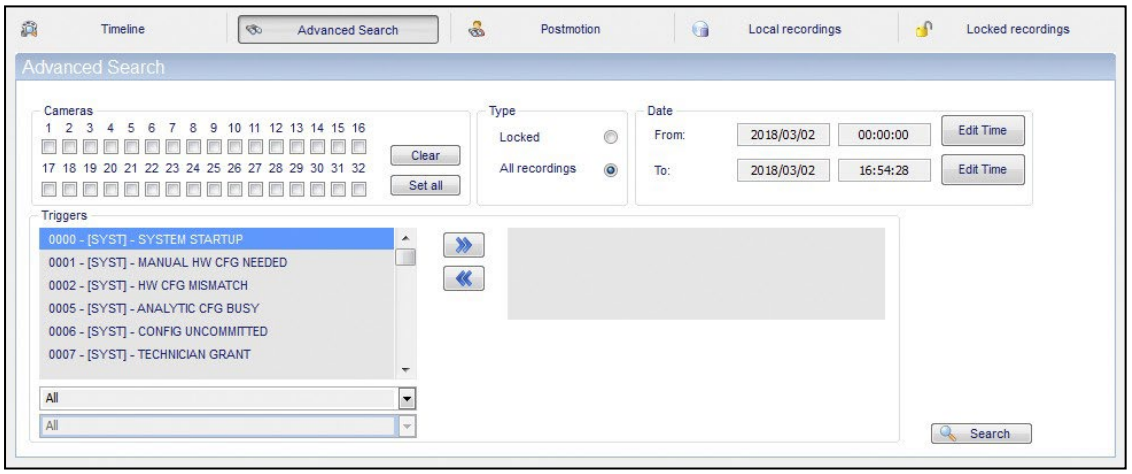


5. To stop synchronised playback and return to the timeline screen:
   - Click the close button  in the top right corner.
   - Click the stop button .

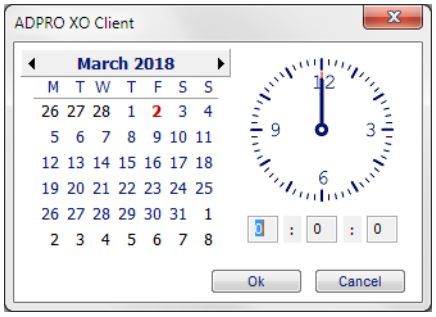
11.3 Searching Recordings via Advanced Search

The advanced search allows you to search for recordings on specific triggers. Proceed as follows:

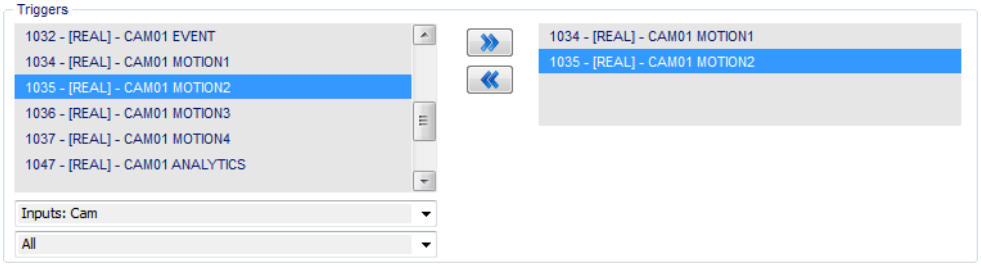
1. In the top menu, click **Recorded video**, and then click the **Advanced Search** tab.



2. Under **Cameras**, select the checkboxes for all the cameras that you want to include in the search. Click **Set all** to select all cameras.
3. Under **Type**, select:
   - **Locked**: to search in locked recordings only.
   - **All recordings**: to search in all recordings.
4. Under **Date**, set the desired time frame.
   You can type the date and time indications in the **From** and **To** boxes, or you can click **Edit Time** to select a date and time:



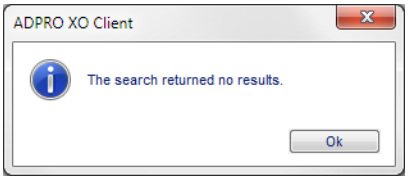
5. Optional: under **Triggers**, click the desired input, and then click the » button to move the selected input to the list on the right. You can select maximum 4 triggers.



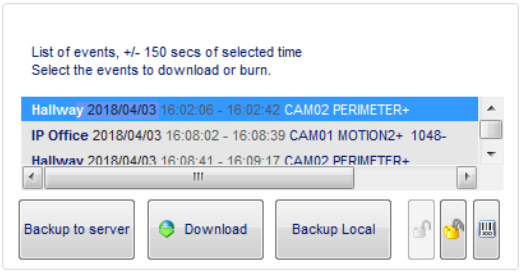
   Use the filters below the list to reduce the list. If you filter on camera inputs, you can filter further on camera number.

6. To remove a selected input from the search, click it in the list on the right-hand side, and then click the « button.

7. Click **Search** to start searching for recordings.
   - If there are no results, the following message appears:



   - If there are results matching your search, they appear in the results list at the top right.



8. You can now watch and/or download this footage:
   - To play a recording, double-click it in the result list.
   - To download a recording, click it in the result list, and then click **Download**.

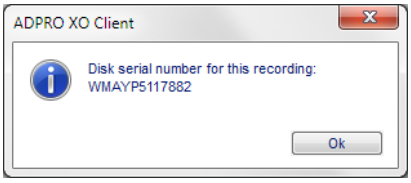
> **Note**
>
> When you perform an advanced search on recorded video, the results pane may display a different trigger than the one you selected for searching. This may happen if you have defined multiple triggers in the recording condition that corresponds with the found recording. The system will take the first trigger that is specified in the recording condition, and display that in the search results pane. That trigger may be different from the one you selected for searching.

11.4 Identifying the Storage Disk

If you have multiple hard disks in your XO device, you can check on which hard disk an event recording has been stored. This feature is not available for continuous recordings.

To identify the storage disk for an event recording, proceed as follows:

1. Select the desired recording in the results list, or click an event recording in the timeline.
2. Click the  button. A popup window appears displaying the serial number of the hard disk:



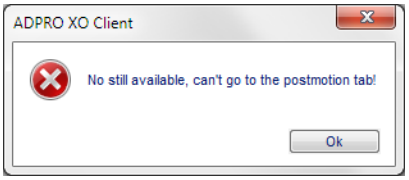
3. Click **OK** to close the message box.

11.5 Searching Recordings via Postmotion

The XO device does not only store the video footage on the hard disk, it also creates a metadata file describing the contents of the footage. This information allows you to quickly find all sequences in which an object was moving inside a specific area of the camera image.

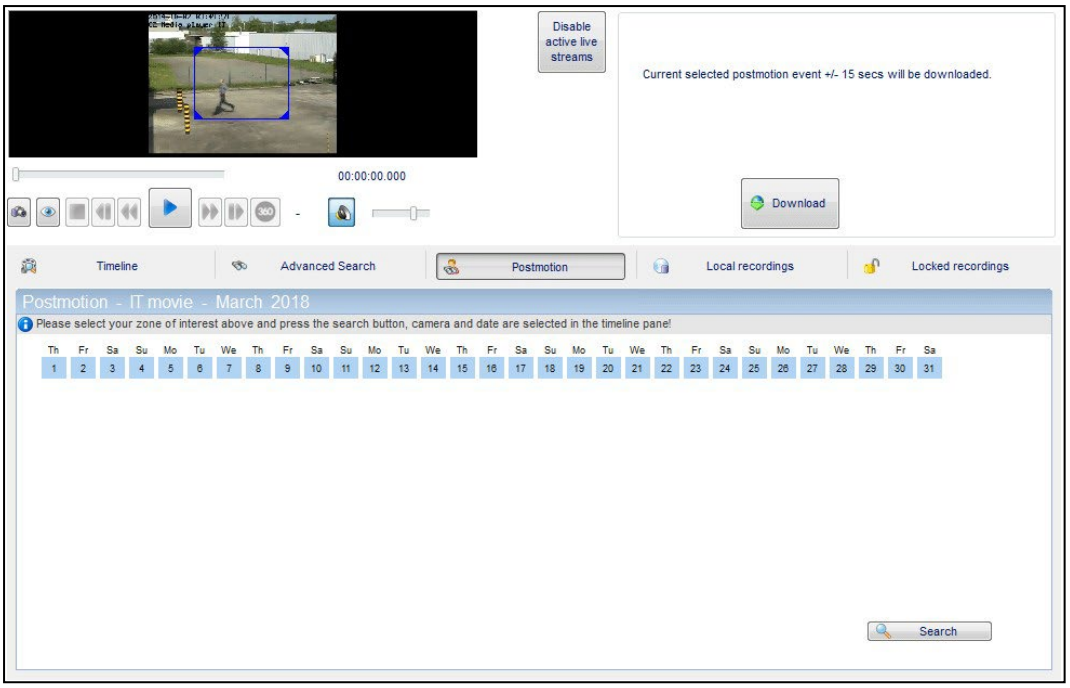
To find recordings via postmotion, proceed as follows:

1. In the top menu, click **Recorded video**, and then click the **Timeline** tab.
2. In the time indicator bar, select the desired date.
3. In the timeline of the desired camera, click in any existing recording. This will allow the postmotion function to create a still image. The still image appears in the preview window at the top of the screen.
4. Click the **Postmotion** tab.
   - If there is no still image available, (for example, because you clicked an empty recording line, or you did not give the system time to load the still image), The following error message appears:



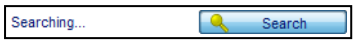
     In this case, click the **Timeline** tab and return to step 3.

   - If the still image is available, the following screen appears:

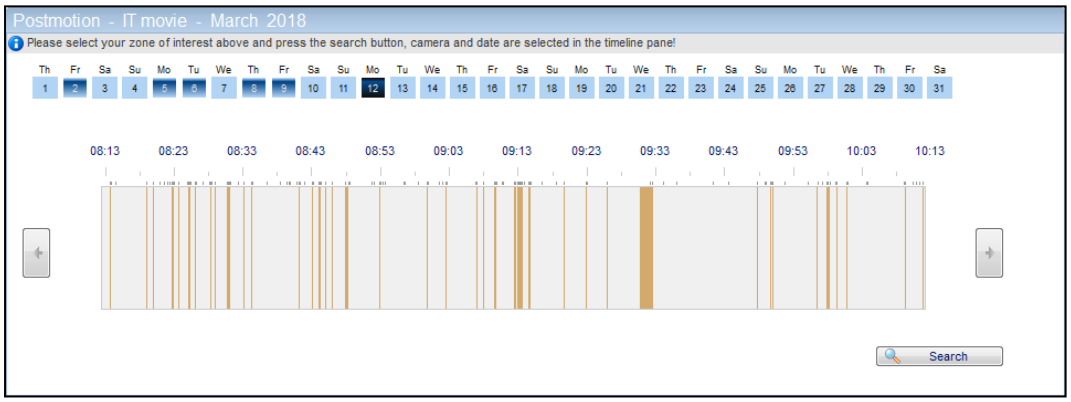


     The blue rectangle in the preview image indicates the zone of interest: the area that the postmotion function will analyse.

5. Adjust the size and position of the zone as desired. Drag the zone to the desired area; drag the corners to resize.
6. Click **Search**. During search, the message *Searching* appears:



When the search has been completed, a timeline with results appears.



Days indicated in light blue contain no results; days in blue contain results. The darkest blue date is the currently selected date.

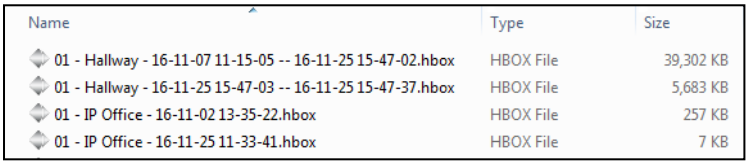
7. Click the day of interest.
8. To zoom in on a specific period, drag the mouse over the time indication line.
9. To zoom out, right-click the time indication line.
10. To play a specific recording, click the recording in the timeline, and then click .
11. To jump to the previous/next result, click the arrow buttons  to the left and right of the timeline.

11.6 Downloading and Storing Selected Video Recordings

11.6.1 Overview

You can download recordings to the hard disk of your PC, or on a USB drive or CD/DVD.

If you download to the PC, the system stores the downloaded footage in the work folder, in the subfolder for this XO device. The file name contains the camera number, camera name, and the time frame of the recording. The file is stored with the extension ".hbox".



For slow network connections it is recommended to disable all live streams in order to increase the download speed, especially with synchronised playback. You can disable all active live streams by clicking the **Disable active live streams** button.



To enable live streams again, click **Live Video** in the top menu, and then add the desired cameras to the live view.

Note

When downloading a recording via **Postmotion**, only part of the recording will be stored: the selected time plus about 10 extra seconds.

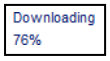
11.6.2 Downloading Recordings to your Local Hard Disk

To download video recordings to the hard disk of your PC, proceed as follows:

1. Search for the desired footage via the timeline, advanced search, or postmotion, then continue as follows:
   - For searches via advanced search: select the desired footage in the results pane.
   - For searches via postmotion: click the desired footage in the timeline.
2. Click **Download**.



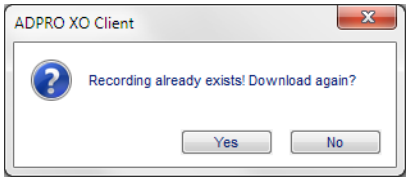
You can see the downloading status:



The system starts playing the footage that you are downloading. To stop playback, click . If you have selected multiple cameras, the synchronised playback window will appear. To stop synced playback, click  twice.

> **Note**
>
> During download, the **Download** button changes: 
>
> . Click the button to stop downloading.

If you have already downloaded the footage and click the **Download** button again, you will be asked whether you want to download the recording once more:



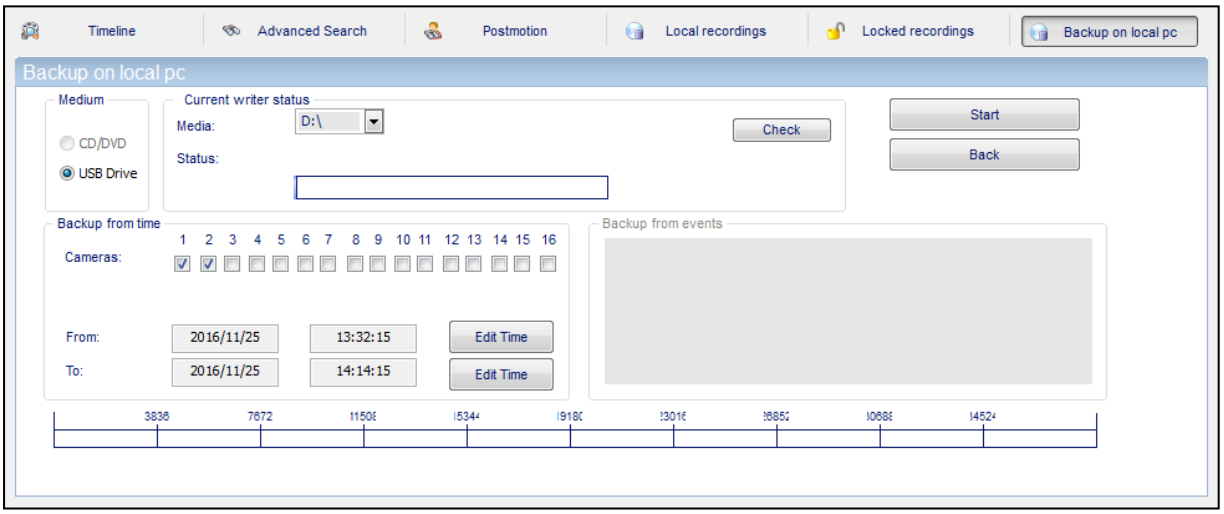
11.6.3 Downloading Recordings to USB Drive or CD/DVD

> **Note**
>
> Software versions XOa 3.00 and above do not support connecting a CD/DVD drive directly to the XO device. Connect the CD/DVD drive to your PC instead.

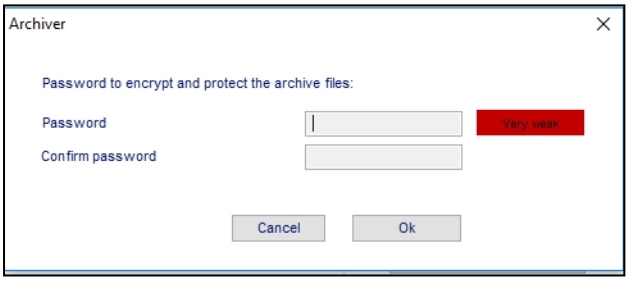
To download video recordings to USB drive or CD/DVD, proceed as follows:

1. Search for the desired footage via the timeline or advanced search.
2. Select the desired footage in the results pane.
3. You have the following options:
   - To store the video on a USB drive connected to the XO device, click **Backup to server**.
   - To store the video on a USB or CD/DVD drive connected to your local PC, click **Backup Local**.

The following screen appears:



4. Under **Medium**, select the desired storage medium: **CD/DVD**, or **USB Drive**.
5. If you selected recordings on the timeline, you can still select additional cameras, and change the date/time.
6. Click **Start** to start writing the video footage to the selected drive.
   If you want to cancel, click **Back**.
7. The **Archiver** window is displayed to password protect the downloaded file once the video footage is download. Enter a new password. The password must have minimum 8 characters and at least once capital letter.
8. Reconfirm password for the downloaded footage and click **Ok**. The download is added to an archive and the file can be extracted only with the password provided while adding it to the archive. Different video footages can be saved with different passwords and all the video footages are added to the same archive. When you extract the archive with a password, only the video footages saved with that password are extracted.



11.7 Managing Local Recordings

11.7.1 Overview of Local Files

From the **Local recordings** tab, you can manage the following files that are stored in the work folder on your local PC, in the subfolders for each XO device:

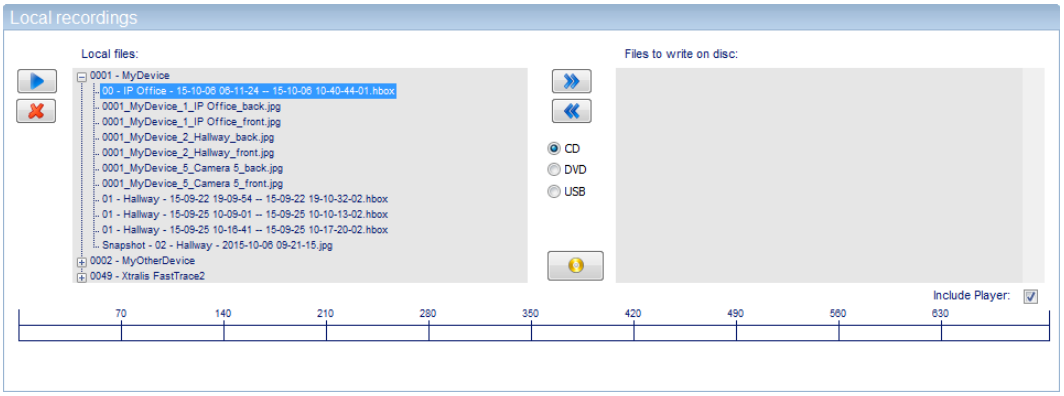
- Recordings that you saved on your PC using the **Download** button
- Recordings that you made from the **Live Video** window.
- Snapshots
- Calibration images.

You can view the files, delete them, or back them up to CD/DVD or a USB drive.

11.7.2 Viewing or Deleting Local Files

To view or delete locally stored files, proceed as follows:

1. In the top menu, click **Recorded Video**, and then click the **Local recordings** tab.



   The **Local files** box displays the local files that are available on your PC, in separate subfolders for the different XO devices. By default, the system expands the folder for the current XO device.

2. Use the ⊞ and ⊟ buttons to expand/collapse the folders.
3. To view a recording, snapshot, or calibration picture: click the desired file, and then click .
4. To delete a recording, snapshot, or calibration picture: click the desired file, and then click .

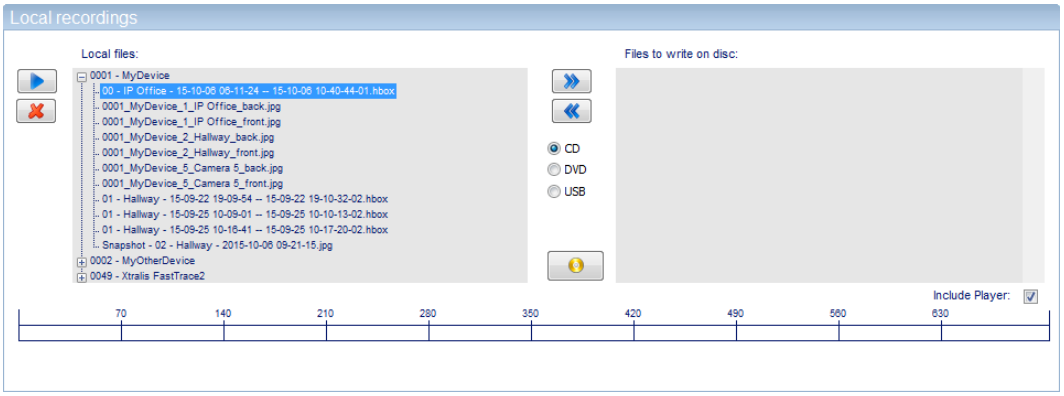
11.7.3 Backing up Local Files

The backup feature for local files allows you to include player software, so that you can play the video recordings on any Windows compatible computer.

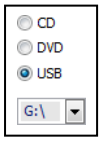
> **Note**
>
> You cannot back up files that are larger than 4 GB to FAT32-formatted USB drives. If you need to back up larger files, you have to use exFAT formatting on the USB drive. NTFS formatting is not supported.

To back up local files on CD/DVD/USB, proceed as follows:

1. In the top menu, click **Recorded Video**, and then click the **Local recordings** tab.



2. Select the medium to where you want to write the files: **CD**, **DVD**, or **USB**. If you click **USB**, then also select the correct drive name:

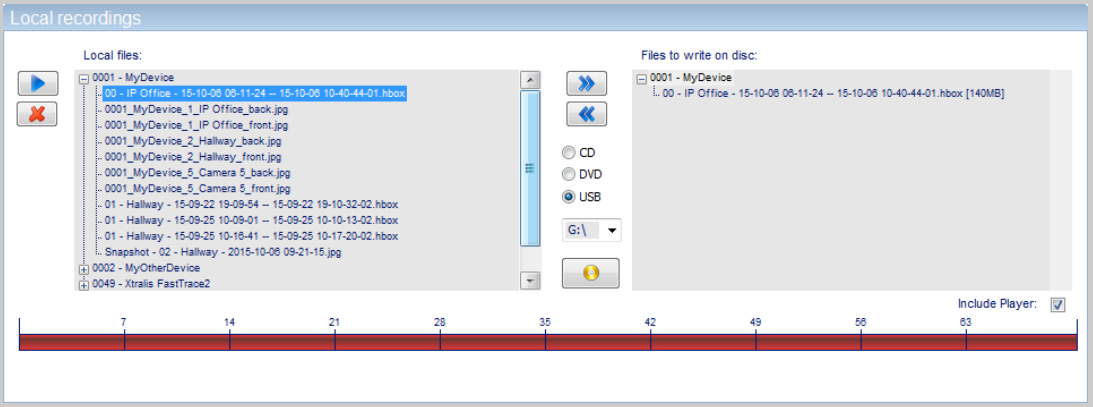


The bar at the bottom of the screen indicates the available disk space on the selected medium.

3. To add a file to the list of files to write, click the file in the **Local files** list, and then click . The file appears in the **Files to write on disc** list. The system automatically creates subfolders per XO device.

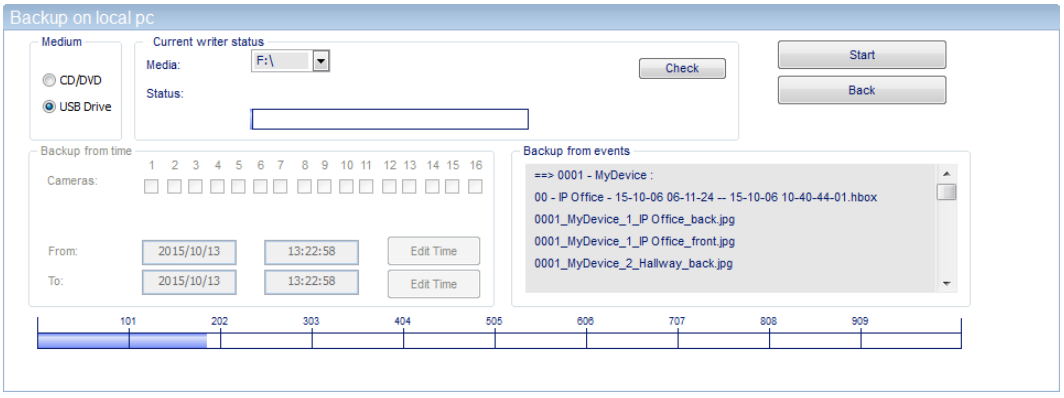
Note

If there is not enough space on the medium for writing the selected files, the bar colours red.



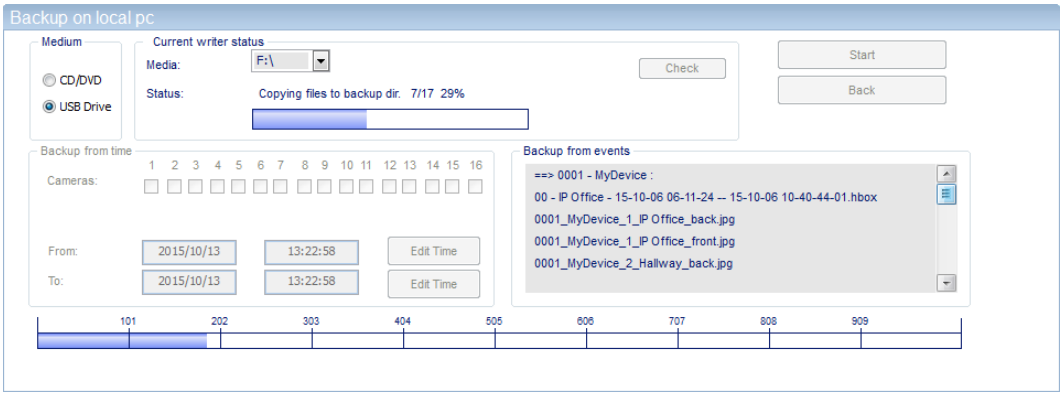
In this case, remove some files from the list of files to write, or use a larger medium.

4. To remove a file from the list of files to write, click the file in the **Files to write on disc** list, and then click .
5. If you want to write the player software for watching the video recordings to the medium, select the **Include Player** checkbox. This allows you to play the video recordings on any Windows compatible computer.
6. To start writing the files from the **Files to write on disc** list to the selected medium, click the button. The following screen appears:

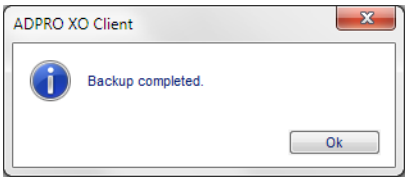


7. You can still change the medium in the **Medium** section. If you do, click **Check** to check the available space on the new medium.
8. The files to write on the medium appear in the **Backup from events** box. If you want to add or remove files, click **Back** to return to the previous screen.

9. To write the files to the selected medium, click **Start**. The system starts writing the files to the selected medium.



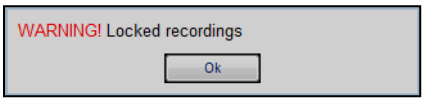
When finished, the following message appears:



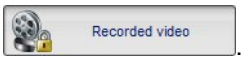
10. Click **OK** to close the message box. The system returns to the **Local recordings** tab.

11.8 Locked Recordings

For recordings on event, you can specify to lock the recordings. The system cannot delete locked recordings automatically. As soon as there is a locked recording, the XO client displays the following warning message:



Click **OK** to close the message box. The message box reappears each time you start the client.

The padlock in the **Recorded Video** button indicates the presence of locked recordings: 

.

Furthermore, locked recordings trigger the system message 0049 – [SYST] – LOCKED RECORDER (by default linked to the alarm profile NORMAL EVENT).

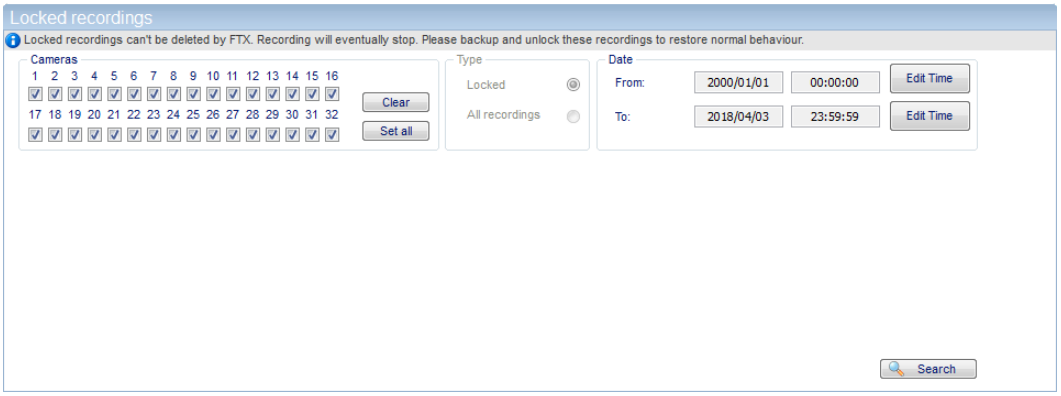
Caution!

The XO device cannot delete locked recordings. When it encounters a locked recording during automatic clean-up (for example after 30 days), it **stops cleaning up**. When the device runs out of storage space, it also **stops recording**.

To prevent that the XO device stops recording, you have to download the locked recordings as soon as you receive the warning message, and then unlock them so that the system can delete them.

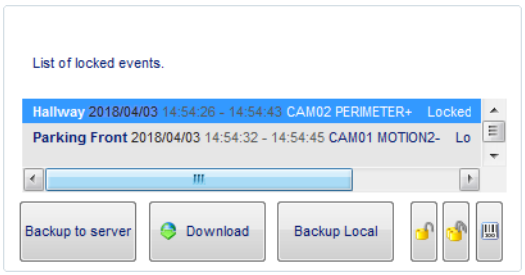
To handle locked recordings, proceed as follows:

1. In the top menu, click **Recorded Video**. If there are locked recordings, the system automatically opens the **Locked Recordings** tab.



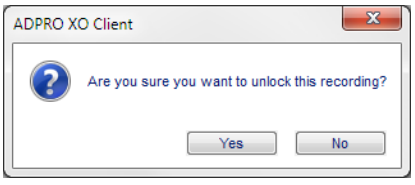
   From this tab, you can search for, select, and download locked recordings. By default, all cameras are selected, and the timeframe is set to cover the full operational time of the XO device (from the year 2000 until the end of the current day). This makes sure that the system finds all existing locked recordings. However, you can adjust the parameters as required.

2. Click **Search**. The locked recordings appear in the **List of locked events** box (top right of the screen).

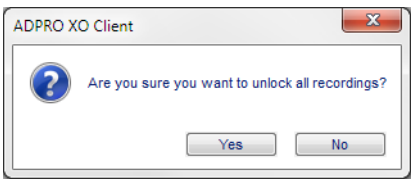


3. Select the recordings in the list, and then click **Download**. The system copies the selected recordings to the work folder on your PC, in the subfolder for this XO device.
4. Wait for downloading to finish. Next, you will unlock the recordings.
5. You can unlock recordings one by one, or all at once:

   — To unlock one recording, click the desired recording in the list, and then click  (button with single padlock). The following message appears:



   — To unlock all recordings in the list, click  (button with the double padlock). The following message appears:



6. Click **Yes** to confirm.
7. Click **Search** again to find remaining locked recordings.

The system can now delete the unlocked recordings and continue with automatic clean-up.

12 360° Camera Images

You can de-warp 360° camera images in the XO client:

- From the live view
- From the recorded video view.

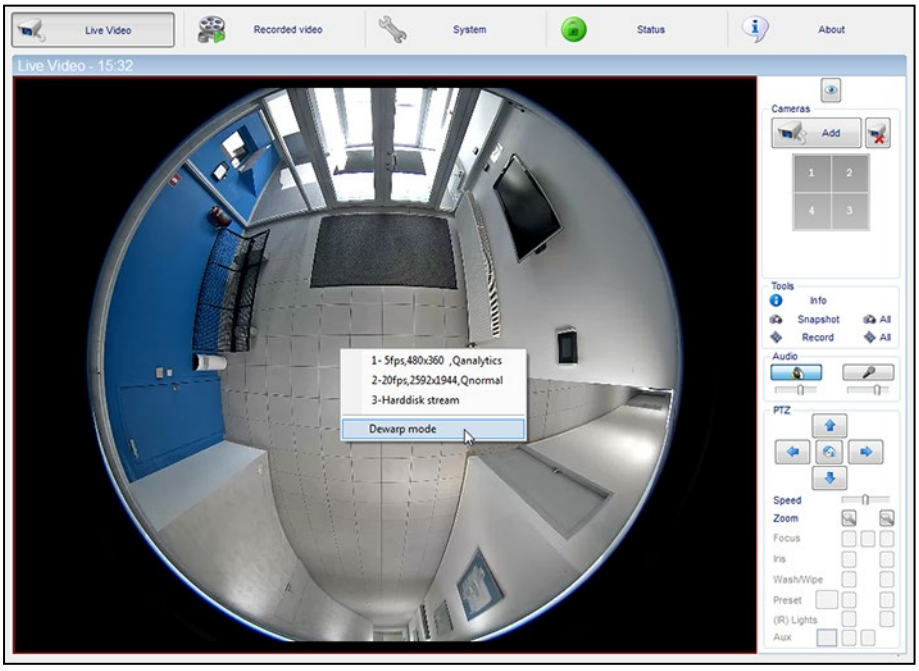
Note

For correct de-warping, select the correct mount type for the camera (available from version XO 4.02). For details, see *General Settings*.

De-warping is not possible in GDI mode. For details, see *System Requirements for the Client PC*.

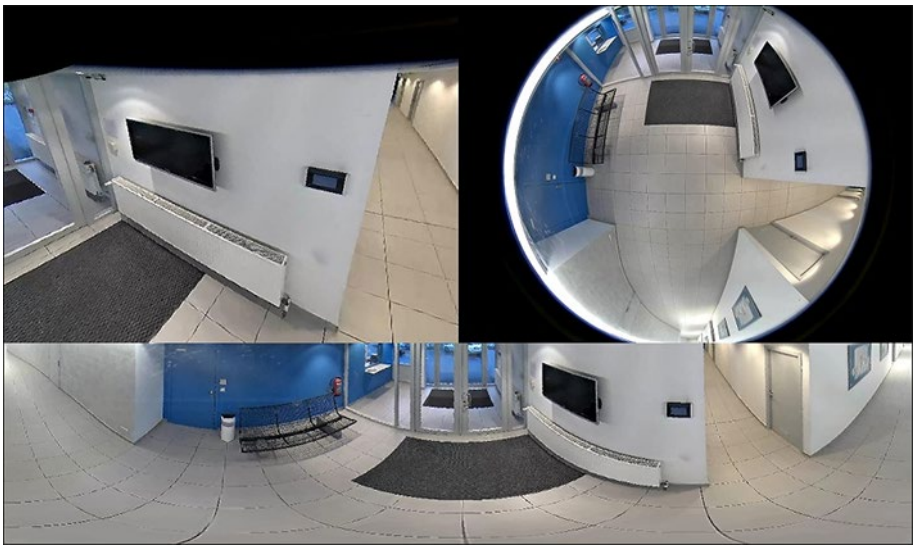
To de-warp 360° camera images, proceed as follows:

1. Open the 360° camera image and proceed as follows:
   - In the **Live Video** screen, right-click the camera image and click **Dewarp mode**.



   - In the Recorded video screen, click the 360 button.

The following screen appears:



The screen displays:

- The original 360° image at the top right
- The full de-warped image at the bottom
- A detail view of the de-warped image in the top left.

2. Proceed as follows:
   - Click anywhere in the 360° image or in the de-warped image to see the detail in the top left corner.
   - Press and hold the mouse button to zoom in. Press and hold Shift, and then press and hold the mouse button to zoom out.
3. To return to the 360° view:
   - In the Live Video screen, right-click the camera image and click Dewarp mode again.
   - In the Recorded video screen, click the  button.

13 Arming and Disarming

13.1 About Arming/Disarming

The security system has to handle events in a different way when the secured premise is left unattended. Therefore, you have to arm the system when it is left unattended. The alarm profiles define how the system behaves when an alarm input is triggered in the armed and disarmed states. Arming and disarming can happen in the following ways:

- Automatically, according to a time schedule.
- Manually, when a user activates an input.
- From the CMS: via a command in the CMS software (for example VideoCentral Platinum), or the CMS can execute the DN command line in Telnet (hint: type HE for syntax help in Telnet).

Note

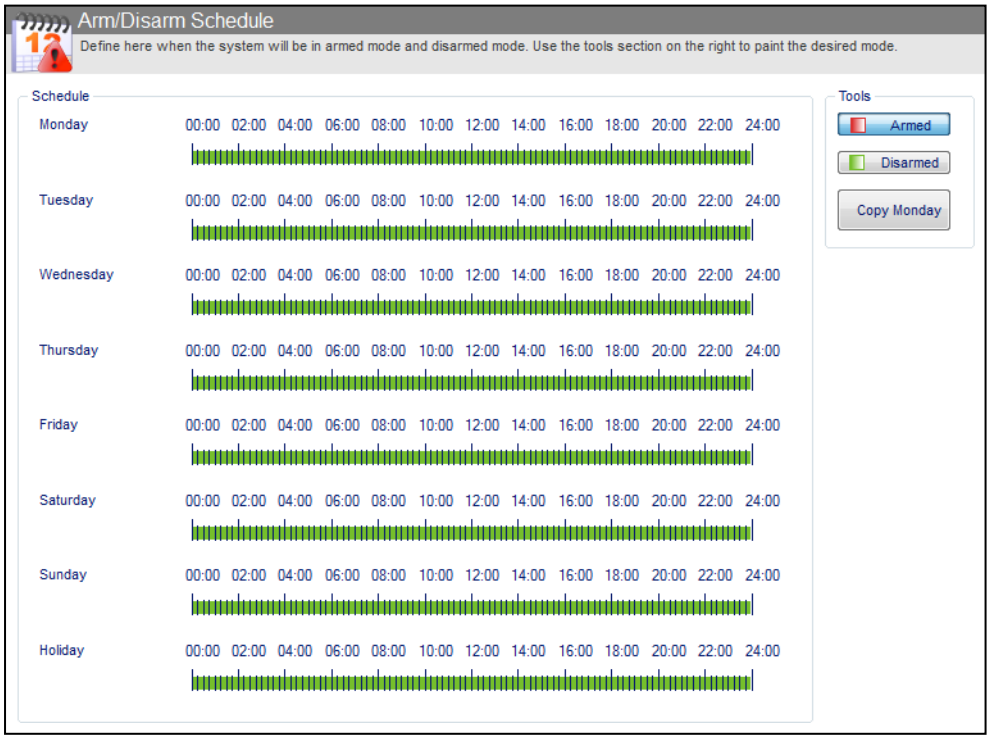
Third-party software developers can use the SDK (software development kit) in order to arm/disarm a system.

13.2 Arming/Disarming Automatically

You can arm/disarm the system automatically, according to a fixed schedule. You can set up an individual schedule for each day of the week (Monday–Sunday), and a separate schedule for holidays. To define the holidays, see *Calendar*.
Tip: you can set up the schedule once for Mondays, and then copy it to all other days.

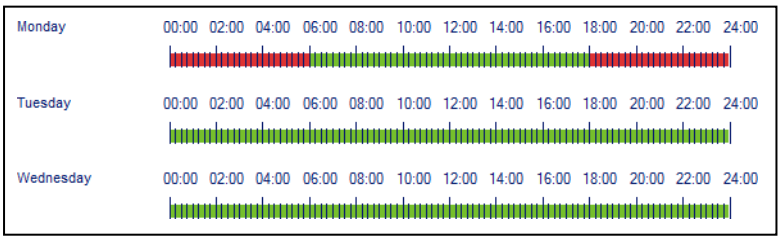
To set up the schedule for automatically arming/disarming the system, proceed as follows:

1. Choose **System** > **Behaviour** > **Arm/Disarm schedule**.



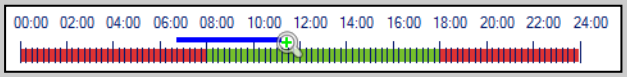
2. Indicate the desired armed/disarmed states on the time bar as follows:
   — To specify when the system is armed: under Tools, click Armed, and then drag the mouse over the time bar. The selected period colours red.

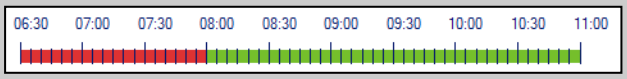
— To specify when the system is disarmed: under Tools, click Disarmed, and then drag the mouse over the time bar. The selected period colours green.



Note

To make accurate selections, you can zoom in on a part of the day (up to the minute): move the mouse pointer just above the coloured time bar. The pointer changes into a magnifying glass. Drag the mouse over the part that you want to zoom in on. A blue line appears while dragging.





