ADPRO iFT Series

Hardware Installation Manual

January 2021
Doc. 27817_09
Firmware version XO 5.1

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, Xchange, 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

Environmental Information



The crossed-out wheeled bin means that within the European Union the product must be taken to separate collection at the product end of life. This applies to the device but also to any accessories marked with this symbol. Do not dispose of these products as unsorted municipal waste.

If you need more information on the collection, reuse, and recycling systems please contact your local waste administration. You can also contact us for more information on the environmental specifications of our products.

Contents

1 Technical Specifications **7**

2 About iFT Series **9**

2.1 Models 9
2.2 Licenses 9
2.2.1 Overview 9
2.2.2 System License 10
2.3 Software 10
2.4 Parts Information 10

3 Hard Disks **11**

3.1 Required Hard Disk Capacity 11
3.2 Adding/Replacing a Hard Disk 11
3.3 Reusing Used Hard Disks 12
3.4 Retrieving Hard Disk Information 12
3.4.1 Using the ta,smart Command 12
3.4.2 Using the XO Client Software 13
3.5 Installing the First Hard Disk 13
3.6 Installing a Second Hard Disk 16
3.7 Installing a Third Hard Disk 20
3.8 Installing a Third and Fourth Hard Disk 22
3.9 Setup Self-Encrypting Drive 26
3.9.1 Using SED as a standard drive 26
3.9.2 Taking ownership of an SED by the XO server 27
3.9.3 The XO server has SEDs owned by another XO server 29
3.9.4 Change the password of an owned SED 30
3.9.5 Reset an owned SED back to factory settings 31
3.10 RAID 1 Support 33
3.10.1 About RAID 1 33
3.10.2 Activating RAID 1 34
3.10.3 Retrieving RAID 1 Information 35
3.11 Remote Formatting of Hard Disks 35

4 Front LED Indicators **37**

5 Motherboards **38**

5.1 BIOS Settings 38
5.1.1 Overview 38
5.2 Connectors 39
5.3 Replacing the Motherboard 40
5.4 Replacing the Motherboard Battery 41

6 Connecting IP Cameras **43**

7 Main I/O Card **45**

7.1 Features 45
7.2 Connection of Inputs and Outputs 45
7.2.1 Overview of Inputs and Outputs 45
7.2.2 Input Circuits 46
7.2.3 Connecting Inputs and Outputs 47
7.2.4 Cable Strain Relief 47
7.3 Configuring the MIO Card 47

8 XO I/O Interface USB Modules **48**

8.1 About the XO I/O Interface USB Modules 48
8.2 Logging on to the Hardware Configuration Tool 49
8.3 Mapping I/O Interface USB Modules to the XO Device 52

8.4 Resetting the Hardware Mapping 54
8.5 About the XO Gateway I/O USB Module 54
9 Network I/O Units (Net I/O) 55
10 Monitor 56
11 Modem 57
12 4G Via Wingle 58
13 Audio 59
13.1 Audio IN 59
13.2 Audio OUT (Talkback) 59
13.2.1 Options 59
13.2.2 Setup for VM22A 60
13.2.3 Setup for VM22E 62
13.2.4 Troubleshooting Talkback 62
13.3 Using IP Audio Devices 64
14 Connecting PIR Detectors 65
14.1 Required PIR Firmware 65
14.2 Connecting PIR Detectors 65
14.3 PIR Address Range 65
14.4 Direct Connection to the MIO Card 65
14.5 Connection via the USB-to-RS-485 8-Channel Distribution Unit 67
14.6 Connection via the USB-to-Serial-Port RS-485 Converter 69
14.7 Connection via the IFM-485-ST Interface Module 69
14.8 Connection via IP Modules (PRO E-IPM) 70
14.8.1 Summary 70
14.8.2 Setting up the IP Modules 70
14.8.3 Connecting the IP Modules to the PIR Detectors 75
15 Power Consumption 76
16 Retrieving the IP Address 77
17 Diagnostics 78
17.1 Log Files and Reports 78
17.2 Retrieving Log Files 78
17.3 Retrieving Reports 80
18 Web Pages 82
19 Maintenance 83
20 Full Reset by Flashing the DOM 84
20.1 Flashing the Image File to the DOM 84
20.2 After a Full Reset 86
21 Product Labelling 87
21.1 Product Number Structure 87
21.2 Declaration of Conformity 88
Appendix A – Abbreviations 89

1 Technical Specifications

Operating system	ADPRO® XO™ Security Operating System, Linux based
Video input	iFT: 1–32[1] IP cameras iFT-E: 1–32 IP cameras
Video output	XGA – Multiple matrix type views
Video compression	H.264/H.265 (H.265 supported with Hikvision, Honeywell, ONVIF, and generic driver)
Video resolution	Up to HD/MP[2] resolution **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).
Frames/second	Full HD @25/30 fps – MPixel: fps is camera dependent.
Bandwidth capacity (video)	32 x 5 Mbps
Bandwidth management	Configurable variable or constant bitrate / Configurable bandwidth limiter
Audio input	Built-in audio input supported[2]
Audio output	Standard 1 line level output. Optional: up to 1 per camera via audio switcher(s). Audio out on IP cameras[2] with ONVIF or brand-specific driver.
Command inputs	• Standard on-the-box: 8 inputs (monitored) • With optional EIO card installed: 20 inputs (monitored) • With external XO I/O Interface USB module: + 20 additional inputs (monitored) • Via Net I/O with PoE: up to 128 inputs (monitored or unmonitored) **Note** The PH10LU and PH10FEU motherboards have similar I/O support.
Relay outputs	• Standard on-the-box: 4 outputs (SPDT) • With optional EIO card installed: 8 outputs (SPDT) • With external XO I/O Interface USB module: + 8 additional outputs (SPDT) • Via Net I/O with PoE: up to 128 outputs (SPDT)
Web server	XO client – integrated web client application (ActiveX)
Ethernet	2 x 100/1000BASE-T, autodetection, full duplex, RJ45
Recording type	Schedule / Detection / Event
IP camera integration	Brand specific, generic, or ONVIF[2] driver
Management	• Web client interface (XO client) • ADPRO VideoCentral Platinum • Event Management Software (EMS) • third-party software (SDK available) • iOS/Android iTrace app.

[1] Using 32 IP channels/16 analytics channels on the iFT requires a new system license. See *Field Alert #7 – Upgrading to 32 Channels* (29477).
[2] Camera dependent. For an overview of compatible IP cameras, see the *Supported IP Camera List* (26742).

Power supply	100–240 VAC, 50/60 Hz, 2.5–1.5 A **Note** You must connect the video system to a 100–240 VAC/16 A mains outlet with proper earthing, applying a separate, locally approved power cord.
Operating temperature	5–40 °C
Humidity	20–93 % RH (non-condensing); indoor use only
Disk capacity	iFT: max. 4 x 14 TB SATA hard disks. iFT-E: max. 4 x 14 TB SATA hard disks. RAID 1 support (requires min. 2 equal HDDs).
Warranty	2 years
Dimensions (W x H x D)	441 x 88 x 305 mm (17.36" x 3.46" x 12.00")
Analytics	Basic motion detection (VMD), camera sabotage detection. Up to 16 (iFT) or 32 (iFT-E) analytics channels for IntrusionTrace™ and LoiterTrace™
Mobile apps	iTrace, iPIR, and iCommission
Performance as NVR	Under the following conditions: • NVR is replaced by a XO device • The site is using only single stream Full HD (1080p/25fps) IP cameras • XO is using only the generic driver Expected performance: • Maximum 5 cameras on iFT platforms with PH10LU motherboard • Maximum 6 cameras on iFT platforms with PH10FEU motherboard
Ordering information	Please contact your local ADPRO provider for detailed product information.

2 About iFT Series

Note

You can find the latest versions of this document and any referenced document on the Security Solutions Support site www.xtralissecurity.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.

2.1 Models

The iFT Series currently consists of the following models:

- iFT: up to 32 IP channels and up to 16 analytics channels via trade-off
- iFT-E: up to 32 IP channels and 32 analytics channels.

On the iFT model, you trade in 1 video channel for 1 analytic channel (balancing mode). This means, for example, that if you need 1 analytic channel, you can use maximum 31 (= 32 – 1) video channels. If you need 2 analytic channels, you can use 30 video channels, and so on. A fully equipped iFT can use maximum 16 analytic channels with 16 (= 32 - 16) video channels.
For optimal performance, disable the monitor output when using more than 16 IP channels on an iFT.

Note

The most recent iFT models come with a system license that supports 32 IP channels. The system license in older systems supports only 16 IP channels. You can upgrade your system license, free of charge, using Xchange. For instructions, see *Field Alert #7 – Upgrading to 32 Channels* (29477).

Note

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

Multi-site configuration is possible:

- Integration of up to 10000 XO devices
- Remote video and audio, live video, and consultation of recordings
- Compatible with S3100, VCP, and M3000
- SDK for third-party integration.

2.2 Licenses

2.2.1 Overview

All XO devices require licenses:

- System license
- IP video channel licenses
- (Optional) PIR interface license (PIR-HLI)
- (Optional) Analytic application licenses: IntrusionTrace and LoiterTrace.

2.2.2 System License

The system license defines the maximum number of video channels allowed, and the maximum number of analytic channels allowed on your system.

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.

For more information on licenses, see the *XO Client Software User Manual* (21796) and the *Xchange Tool User Manual* (27816).

2.3 Software

Honeywell regularly provides software updates for your XO device, which you can easily download and install via the Xchange tool. For more information, see the *Xchange Tool 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 www.xtralissecurity.com (listed under Field Alerts). Also check the Release Notes (listed under Product Release) for information on solved bugs or known issues.

2.4 Parts Information

Please use the reference numbers in this document (for example #17434080) for ordering parts, or for identifying the correct required part. If a part is indicated by a reference number ending in an asterisk (for example #1729121*), this indicates that several variants exist for the part (for example reference numbers #17291210 and #17291211). These variants are interchangeable. Any variant is suitable for the task described.

3 Hard Disks

3.1 Required Hard Disk Capacity

As there are many configuration possibilities, Honeywell has a hard disk space calculator available. You can find this hard disk space calculator on the Security Solutions Support site www.xtralissecurity.com (logon required). Search for keyword 'calculator'.

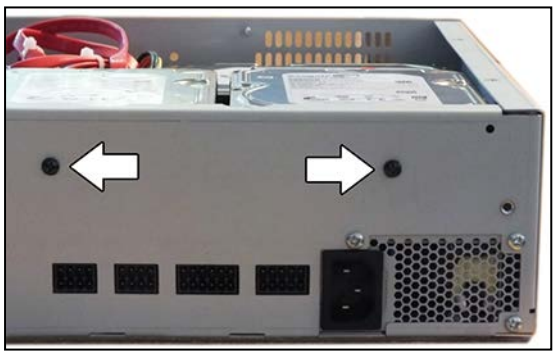
Note

The calculator is an estimating tool only. Figures are purely indicative. The real requirements of the hard disk capacity depend on scene content.

With firmware XO 4 and above, you can specify a minimum number of days to keep recordings on the hard disks. 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 hard disk space based on the past recordings. For details, see the *XO Client Software User Manual* (21796).

The iFT Series devices are standard delivered without, or with 1 hard disk inside. You can install:

- In the iFT model:
  - maximum 2 hard disks in models without extra mounting holes in the rear
  - maximum 4 hard disks in models with two extra mounting holes in the rear. The labels on the suitable iFT devices indicate '4 HDD Ready'.



- In the iFT-E model:
  - Model numbers 61xxxxxx: maximum 2 hard disks.
  - Model numbers 63xxxxxx: maximum 4 hard disks.

3.2 Adding/Replacing a Hard Disk

If the system is running out of disk space, you can add a new hard disk without removing any of the hard disks in use.
If you receive error messages from your hard disk in the **Status** screen of the XO client, you may need to replace the faulty hard disk.

Use these reference numbers to place your order with Honeywell:

HDD capacity	Reference number	
	Disk only	Disk with mounting kit for ADPRO device
1 TB	19150240	39544250
2 TB	19150250	39544260

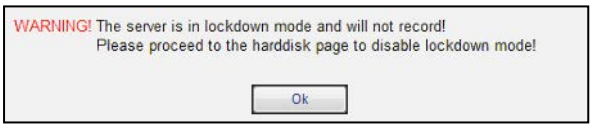
HDD capacity	Reference number	
	Disk only	Disk with mounting kit for ADPRO device
4 TB	19150270	39544262
6 TB	19150280	39544263
8 TB	19150290	39544264
10 TB	19150300	39544266
12 TB	19150310	39544570
14 TB	19150320	39544580

Note

Not all hard disks are compatible with all firmware versions. Upgrade your device to firmware version XO 4.5 or above for full compatibility.

3.3 Reusing Used Hard Disks

It is possible to mount a hard disk coming from another device into a new device. However, you must **format the used hard disk** to erase all data on the disk to prevent any conflicts or data damage. In addition, if you install a used disk in an XO device that runs firmware version XOa 3.00 or above, the system may enter the **hard disk lockdown mode**: recording is then not possible. The following message will appear:



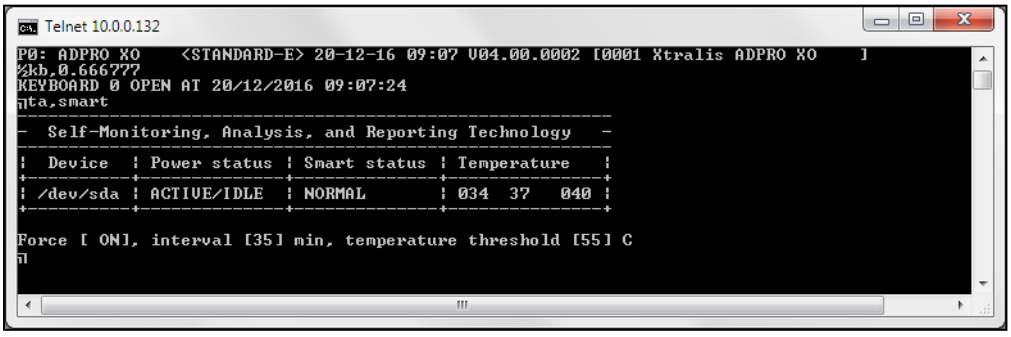
If you want to install a disk from another device, and you need to recover the recordings that are on the used disk, follow the instructions in the Tech Tip *Recovering Recordings from Used HDDs* (29160).

3.4 Retrieving Hard Disk Information

You can retrieve hard disk information and identify possibly faulty hard disks using the Telnet **ta,smart** command, or using the XO client software.

3.4.1 Using the ta,smart Command

SMART stands for Self-Monitoring Analysis and Reporting Technology. Execute the **ta,smart** command in a Telnet session to obtain the SMART information for all hard disks in the XO device.

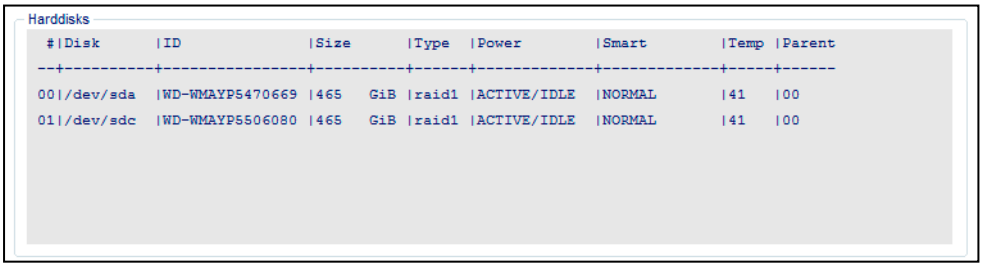


The screen displays the following information:

Item	Description
Device	Device name of the hard disk (Linux).
Power status	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 status	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.
Temperature	The temperature column displays from left to right: • the minimum temperature of the disk • the current temperature of the disk • the maximum temperature of the disk.
Force	• **ON**: SMART is checked on disk in STANDBY or SLEEPING mode. • **OFF**: SMART is only checked on disks in ACTIVE/IDLE mode.
Interval	Indicates the interval (in minutes) between SMART checks.
Temperature threshold	If the disk temperature is higher than the temperature threshold, the system activates system input 0102 – [SYST] – SMART HDD ALERT TEMP.

3.4.2 Using the XO Client Software

To obtain to obtain the (SMART) information for all hard disks in the XO device in the XO client, choose **System** > **Maintenance** > **Harddisks**. The **Smart** column shows the operational status of the hard disks; the **Temp** column indicates the temperature.



3.5 Installing the First Hard Disk

Note

If you need to install 2 or more hard disks, follow the instructions in *Installing a Second Hard Disk* on page 16 instead.

Material required for the first hard disk:

Part	Amount + reference number
Disk screws	4 x #17434080
SATA cable	1 x #16520877

Caution!

- Before installing hard disks, stop the device. Switch it off and unplug the power cord.
- Take all necessary precautions to prevent static discharges that may damage the device: use an anti-static wristband, an anti-static mat…
- The procedure below assumes that you are using a **new disk**, or, in case of a used disk, that you will **format the used disk** and erase all recordings on it. If you want to install a used hard disk while keeping the recordings on it, follow the instructions in the Tech Tip *Recovering Recordings from Used HDDs* (29160).

To install the first hard disk, proceed as follows:

1. Stop the device, switch off the power supply, and then remove the top cover: unscrew 2 screws at the front, 4 at the top, and 3 at the back.





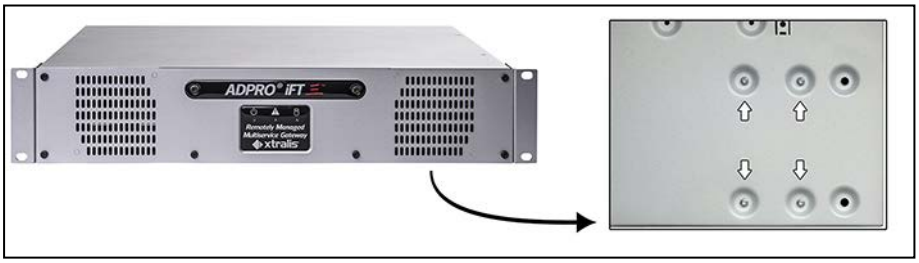
2. Fix the hard disk to the bottom of the casing.

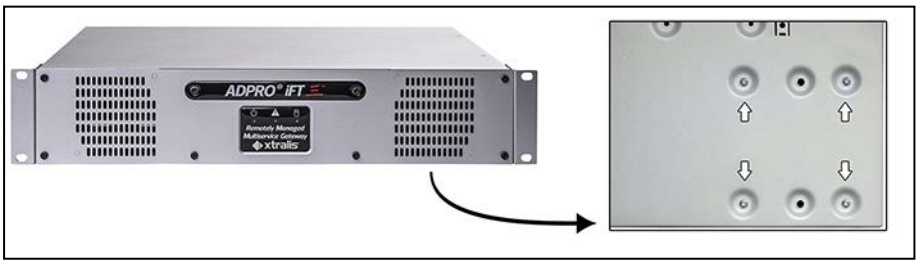
Caution!

If you tilt the casing, rest it carefully on the sides, but not on the back. You may damage the connectors if you do.

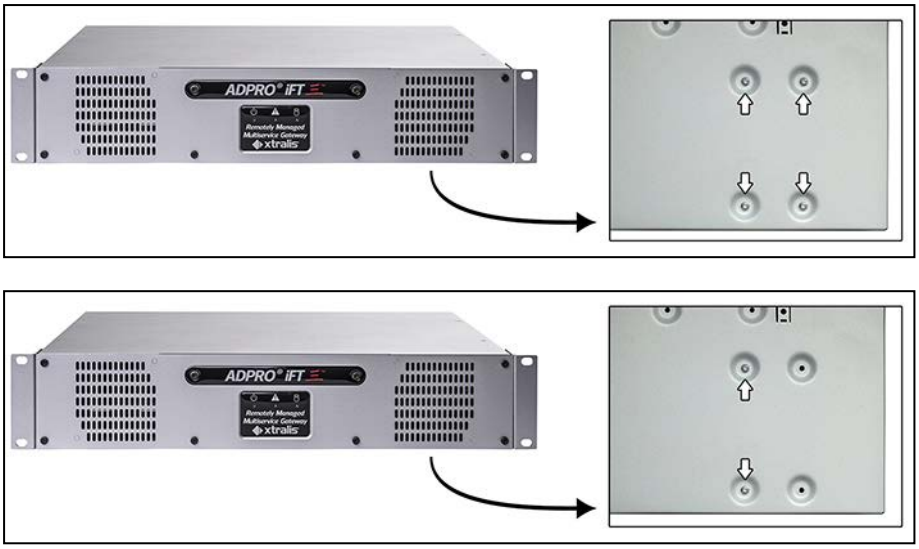
Depending on the available holes in the casing and the hard disk, the following options exist:

- Casing with **6 screw holes** in the bottom: use the first 4 holes, or the outer 4 holes with 4 disk screws (#17434080):





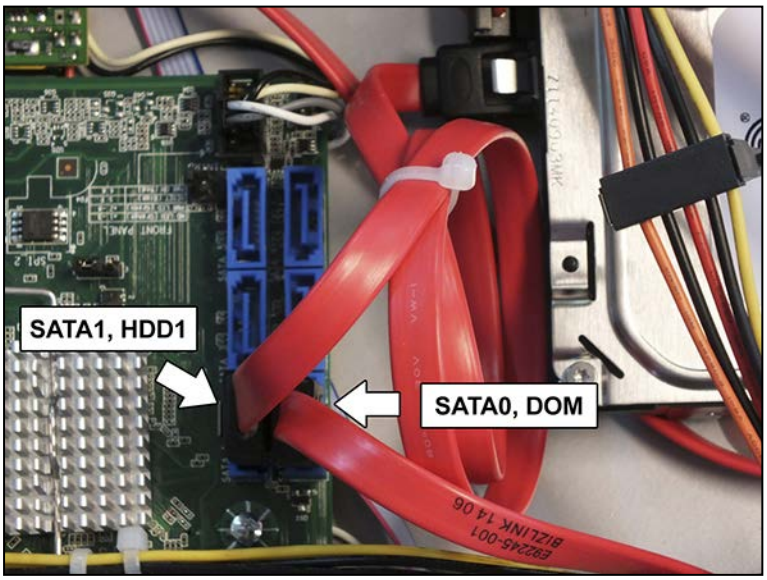
- Old casing with **4 screw holes** in the bottom: use 4 or only 2 disk screws (#17434080):

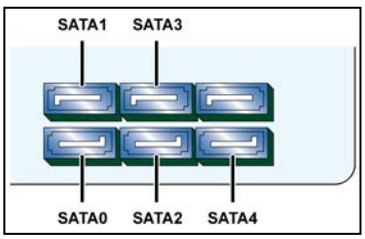


3. Connect the hard disk to the power supply.



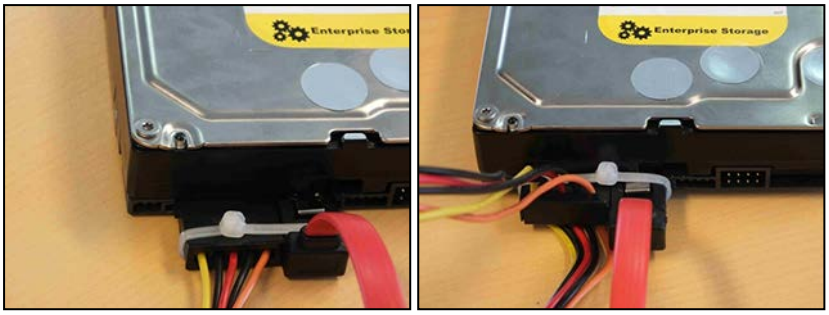
4. Connect the disk to the SATA1 connector on the motherboard with the SATA cable (#16520877).





The SATA cables must not be bent too sharply to prevent cable damage.

5. If the SATA cables do not have a locking mechanism, use tie-wraps to secure the cables on the disk(s) in the following way:



6. If there are unused cables left, bundle them with tie-wraps.
7. Place the top cover back: fix it with 2 screws at the front, 4 at the top, and 3 at the back.
8. Connect a monitor/screen and keyboard to the device. Switch on the power supply and wait for the boot window to appear.
9. Select **XO Installer** and press **Enter**.

> **Note**
>
> The boot window only appears for a few seconds, then the device continues booting. To make sure that you do not miss it, press the arrow keys on the keyboard repeatedly while the device is booting. The device will then stop at the boot window, and this gives you time to select and open the **XO Installer** menu.

10. Choose **Update current system** > **Manage recording disks**.
11. Select the newly installed hard disk in the list and press Enter.

> **Note**
>
> SEDs (self-Encrypting Drives) are supported since XO 5.0. For details, see *Setup Self-Encrypting Drive* on page 26.

12. Choose **Format and use selected disks** (using the tab key). The system formats the selected hard disk.
13. When formatting is finished, choose **Main Menu**, and then choose **Reboot**.

The device now restarts. After restarting, the installed hard disk is ready for use.

3.6 Installing a Second Hard Disk

Material required for the second hard disk:

Part	Amount + reference number
Disk screws	8 x #17434080
SATA cable	1 x #16520877
iFT(-E) HDD bracket	1 x #17011890
iFT(-E) HDD bracket, L-shaped[1]	1 x #17011895

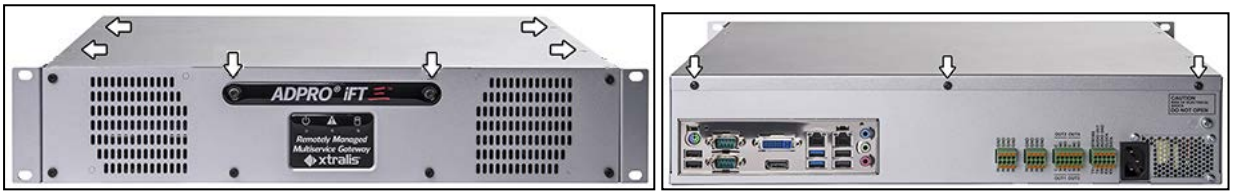
[1] The L-shaped bracket is required if you install more than 2 disks. If you will use only 2 disks, you can use 2 'flat' HDD brackets (#17011890).

Caution!

- Before installing hard disks, stop the device. Switch it off and unplug the power cord.
- Take all necessary precautions to prevent static discharges that may damage the device: use an anti-static wristband, an anti-static mat…
- The procedure below assumes that you are using a **new disk**, or, in case of a used disk, that you will **format the used disk** and erase all recordings on it. If you want to install a used hard disk while keeping the recordings on it, follow the instructions in the Tech Tip *Recovering Recordings from Used HDDs* (29160).

To install a second hard disk, proceed as follows:

1. Stop the device, switch off the power supply, and then remove the top cover: unscrew 2 screws at the front, 4 at the top, and 3 at the back.

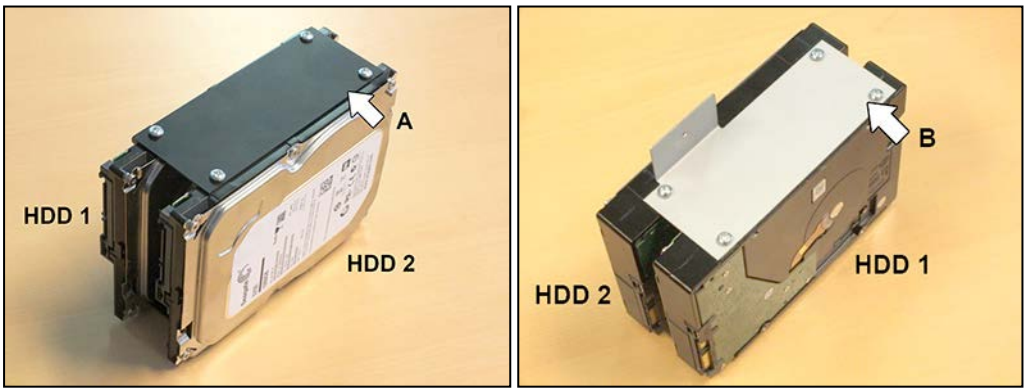


2. If the first disk is already installed, you have to remove it first: unplug its power and data cables, and unscrew it from the bottom of the casing.

Caution!

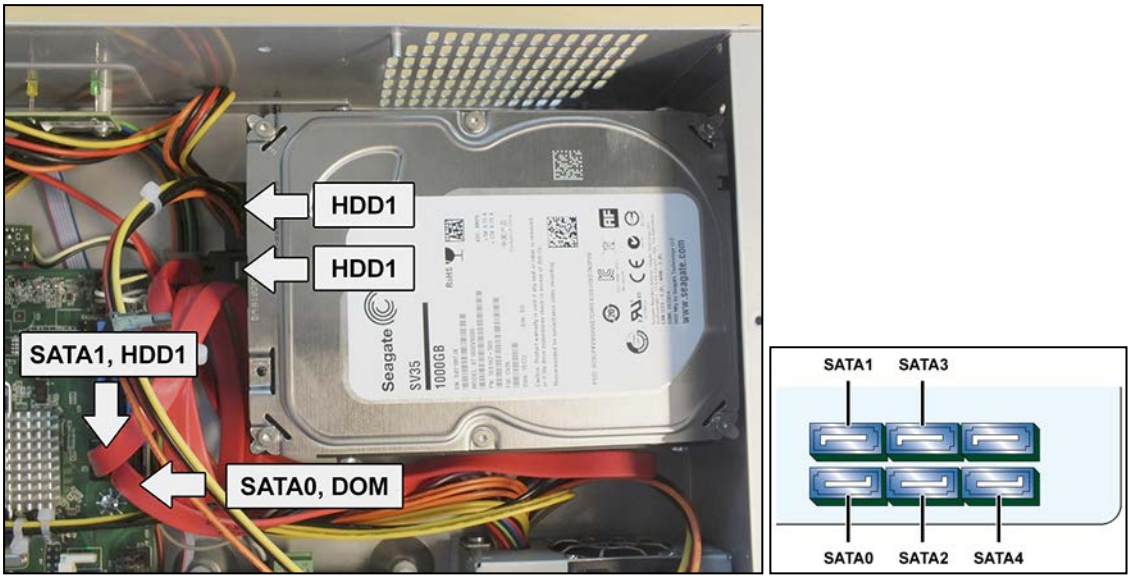
If you tilt the casing, rest it carefully on the sides, but not on the back. You may damage the connectors if you do.

3. Fix the first and second hard disk together using the 2 hard disk brackets (#17011890 and #17011895) and 8 screws (#17434080) as shown below. Make sure that the mounting screw holes on hard disk 1 are on the outside.

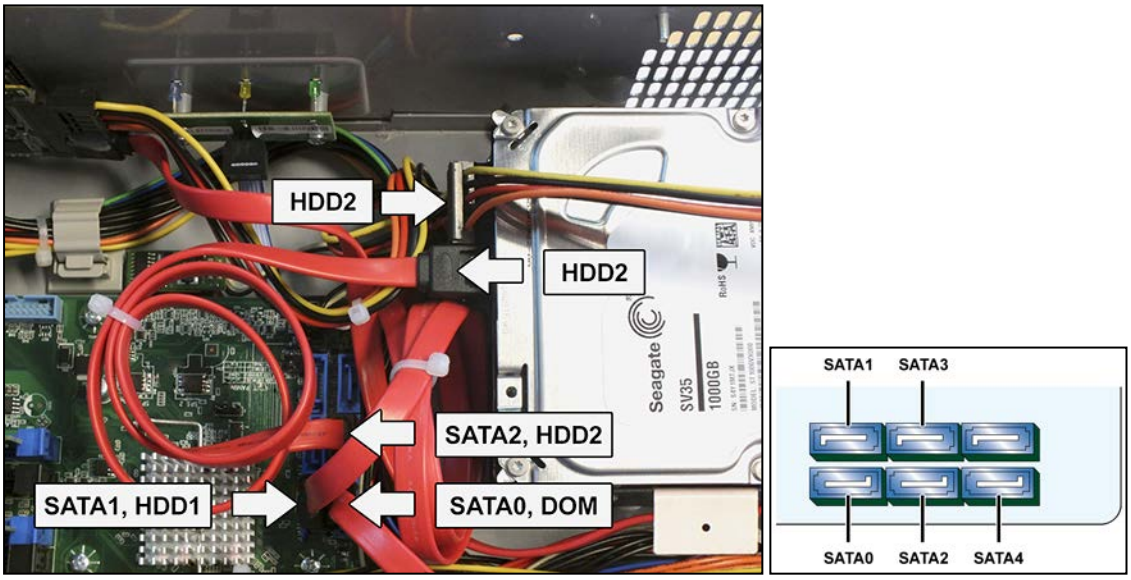


A: bracket #17011890; **B**: L-shaped bracket #17011895

4. Fix hard disk 1 to the bottom of the casing. For instructions depending on the model and hard disk capacity, see *Installing the First Hard Disk*, step 2 on page 14.
5. Connect hard disk 1 to the power supply, and to the SATA1 connector on the motherboard with the SATA cable (#16520877).



6. Connect hard disk 2 to the power supply, and to the SATA2 connector on the motherboard with the SATA cable (#16520877).

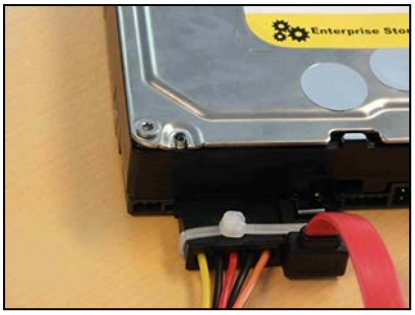


The SATA cables must not be bent too sharply to prevent cable damage.

The table below lists the correct devices and SATA connectors:

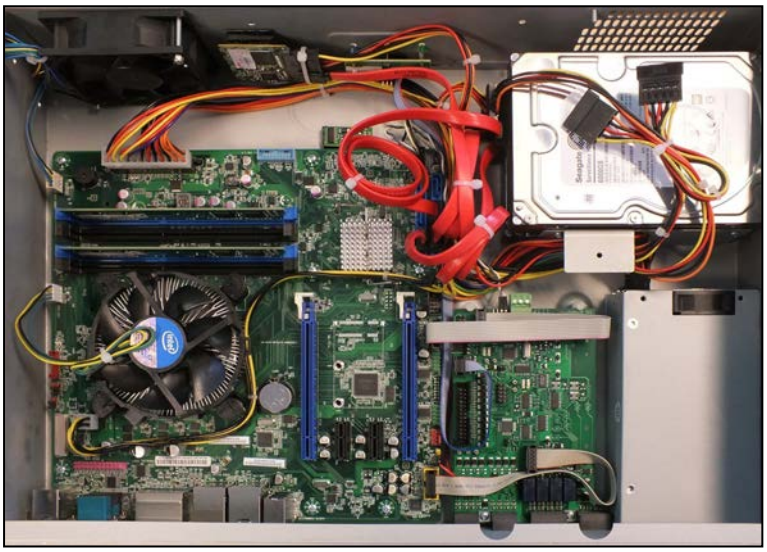
Device	SATA connector
DOM	SATA0
HDD1	SATA1
HDD2	SATA2

7. If the SATA cables do not have a locking mechanism, use tie-wraps to secure the cables on the disk(s) in the following way:





8. If there are unused cables left, bundle them with tie-wraps.



9. Place the top cover back: fix it with 2 screws at the front, 4 at the top, and 3 at the back.
10. Connect a monitor/screen and keyboard to the device. Switch on the power supply and wait for the boot window to appear.
11. Select **XO Installer** and press Enter.

> **Note**
>
> The boot window only appears for a few seconds, then the device continues booting. To make sure that you do not miss it, press the arrow keys on the keyboard repeatedly while the device is booting. The device will then stop at the boot window, and this gives you time to select and open the **XO Installer** menu.

12. Choose **Update current system** > **Manage recording disks**.
13. Select the newly installed hard disk(s) in the list and press Enter.

> **Note**
>
> SEDs (self-Encrypting Drives) are supported since XO 5.0. For details, see *Setup Self-Encrypting Drive* on page 26.

14. Choose **Format and use selected disks** (using the tab key). The system formats the selected hard disks.
15. When formatting is finished, choose **Main Menu**, and then choose **Reboot**.

The device now restarts. After restarting, the installed hard disks are ready for use.

3.7 Installing a Third Hard Disk

Material required for the third hard disk:

Part	Amount + reference number
Disk screws	4 x #17434080
SATA cable	1 x #16520877
iFT(-E) HDD 3+4 bracket	1 x #17011920
Self-tapping screws 3.5 x 6.5 mm	3 x #17362010

Note

Installing a third disk is only possible in **iFT** devices with models that have two extra mounting holes in the rear. The labels on the suitable iFT devices indicate '3 HDD Ready'.

For installing a third disk in an eFT Series device, see *Installing a Third and Fourth Hard Disk* on page 22 instead.

Caution!

- Before installing hard disks, stop the device. Switch it off and unplug the power cord.
- Take all necessary precautions to prevent static discharges that may damage the device: use an anti-static wristband, an anti-static mat…
- The procedure below assumes that you are using a **new disk**, or, in case of a used disk, that you will **format the used disk** and erase all recordings on it. If you want to install a used hard disk while keeping the recordings on it, follow the instructions in the Tech Tip *Recovering Recordings from Used HDDs* (29160).