To zoom out again to the full day, right-click just above the time bar.

3. If you have a repeating schedule, you can copy the schedule from Monday to all other days (including holidays): click **Copy Monday**, and then click **Yes** to confirm.
4. Adjust until you have the correct schedule for each day.
5. Click **Save**.

The system shall now automatically arm/disarm according to your schedule. A switch can always force the system to another state.

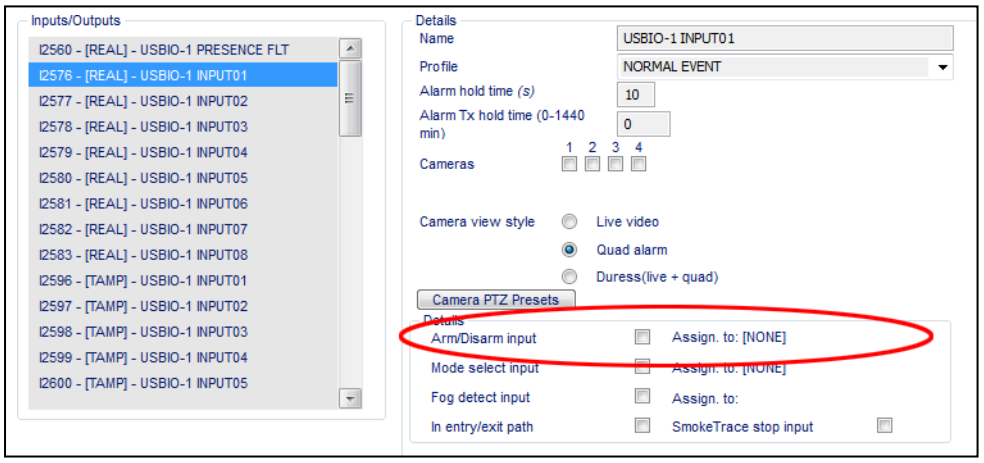
13.3 Arming/Disarming Manually

You can arm/disarm the system manually, by activating/deactivating an input. You can use only one input for arming/disarming. The following input types are suitable:

- The inputs on the MIO/EIO cards or on the Net I/O units.
- The virtual inputs from an S3100 panel.
- Inputs on IP cameras (if available on the camera; see the Supported IP Camera List (26742)).
- Input workbits.

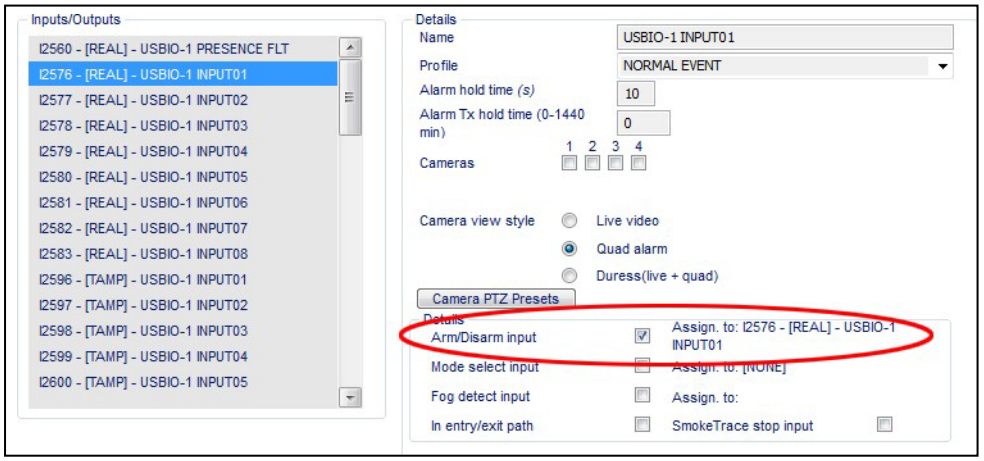
To set up an input for arming/disarming the system, proceed as follows:

1. Choose **System** > **Behaviour** > **Input/Output Behaviour**.
2. Select the desired input in the **Inputs/Outputs** list.
   The system displays the number and name of the input that is currently assigned for arming/disarming at the right side of the **Arm/Disarm input** checkbox. If no input is assigned, it displays NONE:



> ***Caution!***
>
> There can only be one input for arming/disarming the system. If there already is an input assigned, and you assign to a new input, then the system automatically clears the **Arm/Disarm input** checkbox of the previously assigned input.

3. To use the selected input for arming/disarming, select the **Arm/Disarm input** checkbox.



   The input number and name appear to the right of the checkbox.

4. Modify any other settings as necessary. For details on setting up inputs, see *Alarm Input Behaviour*.
5. Click **Save**.

14 Alarm Profiles

14.1 About Alarm Profiles

An alarm profile defines how the XO device responds when an input is triggered. It defines the transmission channel(s) for the alarm message and camera images associated with the input, if the alarm is transmitted when the system is armed and/or disarmed, if the alarm transmission is repeated or sent only once, etc. To each input, you assign one alarm profile. If you change an alarm profile, it affects all the inputs that use that alarm profile.

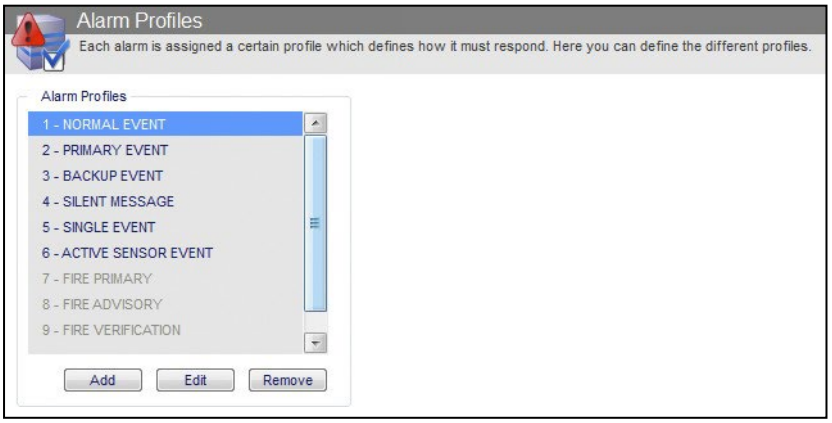
You can select **multiple inputs** at once and quickly assign the same alarm profile to all selected inputs.

The XO device comes with 6 standard alarm profiles. For an overview, see *Default Alarm Profiles*. Honeywell strongly recommends to **keep the default profiles as they are**, and create additional profiles if you need different settings.

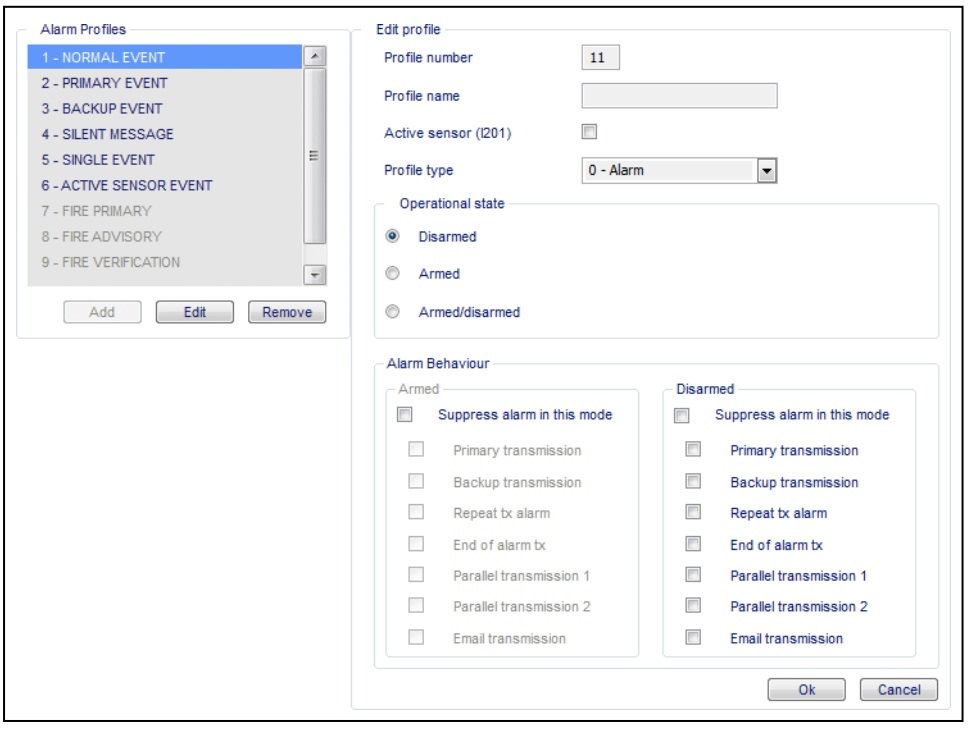
14.2 Adding a New Profile

You can create up to 32 different alarm profiles. To add a new alarm profile, proceed as follows:

1. Choose **System** > **Behaviour** > **Alarm Profiles**.



2. Click **Add**.



3. Provide the following information:

Item	Description
Profile number	Type the profile number (11–32). The system fills in the next free profile number automatically. Numbers 1–10 are reserved for the standard alarm profiles (profiles 7– 10 are no longer available as the SmokeTrace application has been discontinued).
Profile name	Enter a description (max. 20 characters) for the alarm profile. Use a meaningful and relevant description.
Active sensor (I201)	Select this checkbox if you want to use this alarm profile to trigger input I201, the active sensor input. Honeywell recommends to use this option with only one profile. The standard profile ACTIVE SENSOR EVENT already uses this option. For details, see *Active Sensor Event Profile*.
Profile type	The only profile type available is 0 – Alarm; this is the generic type. **Note** The fire type profiles 7–10 are no longer available as the SmokeTrace application has been discontinued.
Operational state	Select in which operational states the XO device has to transmit the alarm: • **Disarmed**: to transmit alarms only when the system is disarmed. • **Armed**: to transmit alarms only when the system is armed. • **Armed/disarmed**: to transmit alarms always. Note that alarms, regardless of the operational state, always appear in the **Status** window and in the log files.
Alarm Behaviour	Define how the XO device has to transmit the alarm: • **Suppress alarm in this mode**: it is possible to suppress alarms in one or both operational states. When you activate this option, the alarms that have been assigned to this profile will no longer be activated during the suppression. By doing this you will disable event-based recordings, emailing, PTZ triggers, logging, etc. ***Caution!*** Suppressing alarms is **not recommended**. Do not use this option unless specifically asked to do so, for example by Honeywell Support staff. XO Client software has been enhanced with a safeguard against suppressing of all alarms. XO 5.0 Client displays a message with the dialog **Warning! You selected to completely suppress the alarms for all inputs having this profile! Are you really sure you want to do this?** when all the alarms in an alarm profile are suppressed. • **Primary transmission**: to send alarms via the primary transmission channel. • **Backup transmission**: to send alarms via the backup (secondary) transmission channel. The system will only use the backup channel if transmission on the primary channel fails. • **Repeat tx alarm**: to send reminders every x minutes as long as the alarm is active. The default interval is 15 minutes. You can specify the interval between the repeated alarm transmissions. For details, see *Alarm Input Behaviour*.However, the system repeats the following alarms only once every 24 hours: ◦ 0050 – [SYST] – STORAGE INSUFFICIENT ◦ 0065 – [SYST] – LICENSE EXPIRED ◦ 0066 – [SYST] – LICENSE OUT OF SYNC ◦ 0067 – [SYST] – APPLICATION STOPPED ◦ 0511 – [SYST] – GENERAL ISOLATION.

Item	Description
	• End of alarm tx: to send a message when the input is no longer active (returns to idle state; also known as 'negative alarm'). • Parallel transmission 1: to send alarms via parallel transmission channel 1. • Parallel transmission 2: to send alarms via parallel transmission channel 2. • Email transmission: to send alarms via email.

4. Click **Save** to apply the new settings.

14.3 Deleting an Alarm Profile

Note

You cannot delete the default alarm profiles or alarm profiles that are in use (= assigned to inputs). To find all inputs that use a specific alarm profile, use the filter in the **Input/Output Behaviour** screen.

To delete an alarm profile, proceed as follows:

1. Choose **System** > **Behaviour** > **Alarm Profiles**.
2. Click the desired alarm profile in the list, and then click **Remove**.
3. Click **Yes** to confirm.
4. Click **Save**.

14.4 Default Alarm Profiles

The XO device comes with 6 standard alarm profiles:

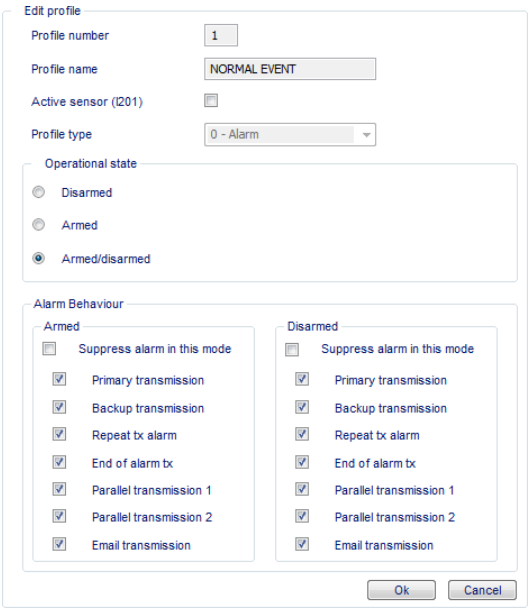
- 1– NORMAL EVENT
- 2– PRIMARY EVENT
- 3– BACKUP EVENT
- 4–SILENT MESSAGE
- 5–SINGLE EVENT
- 6–ACTIVE SENSOR EVENT

All default alarm profiles are described in detail in the sections below.

Note

- Honeywell strongly recommends to keep the default profiles as they are, and create additional profiles if you need different settings.
- Alarm profiles 7–10, the fire type profiles, are no longer available as the SmokeTrace application has been discontinued.

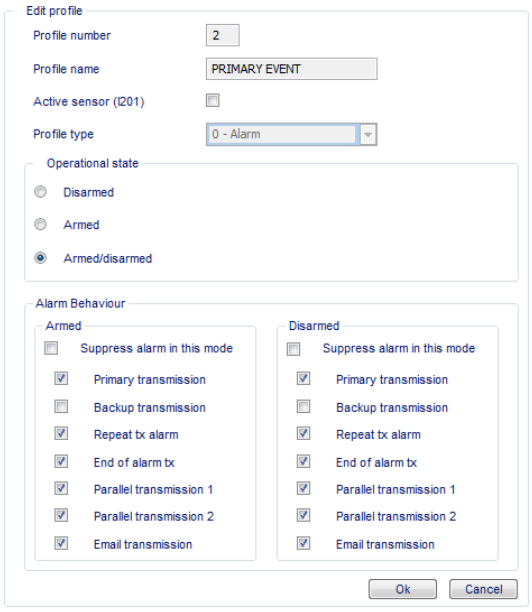
14.4.1 Normal Event Profile



The NORMAL EVENT profile sends the alarm to **all transmission destinations**: primary, backup, parallel, and email.

- Operational state: it does not consider the operational state. The system will transmit the alarm in both armed and disarmed state.
- Repeat: the system will repeat the alarm transmission every x minutes (configurable) as long as the input is active.
- End-of-alarm behaviour: when the input is no longer active (= end of alarm), the system will transmit a new message to indicate this.
- Profile type: **0 – Alarm**. This is the generic profile type. You cannot modify the profile type.

14.4.2 Primary Event Profile

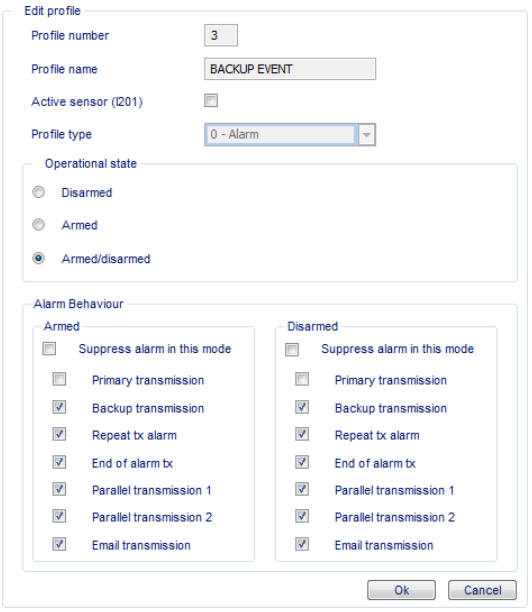


The PRIMARY EVENT profile sends the alarm to the **primary** transmission destination, but **not to the backup** destination. It also sends to the parallel and email transmission destinations.

- Operational state: it does not consider the operational state. The system will transmit the alarm in both armed and disarmed state.
- Repeat: the system will repeat the alarm transmission every x minutes (configurable) as long as the input is active.
- End-of-alarm behaviour: when the input is no longer active (= end of alarm), the system will transmit a new message to indicate this.
- Profile type: 0 – Alarm. This is the generic profile type.

  You cannot modify the profile type.

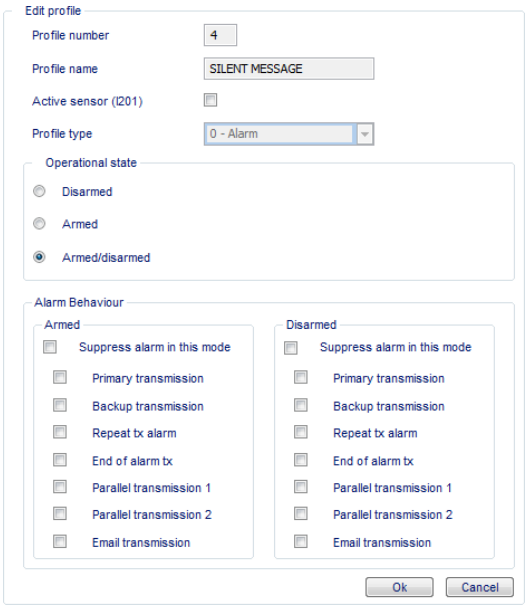
14.4.3 Backup Event Profile



The BACKUP EVENT profile sends the alarm to the **backup** transmission destination, but **not to the primary** destination. It also sends to the parallel and email transmission destinations.

- Operational state: it does not consider the operational state. The system will transmit the alarm in both armed and disarmed state.
- Repeat: the system will repeat the alarm transmission every x minutes (configurable) as long as the input is active.
- End-of-alarm behaviour: when the input is no longer active (= end of alarm), the system will transmit a new message to indicate this.
- Profile type: **0 – Alarm**. This is the generic profile type. You cannot modify the profile type.

14.4.4 Silent Message Profile

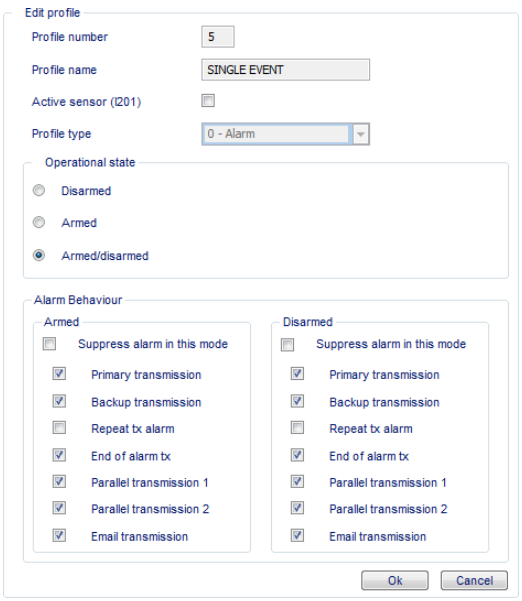


The SILENT MESSAGE profile **does not send** the alarm to any transmission destination. The alarms appear in the log file.

- Operational state: it does not consider the operational state. The system will never transmit the alarm.
- Repeat: there is no transmission, so also no repeat transmission.
- End-of-alarm behaviour: when the input is no longer active (= end of alarm), the system will not transmit a new message to indicate this.
- Profile type: 0 – Alarm. This is the generic profile type.

  You cannot modify the profile type.

14.4.5 Single Event Profile

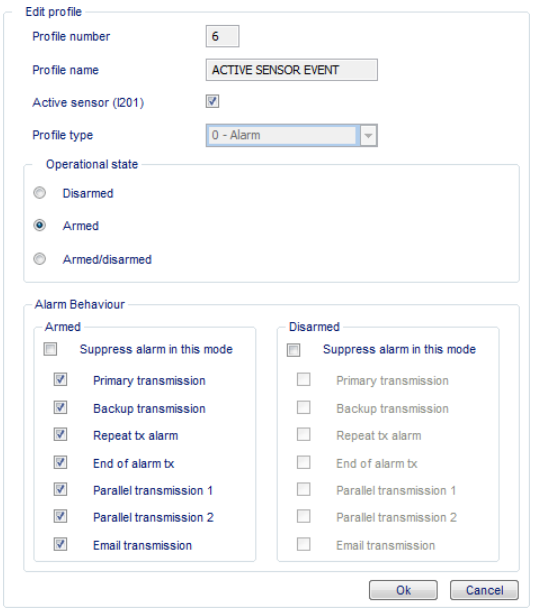


The SINGLE EVENT profile sends the alarm to **all transmission destinations**, but only once.

- Operational state: it does not consider the operational state. The system will transmit the alarm in both armed and disarmed state.
- Repeat: the system will not repeat the alarm transmission, even if the input remains active.
- End-of-alarm behaviour: when the input is no longer active (= end of alarm), the system will transmit a new message to indicate this.
- Profile type: 0 – Alarm. This is the generic profile type.

  You cannot modify the profile type.

14.4.6 Active Sensor Event Profile



The ACTIVE SENSOR EVENT profile sends the alarm to **all transmission destinations**. All inputs with this alarm profile trigger **input I0201**, the active sensor input. Input I0201 is active if one of the inputs with this alarm profile is active (logical function: OR). You can then use an output to inform a user that some inputs are still active. Typical application: light up a LED on a control panel (output), to prevent users from arming the system if, for example, a window in the building is still open (input still active).

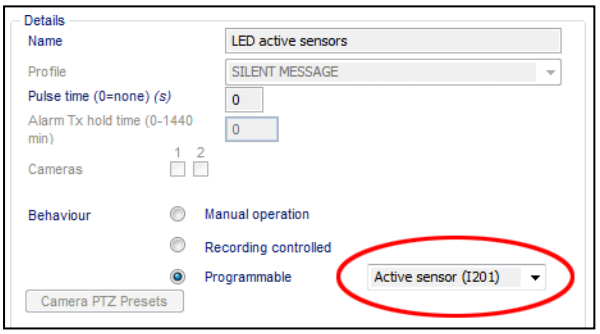
All the inputs using the ACTIVE SENSOR EVENT profile have to return to idle state in order to reset input I0201 and the corresponding output to the idle state. Only when this condition is fulfilled, the user can arm the system without triggering an alarm.

- Operational state: the system will only transmit the alarm when the system is armed.
- Repeat: the system will repeat the alarm transmission every x minutes (configurable) as long as the input is active.
- End-of-alarm behaviour: when the input is no longer active (= end of alarm), the system will transmit a new message to indicate this.
- Profile type: 0 – Alarm. This is the generic profile type.
  You cannot modify the profile type.

To activate an output based on input I201, proceed as follows:

1. Assign the ACTIVE SENSOR EVENT profile to all the inputs that have to trigger input I201.
2. Check if input I0201 has a suitable alarm profile (default is SILENT MESSAGE).
3. Select the desired output (filter on **Outputs: On the box** or **Outputs: Network** to see only the physical outputs), and give it a suitable name.

4. Click **Programmable**, and then select **Active sensor (I201)** in the list.



5. Click **Save**.

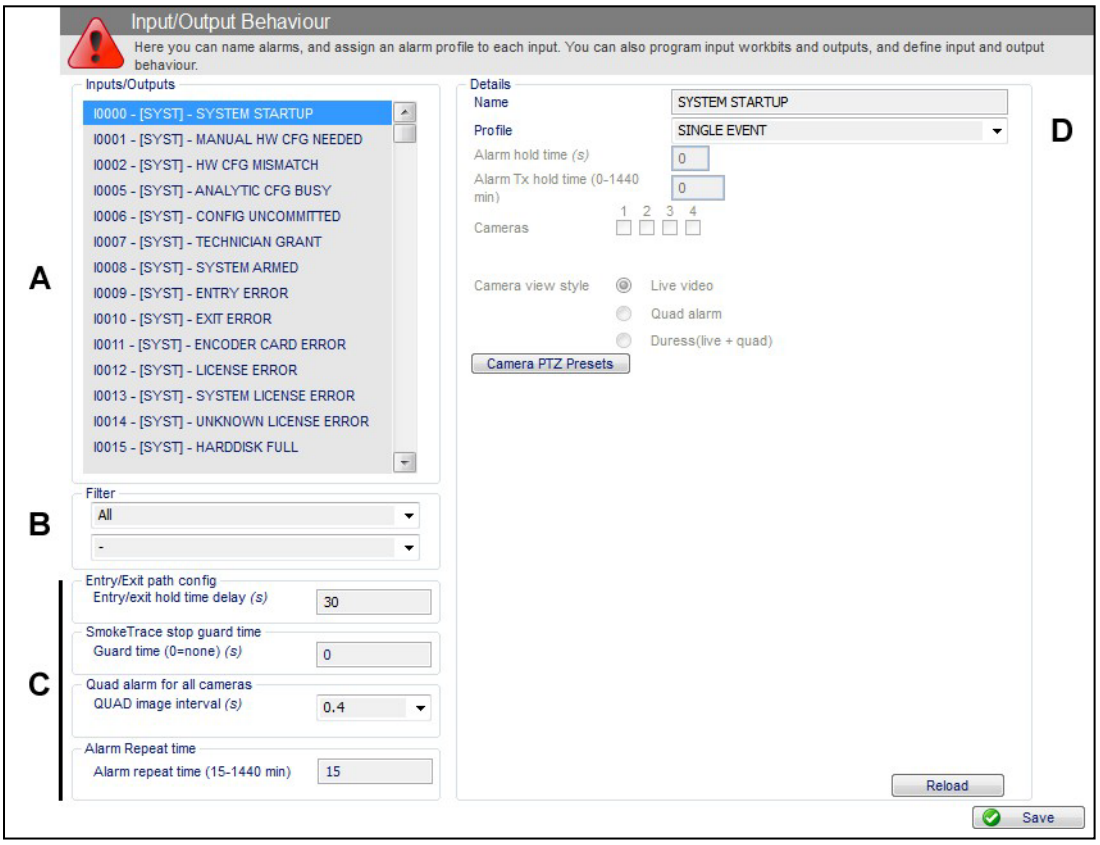
15 Input/Output Behaviour

15.1 About Inputs and Outputs

The XO device offers a long list of inputs and outputs.

- Inputs are events or alarms, originating either from the XO device itself or from connected peripherals such as cameras, PIR detectors, S3100 security panels, etc. You associate each input with an alarm profile, that defines if/how/when the system has to transmit the corresponding alarm message and camera images.
- Outputs are signals that typically drive connected peripherals such as status LEDs, audio switchers, etc. For each output, you define how to activate it.

To open the list with inputs and outputs, choose **System** > **Behaviour** > **Input/Output Behaviour**.



The **Input/Output Behaviour** window consists of the following parts:

A	**Inputs/Outputs**: The list of all inputs and outputs.
B	**Filter**: filters to reduce the list of inputs/outputs and quickly find the input/output you need.
C	General settings that apply to all inputs.
D	**Details**: the detailed settings of the input/output. The available options and settings depend on the input/output that is selected in the list.

The inputs/outputs are all structured in the same way. Some examples:
I0008 – [SYST] – SYSTEM ARMED
C2560 – [OUTP] – USBIO-1 GREEN LED

Details are in the table below:

I0008 C2560	– [SYST] – – [OUTP] –	SYSTEM ARMED USBIO-1 GREEN LED
The unique identification number of the input/output. In lists with both inputs and outputs, the input numbers start with an 'I', and the output numbers with a 'C'. You cannot modify the identification number.	Input/output type. The different types are: • **[SYST]**: system input • **[REAL]**: 'real' input (as opposed to a tamper input) • **[TAMP]**: tamper input • **[OUTP]**: output. You cannot modify the input/output type.	A descriptive name of the input/output. You can modify the name. This is particularly useful for the inputs/outputs on the MIO/EIO cards and Net I/O units, and for the workbits. Honeywell recommends to keep the default names of system inputs.

The setup of inputs and outputs is described in detail in the sections below.

15.2 Inputs

The following groups of inputs are available, depending on the configuration of the XO device:

- **System Messages**: internal events and states, such as communication errors, storage medium errors…
- **Cam**: camera inputs, such as video signal missing, camera sabotage alarm, motion alarm…
- **Network**: alarm inputs connected to the Net I/O units in the local network.
- **On the box**: alarm inputs connected to the MIO and EIO cards, with alarm and tamper state.
- **Workbits**: calculated bits that provide alarm information. A combination of inputs/outputs can trigger a workbit.
- **Virtual**: inputs from events detected on connected S3100 alarm panels.
- **PIRs**: PIR inputs, including normal and double-knock alarms, tamper alarms, etc.
- **SmokeTrace**: not applicable (SmokeTrace no longer available from Honeywell).
- **Analytic details**: extra inputs for the IntrusionTrace analytic application. For more information, see the *IntrusionTrace Technical Manual* (26472).

15.3 Monitored Inputs

The system can detect tampering with monitored inputs, providing extra security. Monitored inputs are available on:

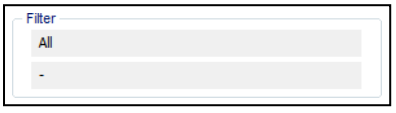
- MIO and EIO cards, both on the built-in cards or in the XO I/O Interface USB modules (= "on the box" inputs)
- the latest Net I/O units with hardware and firmware version 2 + XO version 4.2 or above running on the controlling XO device.

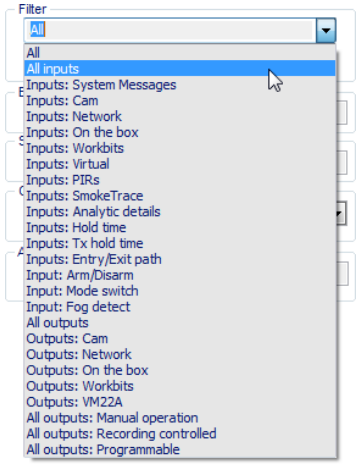
The end of line (EOL) configuration of the input defines if and how the system detects tampering (NEOL = no end of line: the system cannot detect tampering). For details, see the documentation of the MIO cards or Net I/O units.

The XO client offers 2 alarms per monitored input: the 'real' alarm, and the tamper alarm.

15.4 Filtering Inputs

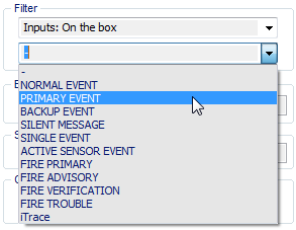
The list of available inputs is very long. Two filter boxes are available to quickly find the input you need.





The first filter box contains the following filters for inputs:

- **All inputs**: to list inputs only, not outputs.
- **Inputs: System messages**: to list all inputs related to internal events and states.
- **Inputs: Cam**: to list all inputs from cameras. You can filter further on camera number, to see only the inputs for 1 specific camera.
- **Inputs: Network**: to list all inputs on Net I/O units.
- **Inputs: On the box**: to list all inputs on MIO/EIO cards (interna or on the XO I/O Interface USB modules).
- **Inputs: Workbits**: to list all input workbits.
- **Inputs: Virtual**: to list all inputs from connected S3100 panels.
- **Inputs: PIRs**: to list all inputs from PIR detectors.
- **Inputs: SmokeTrace**: not applicable (SmokeTrace no longer available from Honeywell).
- **Inputs: Analytic details**: to list all extra inputs for IntrusionTrace
- **Inputs: Hold time**: to list all inputs that have an alarm hold time different from 0.
- **Inputs: Tx hold time**: to list all inputs that have an alarm transmission hold time different from 0.
- **Inputs: Entry/Exit path**: to list all inputs that have been programmed within the entry/exit path (delayed events).
- **Input: Arm/Disarm**: to find the input that has been programme for arming/disarming the system.
- **Input: Mode switch**: to find the input that has been programmed for switching recording modes.
- **Input: Fog detect**: to find the input that has been programmed as the fog detection input for intelligent double knock with ADPRO PRO E PIR detectors



The second filter box allows you to filter inputs on the alarm profile that is assigned to the input.

15.5 Alarm Input Behaviour

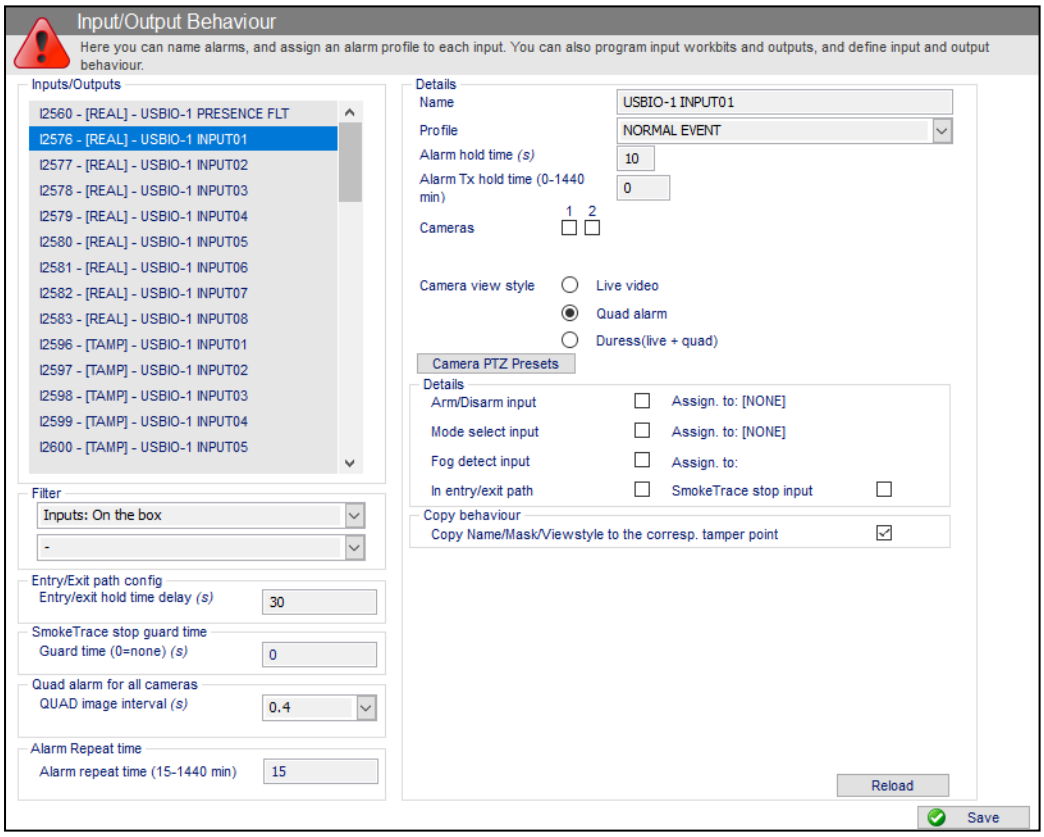
Note

You cannot change the input's unique identification number or the input type.

With software version XO 4.00 and above, you can select **multiple inputs** at once and quickly assign the same alarm profile to all selected inputs. You can only change the alarm profile for multiple inputs, not the other settings.

To set up the input behaviour, proceed as follows:

1. Choose **System** > **Behaviour** > **Input/Output Behaviour**.
2. Select the desired input in the list. Filter the list if necessary.



> **Note**
>
> Depending on the type of input, not all settings and options may be available.

3. Provide the following information:

Item	Description
Name	Type a name (max. 20 characters) to describe the input. Use a description that is meaningful and relevant. The name appears in the alarm message to the CMS and to iTrace, in the screens in the client software (for example, in trigger lists and in the **Status** window), and in the log files. Honeywell recommends to keep the default names of system inputs. **Note** For monitored on-the-box or Net I/O inputs : when you change the default name of the real input (alarm), the system automatically changes the name of the corresponding tamper input accordingly, if you have selected the **Copy Name/Mask/Viewstyle…** checkbox (see further below). In this case, you cannot change the name of the tamper input individually.
Profile	Select the desired alarm profile. The alarm profile defines if/how/when the system has to transmit the alarm to the CMS (or other destinations such as iTrace). For more information, see *Alarm Profiles*.

Item	Description
Alarm hold time (s)	Enter the minimum activation time of the alarm, in seconds. The XO device will only detect the end of alarm after this delay. You can use this, for example, to suppress a flow of events caused by a rattling alarm contact. Set to **0** if you want to detect the end of alarm without delay. This setting is unavailable for some types of inputs, such as system and tamper alarms.
Alarm Tx hold time (0-1440 min)	Enter the alarm transmission hold time, in minutes. The system will only transmit the alarm if the alarm remains active for longer than the specified hold time. This can help to reduce nuisance alarms going to the CMS. Set to **0** if you want to transmit the alarm regardless of the time the alarm remains active. This setting is unavailable for some types of inputs, such as certain system alarms.
Cameras	Select the cameras that will provide live video and/or quad images for the event. Choose the cameras that can reveal important information about the event. This setting is unavailable for some types of inputs, such as system-related alarms (for example storage medium errors).
Camera view style	Select the video information to transmit to the recipient (CMS, iTrace user): • **Live video**: the recipient can open a connection to the site and watch live images on the selected cameras. • **Quad alarm**: the system captures and transmits 3 stills from each selected camera, together with a fourth image that displays the stills in sequence to indicate movement. You set the interval between the stills in the **Quad image interval (s)** box (see further below). • **Duress**: the system sends both live and quad images from each selected camera.
Camera PTZ presets	Click this button to configure PTZ cameras to move to a specific preset position when the input is triggered. For details, see *PTZ Position on Input*.
Arm/Disarm input	Select this checkbox to use the input to arm and disarm the system (see *Arming/Disarming Manually*). You can only use one input for arming/disarming. The system displays the number and name of the input that is currently assigned for arming/disarming at the right side of the checkbox. If no input is assigned, it displays NONE.
Mode select input	Select this checkbox to use the input to switch between recording modes (see *Recording Mode with Manual Selection*). You can only use one input for switching recording modes. The system displays the number and name of the input that is currently assigned for switching at the right side of the checkbox. If no input is assigned, it displays NONE.
Fog detect input	Select this checkbox to use the input as the fog detection input for intelligent double knock (see *Double-Knock Configurations*). You can only use one input as the fog detection input for intelligent double knock. The system displays the number and name of the input that is currently assigned as fog detection input. If no input is assigned, nothing is displayed.

Item	Description
In entry/exit path	Select this checkbox if you want to delay the alarm to allow for entering/exiting the premises before the alarm goes off. You specify the delay itself in the **Entry/Exit hold time delay** box (see further below). This is typically used with motion detection in entry halls: • If you enter the premises while the system is still armed, you trigger the alarm. However, the alarm will not go off if you disarm the system within the delay (counting from the moment that the alarm is triggered). • If you leave the premises and arm the system, the alarm will not go off if you leave within the delay (counting from the moment that you arm the system).
SmokeTrace stop input	Not applicable (SmokeTrace no longer available from Honeywell).
Copy Name/Mask/Viewstyle… to the corresp. tamper point	For monitored on-the-box or Net I/O inputs (real input and tamper input): if you select this checkbox, and you change the **Name**/**Cameras**/**Camera view style** settings of the real input, the system will automatically change these settings for the corresponding tamper input too. In this case, you cannot change the **Name**/**Cameras**/**Camera view style** settings of the tamper input; the system will always use the settings of the corresponding real input.
Logic	Only available for workbit inputs. For more information on programming the workbits, see *Programming Logical Functions*.
Entry/exit hold time delay (s)	Enter the delay for the entry and exit paths, in seconds. The delay is the same for entry and exit, and for all inputs.
SmokeTrace stop guard time (s)	Not applicable (SmokeTrace no longer available from Honeywell).
Quad image interval (s)	Select the interval, in seconds, between the successive quad images. The quad interval setting applies to **all cameras**, and therefore to **all applications**. Different applications may have different ideal quad intervals. For intrusion detection, you may require a short interval, whereas for other alarms you may want a longer interval. In this case, you have to find a compromise that gives acceptable results for all applications. **Always test** the selected setting.
Alarm repeat time (15-1440 min)	For repeating alarms: select the interval, in minutes, between the repeated alarm transmissions. The repeat interval is the same for all inputs. However, the setting does not apply to the following alarms; the system repeats them only once every 24 hours: • 0050 – [SYST] – STORAGE INSUFFICIENT • 0065 – [SYST] – LICENSE EXPIRED • 0066 – [SYST] – LICENSE OUT OF SYNC • 0067 – [SYST] – APPLICATION STOPPED • 0511 – [SYST] – GENERAL ISOLATION.