To install a third hard disk in an iFT device, proceed as follows:

1. Stop the device, switch off the power supply, and then remove the top cover: unscrew 2 screws at the front, 4 at the top, and 3 at the back.



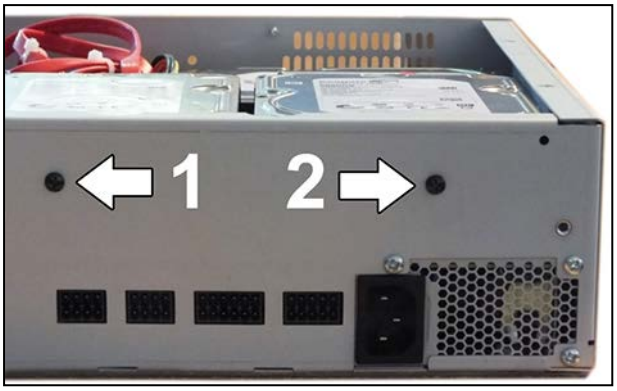


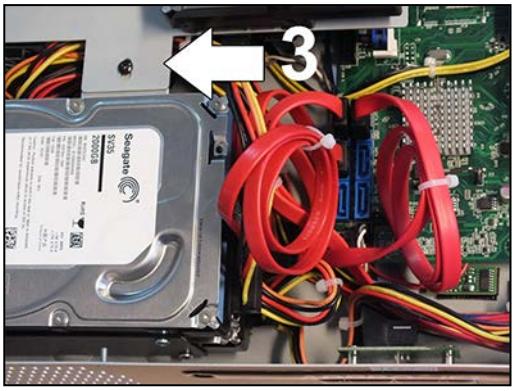
2. Fix the third disk on the mounting bracket (#17011920) using 4 disk screws (#17434080). Make sure that the disk is on the correct side as shown in the image below.



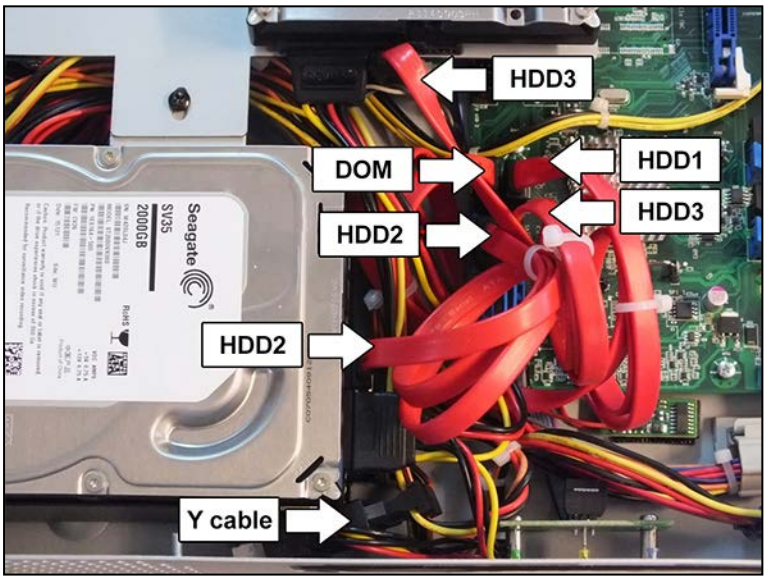
3. Before mounting the bracket with the disk in the XO device, arrange the required SATA power and data cables so that you can access them when the bracket is in place.

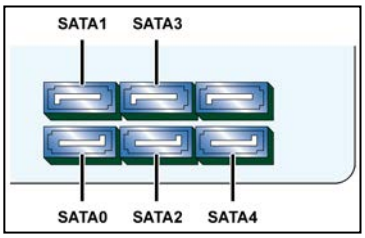
4. Mount the bracket using 3 self-tapping screws (#17362010): use 2 screws to fix the bracket to the rear of the device, and use the third screw to fix the bracket to the L-shaped bracket of the already installed second disk.





5. There is an unused SATA power connector on the same cable on which hard disk 1 is connected. Power hard disk 2 using this connector.
6. Connect hard disk 3 to the SATA3 connector on the motherboard with the SATA cable (#16520877).



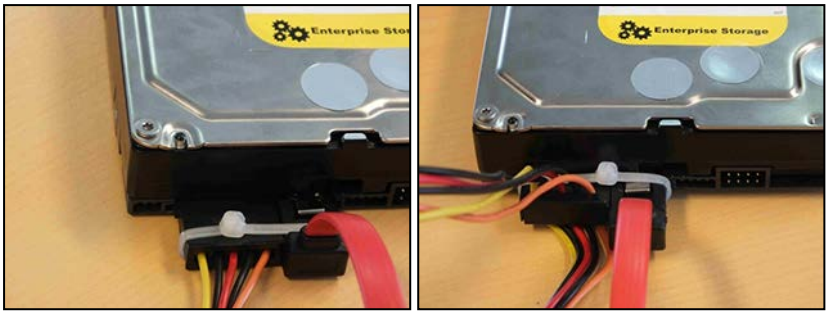


The SATA cables must not be bent too sharply to prevent cable damage.

The table below lists the correct devices and SATA connectors:

Device	SATA connector
DOM	SATA0
HDD1	SATA1
HDD2	SATA2
HDD3	SATA3

7. If the SATA cables do not have a locking mechanism, use tie-wraps to secure the cables on the disk(s) in the following way:



8. If there are unused cables left, bundle them with tie-wraps.
9. Place the top cover back: fix it with 2 screws at the front, 4 at the top, and 3 at the back.
10. Connect a monitor/screen and keyboard to the device. Switch on the power supply and wait for the boot window to appear.
11. Select **XO Installer** and press Enter.

> **Note**
>
> The boot window only appears for a few seconds, then the device continues booting. To make sure that you do not miss it, press the arrow keys on the keyboard repeatedly while the device is booting. The device will then stop at the boot window, and this gives you time to select and open the **XO Installer** menu.

12. Choose **Update current system** > **Manage recording disks**.
13. Select the newly installed hard disk(s) in the list and press Enter.

> **Note**
>
> SEDs (self-Encrypting Drives) are supported since XO 5.0. For details, see *Setup Self-Encrypting Drive* on page 26.

14. Choose **Format and use selected disks** (using the tab key). The system formats the selected hard disks.
15. When formatting is finished, choose **Main Menu**, and then choose **Reboot**.

The device now restarts. After restarting, the installed hard disks are ready for use.

3.8 Installing a Third and Fourth Hard Disk

Material required for the third and fourth hard disk:

Part	Amount + reference number
Disk screws	8 x #17434080 (4 per disk)
SATA cable	2 x #16520877 (1 per disk)
iFT(-E) HDD 3+4 bracket	1 x #17011920
Self-tapping screws 3.5 x 6.5 mm	3 x #17362010

> ***Caution!***
>
> Installing a third and fourth disk is only possible in iFT-E devices with model numbers 63xxxxxx. The 61xxxxxx models are **not** suitable.

Caution!

- Before installing hard disks, stop the device. Switch it off and unplug the power cord.
- Take all necessary precautions to prevent static discharges that may damage the device: use an anti-static wristband, an anti-static mat…
- The procedure below assumes that you are using a **new disk**, or, in case of a used disk, that you will **format the used disk** and erase all recordings on it. If you want to install a used hard disk while keeping the recordings on it, follow the instructions in the Tech Tip *Recovering Recordings from Used HDDs* (29160).

To install a third and fourth hard disk in an iFT-E/eFT device, proceed as follows:

1. Stop the device, switch off the power supply, and then remove the top cover: unscrew 2 screws at the front, 4 at the top, and 3 at the back.



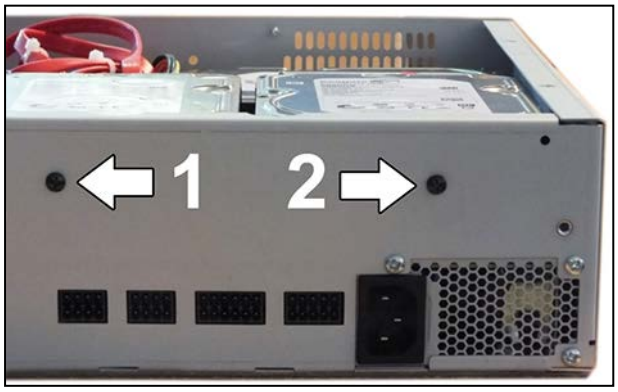


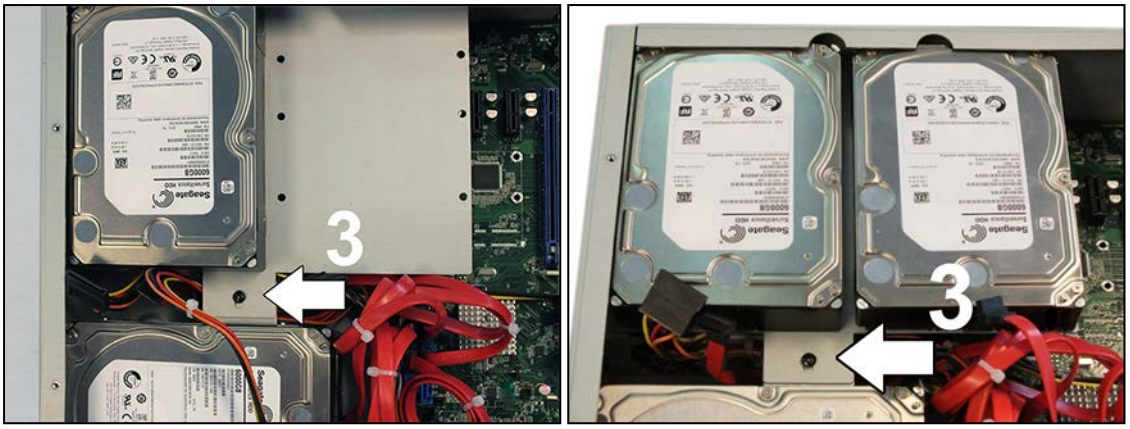
2. Fix disks 3 and 4 on the mounting bracket (#17011920) using 8 disk screws (#17434080).


Disk 3

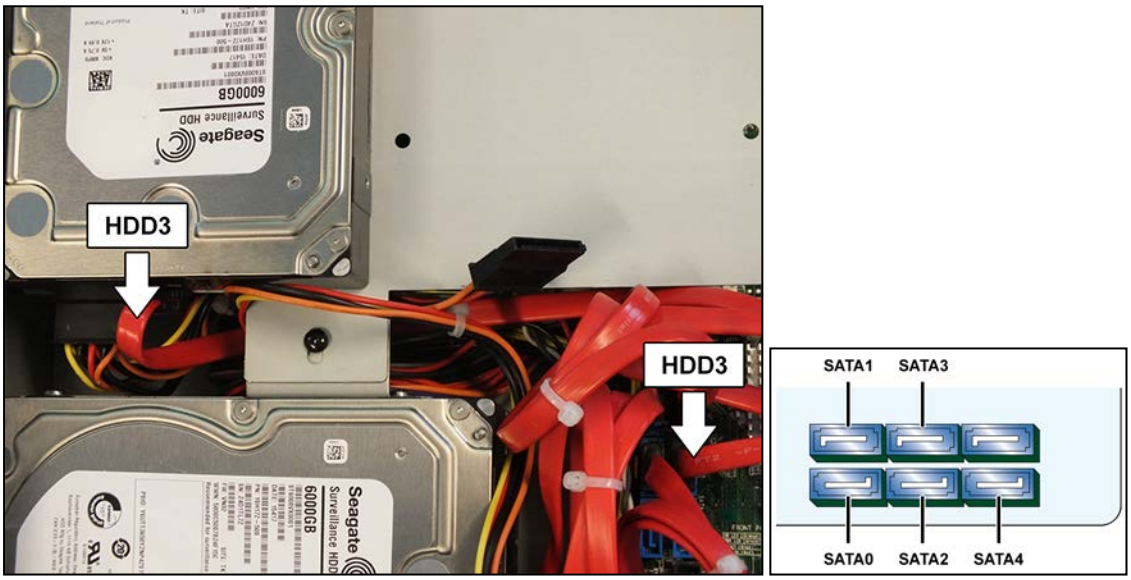

Disk 3 and 4

3. Before mounting the bracket with the disk in the XO device, arrange the required SATA power and data cables so that you can access them when the bracket is in place.
4. Mount the bracket using 3 self-tapping screws (#17362010): use 2 screws to fix the bracket to the rear of the device, and use the third screw to fix the bracket to the L-shaped bracket of the already installed second disk.

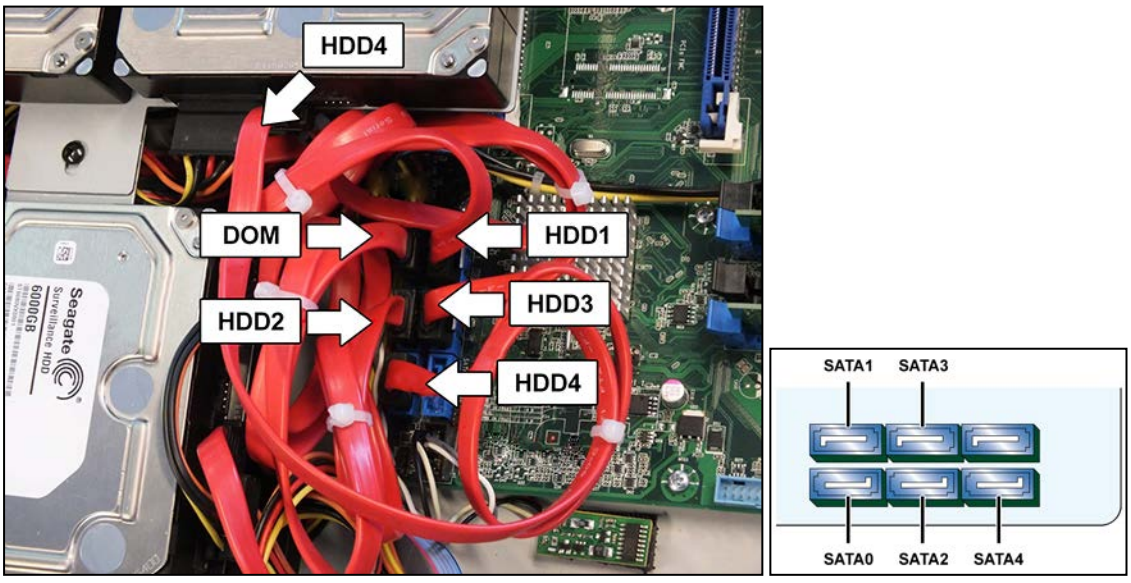




5. Connect hard disk 3 to the power supply, and to the SATA3 connector on the motherboard with the SATA cable (#16520877).



6. Connect hard disk 4 to the power supply, and to the SATA4 connector on the motherboard with the SATA cable (#16520877).

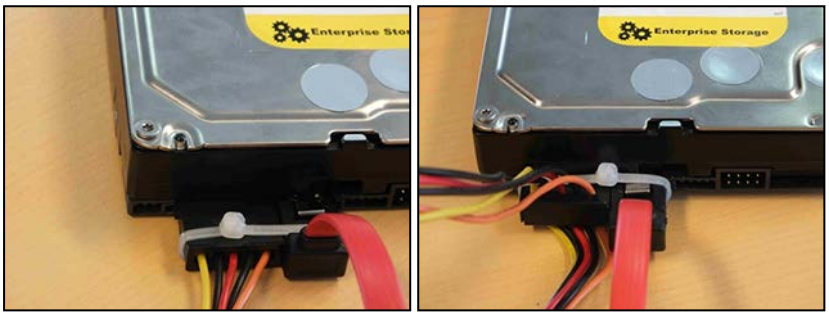


The SATA cables must not be bent too sharply to prevent cable damage.

The table below lists the correct devices and SATA connectors:

Device	SATA connector
DOM	SATA0
HDD1	SATA1
HDD2	SATA2
HDD3	SATA3
HDD4	SATA4

7. If the SATA cables do not have a locking mechanism, use tie-wraps to secure the cables on the disk(s) in the following way:



8. If there are unused cables left, bundle them with tie-wraps.



9. Place the top cover back: fix it with 2 screws at the front, 4 at the top, and 3 at the back.
10. Connect a monitor/screen and keyboard to the device. Switch on the power supply and wait for the boot window to appear.
11. Select **XO Installer** and press Enter.

> **Note**
>
> The boot window only appears for a few seconds, then the device continues booting. To make sure that you do not miss it, press the arrow keys on the keyboard repeatedly while the device is booting. The device will then stop at the boot window, and this gives you time to select and open the **XO Installer** menu.

12. Choose **Update current system** > **Manage recording disks**.
13. Select the newly installed hard disk(s) in the list and press Enter.

Note

SEDs (self-Encrypting Drives) are supported since XO 5.0. For details, see *Setup Self-Encrypting Drive* on page 26.

14. Choose **Format and use selected disks** (using the tab key). The system formats the selected hard disks.
15. When formatting is finished, choose **Main Menu**, and then choose **Reboot**.

The device now restarts. After restarting, the installed hard disks are ready for use.

3.9 Setup Self-Encrypting Drive

For additional data safety, ADPRO XO 5.0 supports data storage in SED (Self-Encrypting Drive) which automatically and continuously encrypts the data on the drive without any user interaction.

A new SED (Self-Encrypting Drive) without a host system owner will act as a standard drive with unrestricted access. The SED functions as a protected self-encrypting drive after performing a few steps to make the XO server as the owner of the SED. A protected SED may be in one of the following states:

- **unlocked**: the XO server has access to the SED
- **locked**: the XO server has no access to the SED

Note

ADPRO XO device types (iFTE/eFT/FT2E) support the following SEDs:

Capacity	Brand / Type	Model Number	Approval Status
4 TB	Seagate SED EXOS	ST4000NM010A	Tested and Approved
8 TB	Seagate SED EXOS	ST8000NM004A	Tested and Approved
12 TB	Seagate SED EXOS	ST12000NM0248	Supported by design
14 TB	Seagate SED EXOS	ST14000NM003G	Supported by design
16 TB	Seagate SED EXOS	ST16000NM003G	Tested and Approved

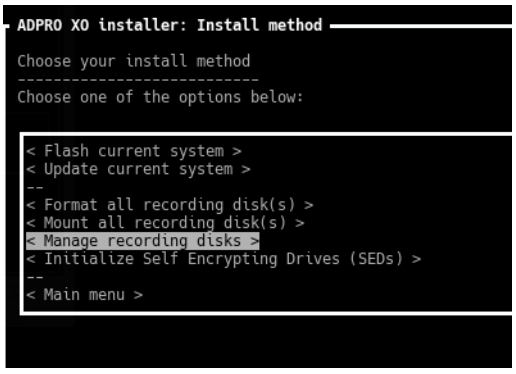
3.9.1 Using SED as a standard drive

`Prerequisite`

One or more SEDs are installed in the XO server with factory settings. There is no ownership of this drives and no file system installed on it.