4. Click **Save**.

15.6 PTZ Position on Input

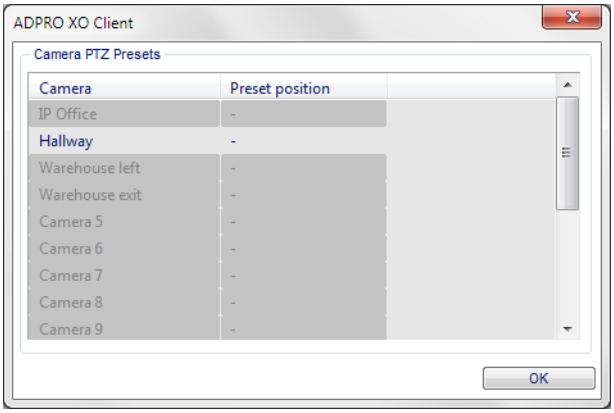
It is possible to make one or more PTZ cameras move to a PTZ preset position when an input is triggered. You can assign one position to each available PTZ camera.

The system delays the alarm transmission until the PTZ positioning time has expired. The PTZ positioning time is the time that you allow for the camera to move and settle into the PTZ position. This makes sure that the quad images recorded with the alarm are sharp. You specify the PTZ positioning time for each PTZ camera in the

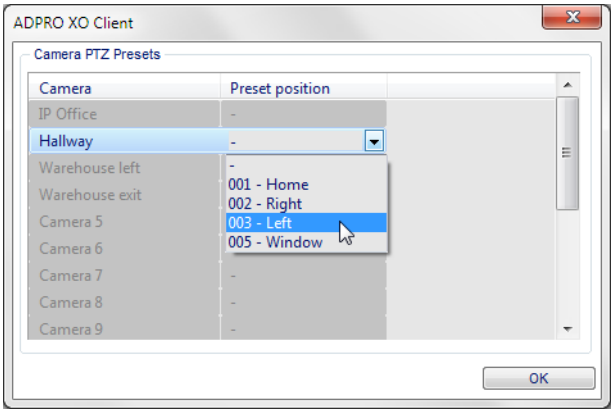
camera setup window. For more information, see *PTZ Setup*.

To make PTZ cameras move to a preset position when an input is triggered, proceed as follows:

1. Choose **System** > **Behaviour** > **Input/Output Behaviour**.
2. Select the desired input, and then click **Camera PTZ Presets**. The following window appears:



3. For the required PTZ cameras, click in the **Preset position** column, and then click the desired preset.



4. Click **OK**.
5. Click **Save**.

15.7 Outputs

The following output types exist, depending on the configuration of the XO device:

- Cam: camera outputs.
- Network: outputs on the Net I/O units, connected to the local network.
- On the box: outputs on the MIO and EIO cards.
- Workbits: calculated bits that can be used to store internal states. A combination of inputs/outputs can trigger a workbit.
- VM22A: outputs that activate the corresponding loudspeaker on the VM22 audio switchers. You can only change the name of these outputs; the system fully controls their behaviour.

  You can activate an output in one of the following ways:

- Manually
- By a recording condition (recording controlled)
- By a logical function (programmable).

  All methods are described in detail further below.

15.8 Filtering Outputs

The list of outputs is very long. Filters are available to quickly find the output you need. The following filters for outputs exist:

- **All outputs**: to list outputs only, not inputs.
- **Outputs**: Cam: to list all outputs from cameras.
- **Outputs**: Network: to list all outputs on Net I/O units.
- **Outputs**: On the box: to list all outputs on MIO/EIO cards (internal or on the XO I/O Interface USB modules).
- **Outputs**: Workbits: to list all output workbits.
- **Outputs**: VM22A: to list all outputs on a VM22 audio switcher.
- **All outputs**: Manual operation: to find all outputs that are controlled manually
- **All outputs**: Recording controlled: to find all outputs that are controlled by recording conditions
- **All outputs**: Programmable: to find all outputs that are controlled by a logical function.

15.9 Output Behaviour

15.9.1 Manual Operation

Manual operation means that you can manually activate the output from within the XO client software; either via the **Status** window or from the **Live Video** window. To control an output from the **Live Video** window, you have to assign at least one camera to the output. Outputs that can be controlled via the **Live Video** window are also available in iTrace.

You can deactivate the output in the same way, or let the XO client automatically reset the output after a specific time (pulse time) or when you close the XO client.

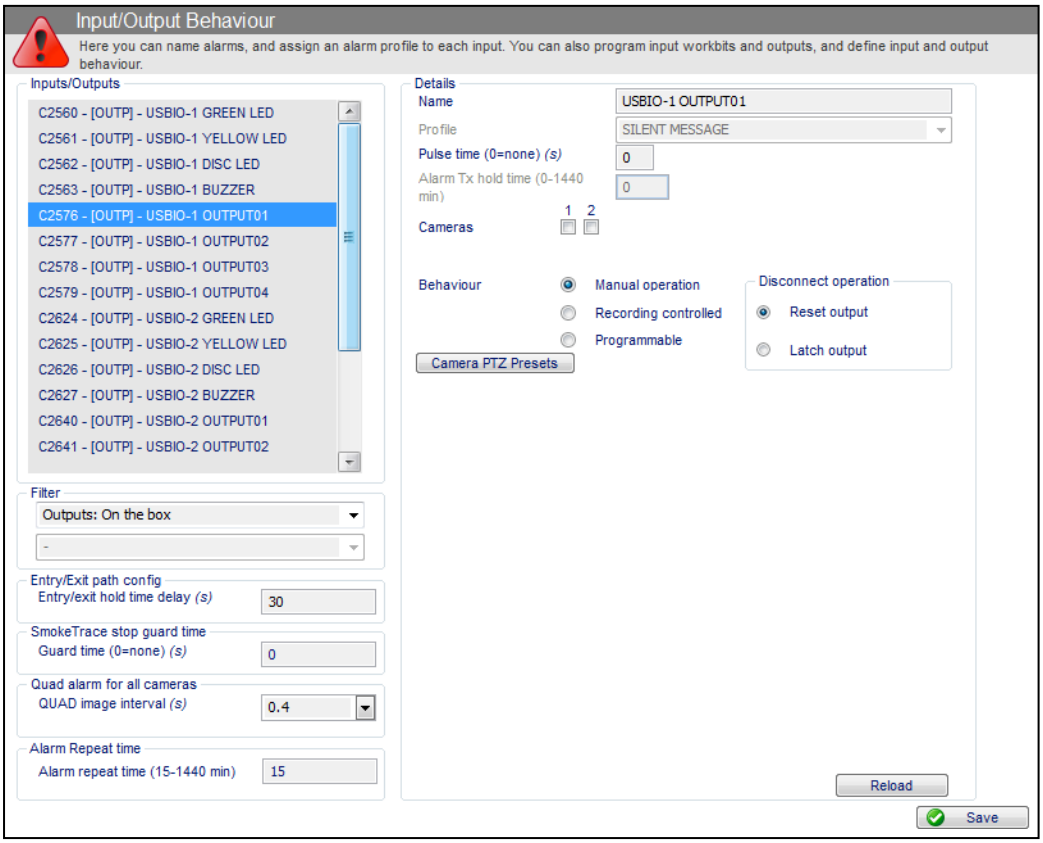
The following outputs are suitable for manual operation:

Output	Activate from	
	Status window	Live Video window / iTrace
Relay outputs on the MIO and EIO cards (on-the-box outputs)	Yes	Yes
Relay outputs on the Net I/O units (network outputs)	Yes	Yes
Workbit outputs	Yes	No
Camera outputs	Yes	Yes

15.9.1.1 Setting up Outputs for Manual Operation

To set up an output for manual operation, proceed as follows:

1. Choose **System** > **Behaviour** > **Input/Output Behaviour**.
2. Select the desired output in the list. Filter the list if necessary.



3. Provide the following information:

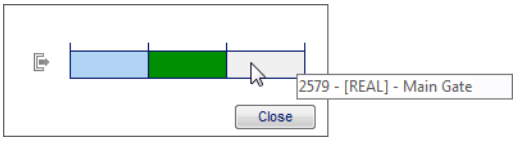
Item	Description
Name	Type a name (max. 20 characters) to describe the output. Use a description that is meaningful and relevant.
Pulse time (s)	To reset the output automatically after a specific time: enter the time, in seconds, in the **Pulse time** box. Set the pulse time to **0** if you want to keep the output active.
Behaviour	Click **Manual operation**.
Cameras	To make the output available for activation in the **Live Video** window and iTrace, select the cameras for which the **Activate outputs** button has to appear. Select at least one camera. This option is not available for workbits.
Disconnect operation	Define what happens when you close the XO client: • Click **Reset output** if you want to reset the output to idle state (inactive) when closing the XO client. • Click **Latch output** if you want to keep the output active when closing the XO client. Keep in mind that the system will reset the output when you restart the XO device.

4. Click **Save**.

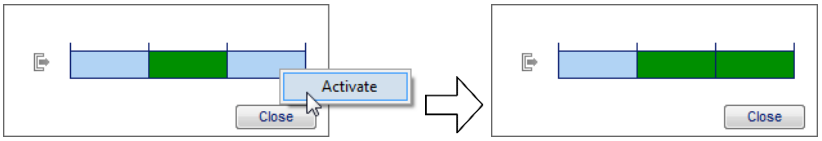
15.9.1.2 Activating/Deactivating Outputs from the Live Video Window

To activate/deactivate an output from the **Live Video** window, proceed as follows:

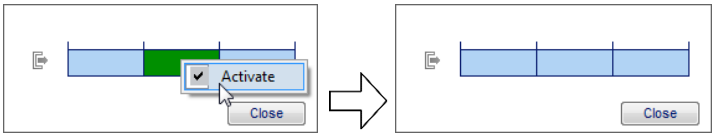
1. In the top menu, click **Live Video**.
2. In the matrix view, click the camera image to which the output is associated.
3. Under **Tools**, click the button. A popup window appears with a status bar for the outputs on the selected camera. Idle outputs are blue, active outputs are green. When you place the mouse cursor over an output, the system displays the output number and name.



4. To activate an output, right-click the desired output in the status bar, and then click **Activate**. The output bar colours green.



5. To deactivate an output, right-click the desired output in the status bar, and then click **Activate**. The output bar colours blue.

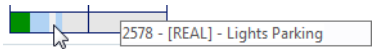


6. Click **Close**.

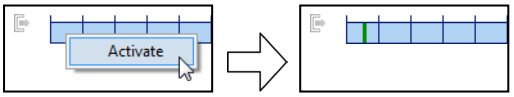
15.9.1.3 Activating/Deactivating Outputs from the Status Window

To activate/deactivate an output from the **Status** window, proceed as follows:

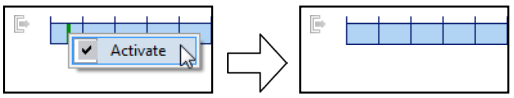
1. In the top menu, click **Status**, and then click the **I/O** tab.
2. Locate the desired output in the status bars. When you position the mouse cursor over an output, the system displays the output number and name. Idle outputs are blue, active outputs are green.



3. To activate an output, right-click the desired output in the status bar, and then click **Activate**. The output bar colours green.



4. To deactivate an output, right-click the desired output in the status bar, and then click **Activate**. The output bar colours blue.

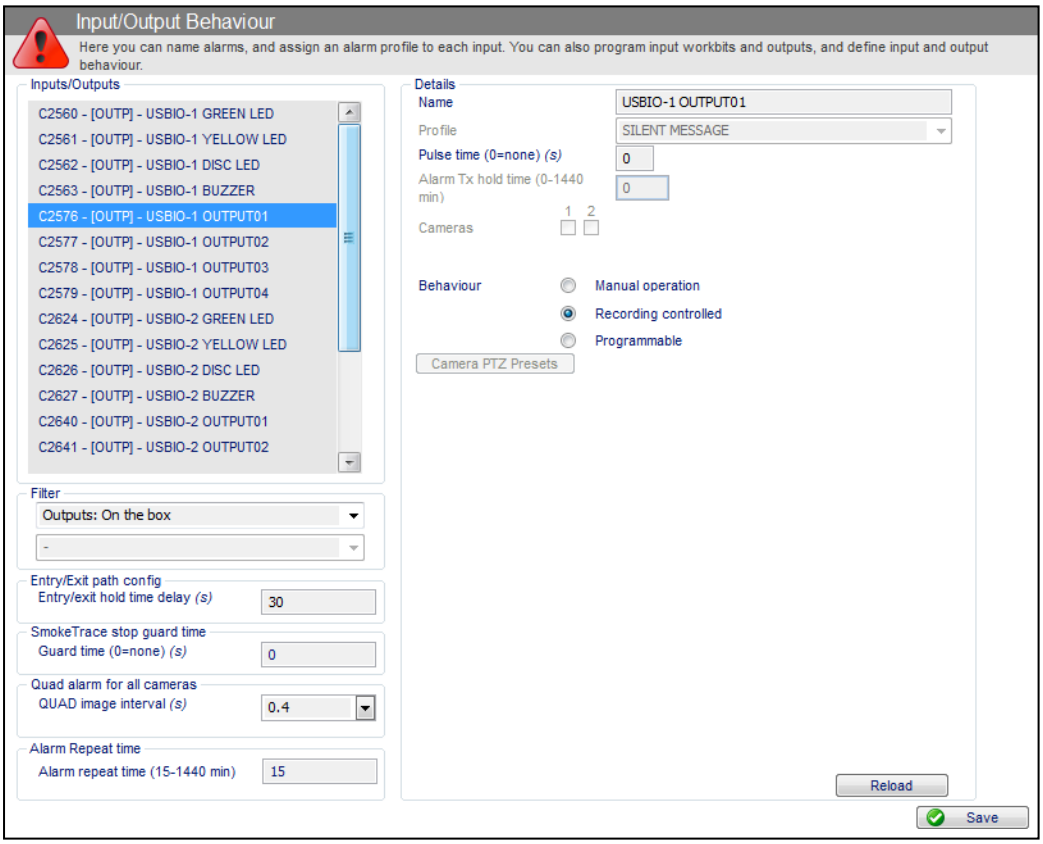


15.9.2 Recording-Controlled Outputs

You can automatically activate outputs when a recording starts. The system deactivates the output when the recording stops, or you can let the system automatically reset the output after a fixed time (pulse time). You can assign one output to each recording condition. You can assign an output to only one recording condition.

To set up a recording-controlled output, proceed as follows:

1. Choose **System** > **Behaviour** > **Input/Output Behaviour**.
2. Select the desired output in the list. Filter the list if necessary.



3. Provide the following information:

Item	Description
Name	Type a name (max. 20 characters) to describe the output. Use a description that is meaningful and relevant.
Pulse time (s)	If you want to reset the output automatically after a specific time: enter the time, in seconds, in the **Pulse time** box. Set the pulse time to **0** if you want to keep the output active as long as the recording condition is active.
Behaviour	Click **Recording controlled**.

4. Click **Save**.

You can now assign the output to a recording condition. For more information, see *Recording Behaviour* .

15.10 Programmable Inputs and Outputs

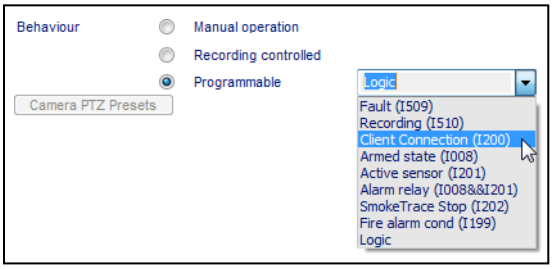
15.10.1 Overview

Under **Logic**, you can program a function that calculates the value for an input or output, based on a combination (AND/OR) of other inputs, outputs, and input isolation statuses. You can program the following inputs and outputs:

- Inputs:
  - the camera EVENT inputs. For example, for camera 1: I1032 – [REAL] – CAM01 EVENT.
  - workbits.
- Outputs:
  - outputs on MIO/EIO cards
  - outputs on Net I/O cards
  - workbits
  - camera outputs.

15.10.2 Predefined Programmable Outputs

For outputs, you can choose from a number of predefined functions.



The available options are:

Option	Description
Fault (I509)	The system activates the output if any fault is present (follows system input I0509). Faults are active inputs indicated in orange in the **Status** window. Active inputs that are isolated, do not trigger the output.
Recording (I510)	The system activates the output if any recording is active (follows system input I0510).
Client Connection (I200)	The system activates the output if any client connection is active (follows system input I0200).
Armed state (I008)	The system activates the output if the system is armed (follows system input I0008).
Active sensor (I201)	The system activates the output if any sensor is active (follows system input I0201).
Alarm relay (I008&I201)	The system activates the output if any sensor is active, but only when the system is armed (follows system input I0201 AND system input I0008).
SmokeTrace Stop (I202)	Not applicable (SmokeTrace no longer available from Honeywell).
Fire alarm cond (I199)	Not applicable (SmokeTrace no longer available from Honeywell).
Logic	The system activates the output depending on a calculation in a logical function that you program yourself.

To set up a programmable output with a predefined function, proceed as follows:

1. Choose **System** > **Behaviour** > **Input/Output Behaviour**.
2. Select the desired output in the list. Filter the list if necessary.
3. Provide the following information:

Item	Description
Name	Type a name (max. 20 characters) to describe the output. Use a description that is meaningful and relevant.
Pulse time (s)	If you want to reset the output automatically after a specific time: enter the time, in seconds, in the **Pulse time** box. Set the pulse time to **0** if you do not want to reset the output automatically.
Behaviour	Click **Programmable**, then select the desired function in the list. If you choose **Logic**, program the function as described in *Programming Logical Functions*.

4. Click **Save**.

15.10.3 Programming Logical Functions

Below is an example of a logical function:

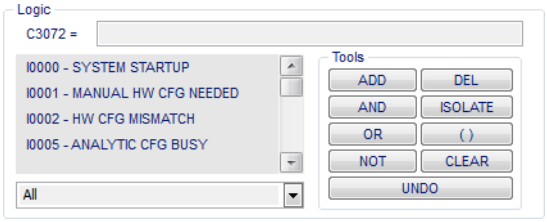
C3072 = I2144 AND I2145 OR M2146 AND NOT I2145.

The system executes the function from left to right. The AND operation is performed first. This means:
C3072 = I2144 AND I2145 OR M2146 AND NOT I2145
is the same as:
C3072 = (I2144 AND I2145) OR (M2146 AND NOT I2145)

Output C3072 (workbit 1) will be active if:
input I2144 AND input I2145 are both active (these are inputs 1 and 2 on Net I/O unit 2)
or if
input I2146 is isolated AND input I2145 is inactive (input 3 on Net I/O unit 2 is isolated and input 2 on the same unit is inactive).

To program a logical function, proceed as follows:

1. Choose **System** > **Behaviour** > **Input/Output Behaviour**.
2. Select the input or output that you want to program.
3. For outputs only: under **Behaviour**, select **Programmable**, and then select **Logic** in the list. The **Logic** section for entering the function appears.
   For inputs, the **Logic** section appears automatically when you select a programmable input.



4. Proceed as follows to create the function:

Desired result	Possible actions
To add an input/output to the function	• Select the input/output in the list (filter the list if necessary), and then click **ADD**. • Double-click the input/output.

Desired result	Possible actions
To use the inverted status of an input/output	• Click **NOT** immediately after adding the input/output. • Click the input/output in the function, and then click **NOT**. The indication **NOT** appears in front of the input/output number in the function. Click **NOT** again to revert to the normal status.
To read the isolation status (isolated or not) of an input	• Click **ISOLATE** immediately after adding the input. • Click the input in the function, and then click **ISOLATE**. The letter **M** appears in front of the input number in the function. Click **ISOLATE** again to read the normal status.
To add an operator	Click **AND** or **OR**.
To execute specific operations first	Use parentheses: • Select the operation(s) that you want to execute first, and then click **( )**. • Click **( )**, position the cursor between the parentheses, and then add the desired inputs/outputs and operators. To remove parentheses: select each parenthesis individually, and then click **DEL** to remove it.
To undo your last action	Click **UNDO**.
To delete a part of the function	Click or select the part, and then click **DEL**.
To delete the whole function	Click **CLEAR**.

5. Click **Save**.

16 Video Content Analytics (VCA)

16.1 Overview

There are several options for video content analytics (VCA) on your XO device:

- You can use one or more of the ADPRO analytic applications:
  - **IntrusionTrace**: outdoor perimeter detection for sterile zone monitoring
  - **LoiterTrace**: indoor/outdoor loitering detection

  These applications are embedded in the XO software, but you need a license to unlock their functionality. You install the licenses on the XO device using the Xchange2 Tool. The menu option for setting up an analytic application in the XO client only appears if you have installed at least one valid license for that application on the XO device.

  LoiterTrace supports deep learning. Activate deep learning with a separate license and select the **Deep Learning** checkbox on the **LoiterTrace configuration** page to use the deep learning feature. Deep Learning (DL-LoiterTrace) is ideal for places such as bank ATMs. The Deep Learning software employs Artificial Intelligence / Machine Learning to improve the accuracy of the software on typical scenarios. Deep Learning LoiterTrace is a version of LoiterTrace that uses machine learning techniques for the increased precision of LoiterTrace. The Deep Learning LoiterTrace tracks individuals instead of groups and classifies peoples/objects, which helps reduce the false alarms and reduces the risk of vandalism, graffiti, substance abuse, arson attacks, harassment, and identity theft.

  Note

  Apply the Deep Learning LoiterTrace licenses in addition to the LoiterTrace licenses while not exceeding the total allowed Video Analytic licenses for the device.

- Maximum of 4 channels of Deep Learning LoiterTrace are allowed on the iFTE device with PH10FEU motherboard.
- Maximum of 3 channels of Deep Learning LoiterTrace are allowed on the iFT device with PH10FEU motherboard.

  Note

  Devices with older motherboard such as PH10LU can't support Deep Learning LoiterTrace.

  The use and configuration of the analytic applications is not described in detail in this document. For more information on the analytic applications, see the respective application’s documentation.

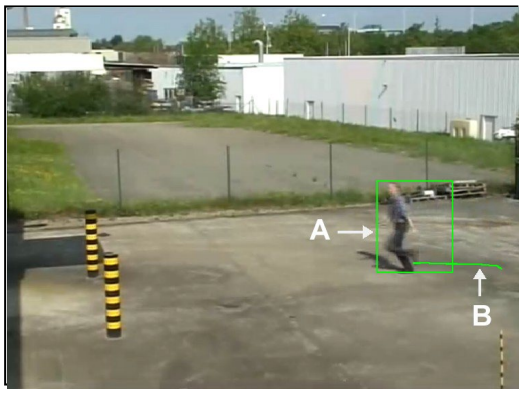
- The **Motion, sabotage feature**: this is always available on the XO device. You do not need a license for it. For details, see *Motion, Sabotage*.

16.2 Rendering Analytic Bounding Boxes

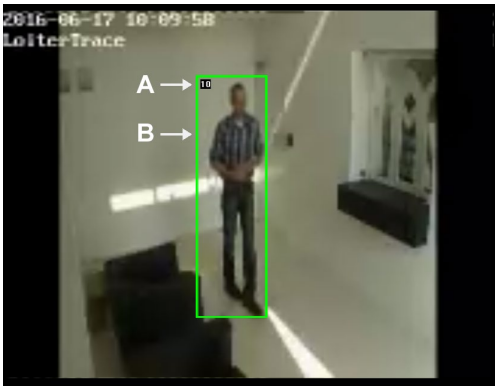
Analytic bounding boxes indicate the presence of detected objects in the scene, detected by the ADPRO analytic applications. The bounding boxes are:

- Green: when the alarm is not triggered
- Red: when the alarm is triggered.

Besides the bounding boxes around the detected object, IntrusionTrace also displays the path that the object follows in the scene. Just like the bounding boxes, the path is displayed in green when the alarm is not triggered, and in red when the alarm is triggered.
As long as the alarm is not triggered, LoiterTrace also displays the time (in seconds) that the object is being tracked in the detection zone.



IntrusionTrace: analytic bounding box (**A**) and path (**B**)



LoiterTrace: analytic bounding box (**B**) and timer (**A**)

For live and recorded images in the **Live Video** and **Recorded video** windows, you can choose whether you want to render analytic bounding boxes and paths, or not. The following options exist:

- **Off**: the system does not display bounding boxes and paths or timers.
- **Alarm only**: the system displays only the red bounding boxes and paths when an alarm occurs.
- **Alarm and tracking**: the system displays the green bounding boxes and paths/timers for tracking (pre- and post-alarm), and the red bounding boxes and paths when the alarm occurs.
- **IntrusionTrace zone outline upon event**: the system highlights the IntrusionTrace detection zone where the alarm occurs.

Below, you can see several examples for IntrusionTrace:



Off:
no bounding boxes or paths visible



Alarm only:
red bounding box and path upon alarm



Alarm and tracking:
green bounding boxes and path for tracking; bounding boxes and path will turn red upon alarm



IntrusionTrace zone outline (with alarm):
red bounding boxes and path + IntrusionTrace detection zone highlighted

Below, you can see several examples for LoiterTrace:



Off:
no bounding boxes or timer visible



Alarm only:
red bounding upon alarm



Alarm and tracking:green bounding box and timer for tracking; bounding box will turn red upon alarm

If you have multiple analytic applications running on the same camera (for example, IntrusionTrace and LoiterTrace), the system will display bounding boxes for all analytics. The example below displays a red bounding box for IntrusionTrace (alarm) and a green bounding box for LoiterTrace (tracking), around the same object.

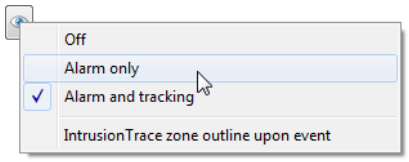


The following limitations apply to bounding box rendering:

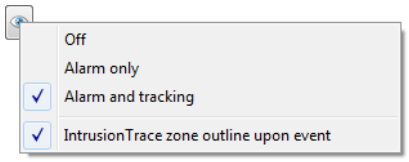
- When playing back recorded images, bounding boxes and paths/timers only appear in normal playback mode, not during fast forward/backward.
- If bounding box rendering is switched off, the IntrusionTrace zone outline upon event option is unavailable.
- The player software that allows you to play downloaded recordings (.hbox files) from your local PC or from a USB drive, offers the same options for rendering analytic bounding boxes and paths/timers. However, the IntrusionTrace zone outline upon event option is not available.
- If you need to see the highlighted IntrusionTrace zone, play the recordings from within the XO client.

To select the desired options for rendering bounding boxes, proceed as follows:

1. From the live or recorded images view, click the button, and then click the desired rendering option.



2. To highlight the IntrusionTrace detection zone where the alarm is triggered, click the button, and then click **IntrusionTrace zone outline upon event**. A check mark appears next to the option when it is active:



16.3 Motion, Sabotage

16.3.1 About Motion, Sabotage Detection

With the **Motion, sabotage** feature, you can define up to 4 rectangular motion detection zones for a camera. Each one triggers its own alarm. For example, for camera 1:

1034 – [REAL] – CAM01 MOTION1
to
1037 – [REAL] – CAM01 MOTION4

You can transmit these alarms to a CMS, or use them to start recordings.

Furthermore, you can define up to 3 rectangular private zones (mask zones). These zones can overlap. Private zones are not available on cameras with PTZ enabled.

Bounding boxes and paths are not available with the **Motion, sabotage** feature. However, if bounding box rendering is enabled, the system will display the motion detection zones edges (in red) upon an alarm in the live and recorded video view.



Optional: you can enable camera **sabotage detection**. With sabotage detection enabled, the system generates an alarm if the camera is being tampered with (for example: the lens is covered). You can set up advanced settings for sabotage detection and save the settings in a profile.

The **Cameras** section displays the numbers of all the cameras on the XO device that are using the **Motion, sabotage** feature. Position the mouse cursor over the number to see the corresponding camera name.



The icons on the camera numbers indicate the following information:

- The green check mark (on the left) indicates that the camera is configured for **motion detection**: you have drawn at least one motion detection zone for that camera. In the example above: on all cameras.
- The red S (on the right) indicates that **sabotage detection** is enabled for the camera. In the example above: on cameras 2 and 4 only.

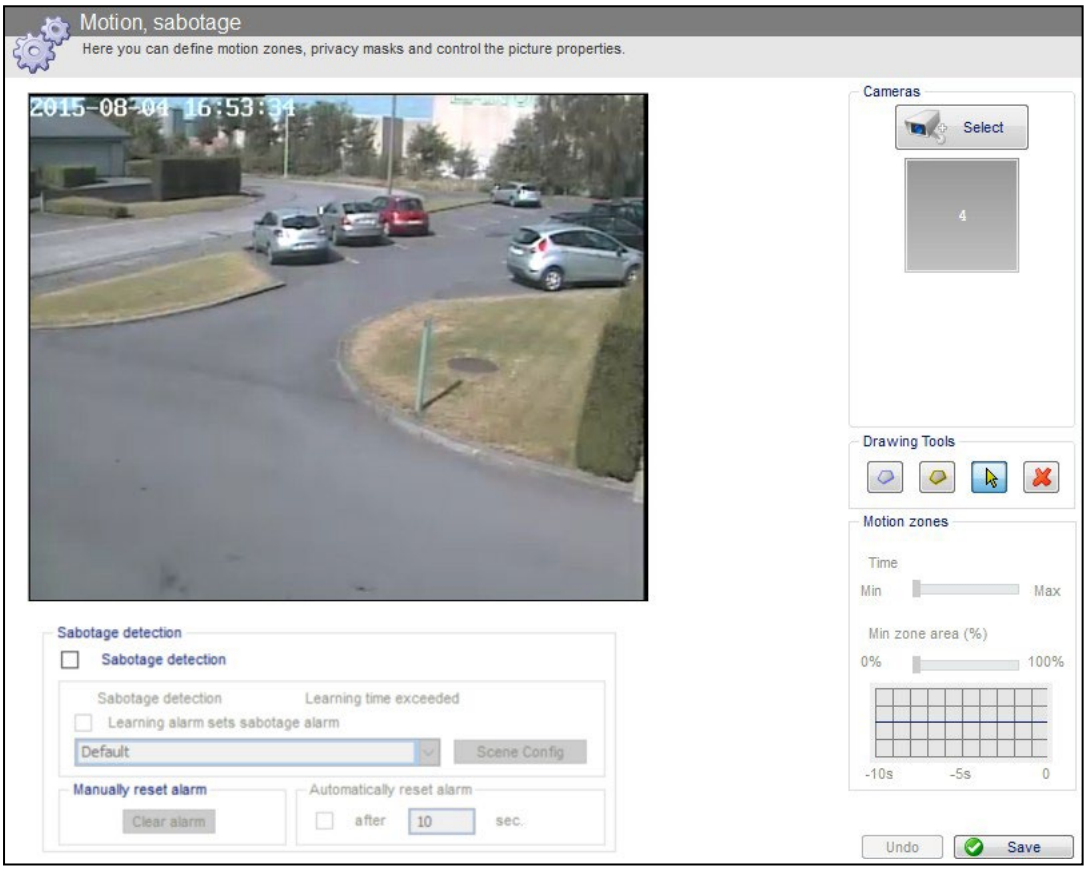
16.3.2 Drawing Detection Zones

Note

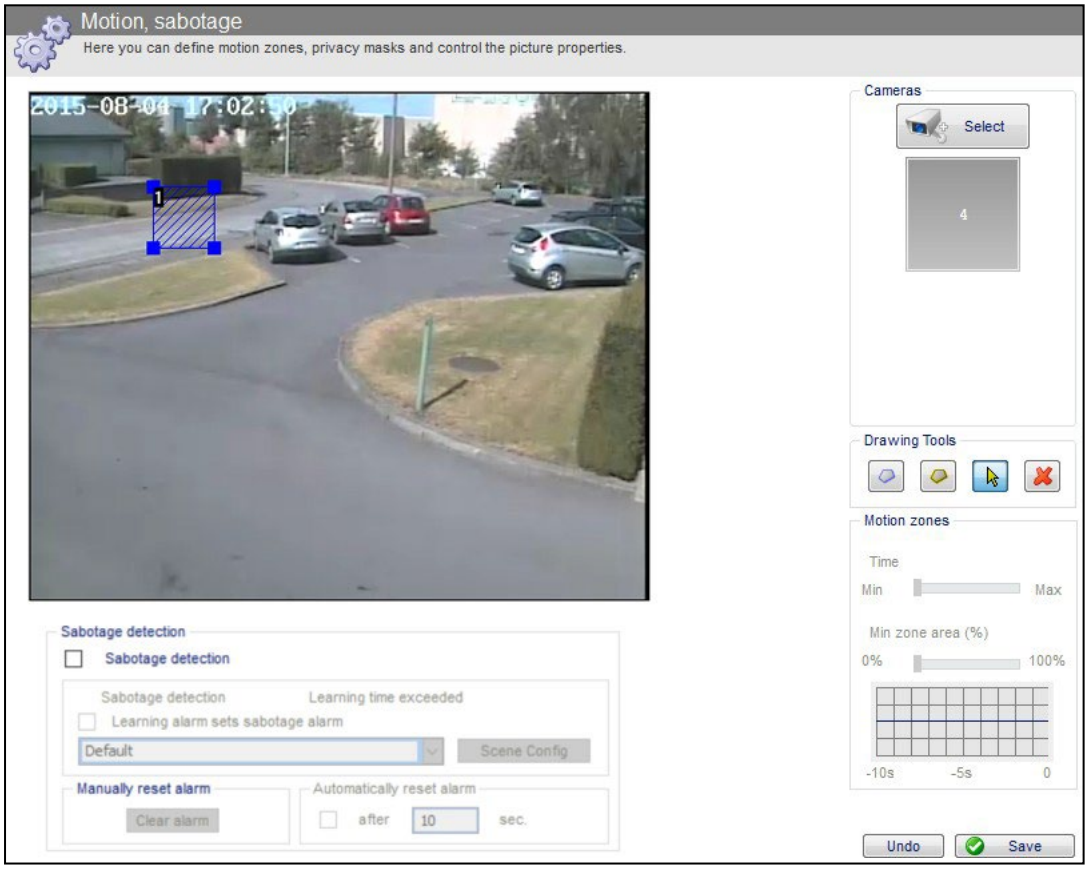
It is usually better to use several smaller detection zones than 1 large zone. A large detection zone may produce false alarms caused by light variations in the scene.

To draw detection zones for motion detection, proceed as follows:

1. Choose **System** > **Behaviour** > **Analytics** > **Motion, sabotage**.
2. Click **Select**, and then click the desired camera. The camera number appears in the grey box and the live image appears.

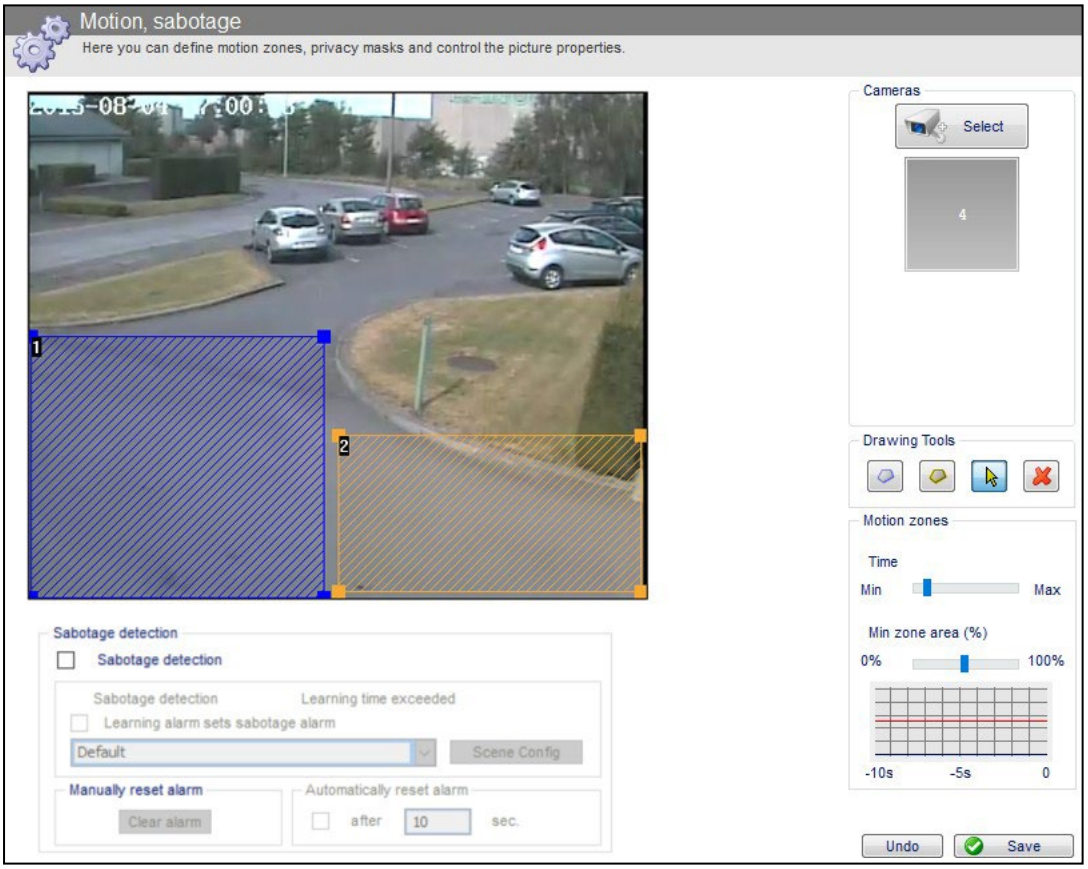


3. Under **Drawing Tools**, click the button (first button).
A blue square (numbered 1) appears on the live image.



4. Adjust the detection zone as follows:
   - Drag the zone to move it to the desired position.
   - Drag one of the corner handles to resize the zone.
   - To delete the zone, click in it, and then click .

5. Repeat for more detection zones. You can define up to 4 detection zones. The currently selected zone is orange.



6. Click **Save**.

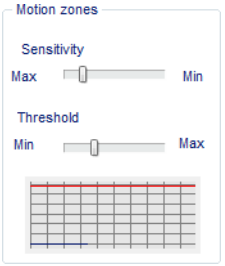
Next, you will set up the detection parameters.

16.3.3 Motion Zone Detection Settings

The detection settings depend on the type of camera: analogue or IP. Both possibilities are described in detail below.

16.3.3.1 Analogue Cameras

For analogue cameras you can adjust the sensitivity and the threshold for each detection zone.



- **Sensitivity**: specifies how much the luminance of the pixels in the zone has to change to detect motion. This setting is valid for all the detection zones.
- **Threshold**: sets the number of pixels in the zone that have to change in order to detect motion. This defines the size of the objects that you can detect. With a large threshold, only large objects will trigger motion detection. You can adjust this setting per detection zone.

It takes some testing to find the optimal settings. Some guidelines for successful motion detection with analogue cameras:

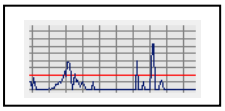
- Use uniform lighting.
- Switch off AGC (automatic gain control) in the camera.
- Keep the sensitivity as low as possible. If sensitivity is high, small illumination changes may cause false alarms.
- Keep the detection zones as small and narrow as possible. With large detection zones, you have to increase the sensitivity in order to detect motion. This in turn may increase the number of false alarms. In addition, relatively small objects may not be detected in a large zone.

Note

To get a feel for how the different settings influence detection, adjust only one setting at a time: sensitivity, threshold, or the size and shape of the detection zone.

To set up motion detection settings for analogue cameras, proceed as follows:

1. Adjust the **Sensitivity** slider.
2. Click a detection zone to select it, and then adjust the **Threshold** slider for that zone.
3. Use the graph to test the settings in the selected detection zone. The horizontal red line indicates the threshold. It moves up if you increase the **Threshold** setting, and down if you decrease it. The detection level (black line) of the zone has to exceed the threshold to trigger motion detection.



4. Repeat from step 2 for other detection zones.
5. Click **Save**.

You can test the settings from the configuration screen: if detection is successful and an alarm occurs, the system highlights the edge of the motion detection zones in red in the configuration screen. You can immediately adjust the settings if necessary.

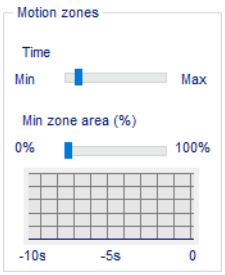


16.3.3.2 IP Cameras

Note

Please check the sensitivity settings, if the firmware version is upgraded from the 4.3.6 version to 4.5.7 or later.

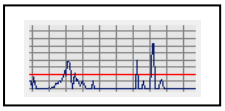
For IP cameras you can adjust time and minimum zone area for each detection zone:



- **Time**: sets the detection delay. Minimal delay means that the motion is detected immediately when an object starts moving in the detection zone. Maximal delay means that the motion is detected when the object is moving inside the detection zone for some time. This setting is valid for all detection zones.
- **Min zone area (%)**: sets the size of the object to detect, relative to the detection zone size (as a percentage). A low zone area percentage means that even very small objects (such as small animals like cats and dogs) will trigger motion detection. A high zone area percentage means that only very large objects will trigger motion detection. You can adjust this setting per detection zone.

To set up motion detection settings for IP cameras, proceed as follows:

1. Adjust the **Time** slider.
2. Click a detection zone to select it, and then adjust the **Min zone area (%)** slider for that zone.
3. Use the graph to test the settings in the selected detection zone. The horizontal red line indicates the threshold for detection. It moves up if you increase the **Min zone area (%)** setting, and down if you decrease it. The detection level (black line) of the zone has to exceed the threshold to trigger motion detection.