3.9.1.1 Setup SED from the XO installer

Select the < *Manage recording disks* > option to format the drives in the XO server.



The **Format recording harddisks** page is displayed.



Using the < *Check status all harddisks* > option at the top of this page, the host system searches for both standard disks and SEDs. If SEDs are found, their status is queried. If **locked** SEDs are present in the system, it may take some time to obtain the status. As shown in the following figure, a separate list of found standard disks and SEDs is displayed.

In this XO server there is one standard drive with path */dev/sdb* and two SEDs with path */dev/sda* and path */dev/sdc*. These drives in the SED list are labeled as **NOT OWNED**.

SEDs with the **NOT OWNED** status can be selected for formatting and mounting in the operating system. At the same time, standard drives can also be selected for formatting. A RAID system with 2 SEDs, both with **NOT OWNED** status, can also be set up.

Note

If a SED is owned by the XO server (see *Taking ownership of an SED by the XO server* on page 27), its status must be **OWNED, UNLOCKED** for formatting or to be set up in a RAID system.

During the startup of the XO server

All formatted SEDs and standard drives are partitioned and mounted in the operating system. The SEDs function as standard drives with unrestricted access. Data can be written to the disk.

3.9.2 Taking ownership of an SED by the XO server

`Prerequisite`

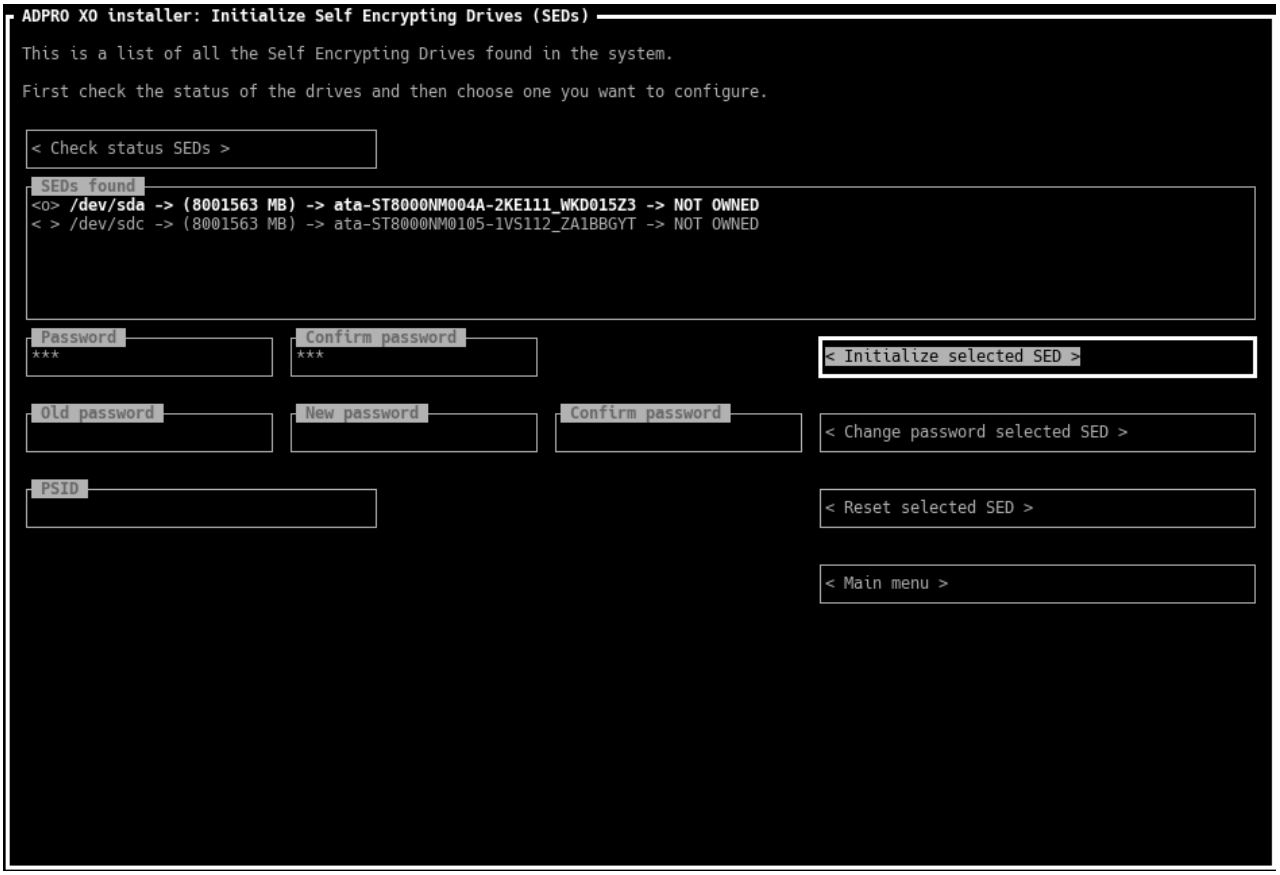
One or more SEDs are functioning as standard, not protected, drives in the XO server. These drives are partitioned and mounted and may contain data.

3.9.2.1 Setup SED from the XO installer

Select the < *Initialize Self Encrypting Drives (SEDs)* > option to initialize the SEDs in the XO server.



The **Initialize Self Encrypting Drives (SEDs)** page is displayed.



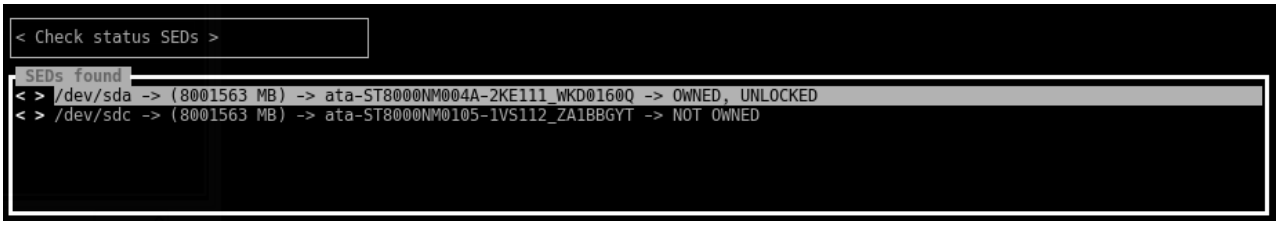
Using the < *Check status SEDs* > option at the top of this page, the host system searches for SEDs. If SEDs are found, their status is queried. If **locked** SEDs are present in the system, it may take some time to obtain the status. As shown in the following figure, a list of found SEDs is displayed.

To initialize a SED:

- One drive with status **NOT OWNED** is selected from the SED list.
- A password is entered and confirmed.
- On pressing < *Initialize selected SED* >: The SED is initialized with the password to perform as a protected drive. Existing data on the disk is preserved. The SED parameters are set so that the drive is locked after switching on the supply voltage. The password is stored encrypted, associated with the drive, on the DOM.

Another drive can be selected from the SED list to initialize and store its password on the DOM.

As shown in the following figure, the status of the SED after initialization is **OWNED, UNLOCKED**.



During the startup of the XO server

After a reboot of the XO server the status of an SED remains unchanged as **OWNED, UNLOCKED**. But after the supply voltage is turned on, its status is **OWNED, LOCKED**. So, during XO server startup, the password for each protected SED is retrieved from the DOM to unlock it.

3.9.3 The XO server has SEDs owned by another XO server

`Prerequisite`

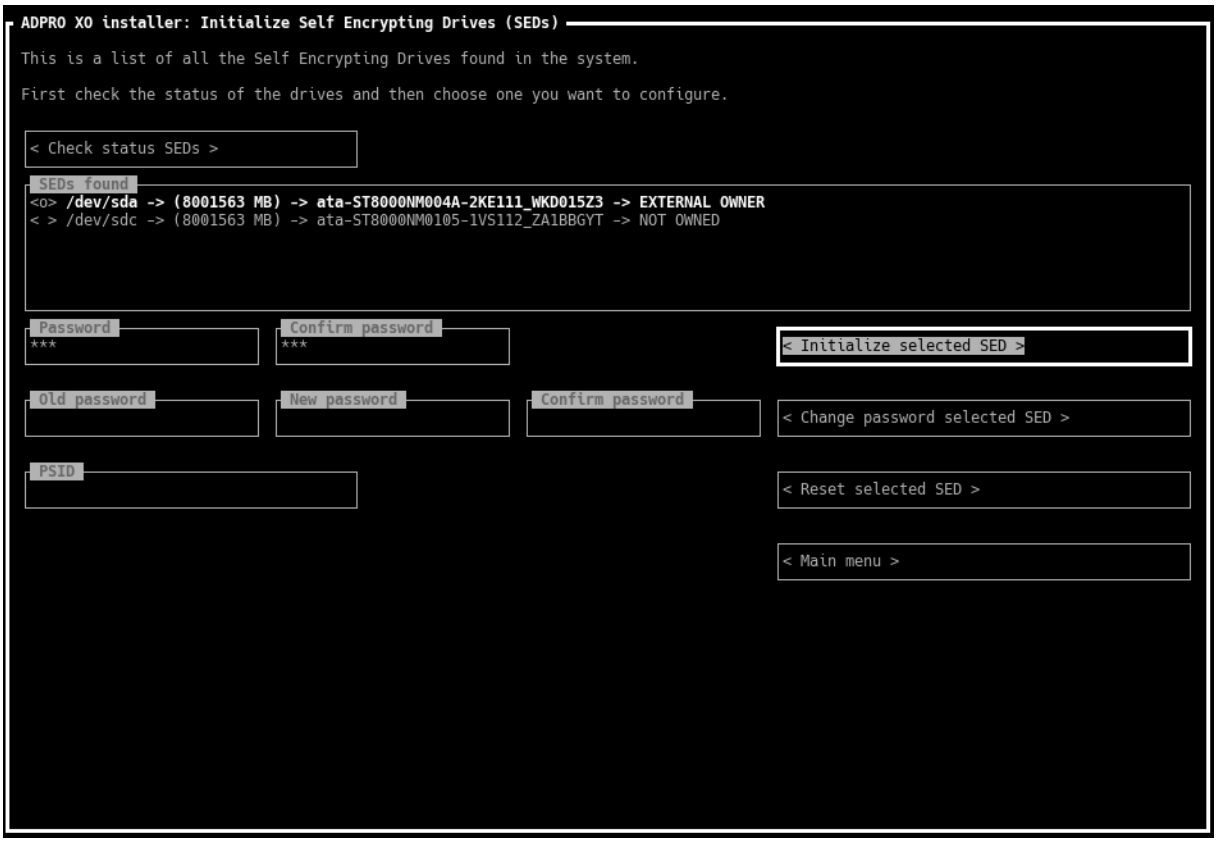
Multiple SEDs are installed on the XO server. Some protected drives can be owned by the XO server, and some can be owned by an external XO server. This means that there is no password on the DOM for any of the SEDs owned by an external XO server.

3.9.3.1 Setup SED from the XO installer

A SED found on the **Initialize Self Encrypting Drives (SEDs)** page can have one of the following status:

- **NOT OWNED**: SED performs as a standard drive
- **OWNED, LOCKED**: SED is owned by the XO server and a correct password was found after switching on the power supply of the device
- **OWNED, UNLOCKED**: SED is owned by the XO server and a correct password was found after rebooting the device
- **EXTERNAL OWNER**: SED is owned by another XO server because no password was found on the device

The following is the figure, for the SED with path */dev/sda*, no password was found on the DOM:

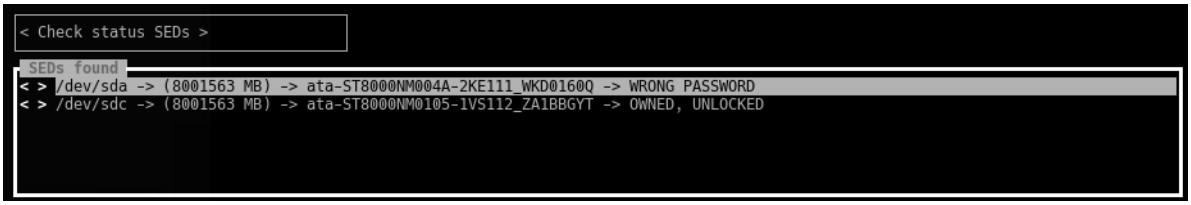


To make the XO server owner of an external SED:

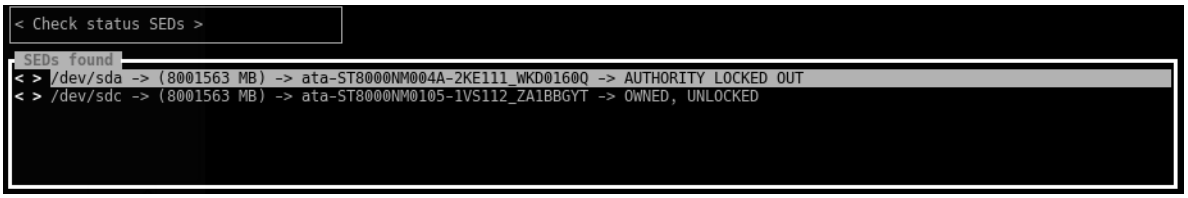
- One drive with status **EXTERNAL OWNER** is selected from the SED list.
- A password is entered and confirmed.
- On pressing < *Initialize selected SED* >: The password is stored encrypted, associated with the drive, on the DOM and the status of the drive is checked with the password entered. If the password is correct the status is **OWNED, UNLOCKED**.

Another drive with external owner can be selected from the SED list to store its password encrypted on the DOM.

If the password entered in the procedure described above was incorrect, the status indicates **WRONG PASSWORD**, as shown in the following figure.



We can try again but after entering the wrong password 5 times, the status becomes **AUTHORITY LOCKED OUT**, as show in the following figure.



After removing and switching on the supply voltage, we can try again to make the XO server the owner of the external SED.

Note

Formatted HDDs of an XO server will have its MAC address as a unique signature differentiable from that of other XO servers. Disconnect a formatted HDD from XO server 'A' and connect it to the SATA-bus of XO server 'B'; the XO server 'B' identifies the newly connected HDD as different from that of its own based on the MAC address signature.

An XO server can mount external HDDs to its file system only in the following scenarios:

- The XO server has no HDDs of its own.
- All the external HDDs have the same signature. The server will not mount any of the HDDs if they have different MAC address signatures.

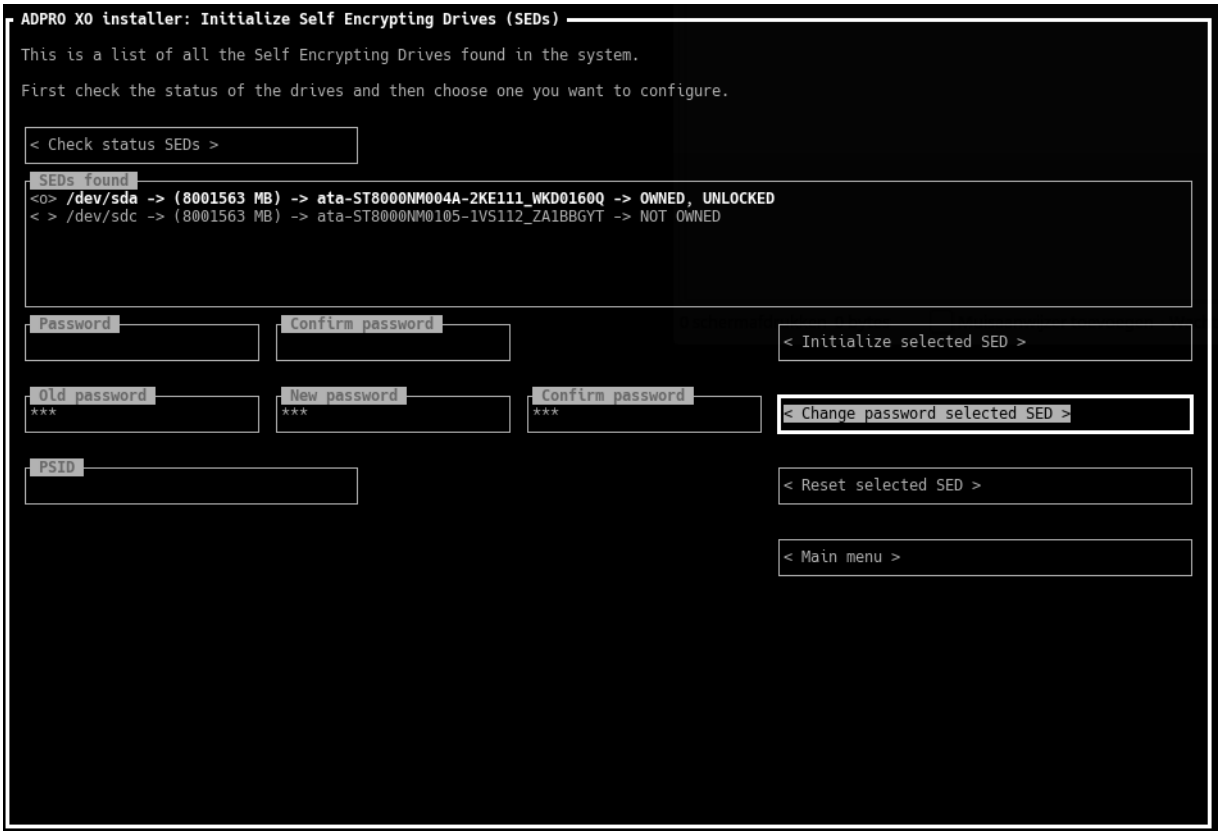
3.9.4 Change the password of an owned SED

`Prerequisite`

One or more SEDs are owned by the XO server.

3.9.4.1 Setup SED from the XO installer

The following figure shows how to change the SED password on the **Initialize Self Encrypting Drives (SEDs)** page.



If the old password entered was correct, the action to change the password is ended with a pop-up message as shown in the following figure.



But if the old password entered was wrong 5 times, the status will change to **AUTHORITY LOCKED OUT**. After removing and switching on the supply voltage, we can try again to change the SED password.

3.9.5 Reset an owned SED back to factory settings

`Prerequisite`

If the password of a protected drive is unknown or lost, there must be a way to reset the SED to factory settings. This can only be done with the Physical Secure ID (PSID) that can be scanned from the label on the disk.