   
4. Repeat from step 2 for other detection zones.
5. Click **Save**.

You can test the settings from the configuration screen: if detection is successful and an alarm occurs, the system highlights the edge of the motion detection zones in red in the configuration screen. You can immediately adjust the settings if necessary.

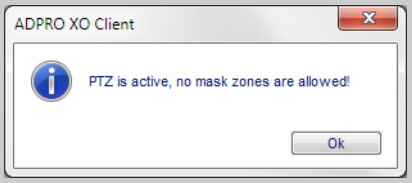


16.3.4 Private Zones (Mask Zones)

Outdoor security cameras may unintentionally look into neighbouring residences. To respect their privacy, you can mask these parts of the picture. You can add up to 3 rectangular private zones. The zones can overlap.

Note

It is not possible to draw private zones if the camera has PTZ enabled. The following message will appear:



To draw detection zones for motion detection, proceed as follows:

1. Under **Drawing Tools**, click the button (second button).
   A yellow striped black rectangle appears in the left upper corner of the image.



2. Adjust the size and position of the rectangle until it masks the required private zone. In the live view, the masked area will be black.



3. Repeat to add more private zones if necessary.
4. Click **Save**.

16.3.5 Sabotage Detection

With sabotage detection enabled, the system generates an alarm if the camera is being tampered with. The sabotage detection feature has been enhanced with the option to reset the alarm manually or automatically. The following actions will result in a sabotage alarm:

- Covering, spray painting the lens
- Changing the position of the camera
- Changing the zoom/focus of the camera image
- Turning off the lights.

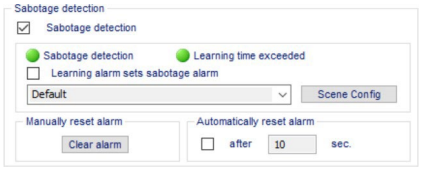
If the system detects sabotage, it triggers the SABOTAGE EVENT alarm on the related camera. For camera 1, this is: 1025 – [REAL] – CAM01 SABOTAGE EVENT. You need to reset this alarm manually.

Note

The CONTRAST EVENT and BAD SCENE alarms from previous versions are no longer triggered; only the SABOTAGE EVENT alarm remains.

To enable sabotage detection, proceed as follows:

1. Select the **Sabotage detection** checkbox.

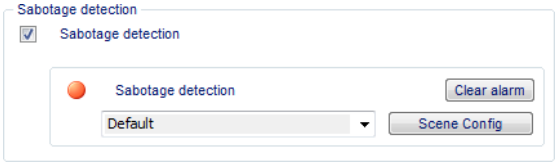


Note

Sabotage detection works by finding lines in the image. A sabotage alarm is triggered when the camera is turned or covered. On turning the camera, the sabotage algorithm learns the new position once again. However, the camera can't detect lines in the image if it turns to a blank wall and the sabotage detection is no longer operational. Select the **Learning alarms sets sabotage alarm** checkbox to trigger the *learning time exceeded* alarm when the sabotage algorithm has not detected lines in the image for a set period.

2. Click **Save**.

When sabotage is detected, the status icon colours red.



If you have to clear the sabotage detection alarm manually, proceed as follows:

- Click **Clear alarm**.

If you have to enable automatic clearing of sabotage detection alarm, proceed as follows:

- Select the **after** checkbox under **Manually reset alarm** and set the number of seconds after which the alarm must get cleared automatically. For example, if you set 60, the alarm is cleared automatically after one minute. The value allowed ranges between 1 and 3600 seconds.

16.3.6 Advanced Settings for Sabotage Detection (Scene Profiles)

You can set up advanced settings for sabotage detection, and save these parameters in a **scene profile**. You can then assign the profile to the desired cameras that have sabotage detection enabled. The parameters are valid for the whole scene (not for individual motion zones).

The default detection settings are suitable for most scenes, and were chosen to provide the best detection while reducing false alarms to the minimum. Honeywell recommends to use the advanced settings only for scenes with specific needs.

16.3.7 Scene Profile Settings

The advanced parameters for sabotage detection are:

- **Sensitivity level**: controls the sensitivity of the sabotage detection.
  - **Increase** sensitivity to detect smaller changes. For example, if you want to detect even very small changes in the camera position. This may lead to more false alarms.
  - **Decrease** sensitivity to prevent false alarms. For example, when a camera switches from day to night mode, the system may trigger the sabotage alarm. To prevent this, decrease the sensitivity.
- **Minimum detection time**: controls the detection of short disturbances. For example, a truck passing in front of the camera may trigger the sabotage alarm. To prevent this, make the minimum detection time longer than the time the truck remains in the scene.

Always test the settings under various conditions to determine the best settings for your particular case.

16.3.8 Default Scene Profile

The table below lists the settings in the default scene profile. You cannot change the default profile.

Parameter	Default value
Sensitivity level	3 (= normal)
Minimum detection time	10 seconds

16.3.9 Creating a Custom Scene Profile

If the default scene profile is not suitable, you can create your own custom scene profile. If need be, you can create different scene profiles for different cameras. Any scene profile that you create is available to all cameras on the XO device that have sabotage detection enabled.

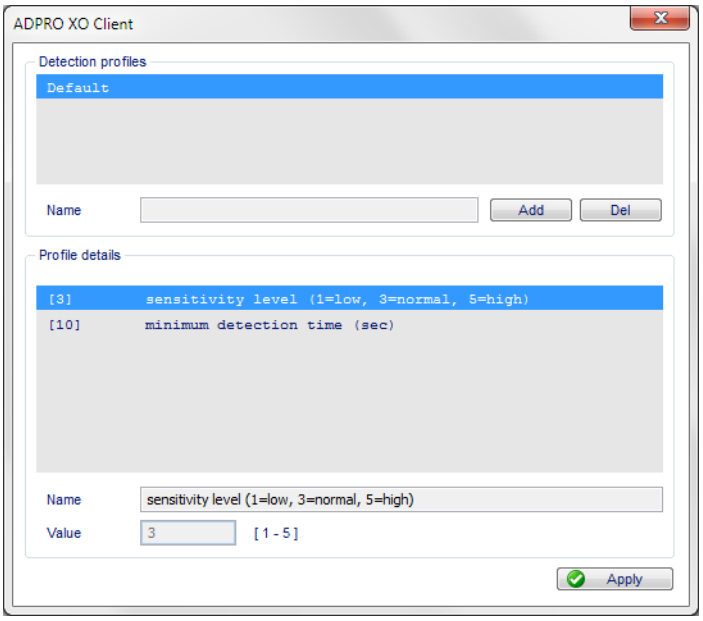
> ***Caution!***
>
> If you assign the same profile to different cameras, make sure to test the settings on all these cameras.

To create a custom scene profile, proceed as follows:

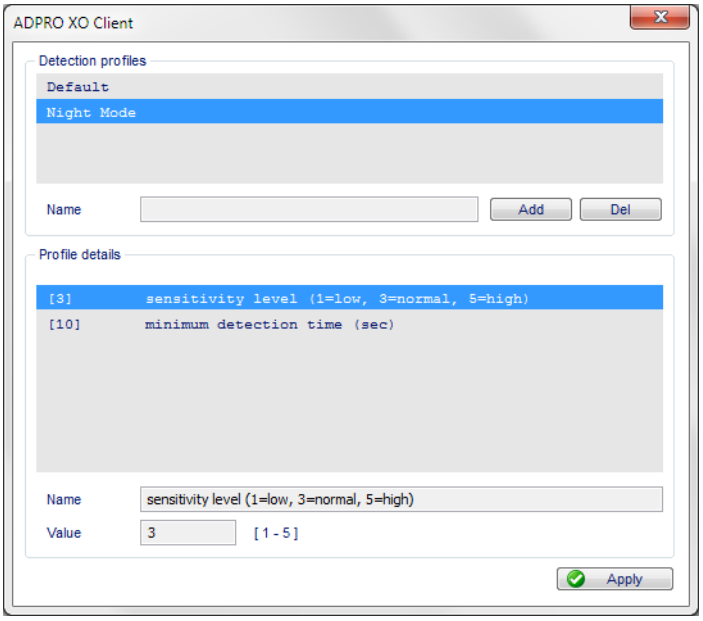
1. From the **Motion, sabotage** window, click the desired camera.



2. Make sure that the **Sabotage detection** checkbox is selected.
3. Click **Scene Config**.



4. In the **Name** box, type a meaningful name for your custom profile.
5. Click **Add**. The system adds a profile with the chosen name and the default settings.



The **Profile details** list shows all the settings, and their current value on the left between brackets.

6. To adjust a setting: under **Profile details**, click the desired setting. The setting's name appears in the **Name** box below the **Profile details** list. (You cannot change the setting's name). The current value appears in the **Value** box. The possible (range of) values appears to the right of the **Value** box.
7. In the **Value** box, type the desired value for the setting. The options are as follows:

Setting	Description
Sensitivity level	Set to any round number from 1 to 5.
Minimum detection time	Set to any value (in seconds) from 10 to 600.

8. Click **Apply** to save the changes, and then close the profile window. The system automatically assigns the new profile to the scene.

9. Click **Save**.
10. Test the settings, and adjust if necessary.

16.3.10 Assigning Existing Scene Profiles to Cameras

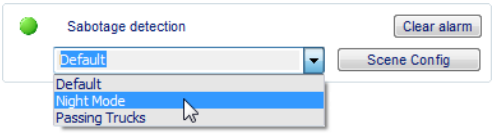
Once you have created a scene profile, you can assign it to any camera on the XO device that has sabotage detection enabled.

To assign an existing profile to a camera, proceed as follows:

1. From the **Motion, sabotage** window, click the desired camera.



2. Make sure that the **Sabotage detection** checkbox is selected.
3. In the box to the left of the **Scene Config** button, select the desired profile from the list.



4. Click **Save**.

16.3.11 Changing an Existing Scene Profile

Note

You cannot change the default scene profile; it is fixed.

To change an existing scene profile, proceed as follows:

1. From the **Motion, sabotage** window, click a camera that uses the desired scene profile.



2. Click **Scene config**.
3. Under **Profile details**, click the desired setting, and adjust its value in the **Value** box.
4. Click **Apply** to save the changes, and then close the profile window.
5. Click **Save**.
6. Test the new settings, and adjust again if necessary.

Caution!

If you assign the same profile to different cameras, make sure to test the settings on all these cameras.

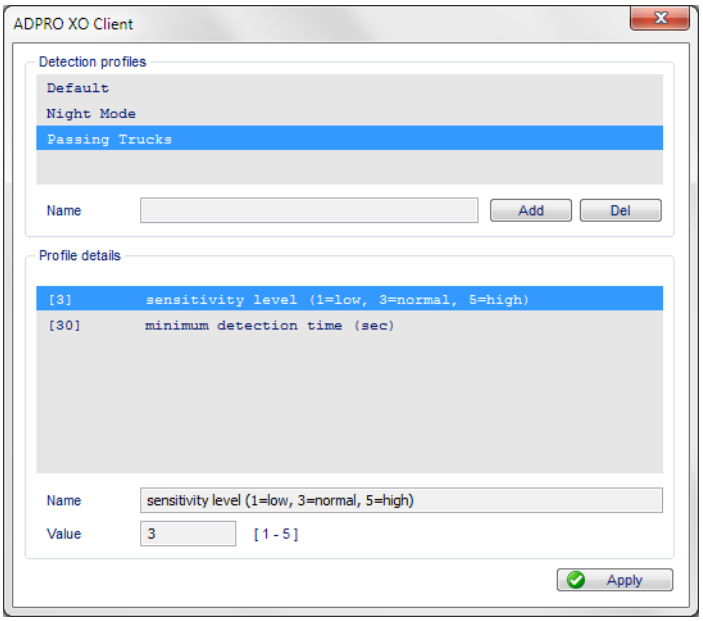
16.3.12 Deleting a Scene Profile

Note

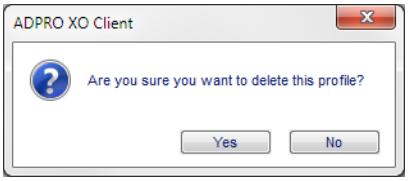
You cannot delete the default scene profile, or a custom scene profile that is still assigned to a camera. Make sure that all cameras on the XO device that use sabotage detection use a different profile (or the default profile).

To delete a scene profile, proceed as follows:

1. From the **Motion, sabotage** window, click any camera that has sabotage detection enabled.
2. Click **Scene Config**.
3. Under **Detection profiles** , click the desired profile.



4. Click **Del**. The following message appears:



5. Click **Yes** to confirm.
6. Click **Apply** to save the changes, and then close the profile window.
7. Click **Save**.

17 PIR Detector Settings

17.1 Prerequisites

To make sure that the XO device can process alarms from the connected PIR detectors correctly, keep the following in mind:

- For correct PIR alarm processing, a minimal PIR firmware version 2.00 is required. Previous firmware versions also work with RS-485 communication, but do not support all features (such as alarm management).
- For physically connecting the PIR detectors, see the Hardware Installation Manual of your XO device (FastTrace 2 Series: 21790; iFT Series: 27817; eFT Series:35450).
- Each PIR detector needs a unique address. For use with the XO device, PIR addresses have to be in the 1–34 range (client version XOa 3.02.0001 or above) or in the 1–32 range (client version below XOa 3.02.0001). The XO device will not discover PIR detectors with addresses outside these ranges. For instructions on setting PIR detector addresses, see the ADPRO PRO E PIR System Setup Manual (26571).
- From firmware version V2.6 onwards, you need a PIR-HLI application license to enable the PIR detectors. Use Xchange2 to install the license on the XO device. For more information, see the Xchange2 user manual (27816).

You use the XO client to:

- Configure the serial port to which the PIR detectors are connected (if you are using an RS-485 bus).
- Configure the IP modules (if you are using IP modules).
- Configure the walk test port for PIR commissioning (iPIR).
- Let the XO device discover the connected PIR detectors.
- Set up alarm behaviour for the PIR alarm inputs.
- Configure double-knock alarms.

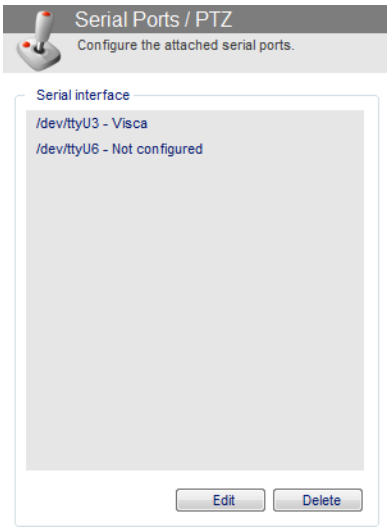
17.2 Configuring the Serial Port

The XO client software automatically detects active serial ports on the XO device. The serial port for the PIR detectors is one of the following:

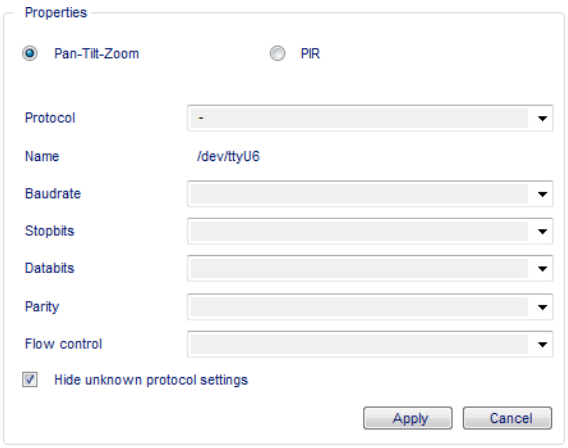
- **/dev/ttyU2** USB port: if you are connecting the PIR detectors using a USB-to-RS-485 distribution unit, a USB-to-serial-port RS-485 converter, or an IFM-485-ST module.
- **/dev/ttyU6** USB port: if you are connecting the PIR detectors directly to the first MIO card of the XO device.
- **/dev/ttyU8** USB port, if you are connecting the PIR detectors directly to the second MIO card of the XO device.

To set up the serial port for the PIR detectors, proceed as follows:

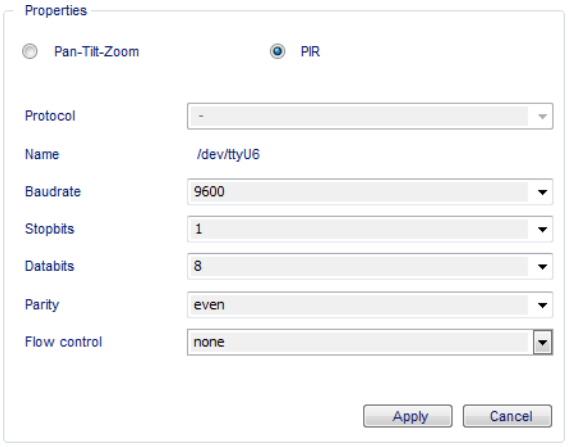
1. Choose **System** > **Connections** > **Serial Ports / PTZ**. The list of active serial ports appears.



2. Select the correct serial port from the list, and then click **Edit**. The following screen appears:

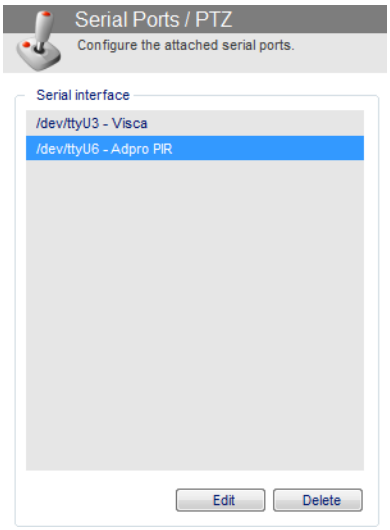


3. Click **PIR**. The system automatically fills in the settings for the serial port.



4. Click **Apply**.

5. Click **Save**.

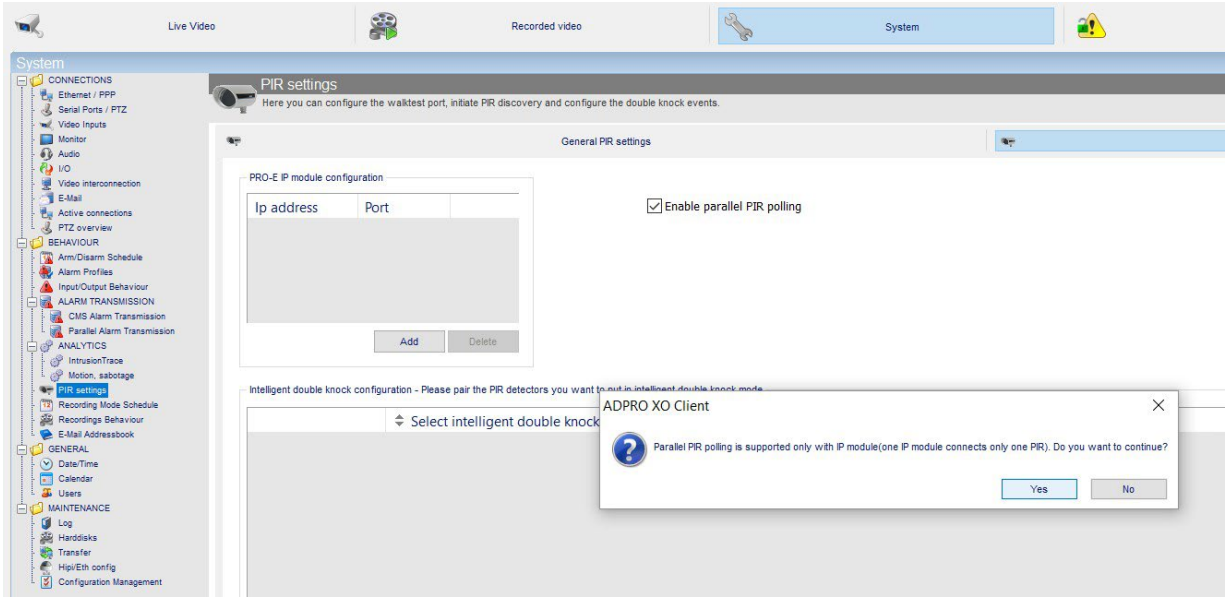


The serial port for the PIR detectors is now listed as **ADPRO PIR**.

17.3 Enable parallel PIR polling

The XO device will do parallel PIR polling if the **Enable parallel PIR polling** setting is enabled. The polling is single-threaded (i.e., one-by-one/sequential) if this option is not enabled. Proceed as follows:

1. Choose **System** > **Behaviour** > **PIR Settings**.
2. Click the **Advanced PIR settings** tab.
3. Select the **Enable parallel PIR polling** checkbox.
4. Click **Yes** in the **Parallel PIR polling is supported only with IP module (one IP module connects only one PIR). Do you want to continue?** dialogbox. Clicking **Yes** selects the **Enable parallel PIR polling** checkbox, and clicking **No** will unselect the checkbox. If you disable parallel PIR polling after enabling it, it goes back to the normal single-threaded mode.



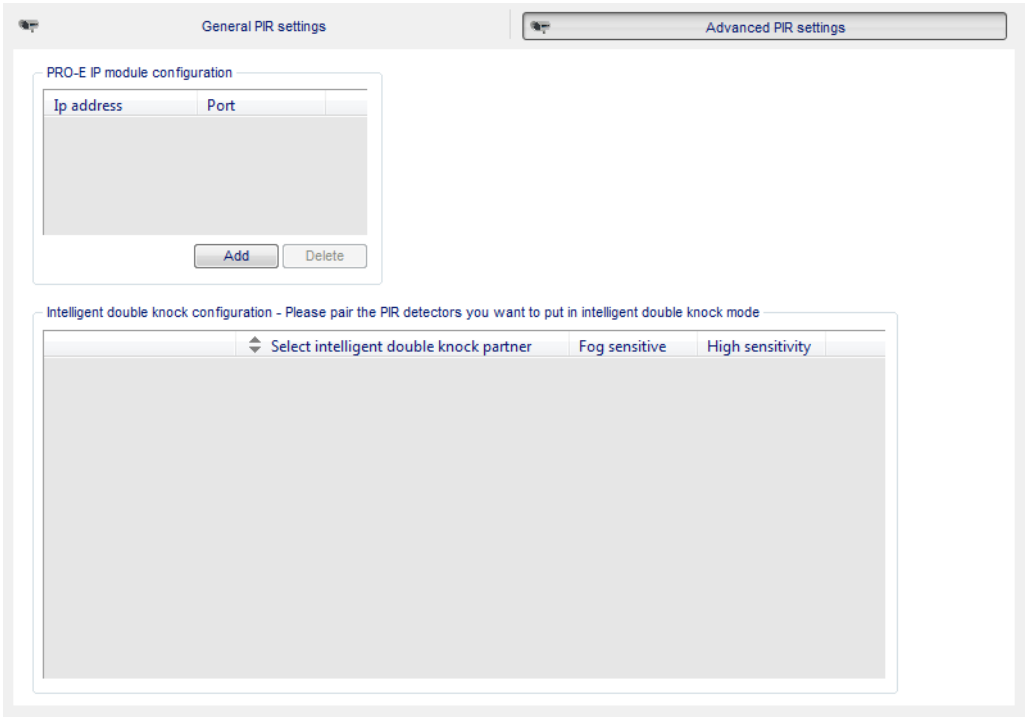
5. Click **Save**.

17.4 Configuring IP Modules

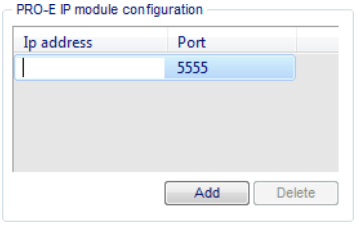
17.4.1 Adding IP Modules

The XO device will only detect the PIR detectors connected via IP modules if you add the IP modules in the client software first. Proceed as follows:

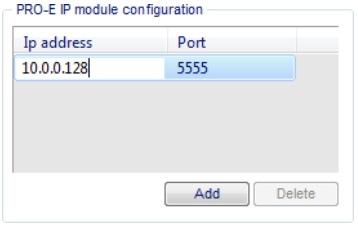
1. Choose **System** > **Behaviour** > **PIR Settings**.
2. Click the **Advanced PIR settings** tab.



3. In the **PRO-E IP module configuration** section, click **Add**.



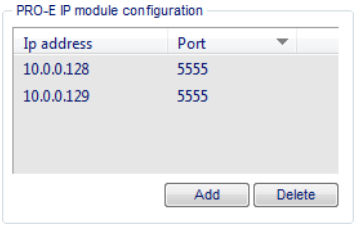
4. In the **Ip address** column, type the IP address of the IP module.



   The system automatically fills in the default walk test port number (5555).

5. To change the walk test port number, click in the **Port** column and type the correct port number.

6. Click **Add** to add more IP modules.



7. Click **Save**.

17.4.2 Deleting IP Modules

To delete an IP module, proceed as follows:

Click the desired IP module in the list, and then click **Delete**.

17.5 Configuring the Walk Test Port

The walk test port is used for the iPIR app, which allows you to configure your PIR settings and visualise PIR detections on a scope on a mobile device. For more information, see the *iPIR User Manual* (27985). The default walk test port to use with iPIR is 5555. The walk test port in the XO client has to correspond with the walk test port in your iPIR app.

To change the walk test port, proceed as follows:

1. Choose **System** > **Behaviour** > **PIR Settings**, and click the **General PIR Settings** tab.
2. In the **Walktest port** box, type the desired walk test port number.



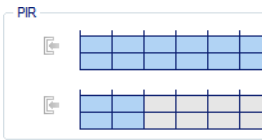
3. Click **Save**.
4. If you are using IP modules, change the walk test port number for the IP modules on the **Advanced PIR Settings** tab.
5. Click **Save**.

> **Note**
> For iPIR to work, you also have to enable Technician access. See *Granting the Technician*.

During PIR commissioning, while the walk test port is in use, the transparent mode is active and the **Transp. Mode** indicator in the PIR settings window is green. In transparent mode, the XO device does not transmit alarms from the PIR detectors to the CMS. This allows for testing and adjusting the PIR detectors before going 'live'.



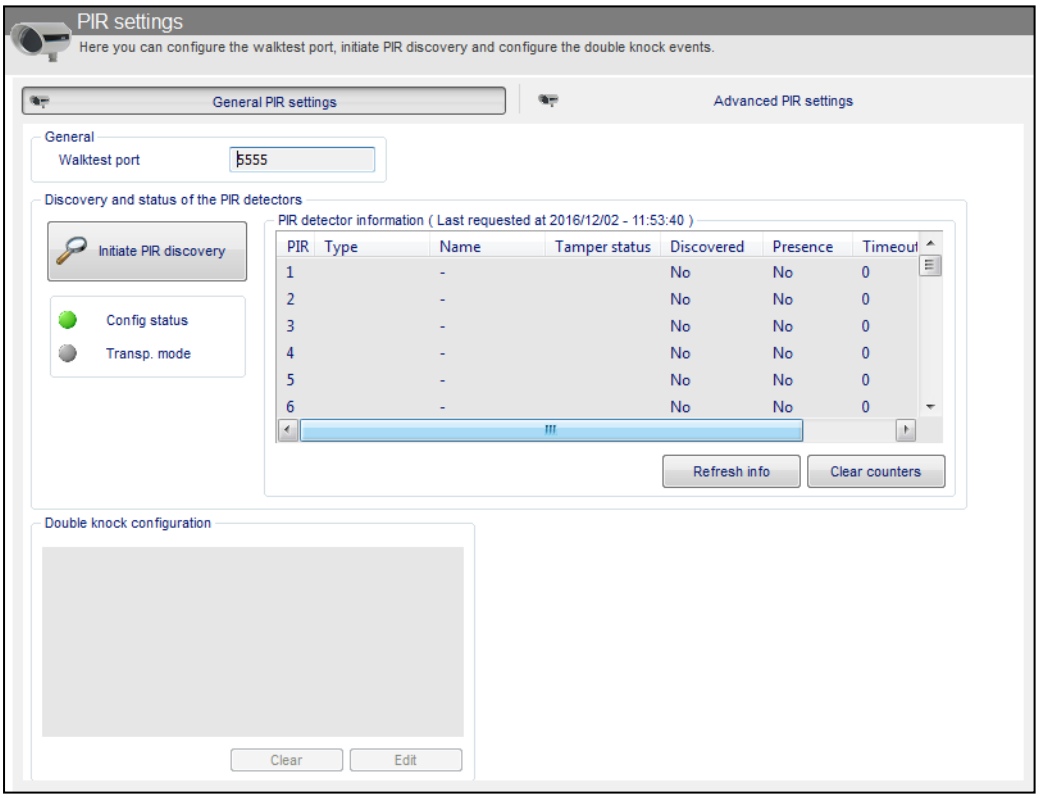
The PIR alarms in the **Status** window remain light blue; they do not change colour:



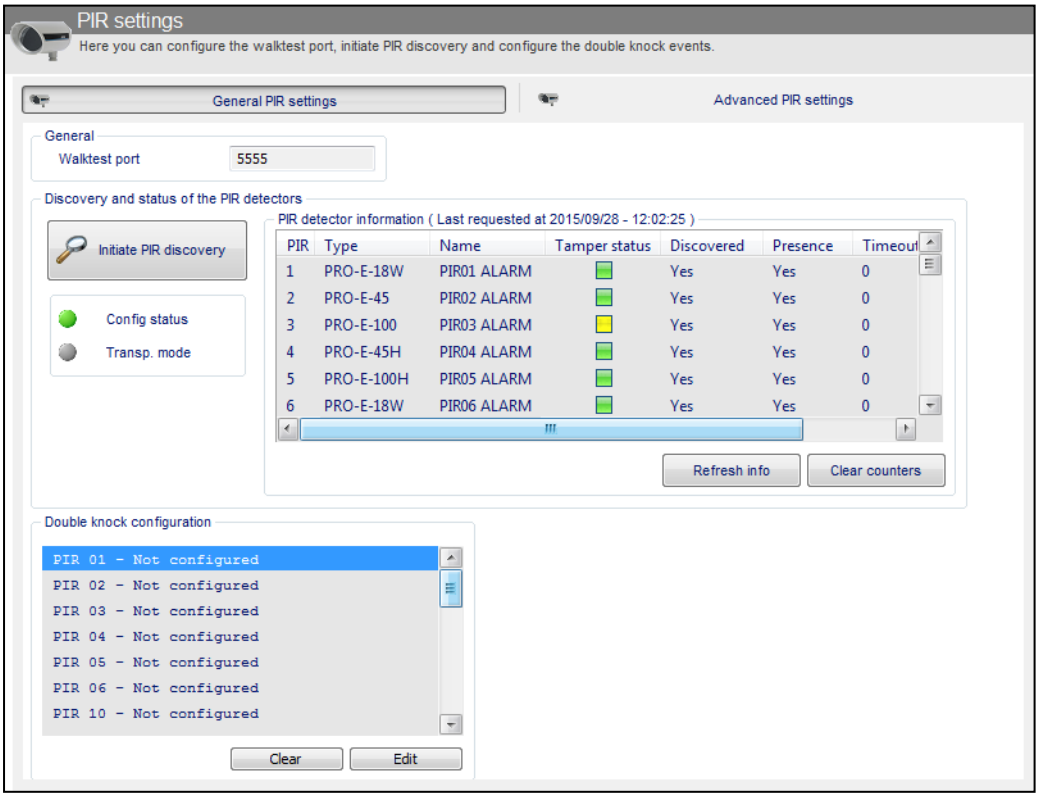
17.6 Initiating the PIR Discovery

To discover the PIR detectors connected to the XO device, proceed as follows:

1. Choose **System** > **Behaviour** > **PIR Settings**, and click the **General PIR Settings** tab.



2. Click **Initiate PIR discovery**. The **PIR detector information** table displays the found PIR detectors:



17.7 PIR Detector Status

Under **Discovery and status of the PIR detectors**, you find a list of connected PIR detectors and their status. If the PIR detectors are operating normally, the **Config status** indicator is green. It turns yellow when there is a problem with the configuration; for example if the serial port is not configured correctly or is disconnected.



The **PIR detector information** table displays the following information:

Item	Description
PIR	The PIR detector's address (1–34).
Type	The PIR detector type. The XO device automatically detects the type. If the XO device cannot detect the type, this column displays **unknown**.
Name	The name of the PIR detector's normal alarm. For more information, see *PIR Alarm Inputs* .
Tamper status	The PIR detector's current tamper alarm status: • (green): tamper alarm inactive. • (yellow): tamper alarm active. Hover the mouse over the icon for detailed information:
Discovered	The PIR detector's current discovery status: • **Yes**: the XO device discovered a PIR detector with this address. • **No**: the XO device did not discover a PIR detector with this address.
Presence	The PIR detector's current presence status: • **Yes**: the PIR detector is present. • **No**: the PIR detector was discovered during the last discovery, but is currently not present.
Time outs	The number of timeouts counted.
Pkt errors	The number of packet errors counted.
IF-type	The type of interface between the PIR detector and the XO device. • **ETH**: connected via an IP module. • **SER**: connected via a MIO card or to a USB port using an RS-485-to-serial converter.

To update the information in the PIR detection list:

- Click **Refresh info** to search for connected PIR detectors again.
- Click **Clear counters** to reset the numbers in the **Time outs** and **Pkt Errors** columns.

17.8 PIR Alarm Inputs

From firmware version V2.06.0020, the system offers detailed PIR alarm inputs for ADPRO PIR detectors. The available alarm inputs depend on the type of detector. The XO device automatically detects the type of ADPRO PIR detector when you use the PIR discovery function.

- Presence: the system triggers this input if the PIR detector has been discovered before, but is currently not present.
- Alarm: the normal PIR detector alarm.

- Tamper: the tamper alarm.
- Double knock: the double-knock alarm.
- Detail 1–3: for details, see the table further below.
- Creep zone: the creep zone alarm (for PRO E models, only available from firmware version XOa 3.02). For each PIR detector (1–34), up to 8 alarms are available, listed in the table below.

	Presence	Alarm	Tamper	Double knock	Detail 1	Detail 2	Detail 3	Creep zone
PIR 1	I0512	I0513	I0514	I0515	I0516	I0517	I0518	I0519
PIR 2	I0520	I0521	I0522	I0523	I0524	I0525	I0526	I0527
PIR 3	I0528	I0529	I0530	I0531	I0532	I0533	I0534	I0535
PIR 4	I0536	I0537	I0538	I0539	I0540	I0541	I0542	I0543
PIR 5	I0544	I0545	I0546	I0547	I0548	I0549	I0550	I0551
PIR 6	I0552	I0553	I0554	I0555	I0556	I0557	I0558	I0559
PIR 7	I0560	I0561	I0562	I0563	I0564	I0565	I0566	I0567
PIR 8	I0568	I0569	I0570	I0571	I0572	I0573	I0574	I0575
PIR 9	I0576	I0577	I0578	I0579	I0580	I0581	I0582	I0583
PIR 10	I0584	I0585	I0586	I0587	I0588	I0589	I0590	I0591
PIR 11	I0592	I0593	I0594	I0595	I0596	I0597	I0598	I0599
PIR 12	I0600	I0601	I0602	I0603	I0604	I0605	I0606	I0607
PIR 13	I0608	I0609	I0610	I0611	I0612	I0613	I0614	I0615
PIR 14	I0616	I0617	I0618	I0619	I0620	I0621	I0622	I0623
PIR 15	I0624	I0625	I0626	I0627	I0628	I0629	I0630	I0631
PIR 16	I0632	I0633	I0634	I0635	I0636	I0637	I0638	I0639
PIR 17	I0640	I0641	I0642	I0643	I0644	I0645	I0646	I0647
PIR 18	I0648	I0649	I0650	I0651	I0652	I0653	I0654	I0655
PIR 19	I0656	I0657	I0658	I0659	I0660	I0661	I0662	I0663
PIR 20	I0664	I0665	I0666	I0667	I0668	I0669	I0670	I0671
PIR 21	I0672	I0673	I0674	I0675	I0676	I0677	I0678	I0679
PIR 22	I0680	I0681	I0682	I0683	I0684	I0685	I0686	I0687
PIR 23	I0688	I0689	I0690	I0691	I0692	I0693	I0694	I0695
PIR 24	I0696	I0697	I0698	I0699	I0700	I0701	I0702	I0703
PIR 25	I0704	I0705	I0706	I0707	I0708	I0709	I0710	I0711
PIR 26	I0712	I0713	I0714	I0715	I0716	I0717	I0718	I0719
PIR 27	I0720	I0721	I0722	I0723	I0724	I0725	I0726	I0727
PIR 28	I0728	I0729	I0730	I0731	I0732	I0733	I0734	I0735
PIR 29	I0736	I0737	I0738	I0739	I0740	I0741	I0742	I0743
PIR 30	I0744	I0745	I0746	I0747	I0748	I0749	I0750	I0751
PIR 31	I0752	I0753	I0754	I0755	I0756	I0757	I0758	I0759
PIR 32	I0760	I0761	I0762	I0763	I0764	I0765	I0766	I0767
PIR 33	I0768	I0769	I0770	I0771	I0772	I0773	I0774	I0775
PIR 34	I0776	I0777	I0778	I0779	I0780	I0781	I0782	I0783

The detail alarms depend on the type of detector:

Detector type	Detail 1 (alarm type)	Detail 2 (alarm type)	Detail 3 (alarm type)
PRO-18 / PRO E-18	IR (infrared)	–	–
PRO-18H / PRO E-18H			
PRO-18W / PRO E-18W			
PRO-18WH / PRO E-18WH			
PRO-18WIS*			
PRO-30 / PRO E-30			
PRO-40 / PRO E-40			
PRO-45 / PRO E-45			
PRO-45H / PRO E-45H			
PRO-45IS*			
PRO-45Z			
PRO-51*			
PRO-45D / PRO E-45D*	Right	Left	–
PRO-45DH / PRO E-45DH*			
PRO-100 / PRO E-100	Short range	Medium range	Long range
PRO-100H / PRO E-100H			
PRO-100HIS*			
PRO-250H			
PRO E-400H			
PRO-85	Left	Centre	Right
PRO-85H			

(*) Supported in firmware version XOa 3.02 and above.

Note

The PRO-50 and PRO E-50 models are no longer supported in firmware version XOa 3.02 and above (replaced by PRO-51).

By default, all PIR alarm inputs use the NORMAL EVENT alarm profile. You can assign a different alarm profile if necessary. For instructions on modifying the alarm behaviour of inputs, see *Input/Output Behaviour*.

17.9 Double-Knock Configurations

To reduce the number of false alarms from a PIR detector, you can use a double-knock configuration. In a double-knock configuration, the double-knock alarm is only triggered when another trigger occurs simultaneously.

- Typically, you combine the PIR detector with a camera for analytics. For details, see *Double-Knock with Camera*.
- For PRO E models only: from firmware version XOa 3.02, you can easily combine the alarms from two PIR detectors. Furthermore, this configuration offers intelligent options for high sensitivity and fog detectors. For details, see *Intelligent Double-Knock between PRO E PIR Detectors*.

You can even create a triple-knock configuration by combining both double-knock methods (two PRO E PIR detectors and a camera).

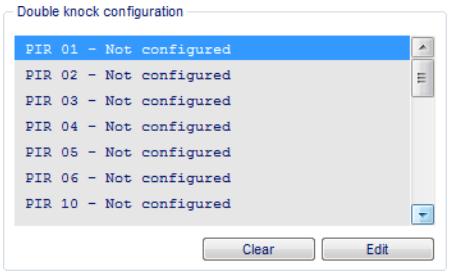
17.10 Double-Knock with Camera

The typical double-knock configuration combines a PIR alarm with a camera intrusion alarm to trigger the PIR detector's double-knock event. (You can, of course, combine the PIR alarm with any other input.)

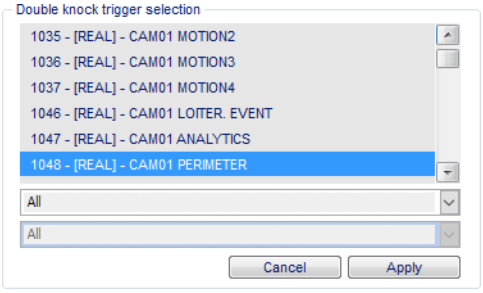
You need to set up the correct alarm profile for the PIR detector's double-knock event so that it transmits the alarm, and you need to set up the individual PIR and camera events so that they do not transmit alarms.

To set up a PIR detector in a double-knock configuration with a camera, proceed as follows:

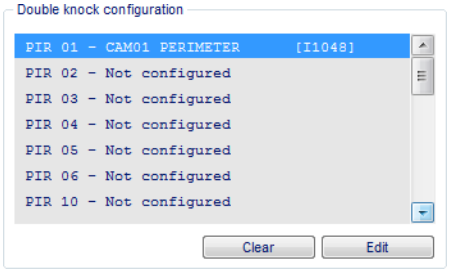
1. Choose **System** > **Behaviour** > **PIR Settings**. The **Double knock configuration** list displays the available PIR detectors.



2. Select the PIR detector that you want to configure, and then click **Edit**. The list of available triggers appears.
3. If necessary, filter the trigger list (for example on camera inputs), and then click the desired trigger. In the example below, the IntrusionTrace alarm on camera 01 is selected.