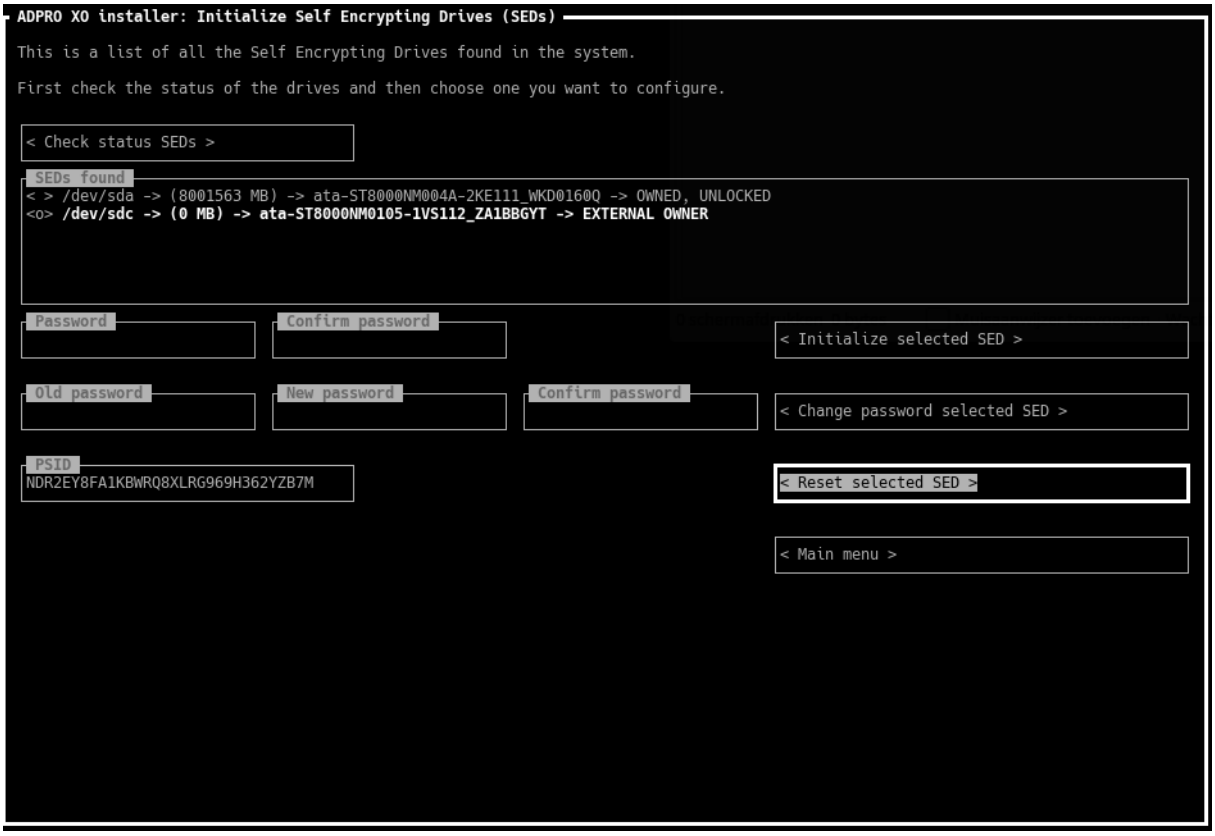
After the reset, the SED needs to be reformatted, which means that the data on it will be lost.

3.9.5.1 Setup SED from the XO installer

The SED can be reset to the factory settings from the **Initialize Self Encrypting Drives (SEDs)** page:

- One drive is selected from the SED list.
- The PSID (32 characters) of the drive is entered.
- On pressing < *Reset selected SED* >: The disk is reset, which means that the file system becomes unknown and the disk has to be reformatted.

Another drive can be selected from the SED list to reset.



As shown in the following figure, the status of the SED after the reset is **NOT OWNED**.

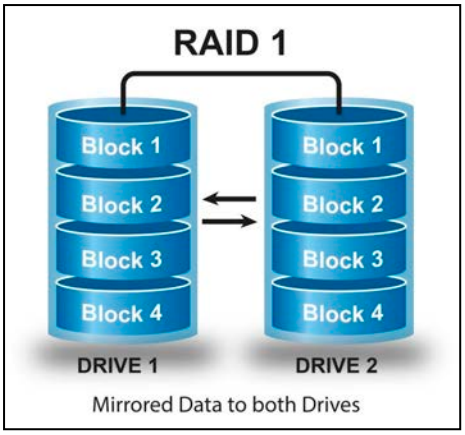


3.10 RAID 1 Support

3.10.1 About RAID 1

RAID stands for Redundant Array of Independent Disks (originally Redundant Array of Inexpensive Disks). It is a storage technology that combines multiple disk drive components into a logical unit. Data is distributed across the drives in one of several ways called RAID levels, depending on the level of redundancy and performance required. RAID has become an umbrella term for computer data storage schemes that can divide and replicate data among multiple physical drives, while the operating system can still access the data as being on one single drive.

RAID 1 is about mirroring without parity or striping. Data is written identically to two drives, thereby producing a “mirrored set”: the read request is serviced by either of the two drives containing the requested data, whichever one has the shortest search time plus rotational latency.



3.10.2 Activating RAID 1

RAID 1 requires minimum 2 hard disks. The size of the RAID 1 recording combination is the smaller of the 2 disks installed in your device. For example: if you have a 1 TB disk and a 2 TB disk, the RAID 1 recording disk has a 1 TB capacity.

> ***Caution!***
>
> When you apply RAID 1, the system formats the selected disks and erases the data on the disks. You will lose all the data on the disks. Back up your recordings first.

To activate RAID 1, proceed as follows:

1. Stop the device, and switch off the power supply.
2. Connect a monitor/screen and keyboard to the XO device.
3. Switch on the power supply and wait for the boot window to appear.
4. Select **XO Installer** and press Enter.

> **Note**
>
> The boot window only appears for a few seconds, then the device continues booting. To make sure that you do not miss it, press the arrow keys on the keyboard repeatedly while the device is booting. The device will then stop at the boot window, and this gives you time to select and open the **XO Installer** menu.

5. Choose **Update current system** > **Manage recording disks**.
6. Use the arrow keys to select the desired hard disk and press Enter. An X appears in front of the selected hard disk (between the brackets).
7. Select also the second hard disk.

> **Note**
>
> Select only two disks, not three or four. If you do, the system will configure the third and fourth disk as spare disks within the RAID 1 configuration. If you want to put disk 1 and 2 in RAID 1, and also disk 3 and 4, execute this step twice: once for disk 1 and 2, and once for disk 3 and 4.

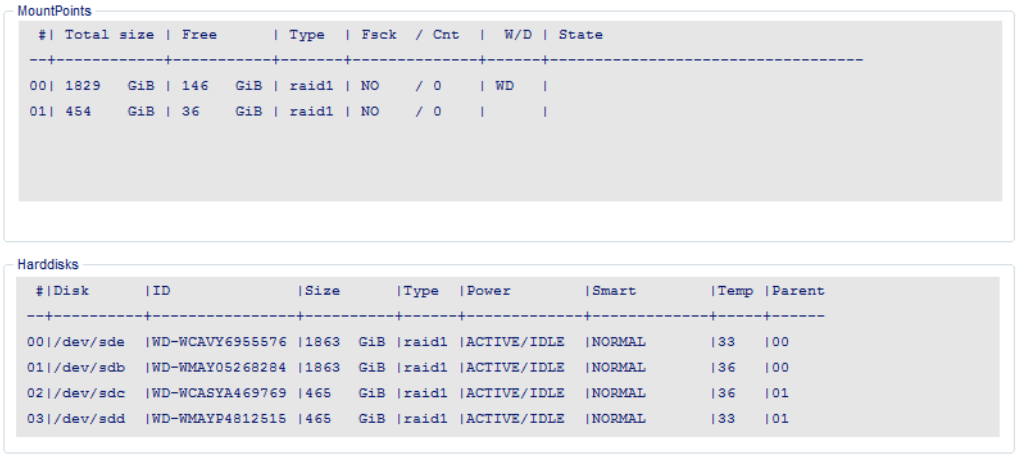
8. Choose **Make RAID 1 (mirror) from selected disks**.
9. When mirroring has finished, choose **Main menu**, and then choose **Reboot**.

3.10.3 Retrieving RAID 1 Information

You can retrieve RAID 1 information using the Telnet **ta,hd,raid** command, or using the XO client software.

To check if disks are in RAID 1 mode in the XO client software, proceed as follows:

1. Launch the XO client software.
2. Choose **System** > **Maintenance** > **Harddisks**. The following screen appears:



The **MountPoints** pane displays the mount points (= writing disks). The **Type** column indicates whether the mount point is a normal disk (**disk**) or a RAID 1 disk (**raid1**).
The **State** column will indicate **degraded** when one of the RAID disks is faulty, and **recovering** when the system is resynchronising after replacing the faulty disk. It will also indicate the progress of the recovery process. For details, see the *XO Client Software User Manual* (21796).

The **Harddisks** pane displays the physical hard disk information. The **Type** column indicates whether the disk is a normal disk or a RAID 1 disk. The **Parent** column indicates the corresponding mount point.
The example above shows a device with 4 disks and RAID 1 (two mount points).

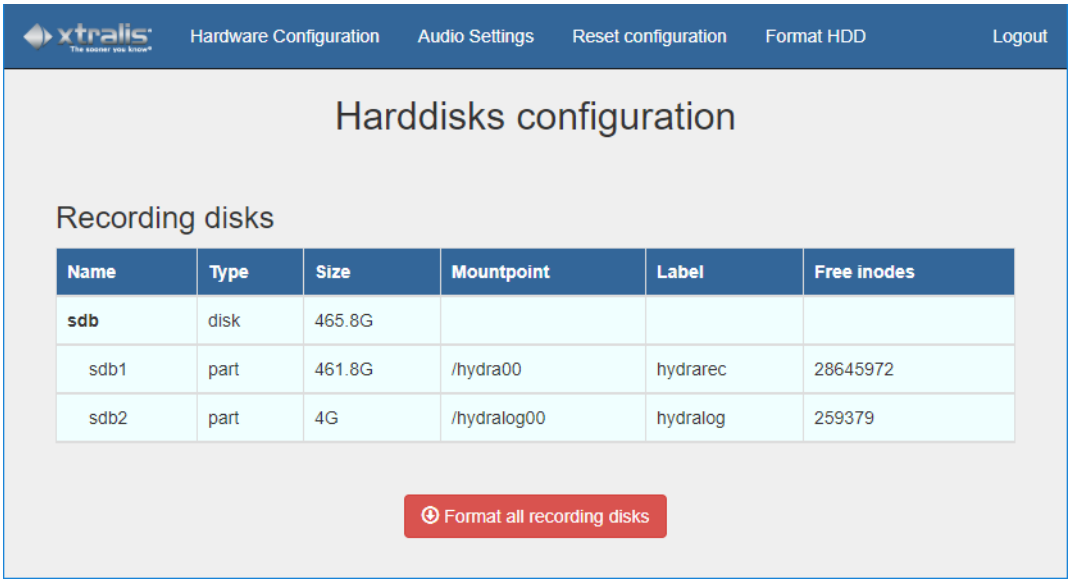
3.11 Remote Formatting of Hard Disks

As of firmware version XO 4.3, you can format the hard disks in your XO device remotely using the hardware configuration tool. You do not have to use the XO Installer menu. If your XO device has several disks, you will format all the disks.

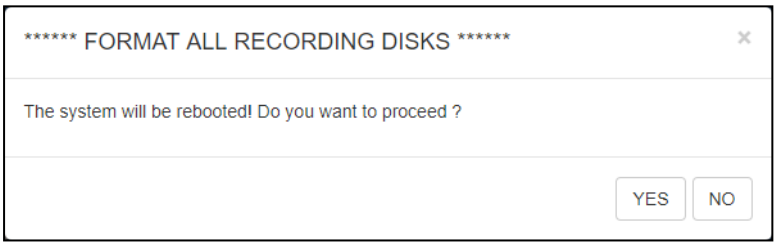
To format the hard disks in an XO device remotely, proceed as follows:

1. Use the XO client to back up the necessary data: recordings, calibration pictures… For details, see the *XO Client Software User Manual* (21796).
2. Log on to the hardware configuration tool. For instructions, see *Logging on to the Hardware Configuration Tool* on page 49.

3. In the top menu, click the **Format HDD** tab.



4. Click **Format all recording disks**. The following message appears:



5. Click **Yes** to confirm.
   The device will restart, format the hard disks, and then continue restarting.
6. Close the hardware configuration tool and wait for the process to finish.

4 Front LED Indicators

There are 3 LEDs on the front of the device.

LED	Icon	Description
Green LED		Indicates that power is on. The green LED periodically blinks (goes out briefly). This is normal behaviour.
Yellow LED		Indicates a fault. If the yellow LED lights up, check the status of your device. For more information, see the *XO Client Software User Manual* (21796).
Blue LED		Indicates storage media activity.



Caution!

When the 3 LEDs are flashing simultaneously, the system is servicing the recording disks (upgrading, formatting…). In that case, do not turn off power.

5 Motherboards

5.1 BIOS Settings

BIOS settings for PH10LU:

1. Choose **Main** > **System Time** to set the system time.
2. Choose **Main** > **System Date** to set the system date.
3. Choose **Chipset** > **PCH-IO Configuration** > **Front Panel Audio** and select **Legacy Front Panel**.
4. Choose **Boot** > **CSM parameters** > **Launch PXE OPROM policy** and select **Legacy only**.
5. Choose **Save & Exit** > **Exit and Reset** and press **Enter**.

Leave all other parameters to the default settings.

BIOS settings for PH10FEU:

1. Choose **Main** > **System Time** to set the system time.
2. Choose **Advanced** > **Hardware Health Configuration**, set **Auto Fan Control** to **[Enabled]**.
3. Choose **Advanced** > **Option ROM Dispatch Policy**, set **LAN1** and **LAN2** to **[Enabled]**, and set **OPROM Type** of **LAN1** and **LAN2** to **[PXE]**.
4. Save and restart once again in **BIOS** mode.
5. Select **Boot Option #1** > **IBA GE Slot 0200 v1585**.
6. Save and restart.
7. After the boot process:
   - Check in BIOS if **Boot Option #1** is set to **UEFI OS (P0: SATA Slim 3ME3)**.
   - Check in **Advanced** > **CPU Config** > **microcode path = B4**.

5.1.1 Overview

The iFT Series operates with a PH10LU or PH10FEU motherboard.

- The PH10LU motherboards came into use since February 16, 2015
- The PH10FEU motherboards came into use since October 25, 2019

PH10LU motherboard



PH10FEU motherboard



5.2 Connectors

Note

You must restart the XO client software after connecting devices to a USB port.

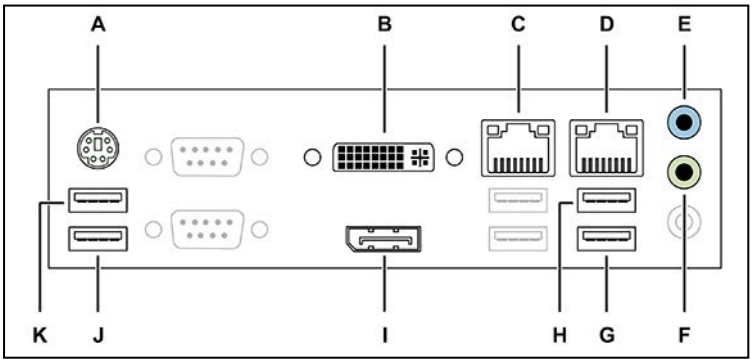
USB input 1 (/dev/ttyU1) is reserved for an external modem.

Note

The illustrations below show the default numbering for the USB ports. If you use external XO I/O Interface USB modules, the system adjusts the internal numbering of the USB ports, and the values in the images below are no longer valid.

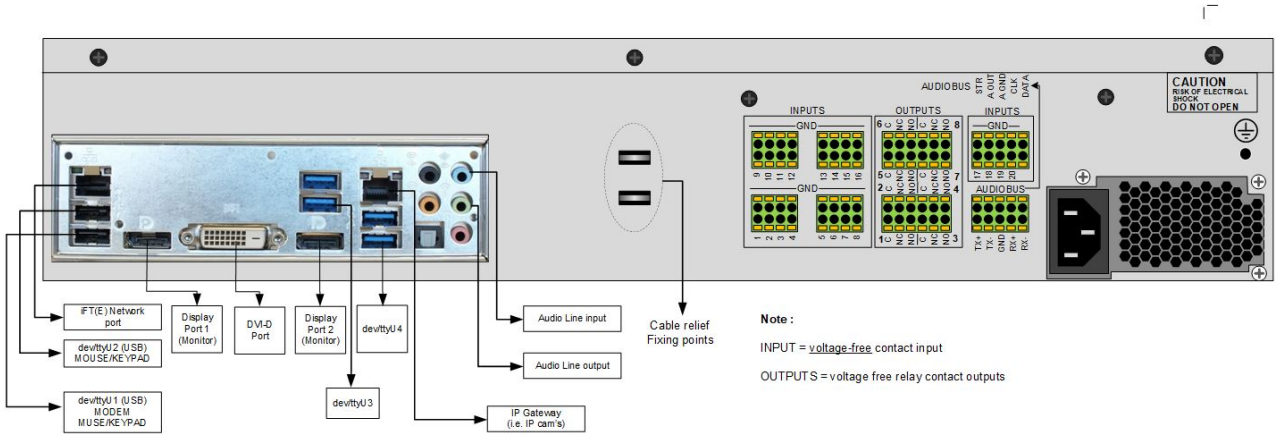
Make sure to map all devices using the hardware configuration tool, and assign new USB port numbers to existing devices on the USB ports. Also, after removing the XO I/O Interface USB modules, you can reset the USB port numbering back to the default values as shown in the images below. For details, see the *XO I/O Interface USB Module Technical Manual* (32688).