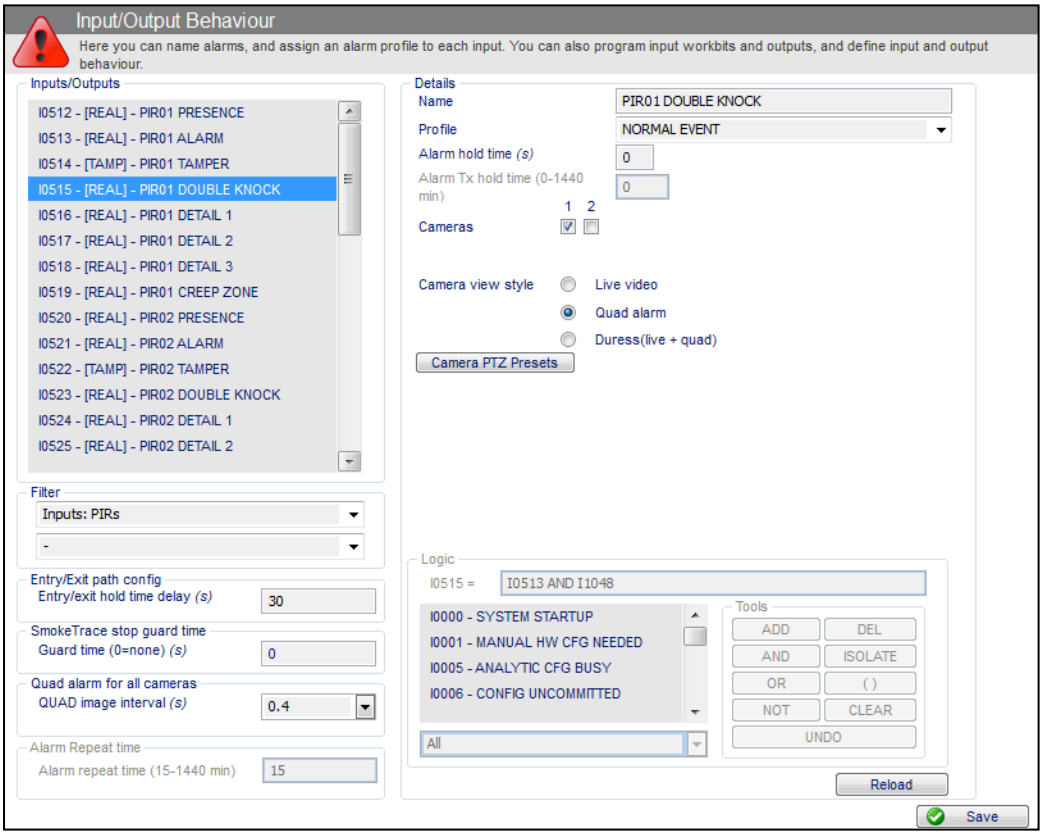


4. Click **Apply**. The selected trigger appears in the **Double knock configuration** list.



5. Click **Save** to save the PIR settings.
   Now you can set up the desired alarm profile for the double-knock input.
6. Click **Input/Output Behaviour**.

7. In the **Inputs/Outputs** list, select the PIR detector's double-knock input (I0515 in the example). Use the **Inputs: PIRs** filter to reduce the list of inputs/outputs.



> **Note**
>
> In the example above, the following logical function appears in the **Logic** section (not editable):
> I0515 = I0513 AND I1048
> This means that the double-knock input (I0515) is activated if the normal PIR alarm of PIR01 (I0513) AND the IntrusionTrace alarm of camera 1 (I1048) are active.

8. In the **Profile** box, select the desired alarm profile for the double-knock alarm.
   Now you can set up the individual inputs so that they do not transmit alarms.
9. Select the normal PIR alarm (I0513 in the example) and set the alarm profile to SILENT MESSAGE.
10. Select each of the PIR detail alarms (including the creep zone alarm if available; I0516–I0519 in the example), and set the alarm profile to SILENT MESSAGE.
11. Select the camera event (I1048 in the example) and set the alarm profile to SILENT MESSAGE.
12. Click **Save**.

17.11 Intelligent Double-Knock between PRO E PIR Detectors

When you pair PRO E PIR detectors in an intelligent double-knock configuration, the system activates the normal PIR alarm and one detail alarm of one of the PIR detectors. The system automatically uses the inputs that are the most precise for moving a PTZ camera to the area of interest. To determine the most precise input, the system ranks the inputs as follows (if available on the PIR detector):

1. Creep zone alarm (most precise)
2. Short range alarm
3. Medium range alarm
4. Long range alarm (least precise).

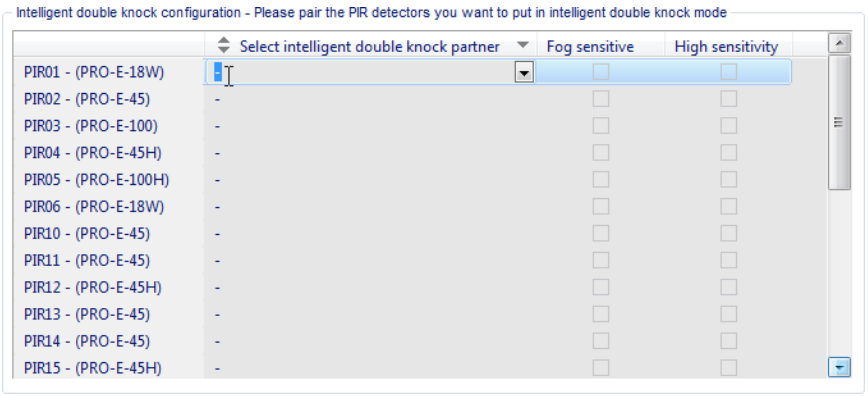
When both long-range alarms are active, the system chooses the first PIR detector in the pair. This is the PIR detector that is in the left column in the intelligent double-knock setup table (for details, see further below).

Furthermore, when you have paired PRO E PIR detectors, you can choose to let the pair operate in fog sensitive mode and/or in high sensitivity mode.

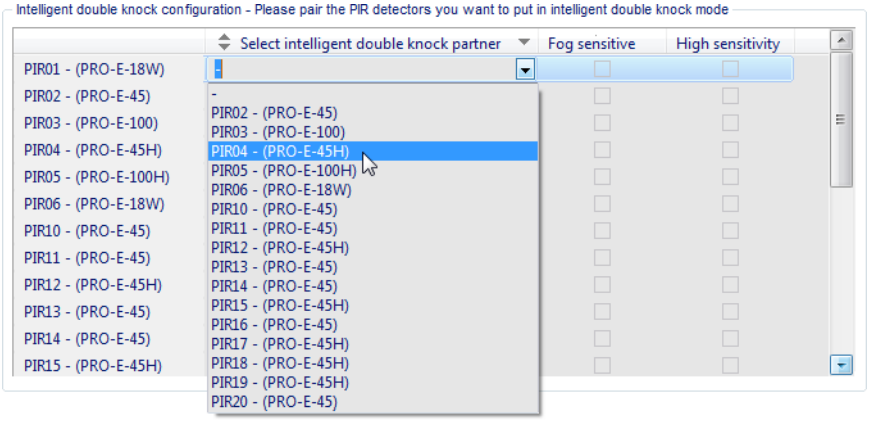
- In **fog sensitive** mode, you can use the input of a fog detector to automatically adjust the sensitivity of the PIR detectors. When the fog detection input is active, the system turns off the ATD (adaptive threshold determination) on both PIR detectors, and sets the sensitivity of both PIR detectors to the maximum. Under fog conditions, both PIR detectors generate their own normal alarms and their own detail alarms (double-knock disabled).
- In **high sensitivity** mode, the system uses not only the alarm status of the PIR detector for double knock, but also the warning indication of the PIR detector (if it exists on the specific PIR type). This automatically results in a higher detection sensitivity.

To pair PIR detectors in an intelligent double-knock configuration, proceed as follows:

1. Choose **System** > **Behaviour** > **PIR Settings**, and click the **Advanced PIR settings** tab.
2. In the **Intelligent double knock configuration** section, click in the **Select intelligent double knock partner** column next to the first PIR detector in the pair.



3. Click the button, and then click the desired second PIR detector for the pair.



4. If you want to use the pair in fog sensitive mode, select the **Fog sensitive** checkbox.

5. If you want to use the pair in high sensitivity mode, select the **High sensitivity** checkbox.



6. Click **Save**.
7. If you have selected **Fog sensitive**, set up the fog detection input.

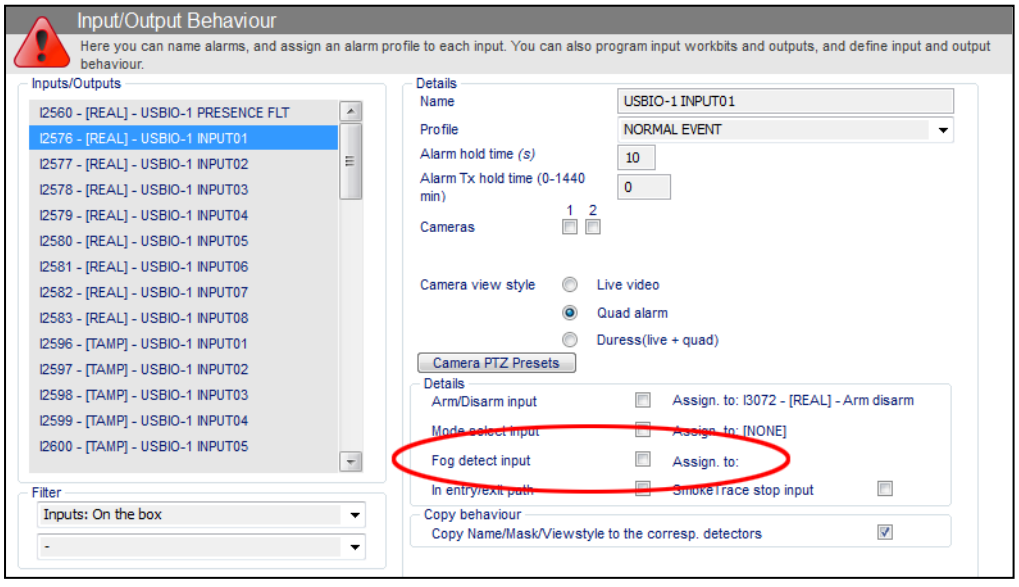
17.12 Setting up the Fog Detection Input

Fog sensitive detection only works if you set up a fog detection input. The following input types are suitable for the fog detection input:

- The inputs on the MIO/EIO cards or on the Net I/O units.
- The virtual inputs from an S3100 panel.
- Input workbits.

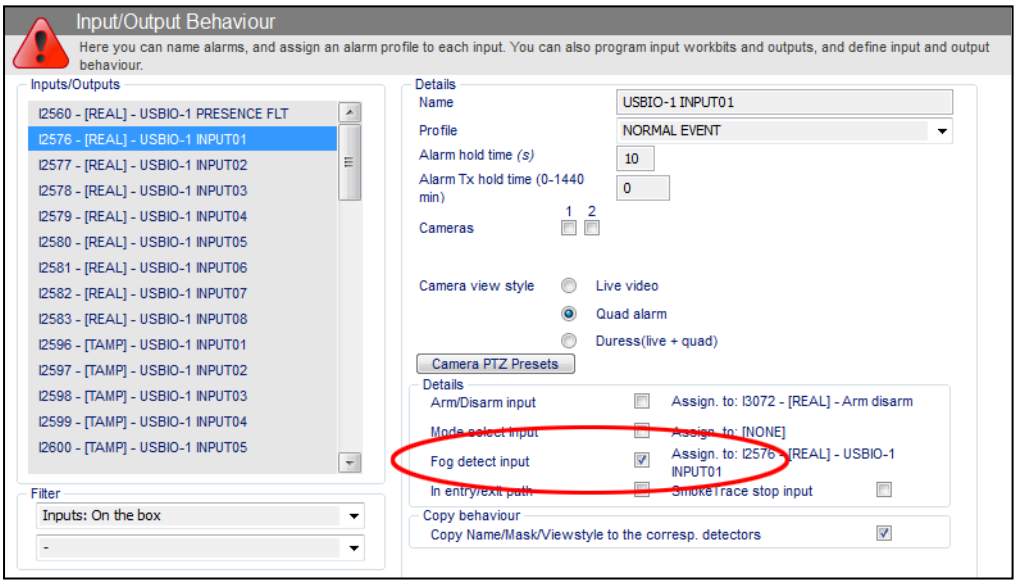
To set up the fog detection input for intelligent double knock, proceed as follows:

1. Choose **System** > **Behaviour** > **Input/Output Behaviour**.
2. Select the correct input in the **Inputs/Outputs** list.
   The system displays the number and name of the input that is currently assigned as fog detection input at the right side of the **Fog detect input** checkbox. If no input is assigned, nothing is displayed.



> ***Caution!***
>
> There can only be one input for the fog detection input. If there already is an input assigned, and you assign to a new input, then the system automatically clears the **Fog detect input** checkbox of the previously assigned input.

3. To use the selected input as a fog detection input, select the **Fog detect input** checkbox.

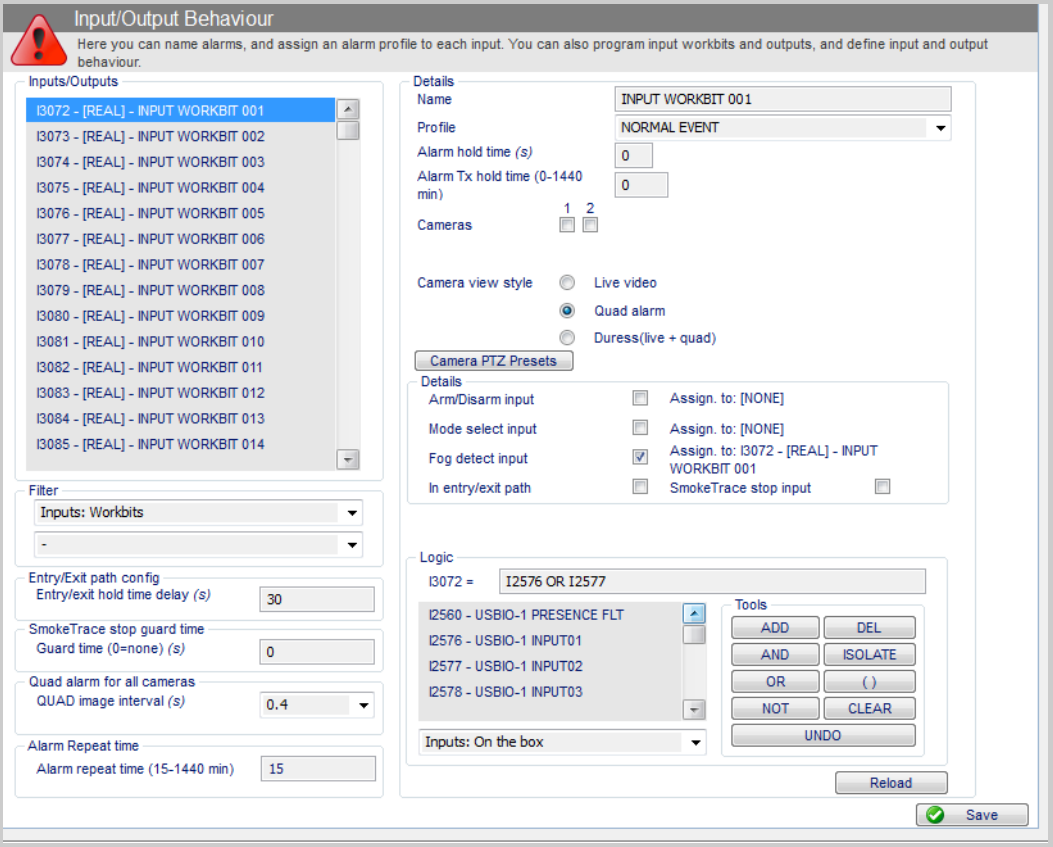


The input number and name appear to the right of the checkbox.

4. Modify any other settings as necessary. For details on setting up inputs, see *Alarm Input Behaviour* .
5. Click **Save**.

Note

You can only use one input as fog detection input for intelligent double knock. However, if your site uses more than one fog detector, you can combine their inputs via a logical function in a workbit, and then set the workbit as the fog detection input for intelligent double knock. The example below shows the combination of two fog detectors (on inputs 1 and 2 of the MIO card) in workbit 001.



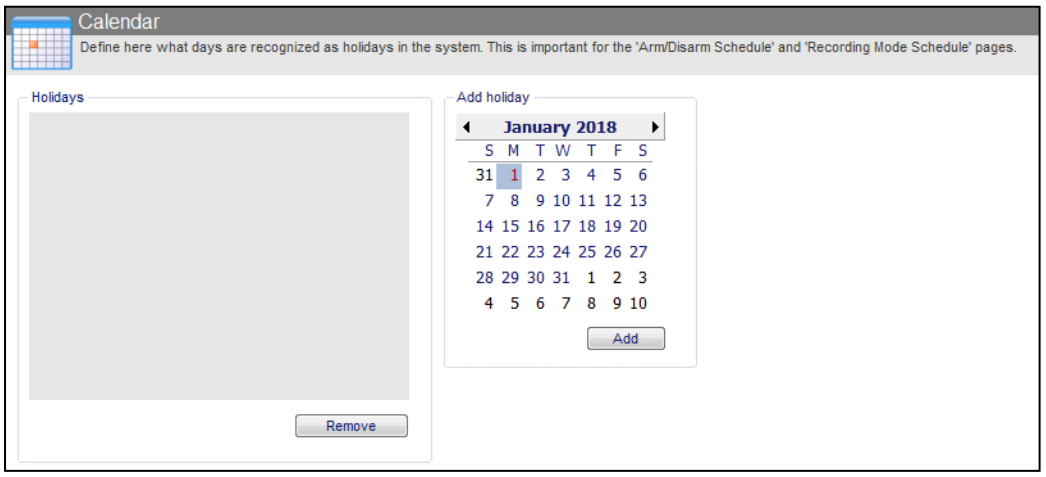
18 Calendar

The calendar contains the dates of the holidays. The holidays are exceptions to the regular weekly schedules (Monday–Sunday), allowing you to define the correct behaviour of the system on these days. The system uses the holidays for:

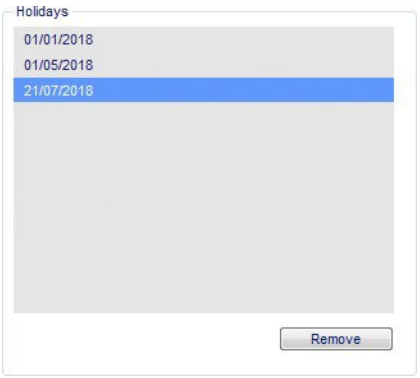
- Recording: in the recording mode schedule and in the individual recording conditions.
- Arming/disarming the system: in the arm/disarm schedule.

To define the holidays in the calendar, proceed as follows:

1. Choose **System** > **General** > **Calendar**.



2. To set a date as a holiday, select the date in the **Add holiday** box, and then click **Add**.
   The holiday appears in **Holidays** list.



3. Repeat for each holiday.
4. To remove a day, click the date in the **Holidays** list, and then click **Remove**.
5. Click **Save**.

Note

Honeywell recommends cleaning up the holiday list once per year and deleting holidays that have passed. Although this is not mandatory, it will help you keep an overview.

19 Users

19.1 About Users

The following user types exist, each with different access rights:

- **Administrator**: has full access rights.
- **User**: has specific rights, adjustable per user.
- **Technician**: has specific rights, adjustable per user. Technicians can only log on if an Administrator or another user has granted them access. Only the Technician user can enable/disable the Telnet connection, access cameras remotely, and access the hardware configuration tool for setting up the XO I/O Interface USB modules.

Caution!

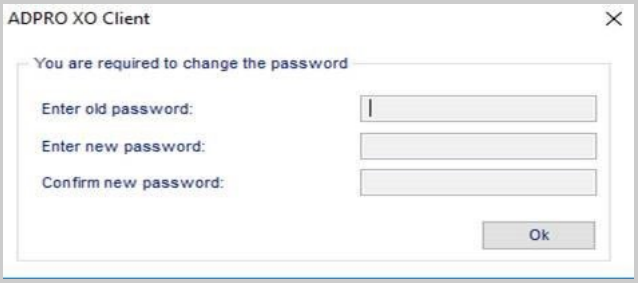
The hardware configuration tool is not accessible by default. The Webserver which is disabled by default must be enabled before accessing the hardware configuration tool. It is recommended to disable the webserver after use for security reasons.

You can create up to 32 users. The following default users are pre-defined:

User ID	Username	Password	User type
0	Administrator	666777	Administrator
1	Administrator2	666777	Administrator
15	Technician	666777	Technician

Note

The default XO password must be changed on initial login while increased password security will be enforced. The new password must have an alphanumeric combination with at least 1 upper case letter, 1 lower case letter, and 1 digit and must be 8 to 15 characters in length.



In versions below XOa 3.00, it was possible to have two or more users with the same username (for example Administrator). It was also possible to have usernames that contain only digits.

As of version XOa 3.00, usernames have to be alphanumeric (= contain at least one letter), and each username has to be unique. Usernames and passwords are case-sensitive. When you upgrade from a version below XOa 3.00, the system will automatically change existing usernames if necessary. If you want to prevent automatic changes to the usernames, you have to check and change the usernames yourself before upgrading.

19.2 About Strong Passwords

To increase security, you can enforce the use of strong passwords. Strong passwords have to meet the following minimum requirements:

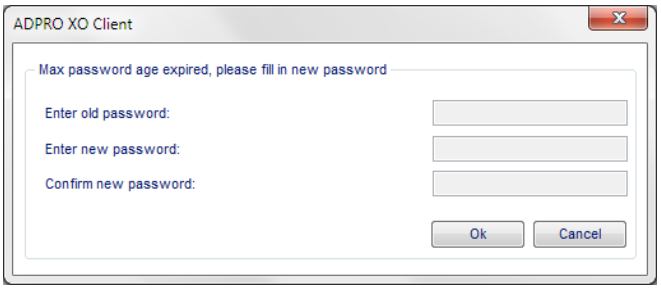
- The password has to contain at least 8 characters.
- The password has to contain at least 1 uppercase letter and at least 1 lowercase letter.

- The password has to contain at least 1 digit.

Examples of strong passwords are:

- Tmus001cl
- 12rtSV5km
- aiGP5rsLZa89

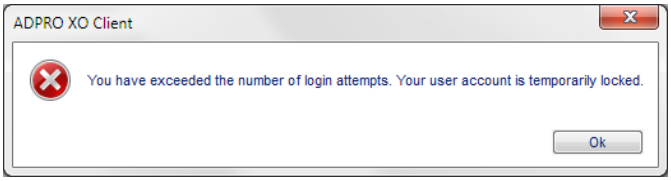
Furthermore, you can set an expiry time (in days) for the password. When the password has expired, the following message appears each time the user logs on to the XO client, until the user changes the password:



Caution!

The expiry time feature is only an incentive for the users to change their password. The users can click **Cancel** to continue with their old password.

Finally, you can limit the number of retries to log on. When the user has reached the maximum number of retries, the system temporarily blocks the user account. You specify how long (in seconds) the user account is blocked. The following message appears when a user is temporarily blocked:



The default values of strong passwords are:

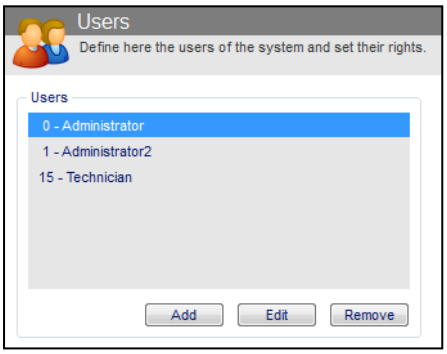
Setting	Unit	Range	Default value
Maximum password age	Days	0–120	0 (= no maximum age, password remains valid indefinitely)
No of invalid login attempts	–	0–10	3
No of seconds user is blocked	Seconds	0–3600	60

19.3 Adding New Users

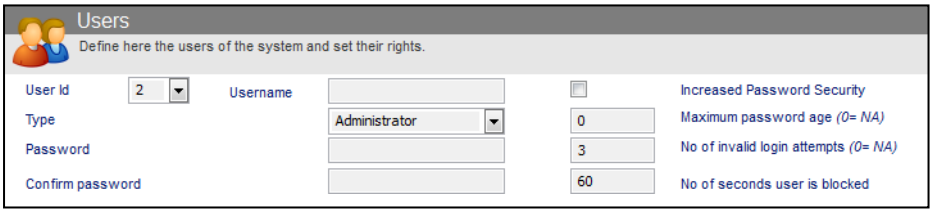
Only Administrator users can add or delete users.

To add a user, proceed as follows:

1. Choose **System** > **General** > **Users**.



2. Click **Add**.



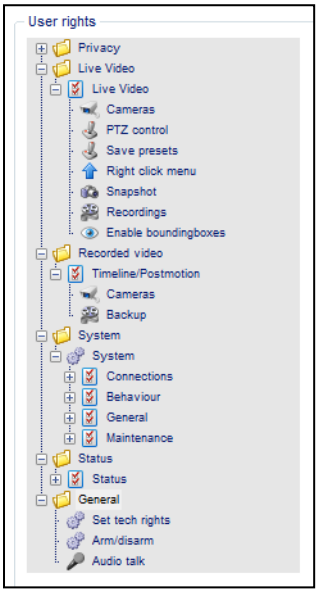
3. Provide the following information:

Item	Description
User Id	Select a user ID (2–31). The system fills in the next free user ID automatically. Numbers 0 and 15 are reserved.
Username	Type a username (max. 20 characters). The username has to be unique and contain at least one letter.
Type	Select the desired user type: **Administrator**, **User**, or **Technician**.
Increased password security	Select the checkbox if you want to use strong passwords, password expiry, and/or restriction of logon attempts for this user.
Maximum password age	Type the number of days (0–120) after which the password expires. Type **0** if you do not want the password to expire. This option is only active if you select the **Increased password security** box.
No of invalid login attempts	Type the number of times (0–10) a user can enter an incorrect username/password before the system blocks the user. Type **0** if you do not want to restrict the number of logon attempts. This option is only active if you select the **Increased password security** box.
No of seconds user is blocked	Type the number of seconds (0–3600) that a user will be blocked. This option is only active if you select the **Increased password security** box.
Password	Type a password for the user.
Confirm password	Type the password again.

4. If you have selected user type **User** or **Technician**, you have to set the access rights. By default, all rights are selected. For details, see *User Rights* .
5. Click **Apply**.
6. Click **Save**.

19.4 User Rights

For users of type User or Technician, you need to specify the rights of the individual user. If you select one of these user types, the list of access rights appears:



Note

If you want to select all access rights, click **Set all**.

If you want to deselect all access rights, click **Clear all**. All options will be cleared, but the user itself will not be deleted. This user still has access to the **About** window to consult the system information.

19.4.1 Pixelation

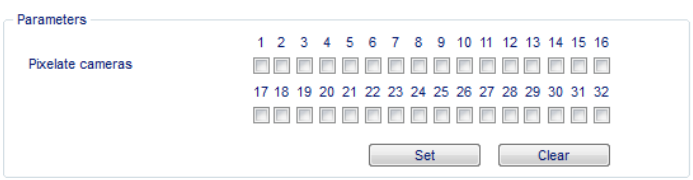
You can specify whether a user is allowed to change the pixelation settings. Furthermore, you can specify for each user which camera images will be pixelated for them (according to the pixelation settings for that camera). This allows you to permit specific users to always see normal images of specific cameras, even if pixelation is set in the camera settings.

To specify the pixelation settings for a user, proceed as follows:

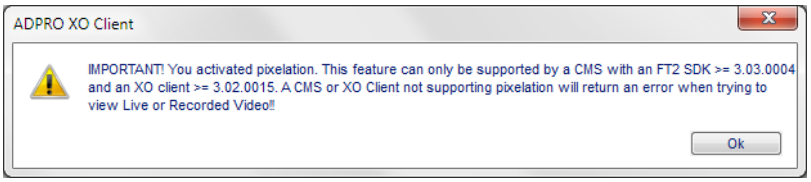
1. In the list of access rights, choose **Privacy** > **Pixelation** > **Adjust settings**.



2. Click **Allow** or **Deny** to define if the user is allowed to change the pixelation settings on the cameras.
3. To define which camera images will be pixelated for the user, click **Cameras**. By default, none of the cameras are selected.



4. Select the checkboxes for the cameras that have to be pixelated. You can click **Set** to select all cameras, and then clear just the few cameras that can remain unpixelated.
5. Click **Apply**. The following message appears:



6. Click **OK** to close the message box.
7. Click **Save**.

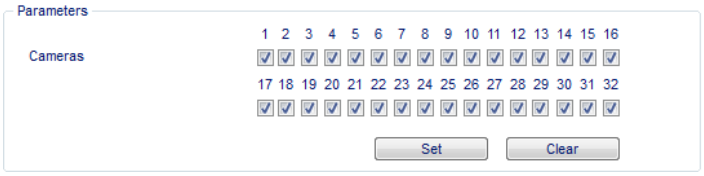
19.4.2 Live Video

To define whether the specific user can access the **Live Video** window in the XO client, proceed as follows:

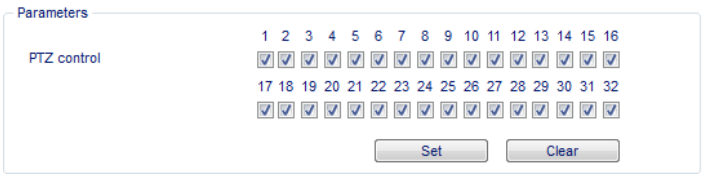
1. In the list of access rights, choose **Live Video** > **Live Video**.



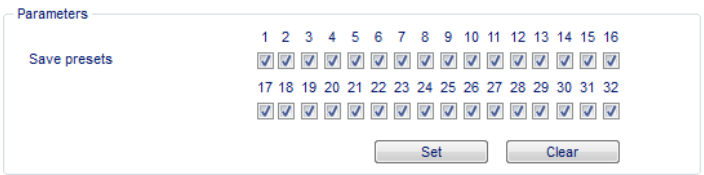
2. Click **Deny** if you do not want the user to access the **Live Video** window. In this case, you can skip all following steps. If you allow the user to access the **Live Video** window, continue with the next step.
3. To define which cameras the user can view, click **Cameras**. By default all cameras are selected.



4. Clear the checkboxes for the cameras that this user is not allowed to view.
   You can click **Clear** to clear all the checkboxes, and then select just the few cameras that are allowed.
5. To define for which cameras the user can control PTZ, click **PTZ control**.



6. Clear the checkboxes for the cameras for which this user is not allowed to use PTZ control.
   You can click **Clear** to clear all the checkboxes, and then select just the few cameras that are allowed.
7. To define for which cameras the user is allowed to save PTZ presets, click **Save presets**.



8. Clear the checkboxes for the cameras for which this user is not allowed to save PTZ presets.
   You can click **Clear** to clear all the checkboxes, and then select just the few cameras that are allowed.

9. Allow or deny access to the following functions:
   - **Right click menu**: right-click to change the resolution or to de-warp 360° camera images in the live view.
   - **Snapshot**: take a snapshot of the video that is available in the live view.
   - **Recordings**: record the video images in the live view.
   - **Enable bounding boxes**: switch bounding boxes on or off in the live view.
10. When finished setting the user rights, click **Apply**.
11. Click **Save**.

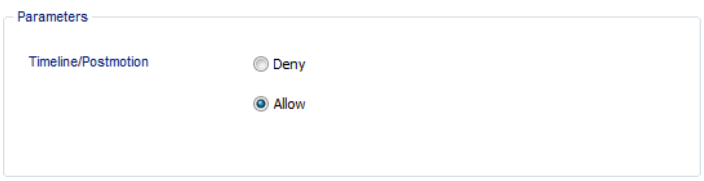
Note

All other functions in the **Live Video** window are by default accessible to every user. For activating outputs, see *Status*. For audio, see *General*.

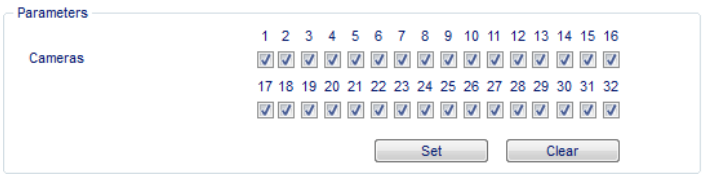
19.4.3 Recorded Video

To define whether the specific user can watch recordings via **Timeline/Postmotion** and back up recordings, proceed as follows:

1. In the list of access rights, choose **Recorded Video** > **Timeline/Postmotion**.



2. Click **Deny** if you do not want the user to access the **Recorded Video** window. In this case, you can skip all following steps. If you allow the user to access the **Recorded Video** window, continue with the next step.
3. To define which cameras the user can access, click **Cameras**. By default all cameras are selected.



4. Clear the checkboxes for the cameras that this user is not allowed to view.
   You can click **Clear** to clear all the checkboxes, and then select just the few cameras that are allowed.
5. To allow or deny backup, click **Backup**, and then click **Allow** or **Deny**.
6. Click **Apply**.
7. Click **Save**.

Note

If the user cannot watch recordings, the user also cannot backup any recordings.

19.4.4 System

To define whether the specific user has access to the system settings, proceed as follows:

1. In the list of access rights, choose **System** > **System**.
2. Click **Deny** if you do not want the user to access the **System** window. In this case, you can skip all following steps. If you allow the user to access the **System** window, continue with the next step.

3. Define the system settings to which the user has access. The user rights are grouped according to the main menu groups in the system settings pages:
   - Connections
     - Ethernet
     - Serial
     - Video Inputs
     - Monitor
     - Audio
     - I/O
     - PresidiumHLI (obsolete)
     - Video interconnection
     - E-Mail
     - Active connections
   - Behaviour
     - Arm/Disarm Schedule
     - Alarm Profiles
     - Input/Output Behaviour
     - CMS Alarm Transmission
     - Analytics
     - If you allow access to the Analytics settings, then also define for which cameras.
     - PIR
     - Recording
     - E-Mail Addressbook
   - General
     - Date/Time
     - Calendar
     - Users (edit own user profile only).
   - Maintenance
     - Log
     - Transfer
     - Harddisks
     - Hipi/Eth config
     - Configuration Management

4. Select or clear the desired checkboxes.
5. Click **Apply**.
6. Click **Save**.

19.4.5 Status

To define whether the specific user has access to the **Status** page, proceed as follows:

1. In the list of access rights, choose **Status** > **Status**.
2. Click **Deny** if you do not want the user to access the **Status** window. In this case, you can skip all following steps. If you allow the user to access the **Status** window, continue with the next step.
3. To allow or deny isolating alarm inputs, click **Isolate**, and then click **Allow** or **Deny**.
4. To allow or deny manually activating outputs, click **Activate outputs**, and then click **Allow** or **Deny**. This setting also applies to activating outputs in the **Live Video** window.
5. Click **Apply**.
6. Click **Save**.

19.4.6 General

To define whether the specific user has access to some general functions, proceed as follows:

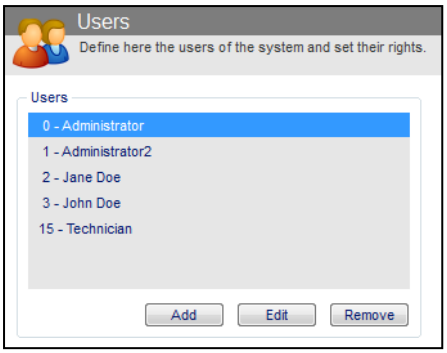
1. In the list of access rights, choose **General**.
2. Click **Set tech rights**, and then click **Allow** or **Deny** to define if the user is allowed to grant access for the Technician users. See *Granting the Technician* .
3. Click **Arm/disarm**, and then click **Allow** or **Deny** to define if the user can arm or disarm the system (change the operational mode). See *Arming and Disarming* .
4. Click **Audio talk**, and then click **Allow** or **Deny** to define if the user can use the microphone to talk to people on-site from the **Live Video** window. See *Audio, Listening* .
5. Click **Apply**.
6. Click **Save**.

19.5 Modifying an Existing User

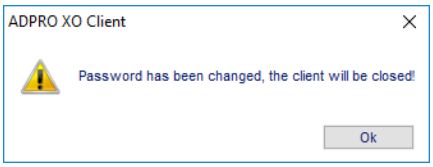
The following restrictions apply to modifying existing users:

- Users can only change their own password (if they have access rights to the Users section). They cannot make any other changes.
- Technicians can only change their own password (if they have access rights to the Users section). They cannot make any other changes.
- Administrator users can modify all settings for all users, except the Technician user password. To modify an existing user, proceed as follows:

1. Choose **System** > **General** > **Users**.



2. Click the desired user, and then click **Edit**, or double-click the user in the list.
3. Change the required settings, and then click **Apply**.
4. Click **Save**.
   If you have changed your own password, the following message will appear:

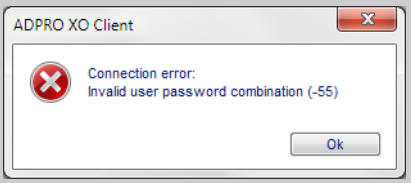


   In this case, click **OK** to close the message box. The system closes the client and returns to the **Login** window (if **Auto restart** is active).

5. If you have changed a username or password, you also have to change the connection settings in the XO client's **Login** window. For details, see *Changing an XO Device* .

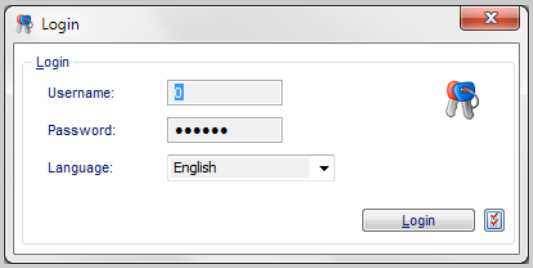
Note

If you have changed a user's username or password, and you do not change the corresponding settings in the **Login** screen, the system will issue an error message when you try to connect to the device:

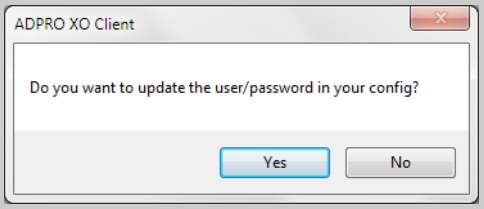


In this case, proceed as follows:

1. Click **OK** to close the message box. The following screen appears:



2. Type the correct user ID or username and the correct password, and then click **Login**.
   If you have entered the correct data, the following screen appears, allowing you to save the new username and/or password in the connection settings:



   (Note that this screen does not appear if you leave the **Password** box blank in the **Login** screen; the system will then never offer to update usernames/passwords.)

3. Click **Yes** to confirm, or click **No** to connect to the device without changing the connection settings.

19.6 Deleting Users

Only Administrators can delete users.

Note

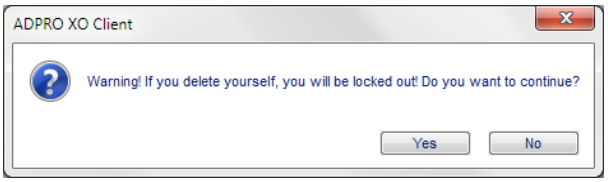
You cannot delete users 0 (Administrator) and 15 (Technician).

To delete a user, proceed as follows:

1. Choose **System** > **General** > **Users**.



2. Click the desired user, and then click **Remove**.
3. Click **Save**.
   If you try to delete your own user profile, the following warning appears:



> ***Caution!***
>
> If you delete your own user profile, you will not be able to log on again. You will lock yourself out of the system.

4. Proceed as follows:
   - Click **No** if you want to keep your user profile.
   - Click **Yes** to delete your own user profile. The system closes the client window, and you cannot log on anymore with your user credentials. You will have to log on with a different username and password.

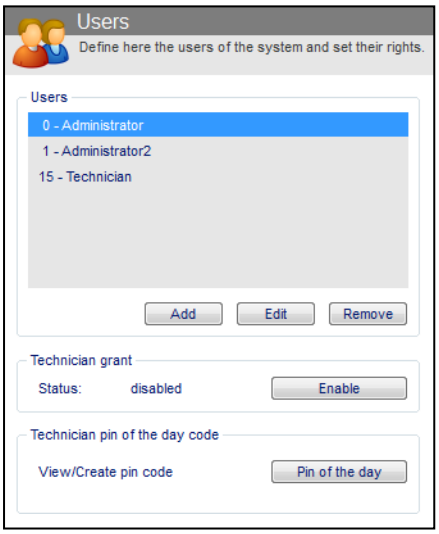
19.7 Granting the Technician

19.7.1 Granting Access to the XO Device

> ***Caution!***
>
> The system automatically disables the technician grant when you restart the XO device. Closing and opening the XO client does not affect the technician status.