The following are the connectors for the PH10LU motherboard at the rear of the device:



A	PS/2: keyboard or mouse	**G**	/dev/ttyU4 (USB)
B	DVI-I: monitor	**H**	/dev/ttyU3 (USB)
C	eth0: network for XO device	**I**	DisplayPort: monitor
D	eth1: network for IP cameras	**J**	/dev/ttyU1 (USB): modem
E	Audio line in	**K**	/dev/ttyU2 (USB)
F	Audio line out		

The following are the connectors for the PH10FEU motherboard at the rear of the device:

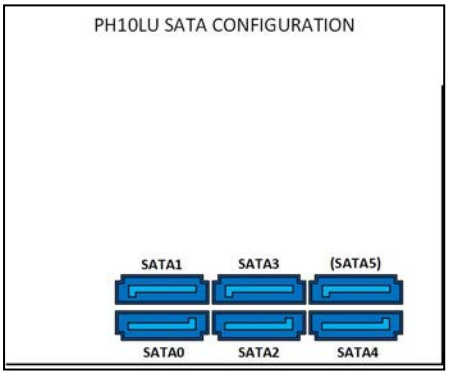


Note

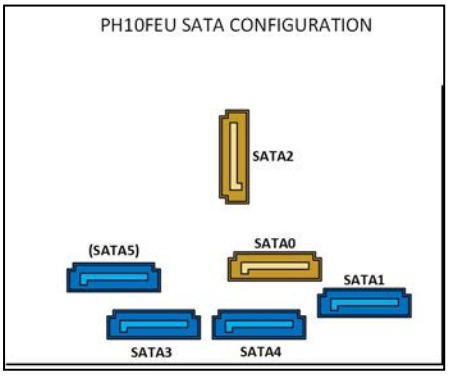
The top line of the green I/O connectors is optional and is not available on some SKUs.

The hard disk installation procedure is similar in both PH10LU and PH10FEU motherboards, and the hard disks connect to the same SATA numbers, but only the SATA connector position is different.

The PH10LU motherboard has the following SATA cable connectors:



The PH10FEU motherboard has the following SATA cable connectors:



Note

The brown-colored SATA cable connectors on the PH10FEU motherboard indicate **Pin7 on +5V** support, and this feature is not used so far by iFT Series.

5.3 Replacing the Motherboard

Do not replace the motherboard in the field. If the motherboard needs replacing, send the device back to your supplier. Remember that the system licenses is linked to the motherboard. If you replace the motherboard, the system may not recognise the system license and will not be functional.

5.4 Replacing the Motherboard Battery

A coin-cell battery (such as CR2032) powers the real-time clock and CMOS memory. When the computer is not plugged into a wall socket, the battery has an estimated life of three years. When the computer is plugged in, the standby current from the power supply extends the life of the battery. The clock is accurate to ± 13 minutes/year at 25 degree Celsius with 3.3 VSB applied.

When the voltage drops below a certain level, the BIOS Setup program settings stored in CMOS RAM (for example, the date and time) might not be accurate.

Replace or supplement the coin-call battery on the motherboard with an equivalent one when one of the following issues occur:

- The time and date settings are lost
- One of the following alerts are displayed when the XO device is rebooted:
  - CMOS Read Error
  - CMOS Checksum Error
  - CMOS Battery Failure
  - System battery voltage is low

> ***Caution!***
>
> Power-off the device and the peripherals connected to the device, and unplug the power cord from the AC power source (wall outlet or power adapter) before opening the device. Beware of the electrostatic discharges and its dangers.
>
> Risk of explosion if the battery is replaced with an incorrect type. Batteries should be recycled where possible. Disposal of used batteries must be in accordance with local environmental regulations.

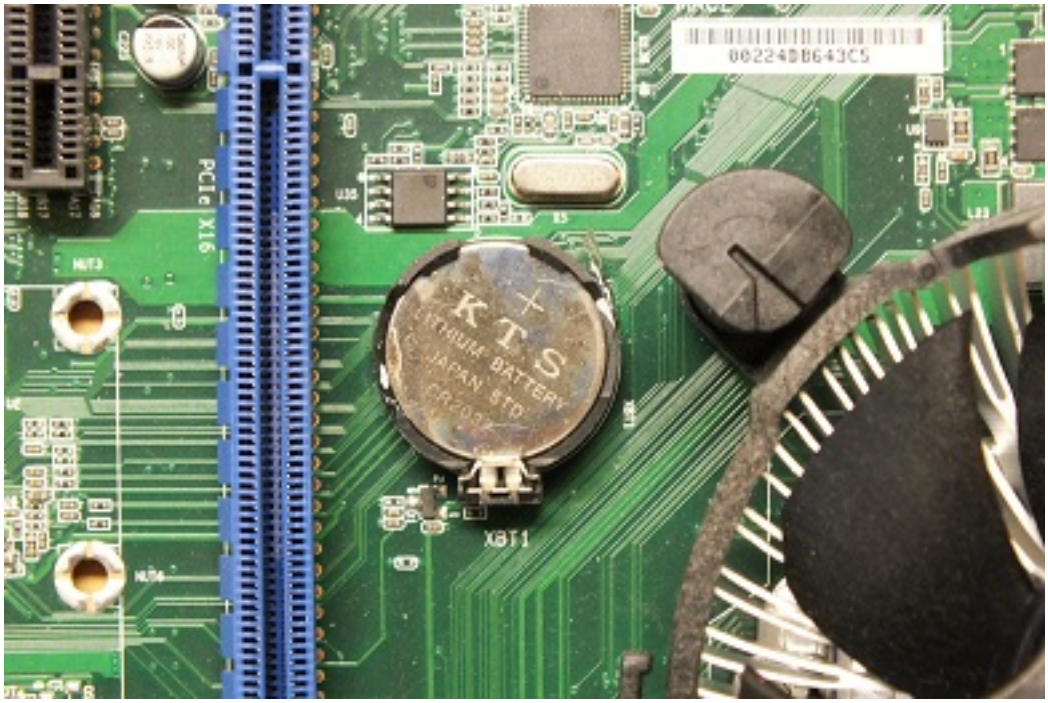
To replace the motherboard battery

1. Remove the device cover.
2. Locate the CMOS battery on the motherboard. The battery may be held by a metal clip or bar. The battery can be removed by sliding it out from under the clip.

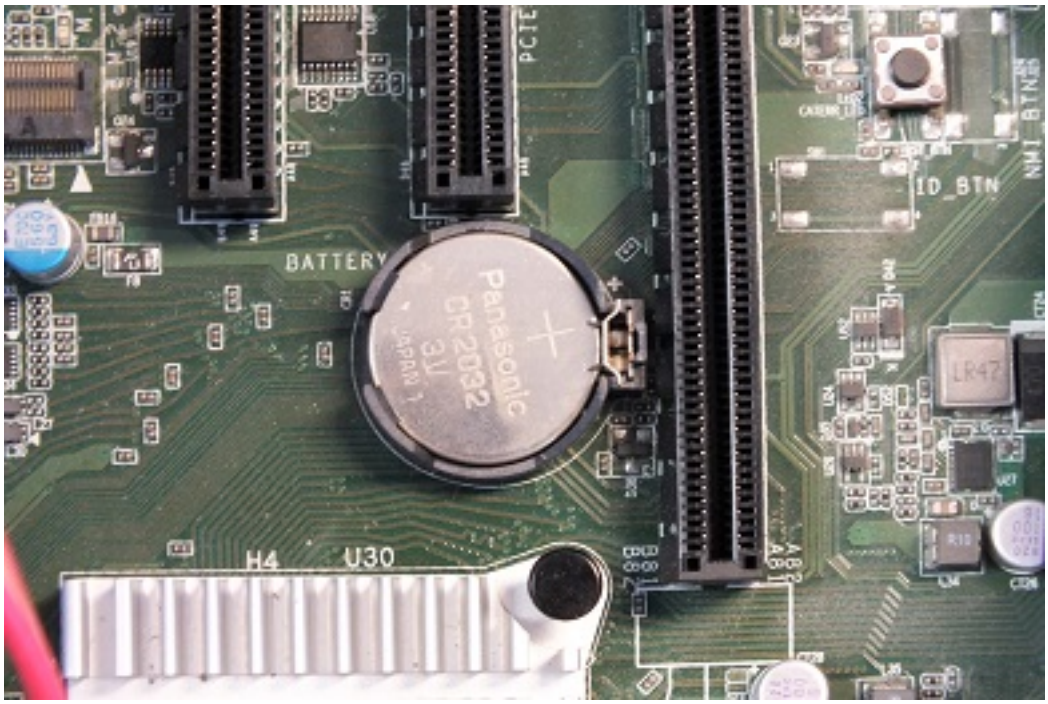
   > ***Caution!***
   >
   > Do not bend this clip to get the battery out, as a bent clip can result in the new battery not staying in the socket.

3. Note the battery specifications and the orientation of the “+” and “-” on the battery.
4. Remove the battery. It is quite easy to remove a coin cell battery. With a medium flat-bladed screwdriver, gently pry the battery free from its connector or use your fingers to grab the edge and pull it out of the socket. If the battery is held by a clip, move the clip up with one hand and pull the battery out with another hand.

   Battery on the PH10LU motherboard:



Battery on the PH10FEU motherboard:



Note

If the battery is not removable, the motherboard may have a secondary battery socket or you may need to set a jumper on the motherboard to insert the new battery.

5. Insert the new battery in the connector, orienting the “+” and “-” correctly.
6. Replace the device cover.
7. Power-on the device and reset the CMOS values to the defaults, and save the settings before exiting.

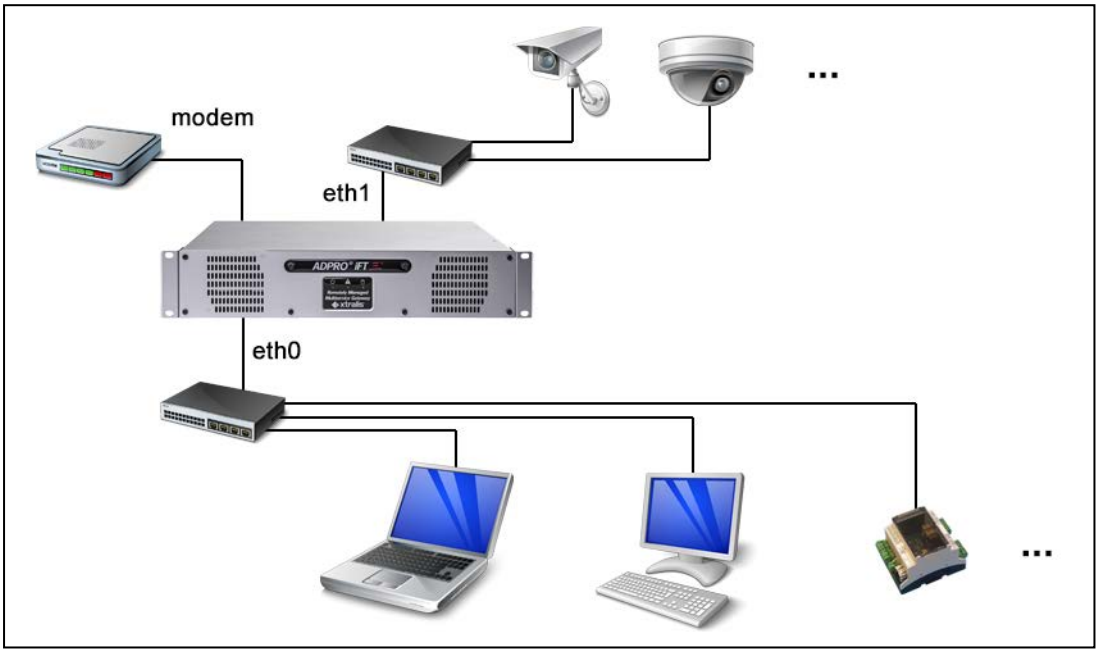
Note

Many CMOS setups allow you to press a key, such as F10, to save values and exit with one action.

6 Connecting IP Cameras

An XO device that uses IP cameras requires separate IP network connections for:

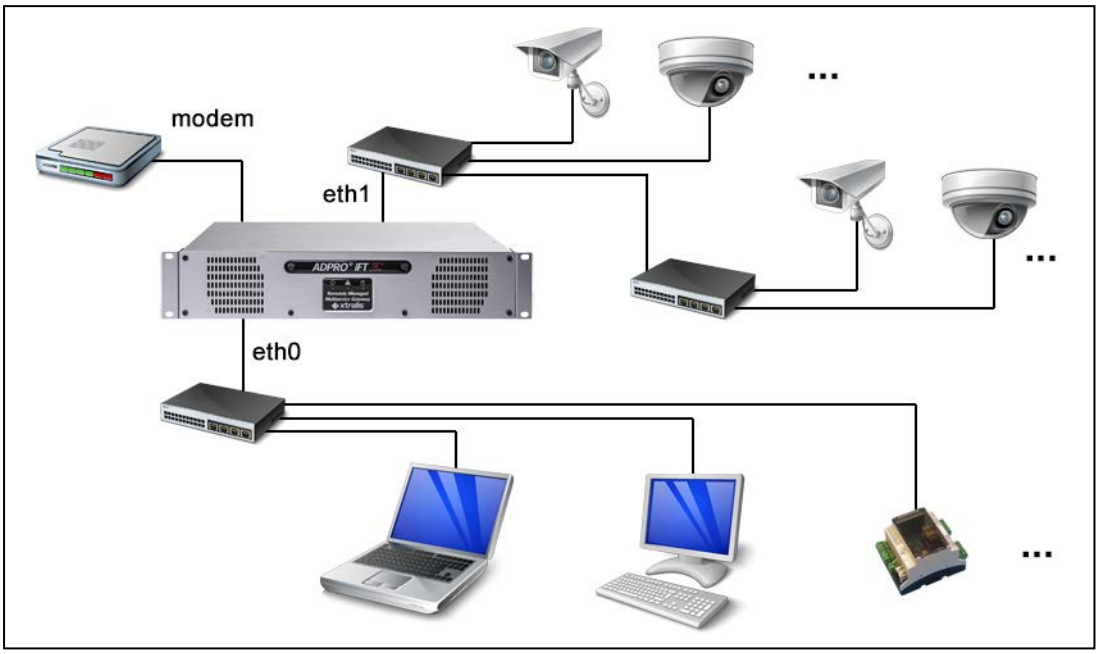
- The network for communicating with the client PC, CMS, Net I/O units, S3100 panels… The primary Ethernet connector (eth0) on the motherboard provides the physical interface for this network.
- The network for the IP cameras. The secondary Ethernet connector (eth1) on the motherboard provides the physical interface for this network.



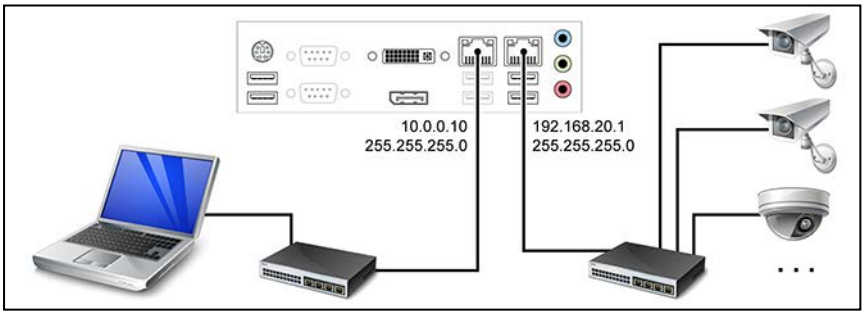
Note

It is not possible to have overlapping IP address ranges in eth0 and eth1; these must be separate. With software version XO 4 and above, the system will check and issue a warning if the IP addresses of eth0 and eth1 are in the same range.

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. As of firmware version XO 4.0, you can use **static routes** to extend the eth1 camera network to these other network segments. For the configuration of the static routes, see the *XO Client Software User Manual* (21796).



The PH10LU and PH10FEU motherboards have two LAN connectors on board. Just connect the IP camera network to the eth1 port using an Ethernet cable.
You must set the Ethernet connection of your XO device (eth0) and the Ethernet connection of the camera network (eth1) to different IP ranges.



7 Main I/O Card

7.1 Features

The Main I/O (MIO) Next Generation card is an internal I/O card, pre-installed inside the iFT Series device. It is also called OTB (on-the-box) card.

Rear connectors for PH10LU motherboard:



Rear connectors for PH10FEU motherboard:



Note

The top line of the green I/O connectors is optional and is not available on some SKUs.

The MIO card offers:

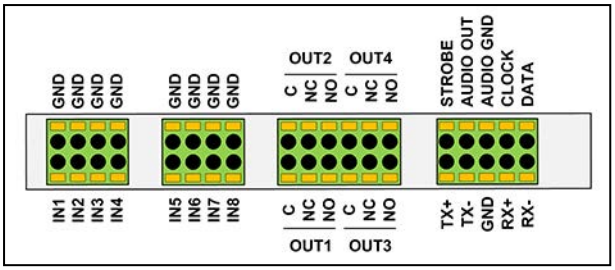
- 8 tamper-protected inputs and 4 relay outputs (rated 14 VDC @ 1 A) on iFT Series with PH10LU motherboard and 8 or 20 tamper-protected inputs and 4 or 8 relay outputs (rated 14 VDC @ 1 A) iFT Series with PH10FEU motherboard depending on the SKU.
- GND for every input
- driver for audio module/VM22 audio switcher; with improved audio quality
- driver for the front LED indicators.

If you need to replace the MIO card, you can find detailed installation instructions in the document *Main I/O and Extension I/O Cards – Next Generation* (27820).

7.2 Connection of Inputs and Outputs

7.2.1 Overview of Inputs and Outputs

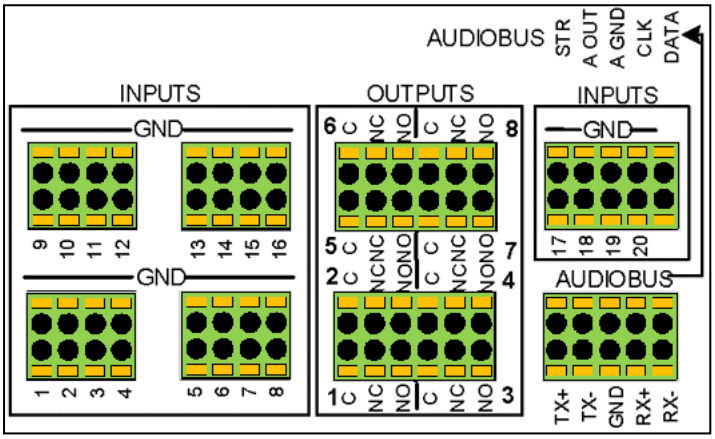
MIO on PH10LU motherboard:



IN1–8 are voltage-free contact inputs.

OUT1–4 are voltage-free relay contact outputs.

MIO on PH10FEU motherboard:

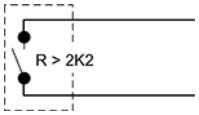


IN1–20 are voltage-free contact inputs.

OUT1–8 are voltage-free relay contact outputs.

7.2.2 Input Circuits

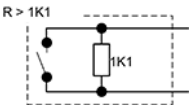
Below are the NEOL, SEOL, and DEOL configurations for the inputs. For correct operation, you also have to indicate the used input circuit configuration in the XO client software. For more information, see the *XO Client Software User Manual* (21796).