To grant the Technician users access to the XO device, proceed as follows:

1. Choose **System** > **General** > **Users**.



2. Under **Technician grant**, click **Enable**.

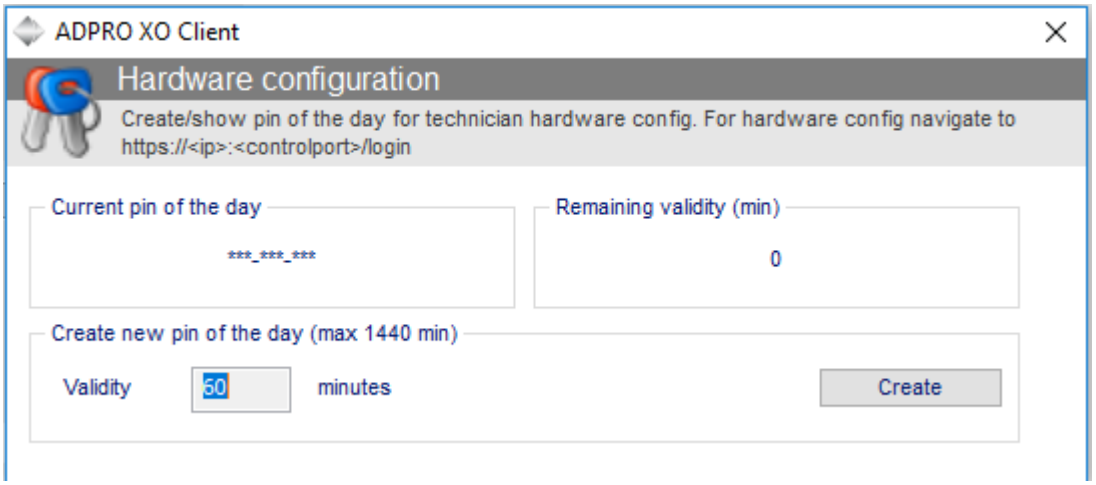
19.7.2 Generating a PIN of the Day

Technician users need an additional PIN (personal identification number) to log on to the hardware configuration tool for setting up XO I/O Interface USB modules. The PIN is only valid for a limited time, and for maximum 24 hours. An Administrator user can generate the PIN using the XO client software, and specify for how long it remains valid.

> ***Caution!***
>
> The PIN is no longer valid after you restart the XO device. You will need to generate a new PIN after restarting. Closing and opening the XO client does not affect the PIN validity.

To generate a PIN for the Technician users, proceed as follows:

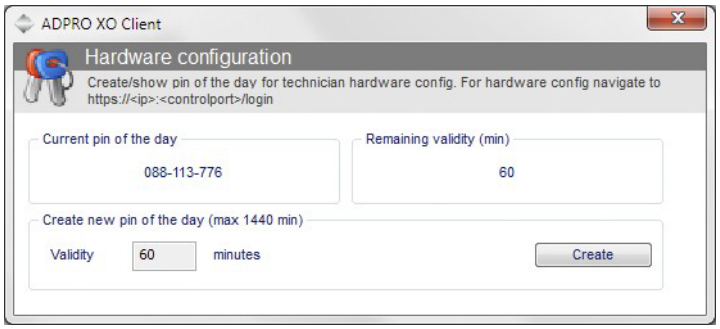
1. Choose **System** > **General** > **Users**.
2. Under **Technician grant**, click **Enable**.
3. Under **Technician pin of the day code**, click **Pin of the day**. The following window appears:



If the last generated code is still valid, it appears under **Current pin of the day**; and the time it is still valid appears under **Remaining validity** (in minutes). In the example above, the current PIN is no longer valid (***-***-*** appears instead of the code; and 0 minutes validity).

> ***Caution!***
>
> If the current PIN is still valid, it will become invalid as soon as you create a new one. Technicians using the current PIN will lose access.

4. In the **Validity** box, enter the time (in minutes) that the PIN has to remain valid. The maximum time is 1440 minutes = 24 h.
5. Click **Create**. A new PIN appears under **Current pin of the day**. The counter in the **Remaining Validity (min)** box displays for how long (in minutes) the new code is still valid.



Technician users can now use this PIN until it expires, or until the XO device restarts.

6. Write down the PIN (including the dashes) so that you can pass it on to the Technician user.
7. To close the window, click the close button in the top right corner.

19.7.3 Disabling Technician Grants

When you disable the Technician grant, you deny the Technician users access to the XO device, the hardware configuration tool, and the IP cameras' web interfaces (remote access).

To disable the Technician grant, proceed as follows:

1. Choose **System** > **General** > **Users**.
2. Under **Technician Grant**, click **Disable**.

> ***Caution!***
>
> The system automatically disables the technician grant when you restart the XO device. Closing and opening the XO client does not affect the technician status.

20 Configuration Management

20.1 Storing a Configuration

The XO device can store up to 8 different configurations. Only 1 configuration can be active. The XO device stores any changes you make in the active configuration (if you save the changes). Any unsaved changes are lost when you close the XO client.

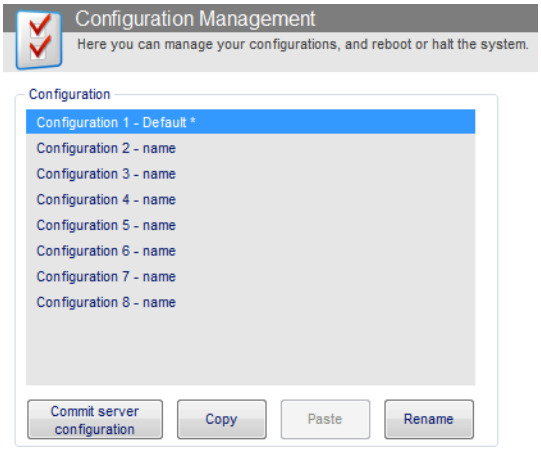
Note

The configuration does **not** include:

- the configuration of MIO/EIO cards and Net I/O units (NO/NC, failsafe, watchdog)
- the users
- the isolation status of inputs
- the licenses.

To store the current settings in the active configuration, proceed as follows:

1. Choose **System** > **Maintenance** > **Configuration Management**. The list of configurations appears. An asterisk (*) marks the active configuration (in the example below: **Configuration 1 – Default ***).



2. To store the current settings in the active configuration, click **Commit server configuration**.

Caution!

When you click **Commit server configuration**, the system stores the current settings in the **active** configuration (= the configuration marked by an asterisk *). It **does not store** the settings in the **selected** configuration (= the configuration that is highlighted in the list).

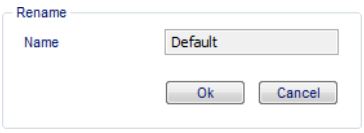
If you want to store the current settings in a **different** configuration than the active configuration, you have to store the settings first in the active configuration, and then **copy** the active configuration into the other configuration.

20.2 Renaming a Configuration

Honeywell recommends using a meaningful and relevant name for the configurations. Tip: it can be useful to include the date in the configuration name.

To change the name of a configuration, proceed as follows:

1. Choose **System** > **Maintenance** > **Configuration Management**.
2. Select the configuration in the list, and then click **Rename**.



3. Type the new name in the **Name** box, and then click **OK**.

20.3 Copying a Configuration

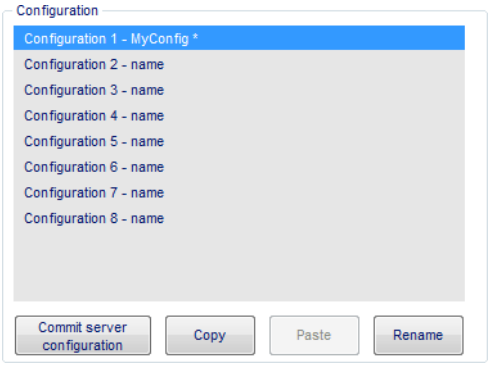
If you want to use a new configuration, you do not have to set up the configuration from scratch. You can copy the settings from any existing configuration to the new one. Afterwards, you can activate the new configuration and make the necessary changes to it.

Note

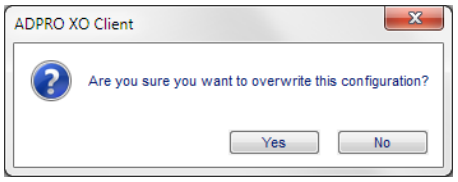
You cannot copy a configuration into the currently active configuration.

To copy the settings of one configuration to another, proceed as follows:

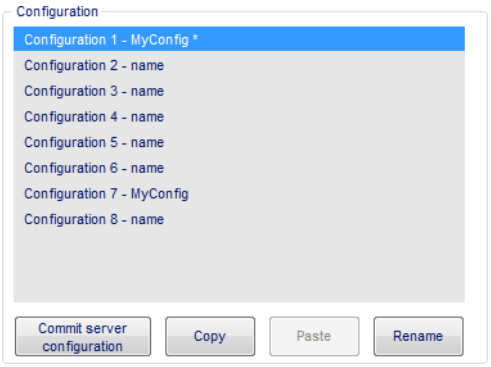
1. In the list of configurations, click the source configuration (the configuration that you want to copy from).



2. Click **Copy**.
3. In the list of configurations, click the target configuration (the configuration that you want to copy to).
4. Click **Paste**. The following message appears:



5. Click **Yes** to confirm.
   The system copies the settings to the target configuration. The target configuration now has the same name as the source configuration. In the example below, configuration 7.



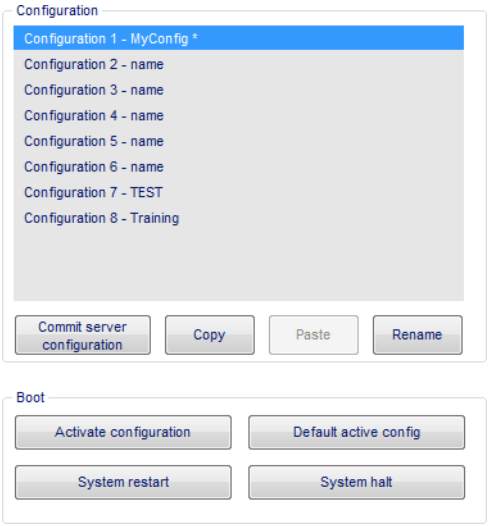
6. Rename the target configuration.

20.4 Activating a Configuration

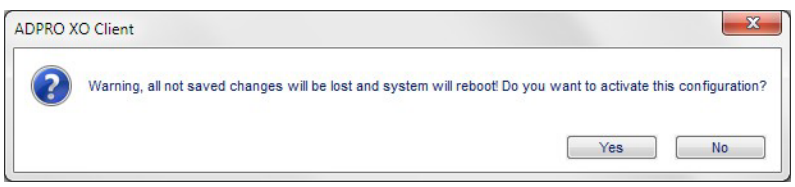
> ***Caution!***
>
> Be very careful when activating a different configuration. If settings are missing or incorrect in that configuration, your XO device may **become unusable or unreachable** (for example, if the IP address changes). Honeywell recommends to start from a configuration that works well, copy that into a new configuration, and then activate the new configuration so you can make the necessary changes.

To activate a configuration, proceed as follows:

1. Choose **System** > **Maintenance** > **Configuration Management**.

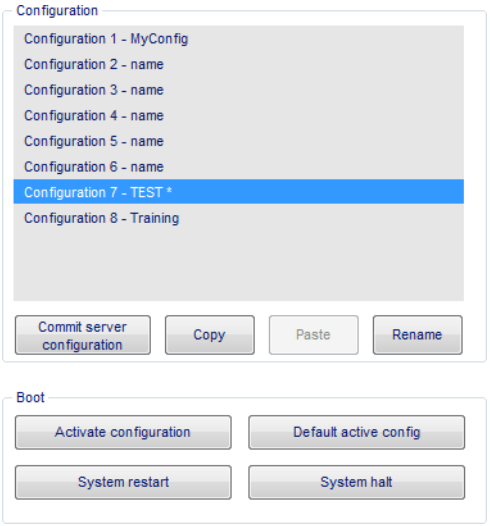


2. Click the desired configuration in the list, and then click **Activate configuration** (or double-click the configuration). The following screen appears:



3. Click **Yes** to confirm.

4. Wait for the XO device to restart, and then open the client again. The selected configuration now has an asterisk (*) in the list of configurations.



20.5 Resetting the Active Configuration to Factory Defaults

You can reset the currently active configuration to the factory defaults using the XO client software. The system overwrites the currently active configuration with the default values, and then activates configuration 1. If configuration 1 was the active configuration, then the device restarts with the default values. You can only reset the active configuration; you cannot reset the other configurations.

Note

There are other options for full or partial resets. For more information, see *Tech Tip #06 Resetting to Defaults* (27986).

If you reset the active configuration, the system restores default values for everything in the **System** menu, including the IP address (reset to 10.0.0.10). The following items are preserved:

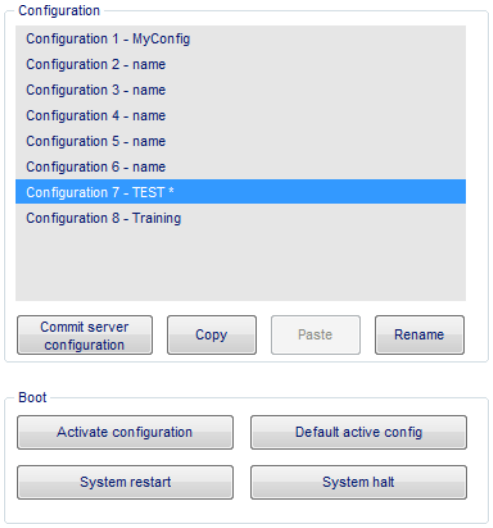
- the other configurations (the ones that were not active)
- the configuration of MIO/EIO cards and Net I/O units (NO/NC, failsafe, watchdog)
- the users
- the isolation status of inputs
- the licenses.

Caution!

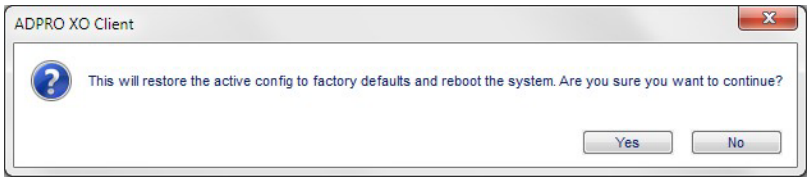
If you reset configuration 1, the device will restart with IP address 10.0.0.10. Make sure that your PC can reach this address and reconnect to the XO device: set the IP address of your PC in the same range.

To reset the active configuration to the factory defaults, proceed as follows:

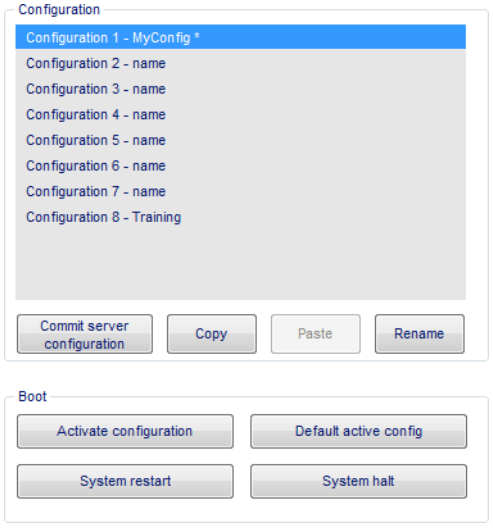
1. First, back up any data that you want to restore afterwards. For more information, see *Downloading Files from the XO Device* .
2. Choose **System** > **Maintenance** > **Configuration Management**. In the example below, configuration 7 – TEST is active.



3. Click the active configuration in the list (the configuration indicated by *), and then click **Default active config**.



4. Click **Yes** to confirm. The system closes all processes and connections, and then restarts. It restores the default values in the configuration that was active, and activates configuration 1.
5. Reconnect the client to the XO device using the settings for configuration 1 (IP address, username/password).
   If you have defaulted configuration 1, then connect with the default IP address (10.0.0.10) and the username/password of a default user.
   In the example below, configuration 7 is reset, and configuration 1 is now active.



21 Downloading and Uploading Files

Note

Disable P2P before you export a configuration file (without this, the P2P function will not work on the device that imports the configuration file with P2P enabled).

21.1 Downloading Files from the XO Device

Before installing new software, or before making major changes to the configuration, Honeywell recommends that you download the following files to your local hard disk:

- License = system license, including encoder card licenses for analogue video channels. The system merges the system license and encoder card licenses into one file when downloading from the XO device.
- User data = all defined users and access rights
- Configurations = all settings in the System menu (except settings for MIO/EIO cards and Net I/O units, users, and licences)
- Camera definitions (only required if you have received a separate camera definition file from Honeywell; this is not required for standard systems)
- Calibration pictures: 3D calibration images for video analytics.

If you lose any of the above data or settings, you can upload the downloaded files again to restore settings.

Note

It is not possible to download application licenses (IP channel licenses, PIR-HLI licenses, licenses for IntrusionTrace, LoiterTrace…) from the XO client. You manage these licenses using Xchange2. For more information, see the *Xchange2 user manual* (27816).

Caution!

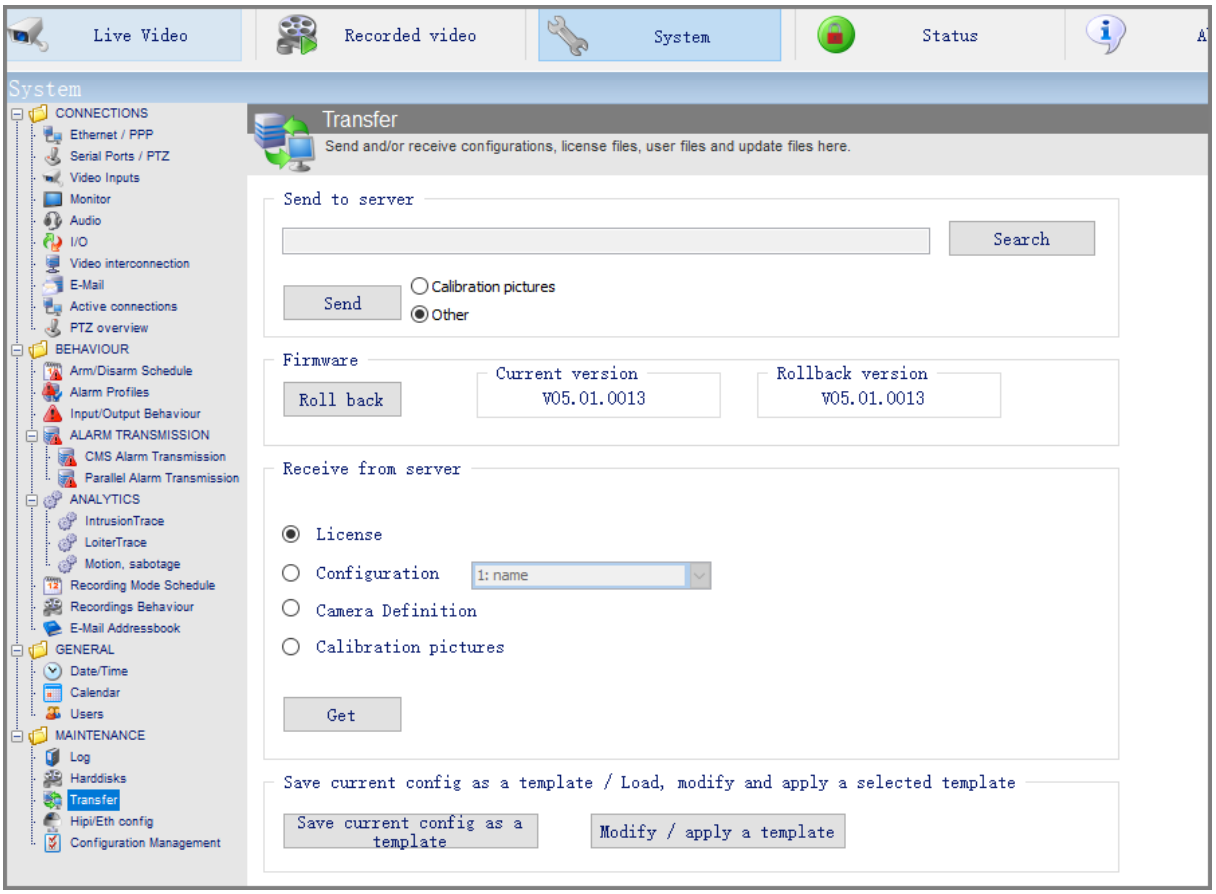
A full upgrade of the firmware and software may cause data to get lost (for example: system license, user data, configuration…). Download the necessary files from your XO device before you start upgrading.

If, by accident, you lose the configuration, you will need to reprogram all settings in the system.

If you also lose your system license, you can first try and restore it using Xchange2 (for requirements and conditions, see the *Xchange2 user manual* (27816)). If restoring via Xchange2 is not possible, you will need to contact your Honeywell supplier (Honeywell Support) to obtain a new license. In this case, you will need to provide the serial numbers of your video cards. Click **About** in the top menu to see the system information, which contains the serial numbers. Click the **Clipboard** button to copy the information, and then paste it into an email to Honeywell Support.

To download files from the XO device, proceed as follows:

1. Choose **System** > **Maintenance** > **Transfer**. For downloading, you will work in the **Receive from server** section:



Note

Versions above XO 4.5.13 don't support user data export.

2. To download the system license (including the encoder card licenses), click **License**, and then click **Get**.
3. Select the destination folder, and then click **Save**.
4. To download user data, click **User Data**, and then click **Get**.
5. Select the destination folder, and then click **Save**.
6. To download a configuration, click **Configuration**.
7. Select the desired configuration from the list, and then click **Get**.
8. Select the destination folder, and then click **Save**.
9. Repeat for each configuration.
10. To download the camera definitions, click **Camera Definition**, and then click **Get**.
11. Select the destination folder, and then click **Save**.
12. To download the calibration pictures, click **Calibration pictures**, and then click **Get**.
13. Select the destination folder, and then click **OK**.

21.2 Uploading Files to the XO Device

21.2.1 Overview

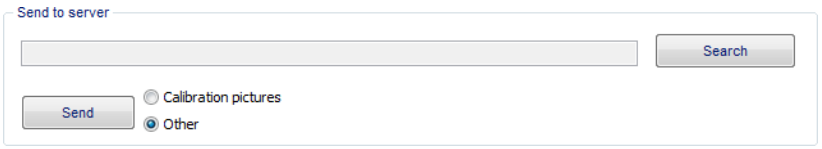
It is possible to upload different types of files to the XO device. Each file type has a specific file extension:

- .bin = software (Linux + application). This method is not recommended for software updates: Honeywell recommends to install new software on your XO device using Xchange2, if possible. Always check the XO Release Notes for instructions on updating.
- .lic = license
- .usr = user data
- .prop = configuration
- .def = camera definitions
- .jpg = calibration pictures. From version XOa 3.02, you can upload multiple calibration pictures at once.

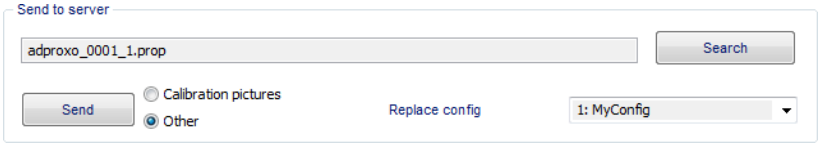
21.2.2 Uploading Configurations

To upload a configuration file to the XO device, proceed as follows:

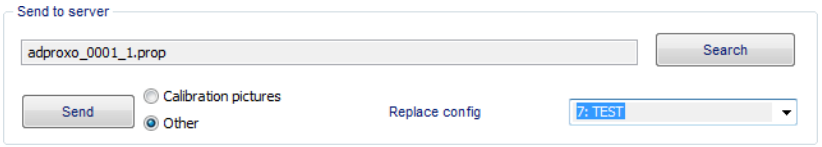
1. Choose **System** > **Maintenance** > **Transfer**. For uploading, you will work in the **Send to server** section.



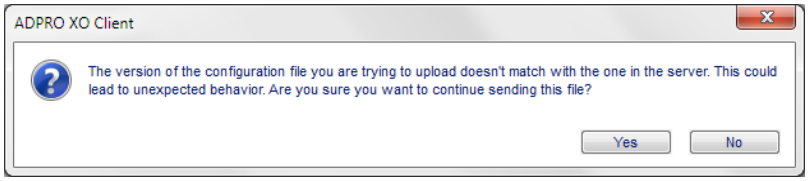
2. Make sure that **Other** is selected.
3. Under **Send to server**, click **Search**.
4. Select the configuration file that you want to upload, and then click **Open**.



5. In the **Replace config** box, select the configuration that you want to overwrite.

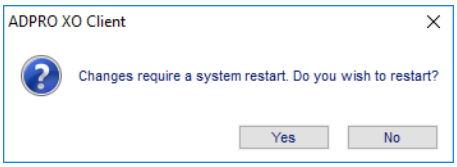


6. Click **Send** to upload the file to the XO device. If the configuration file has a different version than the active configuration, the following screen appears:



> ***Caution!***
>
> Settings from different versions may cause conflicts and unexpected behaviour in the system. Proceed at your own risk.

7. If you are sure that you want to upload the configuration, click **Yes**. The following screen appears:

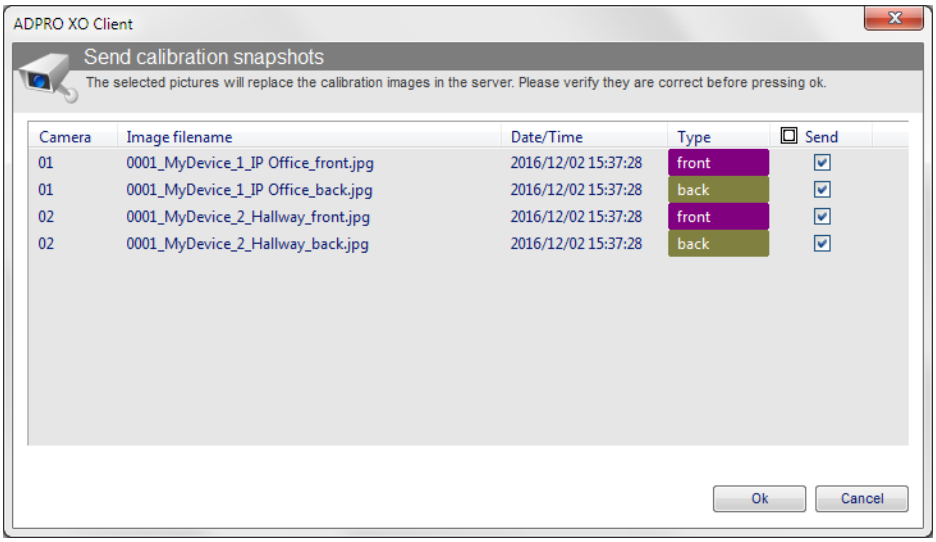


8. Click **Yes** to restart the XO device.

21.2.3 Uploading Calibration Pictures

From client version XOa 3.02, you can upload multiple calibration pictures at once. Furthermore, the system performs various checks before uploading, to help you prevent accidental overwriting of calibration pictures with incorrect images:

- Each calibration picture contains the site name and ID of the XO device from which it was downloaded. When you upload calibration pictures, the system checks if their site name and ID match those of the XO device. If there is no match, the system will not upload the pictures. Therefore, if you change the site name or server unit ID for an XO device, always back up your calibration pictures afterwards.
- If you select more than one front or back picture for the same camera, the system only uses the most recent picture.
- The system filters out snapshots: you cannot upload snapshots as calibration pictures.
- Before uploading, the system presents an overview of the calibration pictures that it will upload. You can then double-check if the selected pictures are the correct ones, if the list is complete, etc. The screen below is an example of such an overview.



The overview contains the following information:

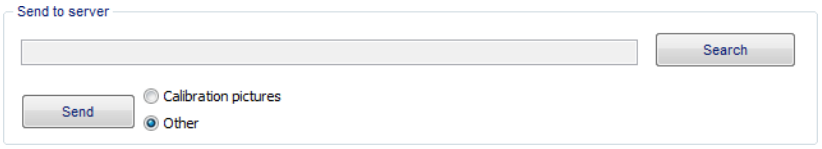
Item	Description
Camera	The number of the camera to which the system will assign the calibration picture.
Image filename	Filename of the calibration picture that the system will upload.
Date/Time	Date and time the calibration picture was downloaded on the PC.
Type	Indicates if the calibration picture is for the front or back of the scene.
Send	Use the checkboxes to indicate which files you want to upload.

Caution!

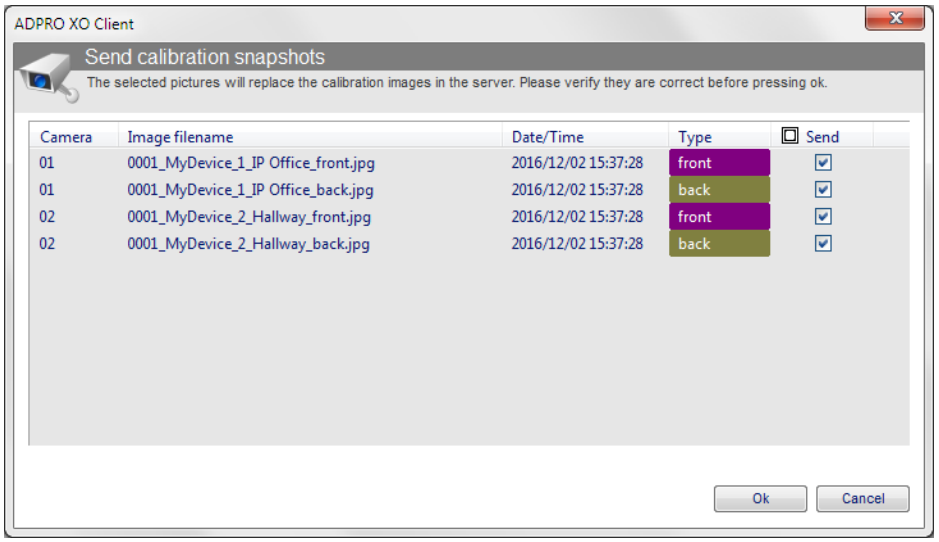
- With client versions below XOa 3.02 you have to upload each calibration picture individually, and the system does not present an overview before uploading. Make sure that the images you select are the correct ones.
- Do not edit the calibration pictures using image editing applications. The calibration pictures may become unusable.

To upload calibration pictures to the XO device, proceed as follows:

1. Choose **System** > **Maintenance** > **Transfer**. For uploading, you will work in the **Send to server** section.

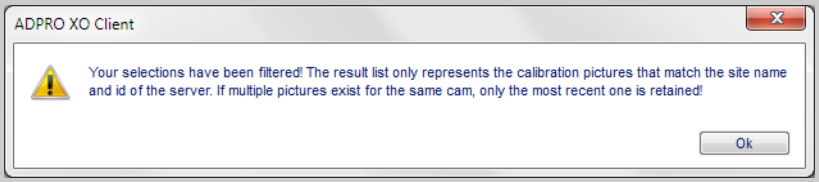


2. Click **Calibration pictures**.
3. Under **Send to server**, click **Search**.
4. Select the file(s) that you want to upload, and then click **Open**.
5. Click **Send**. The system will now check the files you selected, and then present an overview of the calibration pictures that it will upload:



Note

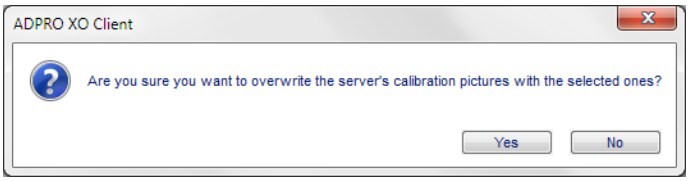
If the system detects one or more files that are not suitable calibration pictures (for example: snapshots), of if you have selected more than one front or back picture for the same camera, the following message appears:



Click **OK** to close the message box. The system filters out the unsuitable pictures, and takes only the most recent version of the suitable pictures.

6. Carefully check the overview, and clear the checkboxes of the listed pictures that you do not want to upload.

7. Click **OK** to confirm. The following screen appears:

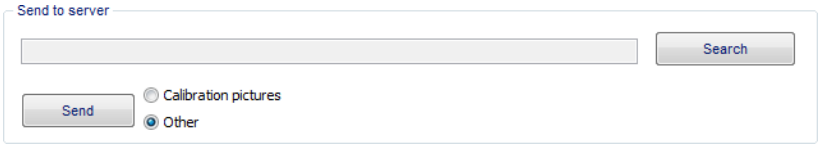


8. Click **Yes** to confirm.
   The system uploads the selected calibration pictures.

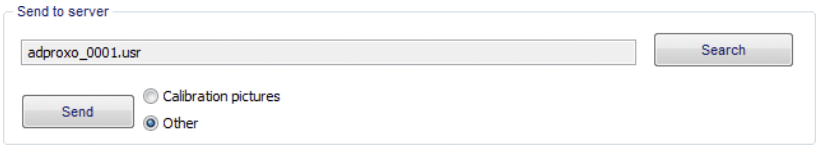
21.2.4 Uploading Other Files

To upload other files than configurations or calibration pictures to the XO device, proceed as follows:

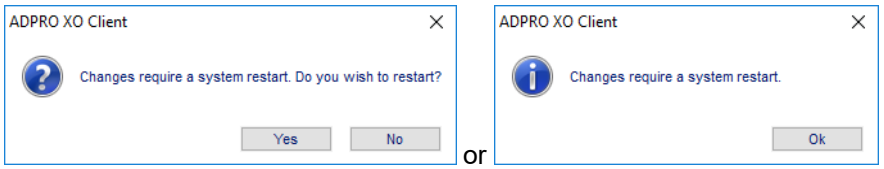
1. Choose **System** > **Maintenance** > **Transfer**. For uploading, you will work in the **Send to server** section.



2. Make sure that **Other** is selected.
3. Under **Send to server**, click **Search**.
4. Select the file that you want to upload, and then click **Open**.
   The example below shows a user data file:



5. Click **Send** to upload the file to the XO device. One of the following screens appears:



6. Click **Yes** or **OK** to restart the XO device and apply the new settings.

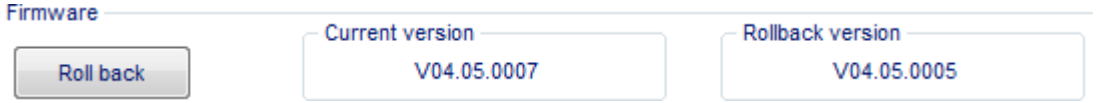
21.3 Firmware Rollback

> ***Caution!***
>
> Backup your system license, user data, configuration data, camera definition, and calibration pictures before performing the rollback. Only the Technician user has rollback privileges.

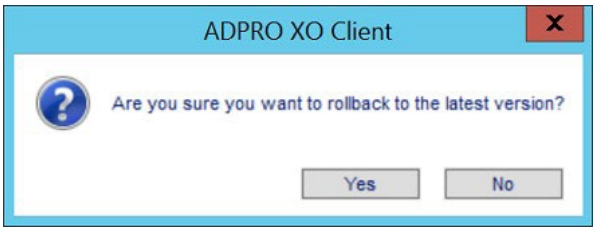
XO 5.0 supports firmware rollback. You can rollback firmware on the ADPRO device from the XO 5.0 Client. The rollback reverts the firmware and all the configured data to the previous version.

Rollback cannot be applied to the eFT Series devices which are supported from XO 5.0 onwards.

1. Choose **System** > **Maintenance** > **Transfer**, and check the **Current version** and the **Rollback version** under **Firmware**.



2. Click **Roll back**. Rollback confirmation dialog box is displayed.

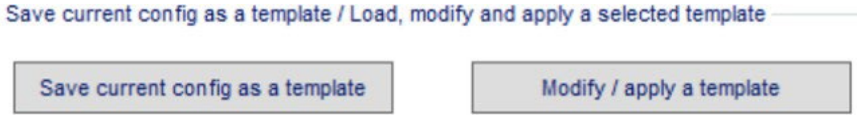


3. Click **Yes**.

21.4 Configuration Template

You can save the configuration settings to a file and then reuse it as a template on other XO devices.

1. Choose **System** > **Maintenance** > **Transfer**.



2. Click the **Save current config as template** button.
3. Save the configuration template (ADPRO XO file) to the disk.

To reuse the saved configuration template:

- Click **Modify / apply a template** and browse the saved file. The configuration settings are imported into the XO device.
- Change the device IP if the template is imported to a different XO device.

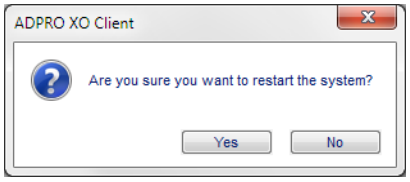
22 Starting and Stopping

22.1 Restarting the System

Follow the procedure below to restart your XO device via the XO client. This allows the system to shut down all processes and connections properly. Do not restart the device by switching the power off and on again.

To restart the system, proceed as follows:

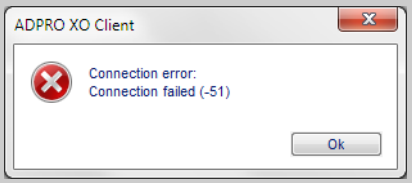
1. Choose **System** > **Maintenance** > **Configuration Management**.
2. Click **System restart**.



3. Click **Yes** to confirm. The system shuts down all processes and connections. This may take a minute. The LEDs on the front panel go out, and then the system restarts automatically.
4. Wait for the system to finish restarting. Restarting is completed when the LEDs on the front panel light up again.

Note

You cannot connect to a device while it is restarting. The following error message will appear:



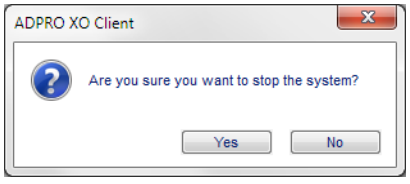
Click **OK** to close the message box and wait for the device to restart completely before trying to reconnect.

22.2 Stopping the System

Before switching off power, you stop the system using the XO client. This allows the system to shut down all processes and connections properly. Do not stop the device by switching off the power.

To stop the system, proceed as follows:

1. Choose **System** > **Maintenance** > **Configuration Management**.
2. Click **System halt**.



3. Click **Yes** to confirm. The system shuts down all processes and connections. This may take a minute.
4. Wait for all the LEDs on the front panel to go out.
5. Switch off the power using the on/off switch at the back of the device.

Note

You have 20 seconds to switch off the device. After 20 seconds the device restarts again automatically.

23 Status

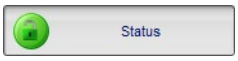
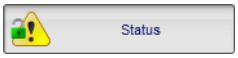
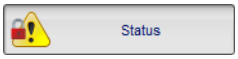
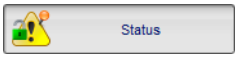
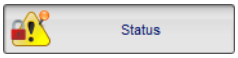
23.1 Front LED Indicators

The following table lists the front panel LED indicators:

LED	Icon	Operation
Green LED		Indicates that power is on. The green LED periodically blinks (goes out briefly). This is normal behaviour. **Note** Red LED on the power button indicates that the device is switched-off. If you press the power button for 3 to 4 seconds, the yellow and blue LEDs flash and the system does graceful shut down. Force shut down happens when you press the power button for 8 seconds are more.
Yellow LED		Indicates a fault. If the yellow LED lights up, check the status of your device.
Blue LED		Indicates storage media activity.

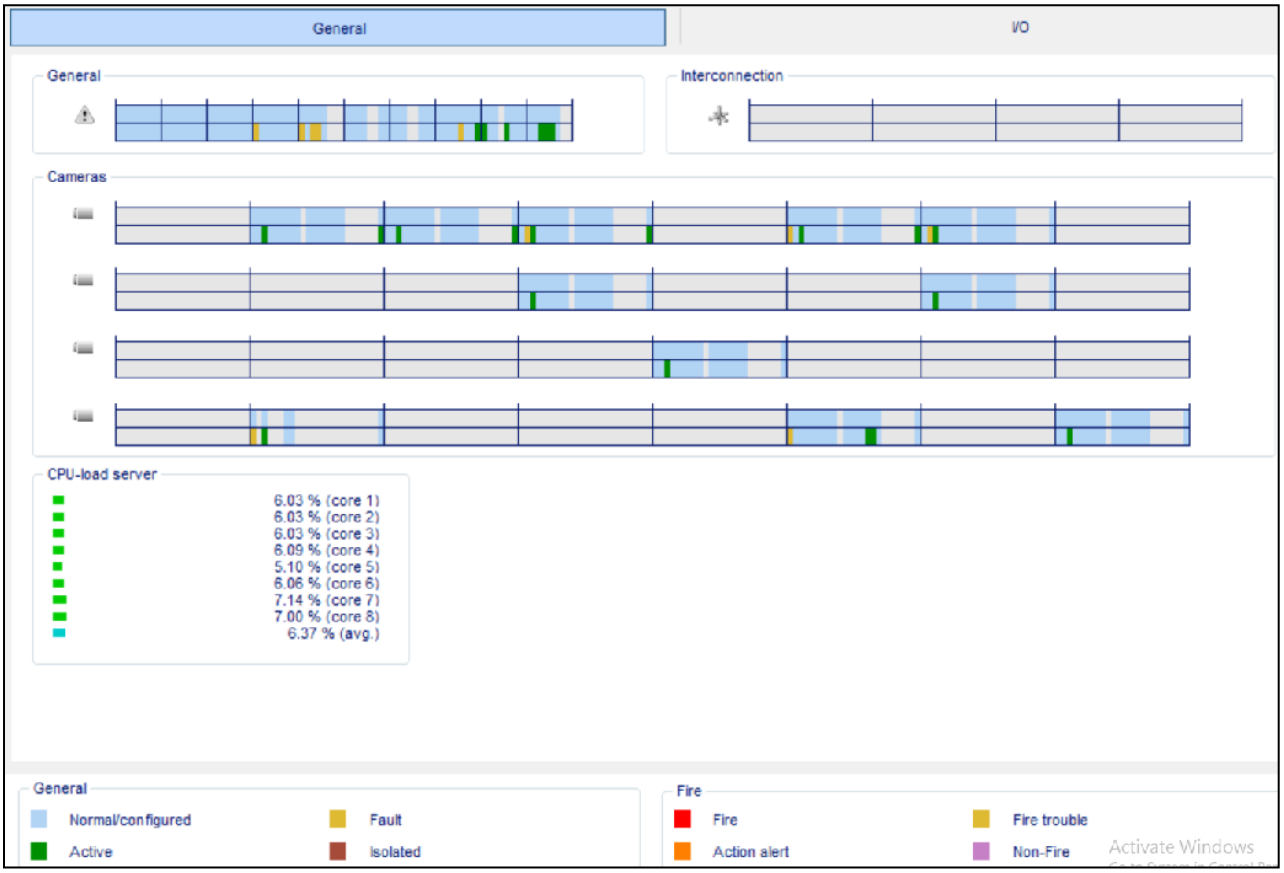
23.2 Status Indicators in the Status Window

The **Status** button in the top menu looks different depending on the system status, providing basic information without opening the **Status** window:

Button	Description
	Normal disarmed status. • The green circle indicates that there are no active faults. • The green padlock indicates that the system is disarmed.
	Normal armed status. • The green circle indicates that there are no active faults. • The red padlock indicates that the system is armed.
	Normal disarmed status with isolated alarm/input. • The pin indicates that there is at least one isolated fault/input. • The green circle indicates there are no active faults that are not isolated. • The green padlock indicates that the system is disarmed.
	Normal armed status with at least one isolated fault/input.
	Fault in disarmed status. • The yellow warning sign indicates that there is at least one active fault. • The green padlock indicates that the system is disarmed.
	Fault in armed status.
	Fault in disarmed status with isolated fault/input.
	Fault in armed status with isolated fault/input.