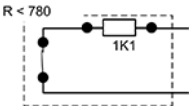
Normally open – NEOL
Short circuit = alarm
Open circuit = idle
(Default setting)



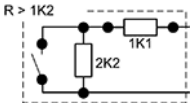
Normally closed – NEOL
Short circuit = idle
Open circuit = alarm



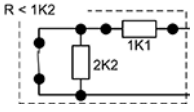
Normally open – SEOL
Short circuit = alarm
1K1 = idle
Open circuit = tamper



Normally closed – SEOL
Short circuit = tamper
1K1 = idle
Open circuit = alarm



Normally open – DEOL
Short circuit = tamper
1K1 = alarm
3K3 = idle
Open circuit = tamper



Normally closed – DEOL
Short circuit = tamper
1K1 = idle
3K3 = alarm
Open circuit = tamper

7.2.3 Connecting Inputs and Outputs

Depending on the type, the I/O card can be equipped with Dinkle (standard) or Phoenix spring insertion connectors. For both types you need a 2 mm slotted screwdriver.

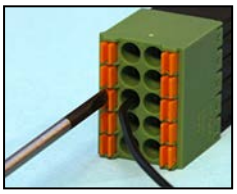
Warning!

Although the picture below shows only the connector, it is strongly recommended to connect the wires with the connectors plugged into the card. Wiring a handheld connector may cause injuries.

Wiring to Dinkle and Phoenix connectors is identical, except that the position of tabs and holes is swapped. The picture in the procedure below shows a Phoenix connector.

To connect inputs and outputs, proceed as follows:

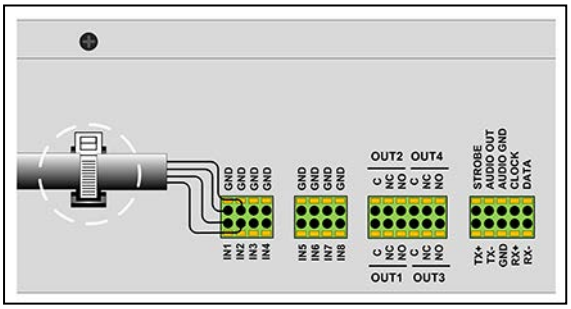
1. Push the slotted tab firmly inwards with the screwdriver.
2. Insert the stripped wire (6–7 mm) into the corresponding round hole as deeply as possible.
3. Release the tab and pull the wire to check if it is properly fitted.



Wire gauge:
Solid and stranded: 16–24 AWG
(diam. 1.3–0.5 mm)

7.2.4 Cable Strain Relief

After connecting all the wires, use a tie-wrap to attach the cables to the XO device's chassis. Run the tie-wrap through the slots in the chassis as shown below. The tie-wrap serves as a strain relief and makes sure that the wiring stays in place when handling the XO device.



7.3 Configuring the MIO Card

To configure the inputs and outputs, or to update the MIO card firmware, see the *XO Client Software User Manual* (21796).

8 XO I/O Interface USB Modules

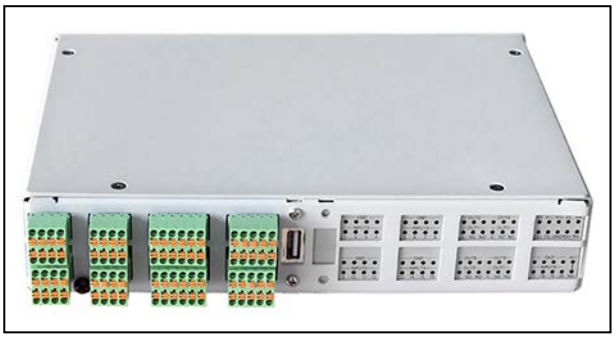
8.1 About the XO I/O Interface USB Modules

Firmware version XO 4.0 and above supports the XO I/O Interface USB modules for extra inputs and outputs. These modules contain sets of Main I/O and Extension I/O cards (Next Generation) that you can connect to your XO device via USB.

XO I/O Interface USB module:



Rear view, single module:



Warning!

XO I/O Interface USB module installation instructions:

- Use the unit indoors only.
- Install on a flat surface.
- Keep away from moisture and heat sources.
- Do not expose to sunlight.
- Do not cover the unit.
- Use a USB cable shorter than three meters.

XO I/O Interface USB module operating instructions:

- XO I/O Interface USB module is not suited for use in locations where children are likely to be present.
- Use only a dry cloth to clean the unit.
- Avoid opening the unit.

The XO I/O Interface USB modules function just like internal MIO/EIO Next Generation cards, but with the following restrictions:

- There are no AUDIO OUT and AUDIO GND outputs: if you want to use a VM22A audio switcher, you have to connect it to the built-in MIO card instead. It is possible to use a VM22E switcher.
- You can add only one set of MIO/EIO cards to your device = a single XO I/O Interface USB module. You then have two MIO cards and one EIO card in total. You cannot use the double module.

You have to map the modules to the correct card set (MIO-1 or MIO-2) using the **hardware configuration tool**. If not, the XO device will not discover the cards and you will not be able to use the inputs/outputs.
Furthermore, if you are using adapters on the USB ports of your XO device (to connect to PIR detectors or for PTZ control of analogue cameras), you also have to map these 'devices' using the hardware configuration tool. If the system detects 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), the system will activate system input 0002 – [SYST] – HW CFG MISMATCH.

Note

Although it is technically possible to disable an existing, built-in MIO/EIO card in the hardware configuration tool, and use an external module instead, Honeywell recommends to keep and use the built-in cards. If you disable a built-in MIO card, you have to switch off the buzzer and watchdog features, or the system will beep continuously. Switching off the buzzer and watchdog seriously reduces the system's reliability and security.

Caution!

Using the XO I/O Interface USB modules changes the internal USB port numbering on the XO device. The default numbering as indicated in the hardware manuals no longer applies. If you have any other devices than XO I/O Interface USB modules on the USB ports of your XO device, you also must remap these devices in the hardware configuration tool, and you must adjust the serial port settings in the XO client.

When you stop using XO I/O Interface USB modules on the XO device, you have to reset the USB port numbering in the hardware configuration tool to return to the default USB port numbers.

8.2 Logging on to the Hardware Configuration Tool

You need to log on to the hardware configuration tool using the XO Technician user. For this, you need to:

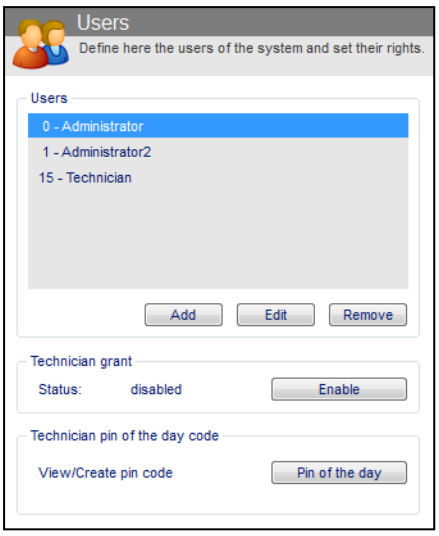
1. Enable the Technician user using the XO client software.
2. Generate a special, temporary access code (PIN of the day) for the Technician user. The PIN limits the time that the Technician user has access to the configuration tool.

Note

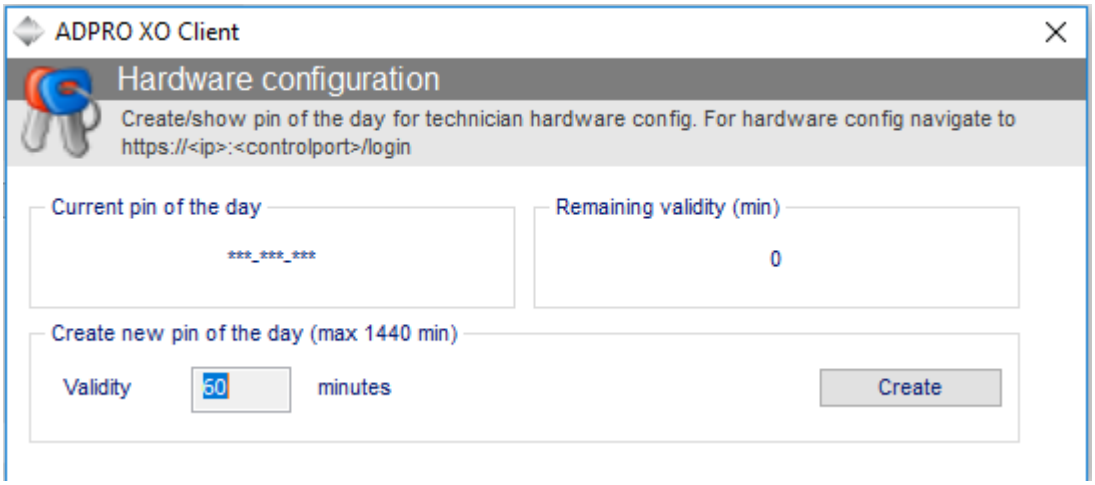
You cannot log on to the hardware configuration tool while the XO device is restarting.

To log on to the hardware configuration tool, proceed as follows:

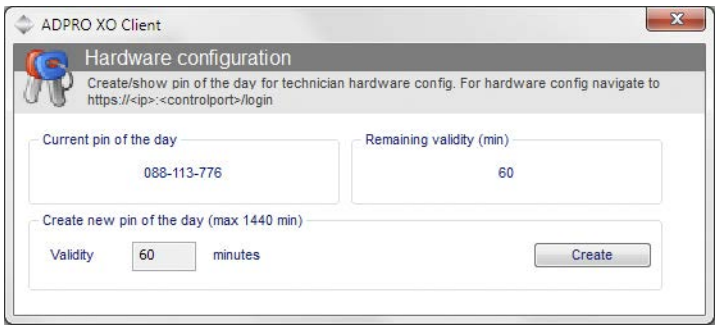
1. Open the XO client, and log on to the desired XO device as an Administrator.
2. Choose **System** > **General** > **Users**.



3. Under **Technician grant**, click **Enable**.
4. Under **Technician pin of the day code**, click **Pin of the day**. The following window appears:

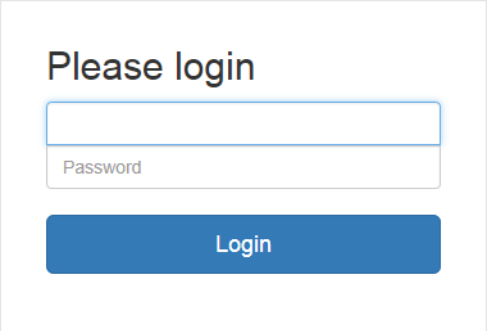


5. In the **Validity** box, enter the time (in minutes) that the PIN has to remain valid. The maximum time is 1440 minutes = 24 h.
6. Click **Create**. A new PIN appears under **Current pin of the day**. The counter in the **Remaining Validity (min)** box displays for how long (in minutes) the new code is still valid.

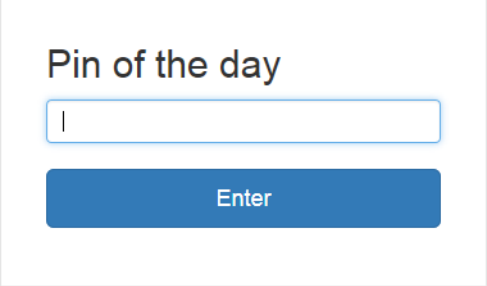


7. Write down the code (including the dashes), or keep the window open and move it to where you will be able to see it while logging on to the hardware configuration tool.
8. Open Internet Explorer, and type the following url in the address bar:
   http://*ipaddress:controlport*/login
   where *ipaddress* is the XO device's IP address and *controlport* is the control port number. For example, with

the default IP address and control port:
http://10.0.0.10:2000/login
The following screen appears:



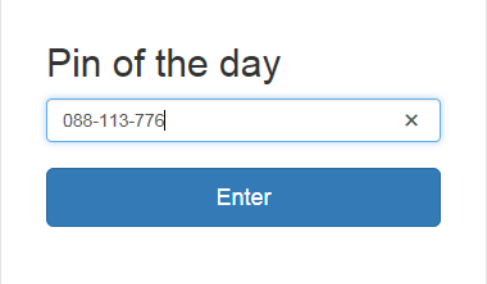
9. Type the username (**15**) and password (default is **666777**) for the Technician user, and click **Login**. The following screen appears:



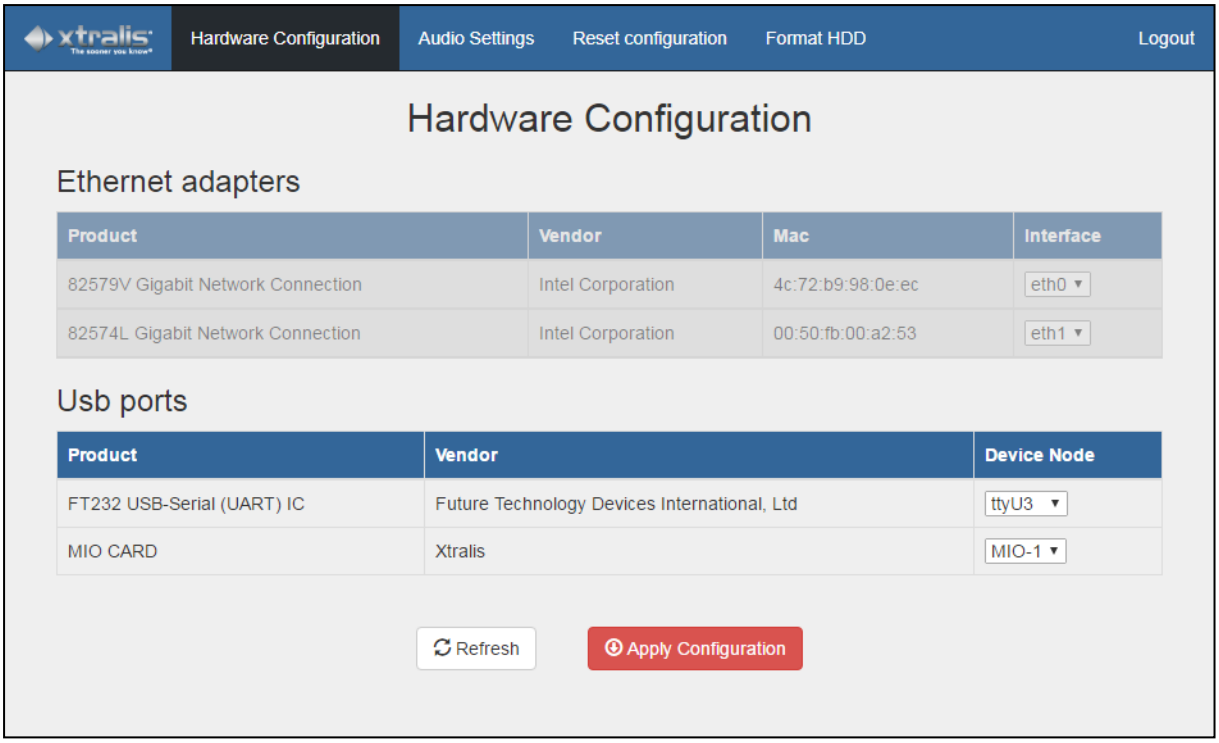
Note

If the **Login** window appears again, check in the XO client software if the Technician user is enabled.

10. In the **Pin of the day** box, type the code that you noted down in step 7. Include the dashes.



11. Click **Enter**. The hardware configuration screen appears:



> **Note**
> If the **Pin of the day** window appears again, you have entered an invalid PIN code.

The **Usb ports** list shows the currently configured USB ports (**Device node** column): **MIO-1** is the first MIO card (or set of MIO+EIO card).

You can now connect the XO I/O Interface USB module and map it.

8.3 Mapping I/O Interface USB Modules to the XO Device

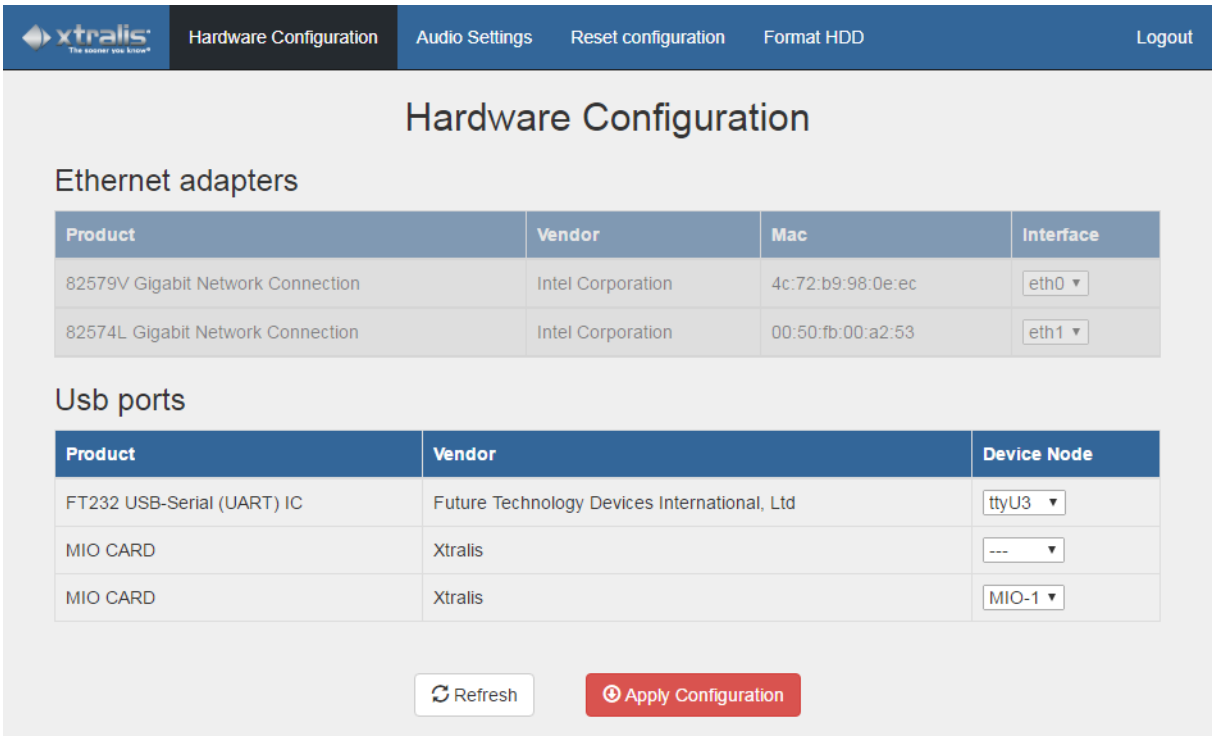
> **Note**
> XO Gateway I/O USB Module is primarily designed for iFT Gateway, but it can be added to any other XO device that does not already have 2 MIO cards via the hardware configuration page.