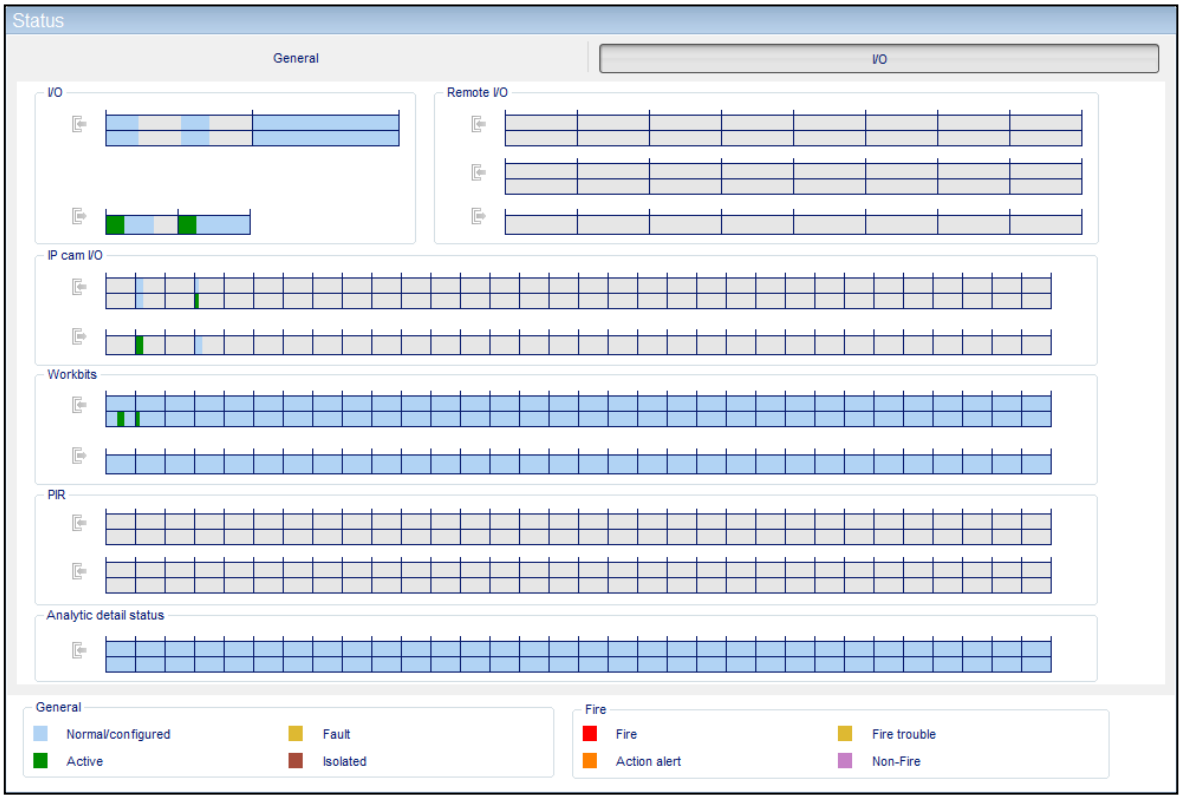
Click the **Status** button to see an overview of inputs and outputs with different status bars. The **Status** window has two tabs: **General** and **I/O**.

NoteYou can check the CPU utilization level of your XO device from the CPU-load server. It displays the Utilization level of each processor core and their average. A warning message is displayed if the CPU utilization is exceeding 90%.



The **General** tab displays the status of the following inputs:

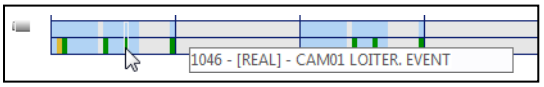
- Under **General**: system inputs.
- Under **Interconnection**: inputs from the S3100 control panels.
- Under **Cameras**: the camera inputs.



The **I/O** tab displays the status of the following inputs ( ) and outputs ( ):

- **I/O**: inputs and outputs on the MIO and EIO cards (on-the-box inputs and outputs)
- **Remote I/O**: inputs and outputs on the Net I/O units
- **IP cam I/O**: inputs and outputs on the IP cameras
- **Workbits**: input and output workbits
- **PIR**: PIR inputs
- **Analytic detail status**: additional inputs for IntrusionTrace.

Place the mouse pointer on an indicator (status bar) to see a detailed description.



Status bars for inputs have two layers: the bottom layer indicates the actual status of the input; the top layer indicates if the input is isolated or not. For more information, see *Isolating an Alarm Input* .

Status bars for outputs only have one layer, indicating the actual status of the output. You cannot isolate outputs.

The bar colour indicates the status. Under **General** (at the bottom of the screen) you find an overview of the colours and a short explanation:

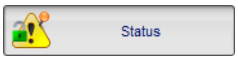
Colour	Description
	A grey bar indicates that the input/output is not available on the XO device.
	A light blue bar indicates that the input/output is inactive. For example, the bar CAMxx PERIMETER for a camera is blue if IntrusionTrace is active on the camera, but no intrusion is being detected now.
	A green bar indicates that the input/output is active. For example, the bar CAMxx PERIMETER for a camera is green if IntrusionTrace is active on the camera, and intrusion is being detected now.

Colour	Description
	A yellow bar indicates that the input is active and indicates a fault in the system. You have to take action. This is typical for system inputs (such as locked recorder or storage insufficient), presence faults, tamper and sabotage events… For example, the bar CAMxx NO VIDEO for a camera is yellow when active.
	A dark red bar in the top layer indicates that the input is isolated.

23.3 Isolating an Alarm Input

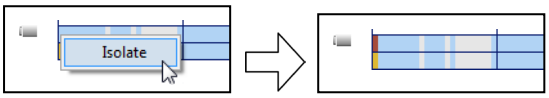
Isolating an alarm input means that system no longer transmits the alarm. The actual input status still appears in the **Status** window. An isolated input is marked in dark red in the top layer of the status bar.

When you isolate an input, the system activates input I0511, and transmits the system message 0511 – [SYST] – GENERAL ISOLATION every 24 hours according to the alarm profile settings, until you activate all isolated inputs again. The **Status** button in the top menu changes shape: a coloured pin indicates that there are isolated inputs.

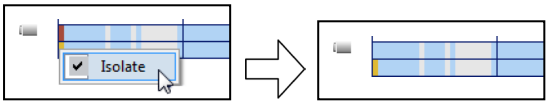
Button	Description
	One or more inputs are isolated; there are no other (not isolated) faults.
	One or more inputs are isolated; there are other (not isolated) faults that you have to check.

To isolate an alarm input, proceed as follows:

1. Click **Status**, and then click the tab that displays the input (**General** or **I/O**).
2. Right-click the desired input, and click **Isolate**. The top layer of the status bar colours dark red.



3. To re-activate an isolated input, right-click the desired input again, and click **Isolate**. The top layer of the status bar colours blue again.



23.4 General Status of the System

Below you find a table with the most common system inputs.

Input	Type	Default name	Description
0000	SYST	SYSTEM STARTUP	The system is starting up (booting).
0001	SYST	MANUAL HW CFG NEEDED	When using XO I/O Interface USB modules on ADPRO devices: the device detected unknown hardware. You have to configure the hardware mapping.
0002	SYST	HW CFG MISMATCH	Hardware configuration mismatch: there is a mismatch between the items configured in the hardware configuration tool and the hardware that the system has detected (either more or less than configured). Check connections and hardware mapping.
0005	SYST	ANALYTIC CFG BUSY	A user is configuring the analytics.

Input	Type	Default name	Description
0006	SYST	CONFIG UNCOMMITTED	Configuration has unsaved changes.
0007	SYST	TECHNICIAN GRANT	Access is granted for the Technician user.
0008	SYST	SYSTEM ARMED	System is armed.
0009	SYST	ENTRY ERROR	Error in the entry path.
0010	SYST	EXIT ERROR	Error in the exit path.
0011	SYST	ENCODER CARD ERROR	Error in the analogue video encoder card(s). None of the cameras on the associated card work.
0012	SYST	LICENSE ERROR	Error in an application license.
0013	SYST	SYSTEM LICENSE ERROR	Error in the system license, or no system license present.
0014	SYST	UNKNOWN LICENSE ERROR	Unknown error concerning licenses.
0015	SYST	HARDDISK FULL	Hard disk is full. In a system with multiple hard disks: all hard disks are full. Recording will stop.
0016	SYST	HARDDISK ERROR	Error on a hard disk.
0017	SYST	HARDDISK CORRUPT	A hard disk is corrupt.
0018	SYST	DATABASE ERROR	Error in the database.
0019	SYST	LOG ERROR	Error in the logs.
0020	SYST	RECORDING ERROR	Error in the recordings.
0021	SYST	SYSTEM LOCKDOWN	A hard disk is in lockdown mode. For details, see *Hard Disk Lockdown Mode* .
0026	SYST	PIR CONFIG. ERROR	Error in the PIR configuration. The configured PIRs do not match the PIRs that the XO device has discovered.
0027	SYST	PIR TRANSP. MODE	PIR transparency mode is active for commissioning; walk test port is in use (for example for iPIR).
0030	SYST	MODEM INIT FAILED	Dial-up connection initialisation failed.
0031	SYST	MODEM PIN INCORRECT	Dial-up connection PIN is incorrect.
0032	SYST	PRIMARY LINE FAULT	Error in the primary transmission path. No communication to the primary destination.
0033	SYST	BACKUP LINE FAULT	Error in the backup transmission path. No communication to the backup destination.
0034	SYST	PRIMARY LIFECHECK	Life check on primary transmission line failed. No answer from the primary destination.
0035	SYST	BACKUP LIFECHECK	Life check on backup transmission line failed. No answer from the backup destination.
0036	SYST	ALMTX QUEUE OVERFLOW	Alarm transmission queue overflow. There are more alarms to transmit than the system can process.
0037	SYST	MODEM INITIALIZING	Dial-up connection is initialising.
0038	SYST	DISPATCHER OVERFLOW	Dispatcher overflow.
0039	SYST	E-MAIL TX OVERFLOW	Email transmission overflow. There are more alarms to transmit via email than the system can process.
0040	SYST	E-MAIL ERROR	Error in e-mail configuration.
0041	SYST	NO ITRACE REACTION	No response from iTrace within specified timeout.
0042	SYST	PARTX1 LINE FAULT	Error in parallel transmission path 1. No communication to parallel destination 1.

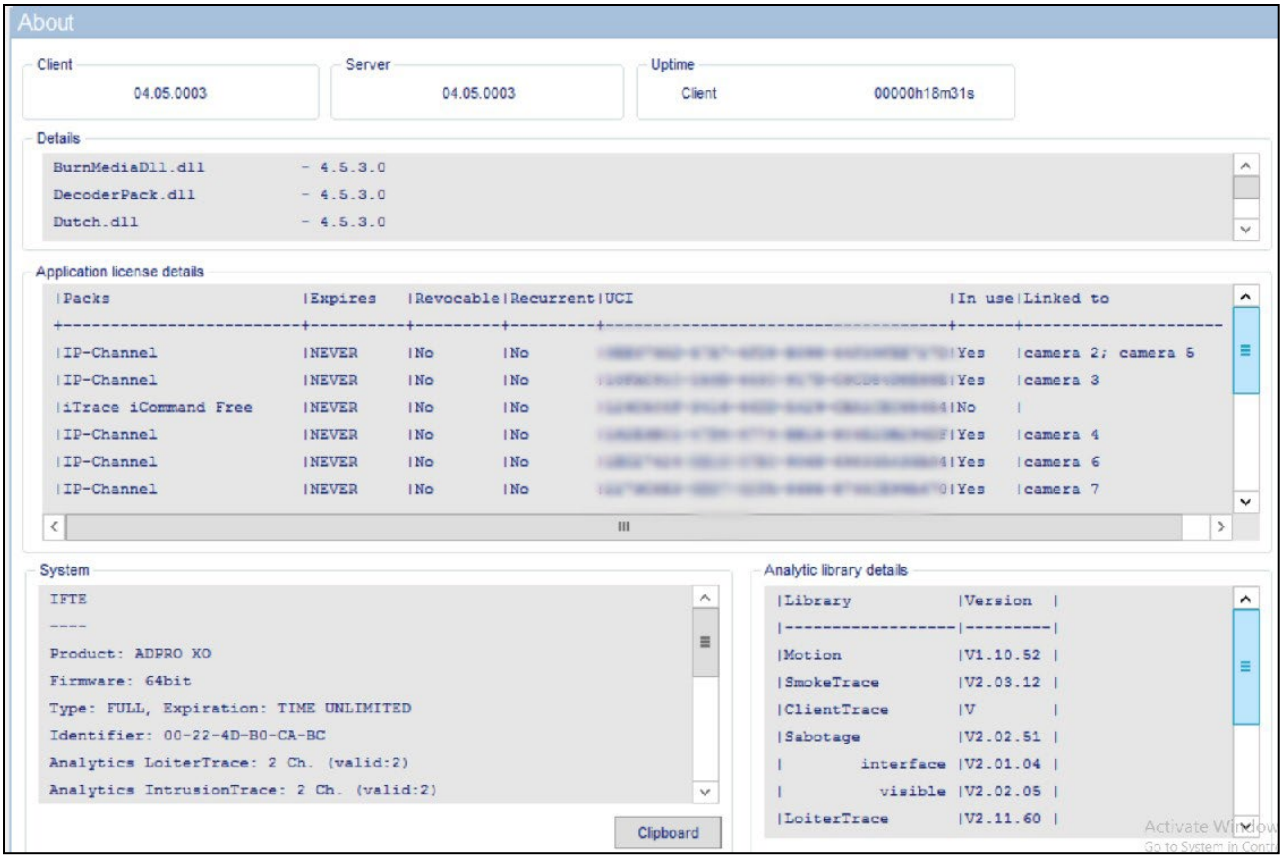
Input	Type	Default name	Description
0043	SYST	PARTX1 QUEUE OVERFL.	Queue overflow in parallel transmission path 1. There are more alarms to send to parallel destination 1 than the system can process.
0044	SYST	PARTX1 LIFECHECK	Life check on parallel transmission path 1 failed. No answer from parallel destination 1.
0045	SYST	PARTX2 LINE FAULT	Error in parallel transmission path 2. No communication to parallel destination 2.
0046	SYST	PARTX2 QUEUE OVERFL.	Queue overflow in parallel transmission path 2. There are more alarms to send to parallel destination 2 than the system can process.
0047	SYST	PARTX2 LIFECHECK	Life check on parallel transmission path 2 failed. No answer from parallel destination 2.
0048	SYST	RECORDER OVERFLOW	Recorder overflow (more than 16 000 events).
0049	SYST	LOCKED RECORDER	There are locked recordings on the hard disk.
0050	SYST	STORAGE INSUFFICIENT	There is not enough free space on the hard disks for the specified minimum days of recording.
0055	SYST	DYN DNS FAILED	Dynamic DNS connection failed.
0056	SYST	NTP SERVER UNREACH	Cannot reach NTP server for date/time sync.
0057	SYST	NTP NOT SYNCHRONIZED	System is not in sync with NTP server.
0060	SYST	EVENT QUEUE OVERFLOW	Event queue overflow.
0065	SYST	LICENSE EXPIRED	A license has expired. Replace the license before the grace period (30 days) expires.
0066	SYST	LICENSE OUT OF SYNC	The application licenses on this device do not correspond with the registered licenses in the Honeywell database. Connect to the device using Xchange2, and sync the device.
0067	SYST	APPLICATION STOPPED	An application has stopped working (timed license has expired more than 30 days ago).
0068	SYST	LICENSE TAMPERING	Tampering with licenses detected (for example, DOM from a different device is installed; contains a system license with the wrong MAC address).
0070	SYST	PRESIDIUM FAULT	Presidium (obsolete) reports a high temperature or general fault, or the XO device detects an incorrect IP port.
0071	SYST	PRESIDIUM PRES.FAULT	Cannot communicate with Presidium (obsolete).
0080	SYST	DECODER CARD ERROR	Error in Ethernet card for IP camera network (for example, card is missing).
0090	SYST	WIFI CONNECTION ERROR	Error connecting to wireless network.
0091	SYST	TUNNEL IP CAM	Remote access to IP camera is active.
0100	SYST	SMART ERROR	Unspecified hard disk SMART error.
0101	SYST	SMART HDD ALERT	Hard disk SMART alert.
0102	SYST	SMART HDD ALERT TEMP	Hard disk temperature too high.
0103	SYST	SMART HDD ERROR	Hard disk SMART error.

Input	Type	Default name	Description
0197	SYST	CHECK ANALYTIC CFG	There is a mismatch between the analytic resolution of at least one camera and the resolution of that camera's calibration pictures. Check calibration, detection zones, and mask areas of the affected cameras. Reconfigure if necessary. For details, see *Troubleshooting Analytic Resolutions* .
0198	SYST	CMS PRIORITY	CMS has taken priority and/or analytics configuration is busy.
0200	SYST	REMOTE CONNECTION	A remote connection (XO client, app) is active.
0201	SYST	SENSOR ACTIVITY	A sensor (input) is active.
0203	SYST	RECORDER INIT	Recorder is initialising.
0204	SYST	RECORDER INIT DONE	Recorder has finished initialising.
0500	SYST	GENERAL MODE1	System is operating in recording mode 1.
0501	SYST	GENERAL MODE2	System is operating in recording mode 2.
0502	SYST	GENERAL MODE3	System is operating in recording mode 3.
0503	SYST	GENERAL MODE4	System is operating in recording mode 4.
0506	SYST	END OF FIRE COND.	Not applicable.
0508	SYST	GENERAL POWER	System is powered.
0509	SYST	GENERAL FAULT	At least one fault input is active.
0510	SYST	GENERAL RECORDING	System is recording.
0511	SYST	GENERAL ISOLATION	At least one input is isolated.

24 System Information

24.1 Software and License Information

To check the software and license information of your XO device, click **About** in the top menu.



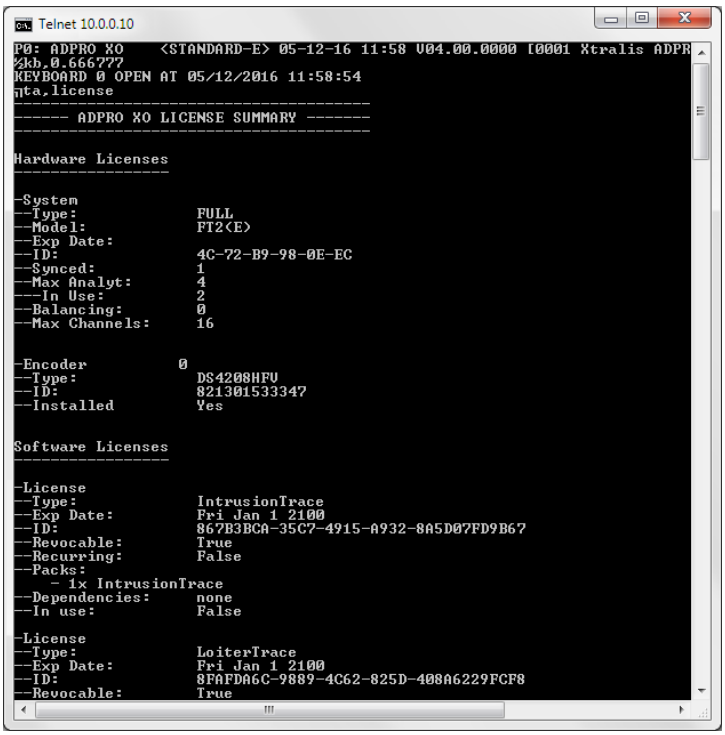
The **About** window displays the following information:

> **Note**
>
> You can do telnet to the device and run the TA, PLATFORMCAP command to check the device brand name from the command line.

Item	Description
Client	The version of the client software that runs on your PC.
Server	The version of the firmware that runs on your XO device.
Uptime	Indicates how long you have been connected to the XO device with this client software in this session.
Details	The firmware versions of the different dll files that the XO device uses.
Application license details	Details of the application licenses installed on the XO device: • **Packs**: name of the license. • **Expires**: — For timed licenses: indicates the license expiry date, or indicates EXPIRED after the grace period for renewing the expired license has ended (when the application stops working). — For perpetual licenses: indicates NEVER. • **Revocable**: indicates if the license is revocable or not. You can use Xchange2 to revoke a revocable license from one XO device, and install it on a different, compatible XO device.

Item	Description
	• **Recurrent**: indicates if the license is recurrent or not. A recurrent license is a license that needs to be renewed on a regular basis. • **UCI**: the unique ID of the license. • **In use**: indicates if the license is in use or not. • **Linked to**: — The video channel(s) to which the application license is assigned. Individual IP channel licenses are all displayed on one line: the Linked to column lists all the cameras that are linked to an individual IP license. — For sets of 4 IP channel licenses: all the cameras that are currently linked to the license. If you want to revoke the license, you have to unlink all these cameras from the license first. — For PIR-HLI licenses: displays the PIR detector connection: Serial (via RS-485 bus), and/or UDP (via IP modules).
System	General system information, from top to bottom: • **Device type**: FastTrace 2, iFT, iFT-E, or eFT. • **Product**: displays the product brand name. • **Firmware**: 32-bit or 64-bit. • **Type**: the system license type: FULL, TRANSMITTER, ENTRY. • **Expiration**: displays TIME UNLIMITED for perpetual system licenses, or the expiry date for timed system licenses. • **Identifier**: the device's MAC address. • **Encoder card**: The type and ID of the installed encoder cards for analogue cameras. If the encoder card license is correctly installed in the device, the line indicates LICENSED. If not, the line indicates UNLICENSED. • **Analytics LoiterTrace and Analytics IntrusionTrace**: for each analytic application, the number of installed licenses (x Ch), and the number of valid licenses (valid: y). • **Pir detector license**: indicates if a PIR-HLI license is available. • **Fire detector license**: not applicable. • **Motherboard, CPU, Memory**: hardware information of the XO device. • **Max simultaneous analytic channels**: the maximum number of analytic channels allowed on the device. • **Balancing mode**: indicates if the trade-off mechanism for IP/analytics licenses is active (for iFT Series and eFT Series models only). • **Max allowed channels**: maximum number of video channels. • **Harddisks**: type and serial number of all the disks in the system. This includes the DOM (disk-on-module) and the recording hard disks. You can click **Clipboard** to copy the system information. You can then, for example, paste the system information into an email to Honeywell technical support staff.
Analytic library details	The version of the libraries that the different analytic applications use.

If you do not have access to the XO client software, you can use the **ta,license** command in a Telnet session to display the license information.



24.2 Licenses

24.2.1 Overview

You can load different types of licenses in the XO device:

- System license
- Encoder card licenses = licenses for the analogue video channels
- IP licenses = licenses for the IP video channels
- Analytics application licenses = licenses for using extra applications.

All license types are explained in detail in the following sections.

24.2.2 System License

From firmware version V2.00, all XO systems require a system license. The system license defines the maximum number of video channels allowed, and the maximum number of analytic channels allowed on your system.

Although the XO software technically allows for 32 IP channels, these 32 channels are only available on:

- FastTrace 2E models with a PH10LU motherboard and 4 GB RAM or more.
  To use the 32 IP channels, the FastTrace 2E requires a **new system license**.
- The latest iFT models with a new system license. The older iFT models (before October 2015), also require a **new system license**.
- iFT-E models.

XO software allows for up to 16 channels on eFT models.

For instructions on upgrading the system license (free of charge), see the *Xchange2 user manual* (27816).

An XO device running without system license will inform the user of the license error via the event message 0013 – [SYST] – SYSTEM LICENSE ERROR, and via a popup window at each connection with the XO client. You have to install or restore the system license immediately to have access to full functionality.

You can back up and restore your system license via the **Transfer** function in the XO client. For more information on uploading licenses, see *Downloading and Uploading Files* . In some cases, you can also try to restore the system license using Xchange2. For details, see the *Xchange2 user manual* (27816).

Note

The system license is locked on the XO device's motherboard and is therefore system specific: the license has to include the correct MAC address. You cannot transfer a system license from one device to another.

When you make a backup copy of the system license using the client software, the video system merges the system license together with the encoder card licenses (for analogue video channels) into one license file. The system license backup file does not contain any other licenses (application licenses, IP channel licenses…), but you can restore those using Xchange2.

24.2.3 Encoder Card Licenses (Analogue Video Channels)

Note

The information below applies to the FastTrace 2 Series only. The iFT Series devices do not support analogue cameras.

For analogue video channels, you need:

- Physical BNC connectors, one per channel. These connectors are available at the back of the device. They come in sets of 4: you can have 4, 8, 12, 16, or 20 connectors, depending on the device model. In a device with a DTC card (for PTZ control via coax), you can have maximum 16 BNC connectors.
- Encoder cards that come with the licenses for the analogue video channels. Depending on the model, the cards provide for 4, 8, or 16 video channels. They can be combined to provide up to 20 analogue video channels.

On a **hybrid system** with a mix of analogue and IP channels, the actual number of available analogue channels also depends on the number of IP channels that are already in use on the device.

Example:
You have a FastTrace 2E device that allows for a total of 32 video channels (analogue + IP).
The device has 12 BNC connectors (+ encoder cards with licensing for 12 analogue channels), so you can theoretically use up to 12 analogue cameras.
However, there are already 25 IP cameras enabled on the device. In this case, you can use only 7 (= 32 – 25) analogue cameras.
If you want to use all 12 analogue channels, you can use maximum 20 IP channels (= 32 – 12).

24.2.4 IP Video Channel Licenses

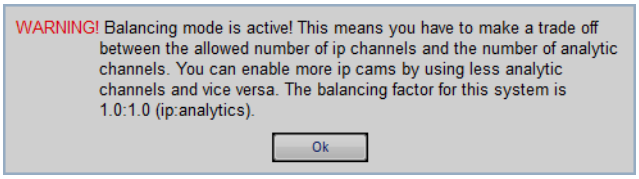
For IP video channels, you need:

- An IP network connection to the camera network. For this, you use the second LAN connector on the PH10LU motherboard.
- An IP license per channel. You have to purchase IP licenses, and install them on the XO device using the Xchange2 tool.

The actual number of available IP channels depends on the following factors:

Device model	Number of IP channels
FastTrace 2E models running firmware version **XOa 3.0 or above** with a **PH10LU** motherboard, more than **4 GB RAM**, and a **new system license**	0–32
iFT models with **old system license** On the iFT model, you trade in 1 video channel for 1 analytic channel (balancing mode).	Max. 16 with 0 analytics Max. 8 with 8 analytics
iFT models with a **new system license** On the iFT model, you trade in 1 video channel for 1 analytic channel (balancing mode). You can update your system license (free of charge) using Xchange2. For details, see *Field Alert #7 Upgrading to 32 Channels* (29477).	Max. 32 with 0 analytics Max. 16 with 16 analytics
All **iFT-E** models	32
All **eFT** models On the eFT model, you trade in 1 video channel for 1 analytic channel (balancing mode).	Max. 16 with 0 analytics Max. 8 with 8 analytics

On the iFT models, the system will display the following reminder regarding the balancing mode when you open the **System** menu:



On a **hybrid system** (FastTrace 2 Series only) with a mix of analogue and IP channels, the actual number of available IP channels also depends on the number of analogue channels that are already in use on the device.

Example:
You have a FastTrace 2E device that allows for a total of 32 video channels (analogue + IP).
However, there are already 12 analogue cameras enabled on the device. In this case, you can use 20 (= 32 – 12) IP cameras (provided that you have 20 IP channel licenses).
You can easily migrate from analogue to a full IP system on the same device: just replace the analogue cameras by IP cameras as required. Remember to purchase additional IP licenses if needed.

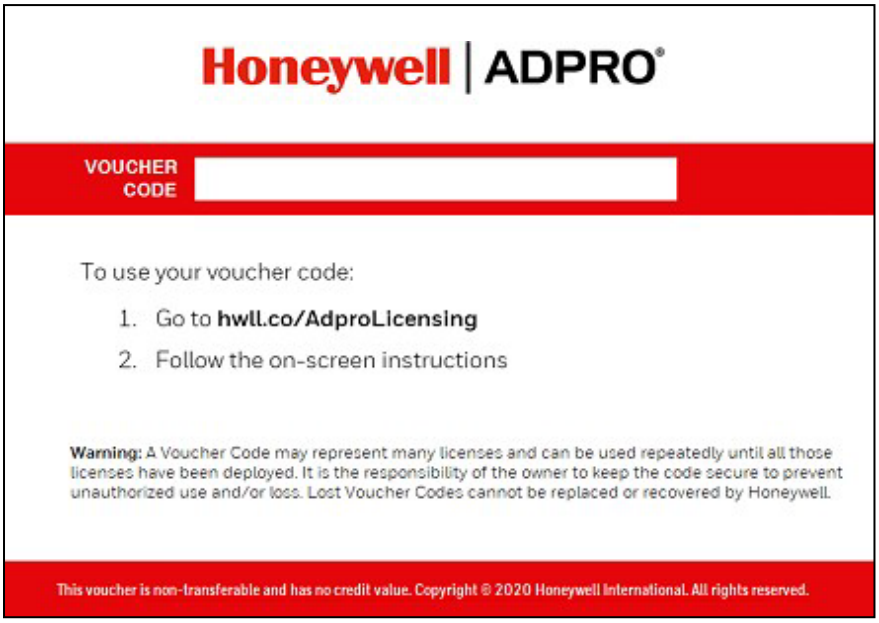
24.2.5 Application Licenses

The XO devices – from software version V2.06 onwards – provide the ability to unlock extra functionality that resides in their system firmware. To unlock functionality, you need to buy an **application license** via your regular Honeywell sales channel.

You can add the following applications to the XO device's functionality:

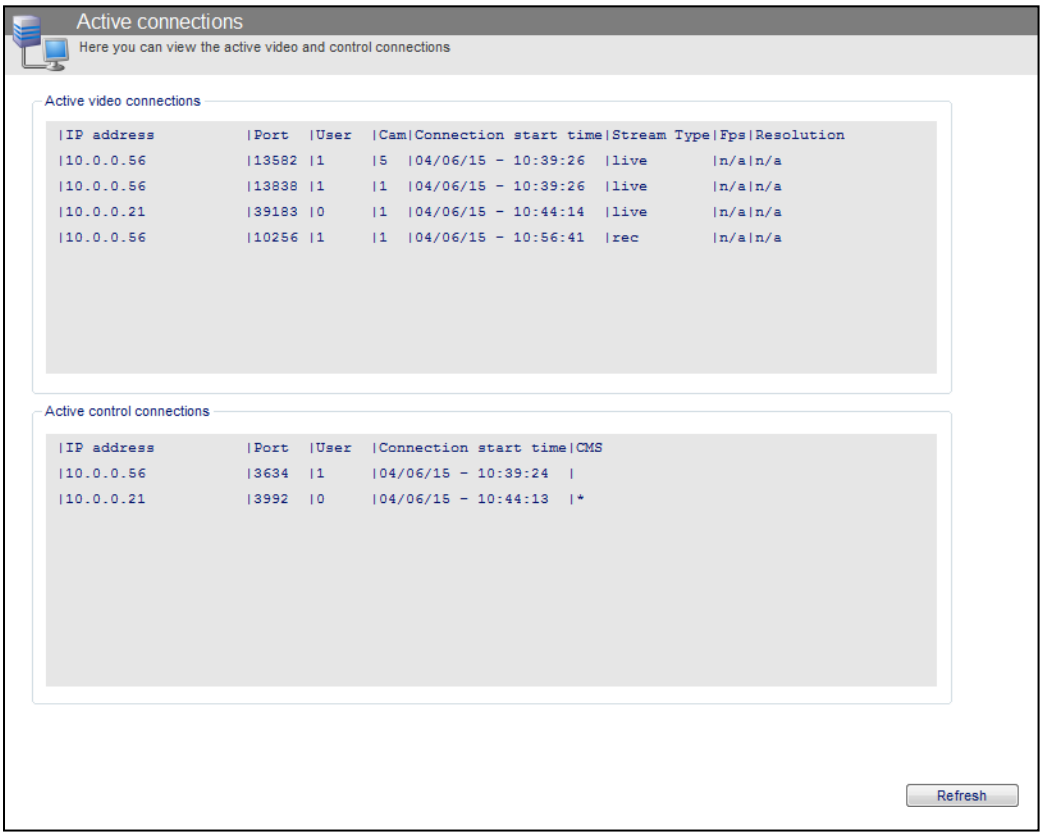
- IntrusionTrace: video analytics application for outdoor perimeter detection for sterile zone monitoring. The new IntrusionTrace on XO licenses always include the PIR-HLI license, allowing for double- and triple knock configurations with ADPRO (PRO-E) PIR detectors. You can upgrade your old IntrusionTrace licenses free of charge using Xchange2: just revoke and then re-install your IntrusionTrace licenses on your devices.
  For more information, see the IntrusionTrace documentation.
- iTrace iCommand: mobile app for remote monitoring, verification, and control (iOS and Android).
  For more information, see the iTrace documentation. The iTrace iCommand functions are included, free of charge, in firmware versions XOa 3 and above.
- LoiterTrace: video analytics application for indoor/outdoor loitering detection.
  For more information, see the LoiterTrace documentation.
- PIR-HLI: interface application for alarm reception, configuration, and walk testing with the PRO or PRO E PIR detectors.

When you buy an application license, you receive a **voucher code** with a credit number. The voucher code can contain one or more licenses. You redeem the voucher code in the Xchange2, and then you can install the licenses on the desired XO devices. For more information on handling application licenses for XO devices, see the *Xchange2 user manual* (27816).



24.3 Viewing Active Connections

To display the active connections, choose **System** > **Connections** > **Active connections**.



The **Active connections** window displays:

- the active video connections for viewing live or recorded camera images (active RTSP connection)
- the active control connections (active client protocol connections).

You cannot modify any settings in this screen; it is for information only.

The system does not refresh the information in the screen automatically: click **Refresh** to update.

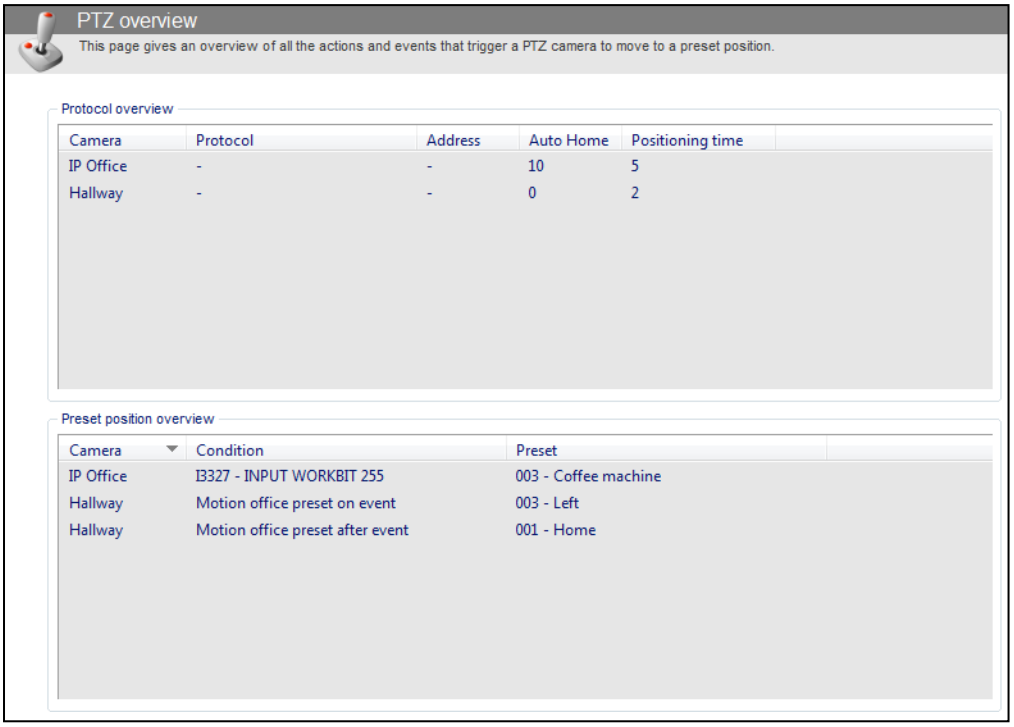
The **Active connections** screen displays the following information:

Item	Description
Active video connections	
IP address	The IP address of the device that established the video connection.
Port	The connection port number.
User	The ID of the user that connected.
Cam	The camera number.
Connection start time	Start date and time of the connection, in dd/mm/yyy – hh:mm:ss format.
Stream Type	The video stream type: • **live**: live video • **rec**: recorded video.
Fps	Frames per second, if available. If the information is not available, this column displays **n/a**.
Resolution	The image resolution, if available. If the information is not available, this column displays **n/a**.
Active control connections	
IP address	The IP address of the device that established the connection.
Port	The connection port number.
User	The ID of the user that connected.
Connection start time	Start date and time of the connection, in dd/mm/yyy – hh:mm:ss format.
CMS	This column displays an asterisk (*) for the connection that has 'CMS priority'. This can be either a connection from a CMS, or a client connection that is busy configuring the analytics. When a connection has CMS priority, the other connections cannot change certain system settings, such as the analytics configuration. This prevents configuration conflicts.

24.4 PTZ Overview

The PTZ overview screen displays an overview of PTZ camera configurations, and of the configured PTZ presets that the XO device can trigger. It includes the presets on and after event recording conditions, and on I/O triggers. You cannot modify any settings in this screen; it is for information only. You can click the column headers to sort the information.

To display the PTZ overview, choose **System** > **Connections** > **PTZ overview**.



The sample screen above displays the following information:

Item	Description
Protocol overview	
Camera	The PTZ camera name.
Protocol	The port number and PTZ protocol. For IP cameras, this column displays –.
Address	The camera address for PTZ control. For IP cameras, this column displays –.
Auto Home	The time (in seconds) after which the camera automatically moves back to its home position. This corresponds with the **Auto-Home Expire Time** setting in the camera configuration screen.
Positioning time	The time (in seconds) allowed for the camera to move to the preset position. This corresponds with the **Positioning Time** setting in the camera configuration screen.
Preset position overview	
Camera	The PTZ camera name.
Condition	The trigger that instructs the camera to move to a preset position. The example screen shows: • Event trigger: the number and name of an input (I3327 – INPUT WORKBIT 255) that triggers camera 'IP Office' to move to preset position 3 'Coffee machine'. • For recording: the recording condition named 'Motion office' triggers camera 'Hallway' to move to preset position 3 ('Left') when recording, and back to the preset position 1 ('Home') after recording.
Preset	The number and name of the position that the camera moves to.

24.5 Logs

24.5.1 About Logs

Local legal requirements (variable and depending on state and region, please check with your local authorities) may stipulate that a video system must keep a logbook (for example the Law Sarkozy in France). The logbook, or log for short, registers all user interventions and events.

The XO device offers different log types with different information, to make it easier to keep an overview and find the data you need.

Note

A log is limited to 100 000 events per type (log, event, or command; see below) and has a time period limit of 6 months. The XO device automatically deletes any logged data older than 6 months. If you need to keep logged data longer than that, you can save the log on a local hard drive or USB stick.

The following log types are available:

Type	Description
Log	Log of users and what they viewed. You can filter the log to display one or more of the following view types: • **Live video view**: lists the users that started a live video stream. • **Live multicast view**: lists the users that started a live multicast video stream. • **Still image view**: lists the users that viewed still images = starting/stopping playback of recorded video. • **Recorded video view**: lists the users that watched or downloaded recorded video.
Event (CMS Tx)	Log of events that are configured for transmission to the CMS. You can filter the log to display one or more of the following event types: • **Faults**: alarms and errors, such as tamper alarms, locked recordings, etc. • **Fire**: not applicable. • **Other**: other events, such as system messages, motion detection, live viewing, inputs and outputs, etc. From XO version 4.02, you can also filter on specific event triggers (inputs). If you are using custom data from third-party applications (for example, a license plate recognition app) in workbits, you can search for that custom data in the log.
Event (E-mail Tx)	Log of events that are configured for transmission to email. You can filter the log using the same event types as described for transmission to the CMS.
Event (ParTx 1)	Log of events that are configured for transmission to parallel destination 1. You can filter the log using the same event types as described for transmission to the CMS.
Event (ParTx 2)	Log of events that are configured for transmission to parallel destination 2. You can filter the log using the same event types as described for transmission to the CMS.
Command	Log of users and the commands that they executed, such as connecting to XO devices, saving configurations, etc.

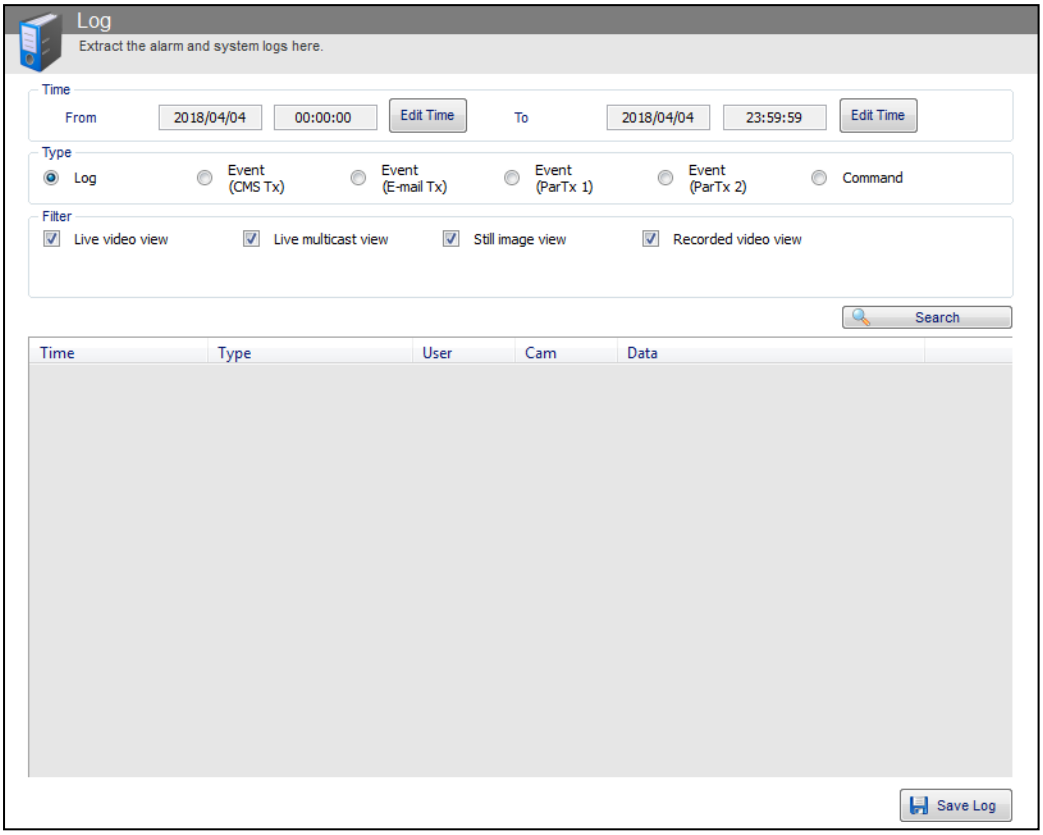
Note

The logs contain events that actually occurred, and that are configured for the selected transmission. However, this does not imply that the destination has actually received the event message. For example, if you set up LICENSE EXPIRED for email transmission, the event appears in the log when a license expires. However, if you did not set up a mailing list for it, then the message LICENSE EXPIRED does not reach any email destination.

24.5.2 Generating a Log

To generate a log, proceed as follows:

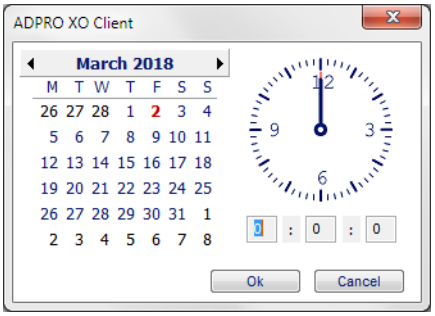
1. Choose **System** > **Maintenance** > **Log**.



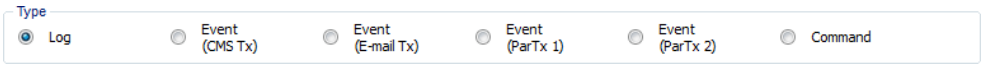
2. Under **Time**, set the desired time frame.



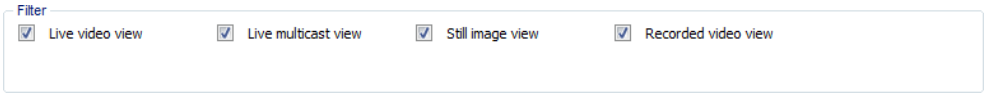
You can type the date and time indications in the **From** and **To** boxes, or you can click **Edit Time** to select a date and set a time:



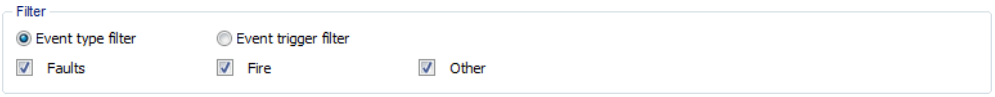
3. Under **Type**, select the type of log data that you want to display.



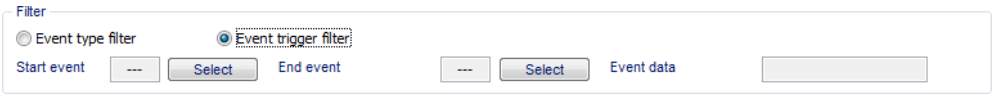
4. Under **Filter**, select the log or event types that you want to include in the log.
   Log filters:



   Event filters, filter on event type:



   Event filters, filter on event trigger:



5. If you are generating an event log and want to filter on a range of event triggers, select the desired start trigger and end trigger in the **Start event** and **End event** boxes.
   Optionally, type a text string to search for in the **Event data** box (for example, a license plate recognition app).

> **Note**
>
> The system will search for the entered text string in the **Data** column only. If you want to perform a full-text search in the log, save the log and open it in a text editor.

6. Click **Search** and wait for the XO device to display the requested data.
   Retrieving the data may take several minutes. In this case, you can click **Stop** to stop data retrieval. You can then shorten the time frame or adjust the filters, and try again.

For examples of log data, see the sections further below.

24.5.3 Saving a Log

You can save a log file in text format (.txt) to your local hard disk. You can open the log files in any text editor, such as Notepad.

The file name indicates the type of log (log, event, command) and the timeframe. For example:
Command 2016-11-06 00-00-00 -- 2016-11-06 23-59-59.txt
This file contains the command log of November 6, 2016.

The first line of the log file contains the server's unit ID, the site name, the IP address, the type of log, and the timeframe:

```
0001 - FT2 MainBuilding (10.0.0.10): Command 2016-01-01 00-00-00 -- 2016-11-06 23-59-59
-------------------------------------------------------------------------------------------------------------------------------------------------------
| Time                | Id  | Group      | Command    | Data
| 2016/11/06 09:21:57 | C26 | transfer   | download   | camera definitions
| 2016/11/06 09:21:57 | C26 | transfer   | download   | user data
| 2016/11/06 09:21:56 | C26 | login      | user       | (00) => authorized
| 2016/11/06 09:21:56 | C26 | connection | open       | (10.0.0.2                )
| 2016/11/06 09:21:49 | C25 | connection | closed     | (10.0.0.2                )
...
```

To save a log, proceed as follows:

1. Choose **System** > **Maintenance** > **Log**.
2. Generate the desired log data.
3. Click **Save Log**.
4. Browse to the desired folder and click **Save**.

24.5.4 Example of a Log Record

Time	Type	User	Cam	Data
2017/10/01 13:34:51	Live video view	00	25	
2017/10/01 13:30:56	Live video view	01	25	
2017/10/01 13:26:57	Still image view	01	21	2017/10/01 12:20:45
2017/10/01 13:26:44	Recorded video view	01	21	2017/10/01 12:17:48 2017/10/01 13:25:36
2017/10/01 13:26:36	Still image view	01	21	2017/10/01 12:18:43
2017/10/01 13:25:40	Still image view	01	01	2017/10/01 13:25:36

You can click the column headers to sort the information alphabetically. The log record displays the following information:

Item	Description
Time	Date and time when the event occurred (started)
Type	View type (live video, recorded video…)
User	ID of the user that viewed the video
Cam	Number of the camera
Data	Additional information, for example the date/time of the still image.

24.5.5 Example of an Event Log

Time	Input/Output Behaviour	E	T	Quad ID	Camera mask
2017/10/01 13:20:11	I1036 - [REAL] - CAM01 MOTION3	+	Q		
2017/10/01 13:20:09	I3840 - [REAL] - INTRUDER garden	-	D	94614218989896554	0000000000000010
2017/10/01 13:20:09	I1080 - [REAL] - CAM02 PERIMETER	-	D	94614218989765481	0000000000000010
2017/10/01 13:20:09	I3840 - [REAL] - INTRUDER garden	+	D	94614218958242662	0000000000000010
2017/10/01 13:20:09	I1080 - [REAL] - CAM02 PERIMETER	+	D	94614218958242661	0000000000000010
2017/10/01 13:20:03	I1034 - [REAL] - CAM01 MOTION1	+	Q	94614218568631138	0000000000000001
2017/10/01 13:19:28	I3840 - [REAL] - INTRUDER garden	-	D	94614216271397727	0000000000000010

You can click the column headers to sort the information alphabetically. The event log displays the following information:

Item	Description
Time	Date and time when the event occurred
Input/Output Behaviour	Identification of the event: input/output number and name
E	Type of event: • +: start of the event • –: end of the event • R: repeated event
T	What the event has transmitted to the CMS (corresponds with the **Camera view style** as defined for the input/output): • **L**: Live video • **Q**: Quad alarm • **D**: Duress (live + quad) • **S**: System event, does not trigger a camera view.

Item	Description
Quad ID	Identification number of the quad images that the event generated.
Camera mask	The camera mask indicates the cameras associated with the input/output, as defined in the input/output behaviour. For camera 1, the first digit counting from the right = 1. For camera 3, the third digit counting from the right = 1. If both camera 1 and 3 are associated with the input, both the first and the third digit = 1 (always counting from the right). On a system with 16 video channels: 0000000000000101
ATX	Alarm transmission status: • **blank** = no transmission required • **OK** = transmission successful • **NOK** = transmission not successful.
Alarm Time	Date and time of the alarm
Alarm Dest.	Alarm destination = the IP address of the destination where the alarm was sent to.
Data	Extra information, for example the IP address of the PC that established a remote connection.

From the event log, you can display and save quad images that an event generated.

Note

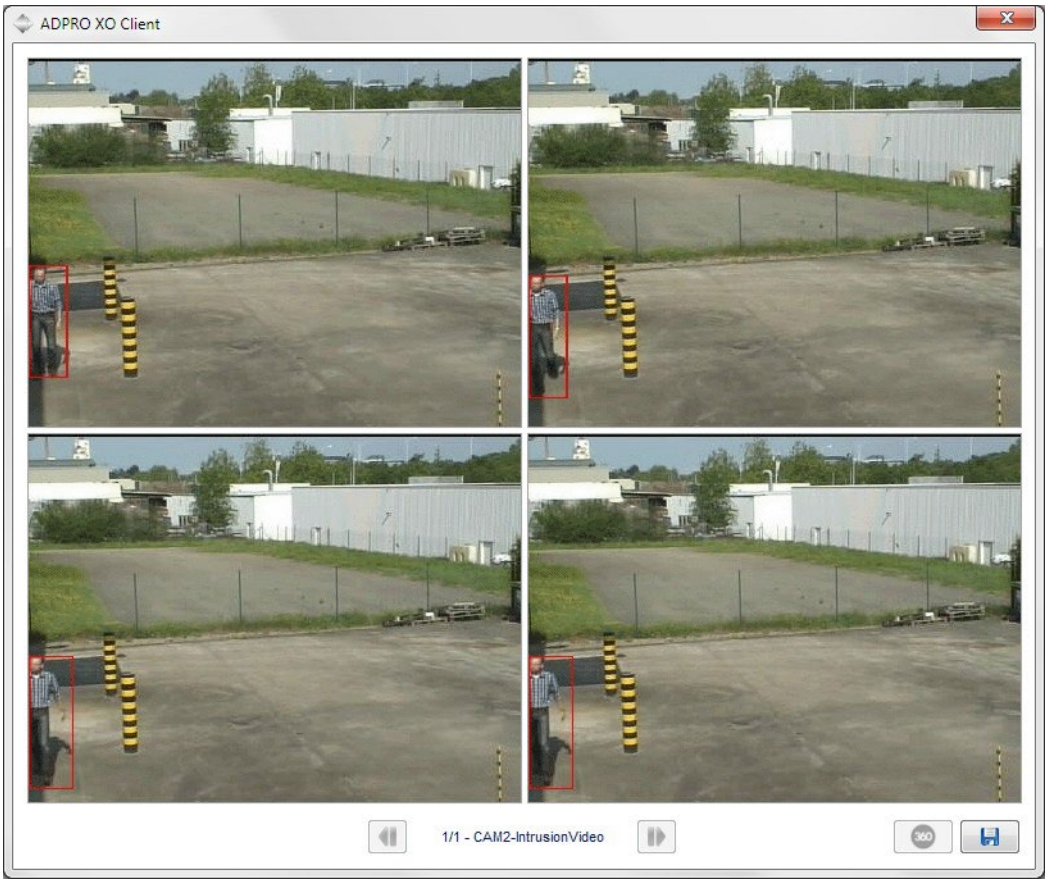
The system automatically cleans up the quad images. To find the quad ID and timestamp of the oldest quad imags that are still retrievable for your XO device, execute the **ta,lastquad** command in a Telnet session.

To display quad images from the event log, proceed as follows:

1. In the event log, click the desired event line that has quad images:

Time	Input/Output Behaviour	E	T	Quad ID	Camera mask
2017/10/01 13:20:11	I1036 - [REAL] - CAM01 MOTION3	+	Q		
2017/10/01 13:20:09	I3840 - [REAL] - INTRUDER garden	-	D	94614218989896554	0000000000000010
2017/10/01 13:20:09	I1080 - [REAL] - CAM02 PERIMETER	-	D	94614218989765481	0000000000000010
2017/10/01 13:20:09	I3840 - [REAL] - INTRUDER garden	+	D	94614218958242662	0000000000000010
2017/10/01 13:20:09	I1080 - [REAL] - CAM02 PERIMETER	+	D	94614218958242661	0000000000000010
2017/10/01 13:20:03	I1034 - [REAL] - CAM01 MOTION1	+	Q	94614218568631138	0000000000000001
2017/10/01 13:19:28	I3840 - [REAL] - INTRUDER garden	-	D	94614216271397727	0000000000000010

2. Click **Show quads**. The quad images appear.



3. Proceed as follows:
   - If more than one camera is associated with the event, use the  and  buttons to browse through the different cameras.
   - To save the currently displayed quad images, click . Browse to the desired storage folder and click **OK**. Repeat for images of different cameras.
4. Close the quad images screen to return to the event log.

24.5.6 Example of a Command Log

Time	Id	Group	Command	Data
2017/10/01 11:52:36	C06	transfer	download	camera definitions
2017/10/01 11:52:36	C06	transfer	download	user data
2017/10/01 11:52:36	C06	login	user	(00) => authorized
2017/10/01 11:52:36	C06	connection	open	(10.0.0.56)
2017/10/01 11:37:47	C05	connection	closed	(10.0.0.56)

You can click the column headers to sort the information alphabetically. The command log displays the following information:

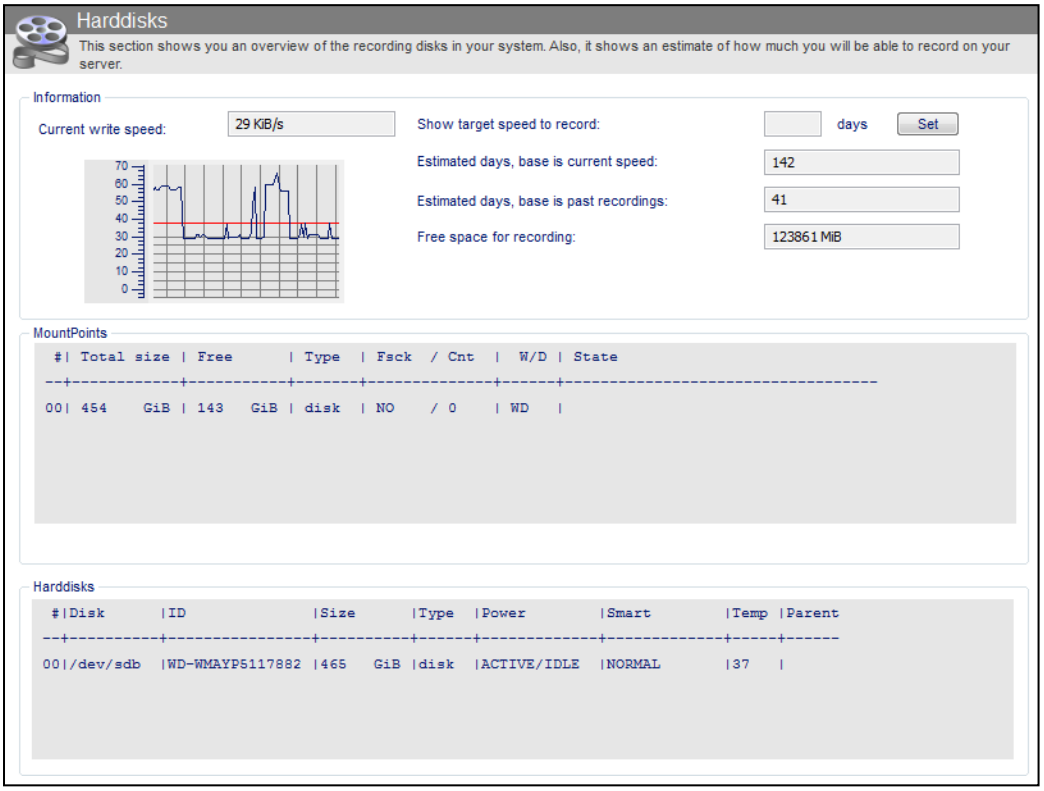
Item	Description
Time	Date and time when the command is executed
Id	Event identification: session type and session number: • **C** = client session • **T** = Telnet session All commands within the same session have the same ID.
Group	Command group

Item	Description
Command	Executed command
Data	Additional information (such as an IP address)

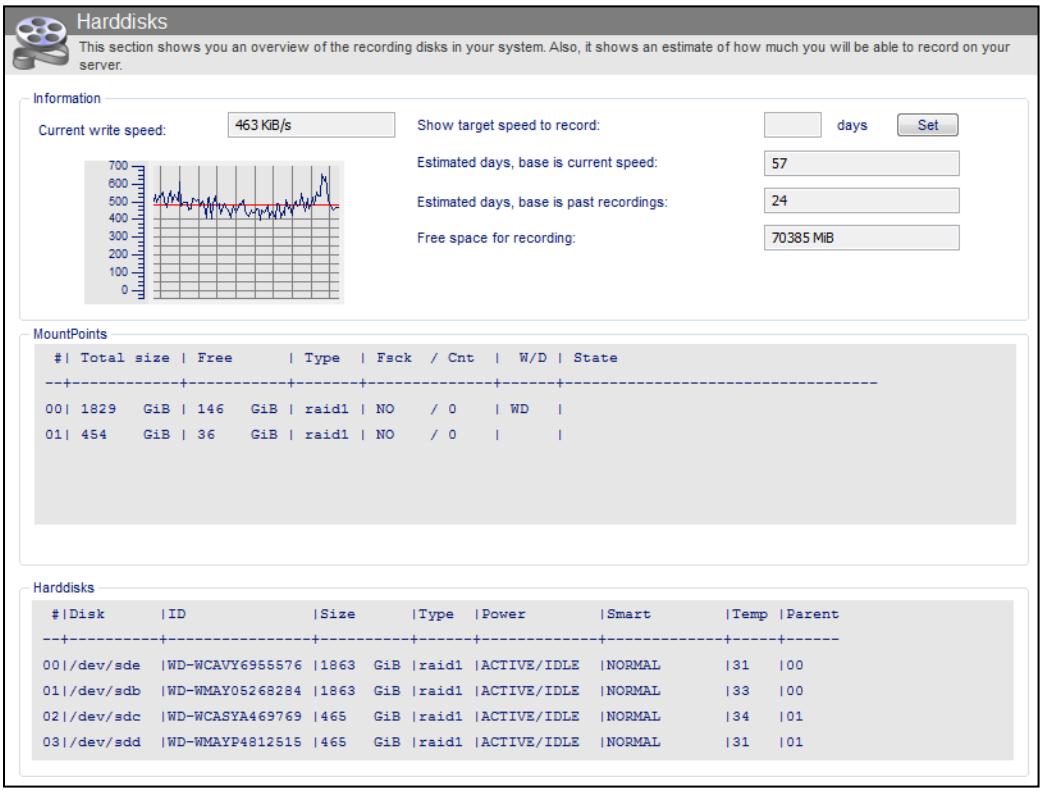
24.6 Hard Disks

24.6.1 Hard Disk Information

Recordings are stored on the available hard disks in the XO device. To display information about the hard disks and the available storage space, choose **System** > **Maintenance** > **Harddisks**. The example below shows a device with one hard disk.



The example below shows a device with 4 disks and RAID 1 (two mount points).



The **Harddisks** window displays the following information:

Item	Description
Information: general information about disk space availability.	
Current write speed	The current write speed in kilobytes per second. The actual write speed depends on video contents and may vary continuously. The horizontal red line in the graph indicates the average write speed.
Show target speed to record	This box is normally empty. You can use it for calculating the write speed based on a required number of days of recordings. For more information, see *Calculating the Write Speed* .
Estimated days, base is current speed	Estimated hard disk storage capacity based on the current measured write speed. This value is expressed in number of days.
Estimated days, base is past recording	Estimated hard disk storage capacity based on the existing footage stored on the hard disk. This value is expressed in number of days. If you set a minimum number of days for recording, make sure that value is lower than the estimated value displayed here.
Free space for recording	Remaining storage space for recording in MB.
MountPoints: overview of the writing disks that are in use. If you are using RAID 1, the hard disks are not identical to the writing disks. All physical hard disks used in a RAID 1 configuration represent one writing disk (one mount point).	
#	Sequence number of the mount point.
Total size	Total size in GB of the mount point.
Free	Free storage space in GB on the mount point.

Item	Description
Type	Disk type: • **disk**: normal writing disk. • **raid**: RAID 1 disk.
W/D	Indicates if the system is writing (**W**) and/or deleting (**D**) on the mount point.
State	Displays extra information about the state of the mount points; for example during disk optimisation when upgrading, or during RAID disk recovery: blank: this area is blank if the RAID disks are synchronised. **degraded**: indicates a faulty disk. If a disk is faulty, the system will active input 0016 - [SYST] - HARDDISK ERROR. **recovering**: indicates that the system is resynchronising the RAID disks after a faulty disk has been repaired. The system also indicates the progress of the recovery (in percentage). After a successful recovery, the column will indicate **no repair**.
Harddisks: overview of the physical hard disks in the XO device.	
#	Sequence number of the hard disk.
Disk	Device name of the hard disk (Linux).
ID	Serial number of the hard disk.
Size	Hard disk size in GB.
Type	Disk type: • **disk: normal writing disk.** • **raid: RAID 1 disk.**
Power	The power status column displays one of the following statuses: • **ERROR**: there is a problem retrieving the power status of the drive • **ACTIVE/IDLE**: drive operates normally • **STANDBY**: drive is in low power mode (drive is in spin-down status) • **SLEEPING**: drive is in lowest power mode (drive is completely shut down).
Smart	The smart status column displays one of the following statutes: • **ERROR**: drive is failing • **ALERT**: there is a problem retrieving SMART info from the drive, or the drive may be in the process of failing • **NORMAL**: no problems found with the drive.
Temp	Hard disk temperature in °C.
Parent	For RAID 1 disks: the sequence number of the parent disk (mount point).

24.6.2 Calculating the Write Speed

You can calculate the maximum average write speed for a required number of recording days. The average write speed has to be lower than the calculated value. If your average write speed is higher than the calculated value, you can adjust the following recording settings to obtain the desired number of recording days:

- The recording parameters for the individual cameras (recording frame rate, resolution, quality).
- The recording behaviour (what to record and when).
- The recording mode schedule (if using mode-based recording).

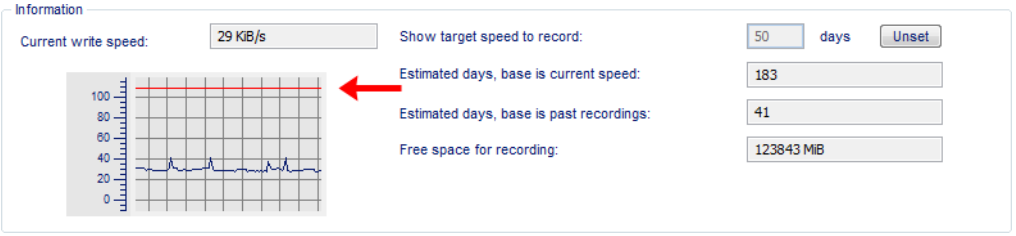


Note

The write speed calculation is an estimate only. Figures are purely indicative. The real requirements depend on actual scene content.

To calculate the write speed, proceed as follows:

1. Choose **System** > **Maintenance** > **Harddisks**.
2. Type the required number of days in the **days** box.
3. Click **Set**.
   The horizontal red line in the write speed graph moves to the calculated write speed.

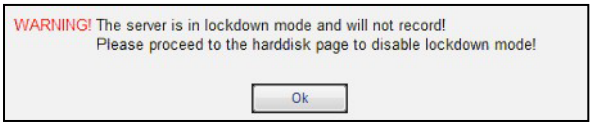


4. To stop the calculation, click **Unset**. After a few seconds, the horizontal red line displays the average write speed again.

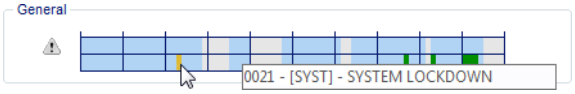
24.6.3 Hard Disk Lockdown Mode

If you have installed a used hard disk in an XO device running firmware version XOa 3.00 or above, and you did not format the hard disk, the XO device will automatically **lock the disk** (read-only). This prevents the system from erasing or overwriting recordings that may be present on the used disk. **Recording is not possible** until you unlock the disk.

The following warning appears when you open the client:



In the **Status** window, the system input 0021 – [SYST] – SYSTEM LOCKDOWN is active (yellow).



Caution!

When you unlock the disk for further recording, the system will delete recordings older than the maximum number of recording days.
Furthermore, depending on the original disk format, the system may start upgrading the disk when you unlock it. This may take a long time, and you may lose recordings.

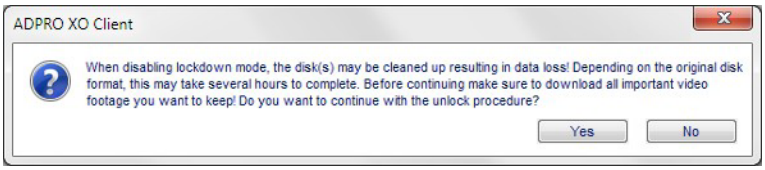
Back up the existing recordings first if necessary.

Honeywell strongly recommends that you **format used hard disks** to erase all existing recordings if you want to re-use a hard disk in a different device. For more information on used hard disks, see *Tech Tip #07 Recovering Recordings from Used HDDs* (29160).

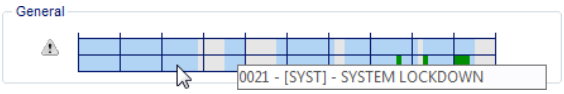
To unlock the used disk for further recording, proceed as follows:

1. Back up the necessary recordings first.
2. To unlock the hard disk, choose **System** > **Maintenance** > **Harddisks**.

3. Click **Disable lockdown** (button in the bottom right corner). The following warning message appears:



4. Click **Yes** to confirm.
   The device will resume recording. In the **Status** window, the system input 0021 – [SYST] – SYSTEM LOCKDOWN becomes inactive (blue).



Appendix A – Networks, Subnet Masks, and IP Addresses

If you want to use static routing, you have to provide the values for network and subnet mask in dot-decimal notation. A network administrator may give you values in a different notation, or just a range of IP addresses. In this case, you can calculate the required values yourself, using the information and examples provided. If you experience any issues connecting to a specific IP address, you can calculate if the IP address is in the network range or not.

A.1 The Basics

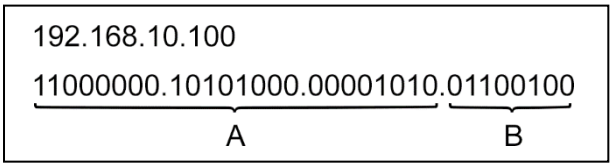
An IP address consists of 32 bits. For ease of reading (and typing), these bits are represented by 4 decimal numbers (0–255) separated by dots. This is the dot-decimal notation.

For example, the IP address 192.168.10.100 represents the following 32 bits:

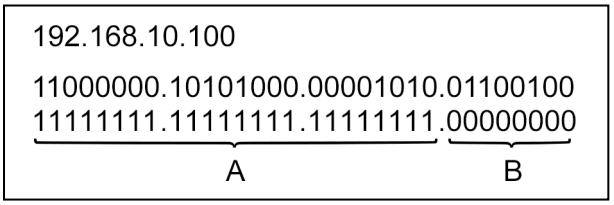
Decimal:	192	.	168	.	10	.	100
Binary:	11000000	.	10101000	.	00001010	.	01100100

Each IP address consists of two parts:

- The **first bits** make up the **network identifier** (**A** in the image below). This part is identical for each IP address in the same network.
- The **last bits** make up the **host identifier** (**B** in the image below). This part is unique for each IP address in the network.



The **subnet mask** defines how many bits are in the network identifier (the length of **A**, 24 in the example above). The subnet mask consists of 32 bits, just like an IP address, where a 1 indicates that the bit is part of the network identifier, and a 0 that the bit is part of the host identifier.



Often, the subnet mask is represented in dot-decimal notation just like an IP address. For example, a network mask that defines the first 24 bits as the network identifier starts with 24 times 1, followed by 8 times 0 (24+8 = 32 bits in total), which converts to the dot-decimal notation 255.255.255.0 as follows:

Binary:	11111111	.	11111111	.	11111111	.	00000000
Decimal:	255	.	255	.	255	.	0

In CIDR notation, the subnet is represented by a "/" followed by the number of bits in the network identifier. For example: 192.168.10.1**/24** indicates a network where the first 24 bits represent the network identifier. 192.168.10.1**/26** indicates a network where the first 26 bits represent the network identifier. For an overview of all possible subnet masks and their notations, see *Subnet Mask Notations* .

All hosts (devices) in the same network (= with IP addresses with identical network identifiers) can communicate directly with each other. Usually, devices also need to communicate with other devices in different networks (for example, the internet). The route between networks runs via **gateways**: these are routers that allow (or block) the route to other networks. Usually, the IP address of a gateway ends in '.1'.

A.2 Calculation Examples

Values Provided: 192.168.10.1/24

A network administrator gives you the following network information:
192.168.10.1/24

To know the subnet mask in dot-decimal notation, check the table in *Subnet Mask Notations* . '/24' corresponds with 255.255.255.0

To know the network identifier, first convert the given IP address into its binary notation:

IP address:	192	.	168	.	10	.	1
Binary:	11000000	.	10101000	.	00001010	.	00000001

The first 24 bits are the network identifier (/24). Take the first 24 bits from the IP address, and replace the remaining 8 bits by zeros. Then convert the resulting values back to dot-decimal notation:

Binary:	**11000000**	.	**10101000**	.	**00001010**	.	00000000
Decimal:	192	.	168	.	10	.	0

Values to use in the XO client:

- Network: 192.168.10.0
- Subnet mask: 255.255.255.0

This network covers all IP addresses ranging from 192.168.10.0 to 192.168.10.255. This is calculated as follows. The last 8 bits (= 32 – 24) are free, ranging from 00000000 to 11111111. This converts into the following IP address range (network identifier followed by host identifier):

First, binary:	**11000000**	.	**10101000**	.	**00001010**	.	00000000
Decimal:	192	.	168	.	10	.	0
Last, binary:	11000000	.	**10101000**	.	**00001010**	.	11111111
	192	.	168	.	10	.	255

Values Provided: 192.168.10.1/26

A network administrator gives you the following network information:
192.168.10.1/26

To know the subnet mask in dot-decimal notation, check the table in *Subnet Mask Notations* . '/26' corresponds with 255.255.255.192

The first 26 bits are the network identifier (/26). Take the first 26 bits from the IP address, and replace the remaining 6 bits by zeros. Then convert the resulting values back to dot-decimal notation:

IP address:	192	.	168	.	10	.	1
Binary:	11000000	.	10101000	.	00001010	.	00000001
Network binary:	**11000000**	.	**10101000**	.	**00001010**	.	**00**000000
Decimal:	192	.	168	.	10	.	0

Values to use in the XO client:

- Network: 192.168.10.0
- Subnet mask: 255.255.255.192

This network covers all IP addresses ranging from 192.168.10.0 to 192.168.10.63. This is calculated as follows. The last 6 bits (= 32 – 26) are free, ranging from 000000 to 111111. This converts into the following IP address range (network identifier followed by host identifier):

First, binary:	**11000000**	.	**10101000**	.	**00001010**	.	**00**(00000
Decimal:	192	.	168	.	10	.	0
Last, binary:	11000000	.	**10101000**	.	**00001010**	.	**00**· 11111
Decimal:	192	.	168	.	10	.	63

IP Range Provided: 192.168.4.0–192.168.4.100

If you receive a range of IP addresses of cameras to add via static routing, you can calculate the network and subnet mask as follows. For example, for the range:
192.168.4.0–192.168.4.100

First, convert the IP addresses to their binary notation:

Decimal:	192	.	168	.	4	.	0
Binary:	11000000	.	10101000	.	00000100	.	00000000
Decimal:	192	.	168	.	4	.	100
Binary:	11000000	.	10101000	.	00000100	.	01100100

Next, see how many bits on the left are identical in both IP addresses. In this case, the first 25 bits are identical (indicated in **bold** below). They make up the network address. The subnet mask then consists of 25 times 1 followed by 7 times 0.

Start address:	**11000000**	.	**10101000**	.	**00000100**	.	**0**(000000
End address:	**11000000**	.	**10101000**	.	**00000100**	.	**0**· 100100
Network (identical part):	**11000000**	.	**10101000**	.	**00000100**	.	**0**› xxxxxx
Subnet mask:	11111111	.	**11111111**	.	**11111111**	.	**1**(000000

Now you will convert the network address and subnet mask to the decimal notation for entering in the XO client. First, add zeros to the 25 leading bits of the network address to make up 32 bits. Then convert each group of 8 bits to its decimal value.

Network, binary:	**11000000**	.	**10101000**	.	**00000100**	.	**0**00(0000
Network, decimal:	192	.	168	.	4	.	0
Subnet mask, binary:	**11111111**	.	**11111111**	.	**11111111**	.	**1**00(0000
Subnet mask, decimal:	255	.	255	.	255	.	128

To enter in the the XO client:

- Network = 192.168.4.0
- Subnet mask = 255.255.255.128

This will appear as 192.168.4.0/25.

Note that these settings include all IP addresses from 192.168.4.0–192.168.4.**127**, which is a slightly larger range than the indicated 192.168.4.0–192.168.4.**100**. Due to the structure of network address and subnet mask, only certain ranges of IP addresses can be defined as a network.

If you are confused, always go back to the binary notation of the IP addresses. The first 25 bits are fixed, the last 7 bits are free. The first possible IP address in the network ends in 000000 (7 zeros), and the last possible address ends in 1111111 (7 ones). If you convert these binary values into decimals, the results are:

First possible address:	**11000000**	.	**10101000**	.	**00000100**	.	**0**000 0000
Decimal:	192	.	168	.	4	.	0
Last possible address:	**11000000**	.	**10101000**	.	**00000100**	.	**0**111 1111
Decimal:	192	.	168	.	4	.	127

A.3 Subnet Mask Notations

The table below provides an overview of the possible subnet masks in CIDR and dot-decimal notations:

CIDR	Decimal	CIDR	Decimal
/32	255.255.255.255	/15	255.254.0.0
/31	255.255.255.254	/14	255.252.0.0
/30	255.255.255.252	/13	255.248.0.0
/29	255.255.255.248	/12	255.240.0.0
/28	255.255.255.240	/11	255.224.0.0
/27	255.255.255.224	/10	255.192.0.0
/26	255.255.255.192	/9	255.128.0.0
/25	255.255.255.128	/8	255.0.0.0
/24	255.255.255.0	/7	254.0.0.0
/23	255.255.254.0	/6	252.0.0.0
/22	255.255.252.0	/5	248.0.0.0
/21	255.255.248.0	/4	240.0.0.0
/20	255.255.240.0	/3	224.0.0.0
/19	255.255.224.0	/2	192.0.0.0
/18	255.255.192.0	/1	128.0.0.0
/17	255.255.128.0	/0	0.0.0.0
/16	255.255.0.0		

Appendix B – Abbreviations

3G: third generation

4G: fourth generation

A: ampere

AGC: automatic gain control

AHCI: Advanced Host Controller Interface

APN: Access Point Name

ATD: adaptive threshold determination

A/V card: audio/video card

AWG: American wire gauge

BIOS: basic input output system

BNC: Bayonet Neill–Concelman

Cam: camera

CBR: constant bitrate

CD: compact disk

CHAP: Challenge-Handshake Authentication Protocol

CIDR: Classless Inter-Domain Routing

CIF: common intermediate format

CMS: central monitoring station

CPU: central processing unit

DCE: data circuit-terminating equipment

DCIF: double CIF

DEOL: dual end of line

/dev/ttyU1: USB input 1

DHCP: Dynamic Host Configuration Protocol

DIN: Deutsches Institut für Normung (German national organisation for standardisation)

DNS: domain name system

DOM: disk-on-a-module

DP: DisplayPort

DTC: down the coax

DTE: data terminal equipment

DVD: digital video disk

DVI-I: Digital Visual Interface (digital and analogue)

EIO: Extension I/O

EMS: Event Management System

eth: Ethernet interface

fps: frames per second

ft: foot/feet

FTDI: Future Technology Devices International

FTP: file transfer protocol

GB: gigabyte

GDI: Graphics Device Interface

GHz: gigahertz

GND: ground

GUI: graphical user interface

HD: high definition

HDD: hard disk drive

HPET: High Precision Event Timer

HTTP: hypertext transfer protocol

Hz: Hertz

IC: interconnection

ID: identifier

I/O: input/output

IP: internet protocol

ISDN: Integrated Services for Digital Network

IT: Information Technology

jpg: Joint Photographic Experts Group

kbps: kilobits per second

kB: kilobyte

LAN: local area network

LED: light emitting diode

m: metre

mA: milliampere

MAC: Media Access Control

MB: megabyte

Mbps: megabits per second

MIC: microphone

MIO: Main I/O

mm: millimetre

MS-CHAPv1/MS-CHAPv2: Microsoft Challenge-Handshake Authentication Protocol, version 1/2

NAT: network address translation

NC: normally closed

NEOL: no end of line

NO: normally open

NTFS: new technology file system

NTP: network time protocol

NTSC: National Television System Committee

OS: operating system

OSD: on screen display

OTB: on the box

PAL: Phase Alternating Line

PAP: password authentication protocol

PC: personal computer

PCI: peripheral component interconnect

pF: picofarad

PIN: personal identification number

PIR: passive infrared

PoE: power over Ethernet

PPP: point-to-point protocol

PSTN: public switched telephone network

PTZ: pan tilt zoom

QCIF: quarter CIF

QSIF: quarter SIF

RAID: redundant array of independent disks

RH: relative humidity

RTP: real-time transport protocol

RTSP: real-time streaming protocol

SATA: serial ATA

SDK: software development kit

SEOL: single end of line

SIF: source input format

SIM: subscriber identity module

SMART: Self-Monitoring, Analysis, and Reporting Technology

SMTP: Simple Mail Transfer Protocol

SP: Service Pack

SPDT: single pole double throw

SPK: speaker

SVGA: Super Video Graphics Array

SXGA: Super Extended Graphics Array

Sync: synchronisation

TB: terabyte

TCP: transmission control protocol

TLS: transport layer security

TX: transmission

UDP: user datagram protocol

USB: Universal Serial Bus

VAC: voltage alternating current

VBR: variable bitrate

VCP: VideoCentral Platinum

VDC: voltage direct current

VGA: Video Graphics Array

Vp-p: voltage peak-to-peak

W: watt

W x H x D: width x height x depth

XGA: eXtended Graphics Array

YUV: colour space with separate luminance (brightness) and chrominance (colour) components