To connect and map the XO I/O Interface USB modules or the XO Gateway I/O USB Module, proceed as follows:

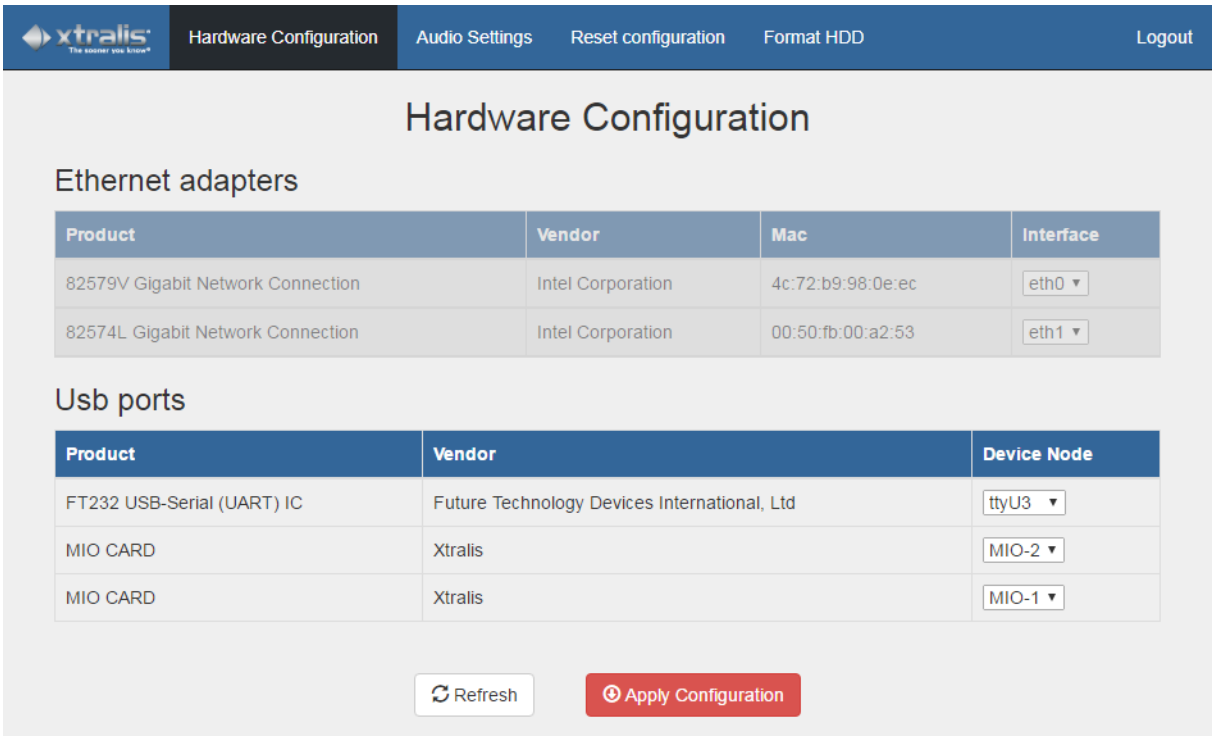
1. If you have not done so already, log on to the hardware configuration tool.
2. Connect the XO I/O Interface USB module or the XO Gateway I/O USB Module to the XO device using the provided USB cable: insert one end into the module, and the other end into a free USB port on the XO device.

> **Note**
> If you are using a double module, Honeywell recommends to connect and map each module separately. Because the modules all appear with the same name in the **Product** column (**MIO CARD**), this will prevent incorrect mapping.

3. In the hardware configuration tool, click **Refresh**. The module will now appear in the list, with the **Device Node** column empty.
   The example below shows a device that already has a first set of MIO/EIO cards: **MIO-1** is already configured. The row above (**- - -**) indicates the newly connected module that needs to be mapped.

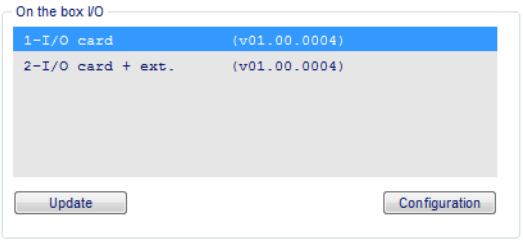


4. Select the desired set number for the module in the **Device Node** column.



5. Click **Apply Configuration**.
   The message *Are you sure to apply your configuration?* appears.
6. Click **Apply**.
   The *Waiting to apply…* message appears.
7. Wait for the message to disappear.

8. If you are mapping a double module, repeat for the second module: connect it to the XO device using the USB cable, click **Refresh** in the configuration tool, and map the module to the correct set number.
9. If the **Product** columns shows any other devices (in the example screen above, the FT232 USB Serial = an RS-485-to-USB converter), make sure that these devices are also mapped to a suitable USB port.
10. Click **Logout**.
11. Restart the XO device.
    The XO client will not discover the I/O cards until you have restarted the device.
12. Open the XO client and check if the added module is visible in the **I/O** window: choose **System** > **Connections** > **I/O**. For example, if you have added a single module to serve as a second set of I/O cards, you will see a second line indicating **2-I/O card + ext**.



13. If there were other devices in the hardware mapping list, then:
    - Check their serial ports settings (**System** > **Connections** > **Serial Ports / PTZ**).
    - Test all related functionality (PIR detectors, analogue PTZ camera, modem…).

You can now use the MIO/EIO cards in the module in the same way as the MIO/EIO Next Generation cards. The LEDs on the XO I/O Interface USB module follow the LEDs on the front of the XO device.

8.4 Resetting the Hardware Mapping

When you use XO I/O Interface USB modules, the system reconfigures the USB ports and they no longer have the default numbering as described in the hardware manuals.

If you have **removed all** the XO I/O Interface USB modules from your XO device, you can reset the USB port configuration back to the defaults. For details, see the *XO I/O Interface USB Module Technical Manual* (32688).

8.5 About the XO Gateway I/O USB Module

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.

> ***Caution!***
>
> The on-the-box IO gets disabled when you configure XO Gateway I/O USB Module to a XO device.
>
> XO 5.0 is needed to support XO Gateway I/O USB Module on iFT Gateway.

The module offers:

- Extra I/O: 4 voltage free monitored inputs + 4 voltage free relay out + RS485, and an internal buzzer.

All this is configurable via XO Client.

The Gateway I/O USB port connects to a USB port on a XO device (eFT, iFT, iFT Gateway, FT2).

For detailed information, see the *XO I/O Interface USB Module Technical Manual* (32688).

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

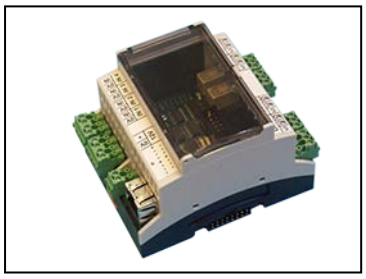
The Network (Net) I/O units provide extra inputs and outputs for your XO device. You mount the units on a DIN rail and connect them to the local network. To power the units: use PoE, a PoE injector, or a local power adapter (12 VDC; min. 350 mA).

Each base unit offers 4 inputs and 4 outputs, and LED indicators and a buzzer controlled by the XO device. You can extend each base unit with 1 to 3 extension units, to obtain up to 16 inputs and outputs.
As you can link your XO device to up to 8 units (8 base units, each with up to 3 extension units), you can obtain a total of 128 extra inputs and 128 extra outputs.

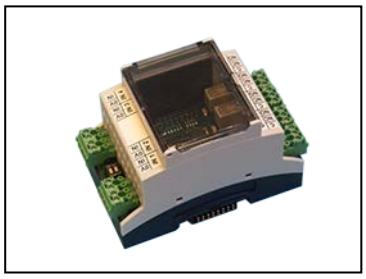
The latest Net I/O units offer monitored inputs (requires V2 hardware and firmware, and min. firmware version XO 4.02 running on the controlling XO device. For details on monitored inputs, see the *ADPRO Network I/O Units Technical Manual* (33355).

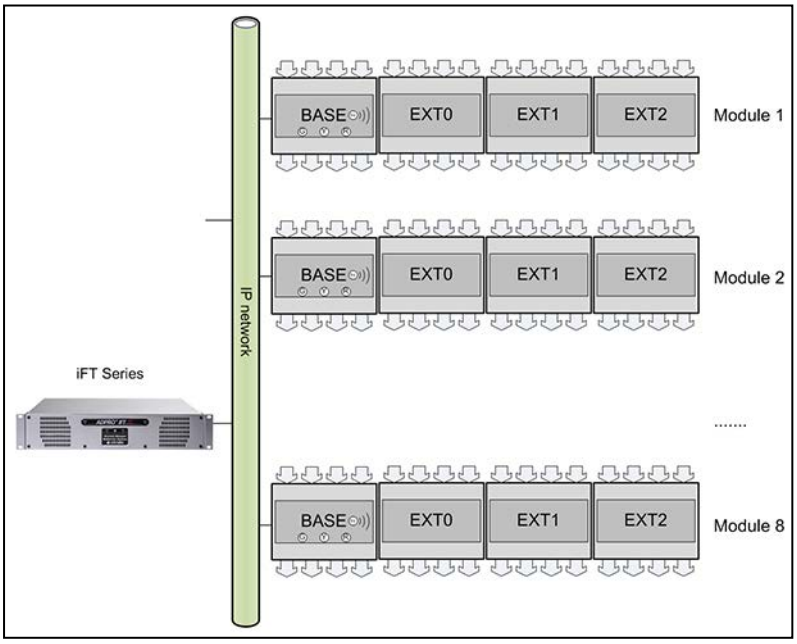
> ***Caution!***
>
> **Before plugging or unplugging any extension units, switch off the power to the base unit.**
>
> Plugging or unplugging extension units with power on may result in **permanent and irreparable damage** to the base and/or extension units.

Base unit:



Extension unit:





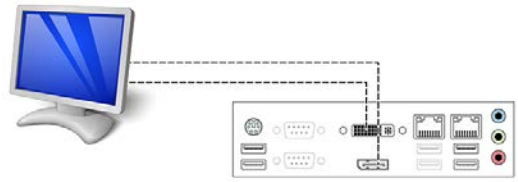
For detailed installation instructions, including programming the IP address and updating the software, see the *ADPRO Network I/O Units Technical Manual* (33355).
To configure the inputs and outputs, see the *XO Client Software User Manual* (21796).

10 Monitor

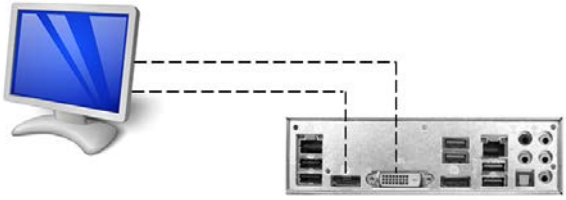
You can connect a monitor directly to the XO device, and use it for:

- Live viewing in a matrix view
- Consulting basic system information in the XO welcome screen
- Accessing the **XO Installer** menu for advanced hardware setup.

The PH10LU motherboard monitor connections:



The PH10FEU motherboard has two DP ports, which enable connecting one Matrix monitor and one Spot monitor.



Note

For VGA, you can use either a DP to VGA or DVI-D to VGA converter.

To set up live viewing on the monitor, see the *XO Client Software User Manual* (21796).

Note

- 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.
- 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.

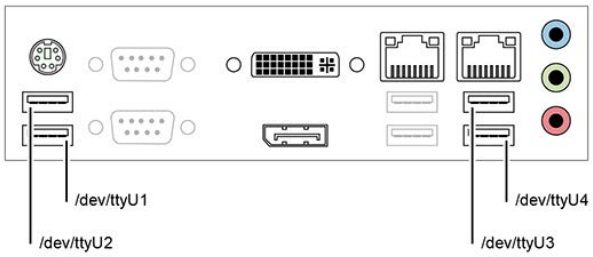
11 Modem

You can connect one modem to the XO device, to the /dev/ttyU1 USB port. You can use either a PSTN/ISDN or a 3G/4G modem.

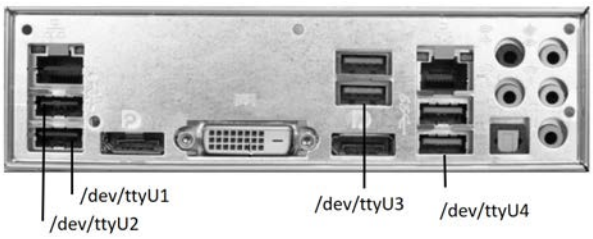
- **PSTN or ISDN modem**: you connect a classic PSTN (ISDN) modem with serial port to the device by means of a USB-to-RS-232 converter. This USB-to-RS-232 converter needs a specific FTDI chip.
  The Stollman TA+USBA is the only ISDN modem with USB interface that you can use without a converter.
- **3G/4G modem**: 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.
  With firmware version XO 4.02 and above, you can also use the 4G Huawei E8372 wingle. For details, see *4G Via Wingle* on page 58.

Connect the modem to USB input 1 (/dev/ttyU1).

PH10LU USB inputs



PH10FEU USB inputs



Restart the XO client software before configuring the modem. For more information, see the *XO Client Software User Manual* (21796).

12 4G Via 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. For details, see the *XO Client Software User Manual* (21796).

13 Audio

You can use not only video images on the XO device, but also audio – both in and out.

13.1 Audio IN

Audio input is available from the cameras' audio inputs, or from IP audio devices such as the Axis horn speaker. The iFT Series does not support analogue audio in.

You can choose to record audio, and listen to audio in the live view. For an overview of IP cameras that support audio in, see the *Supported IP Camera List* (26742). Usage of IP audio modules is similar to IP cameras with audio in capabilities. For details, see *Using IP Audio Devices* on page 64.

Note

- If the connection bandwidth is low, it is recommended to disable live audio streaming.
- Audio IN is unbalanced audio.
- Changing the audio settings requires a system restart.

In the XO client, you have to enable the audio inputs for recording and listening in the live view. For more information, see the *XO Client Software User Manual* (21796).

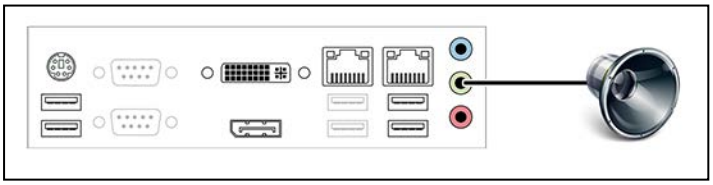
13.2 Audio OUT (Talkback)

13.2.1 Options

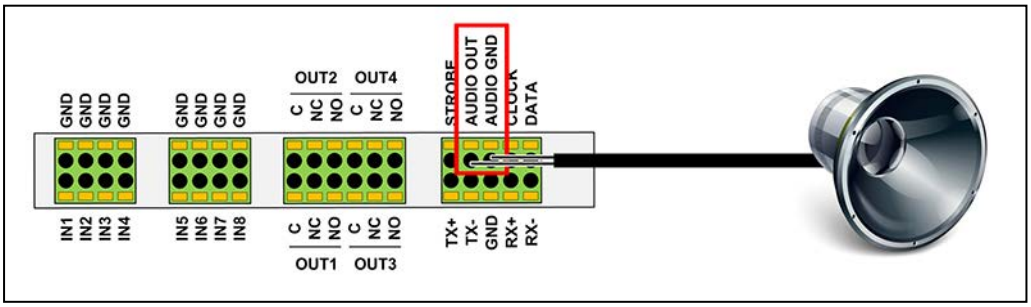
Talkback to the site works via the **Live Video** window in the XO client software. You select a camera, and then use the microphone (typically connected to the client PC) to talk to the site via the speaker that is associated with that camera.

If you need **only one speaker** on your site, you have the following options:

- Connect an amplified loudspeaker to the audio out plug of the motherboard (= green 3.5 mm jack).



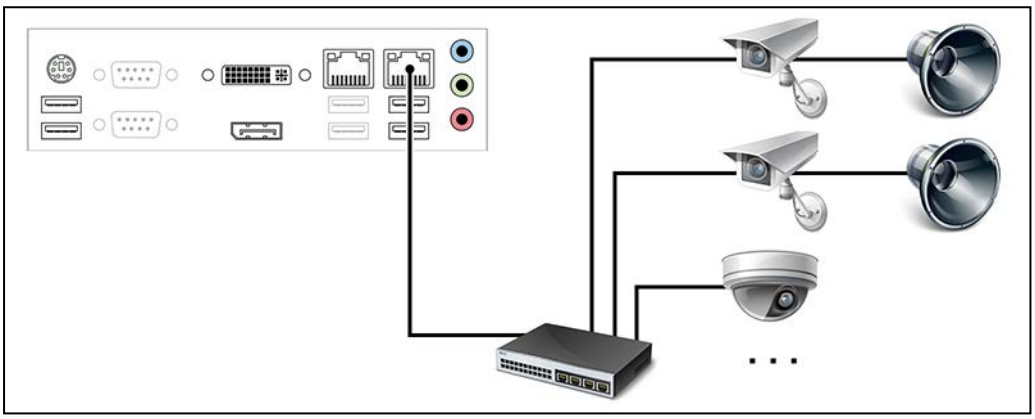
- Connect an amplified loudspeaker to the audio output on the MIO card (with built-in MIO card only, not available on an external XO I/O Interface USB module).



In this case, all cameras are automatically associated with that one speaker.

If you need **more than one speaker** (audio zoning) on your site, you have the following options:

- Use **VM22A** audio units (with built-in MIO card only) to connect up to 20 loudspeakers. Install one or two VM22A units connected in cascade:
  - Unit 0 is controlled by the MIO card, and drives loudspeakers 1 to 10.
  - Unit 1 connects to unit 0 via the loop connector on the VM22A, and drives loudspeakers 11 to 20.
- Use **VM22E** audio units to connect up to 32 loudspeakers. Install up to 8 VM22E units in cascade:
  - Unit 0 drives speakers 1 to 4.
  - Unit 1 drives speakers 5 to 8…
- Use the IP audio outputs on your IP cameras with (built-in) speakers. This feature is available with firmware version XOa 3.02 and above; and for specific camera models only. For more information, see the *Supported IP Camera List* (26742).



- Use an IP audio device such as the Axis Network Horn Speaker (C3003-E). Usage is similar to IP cameras with audio out capabilities. For details, see *Using IP Audio Devices* on page 64.

You use the XO client software to assign the different speakers to the cameras. For each camera, you can choose:

- One output on a VM22 output switcher
- One or more outputs on IP cameras.

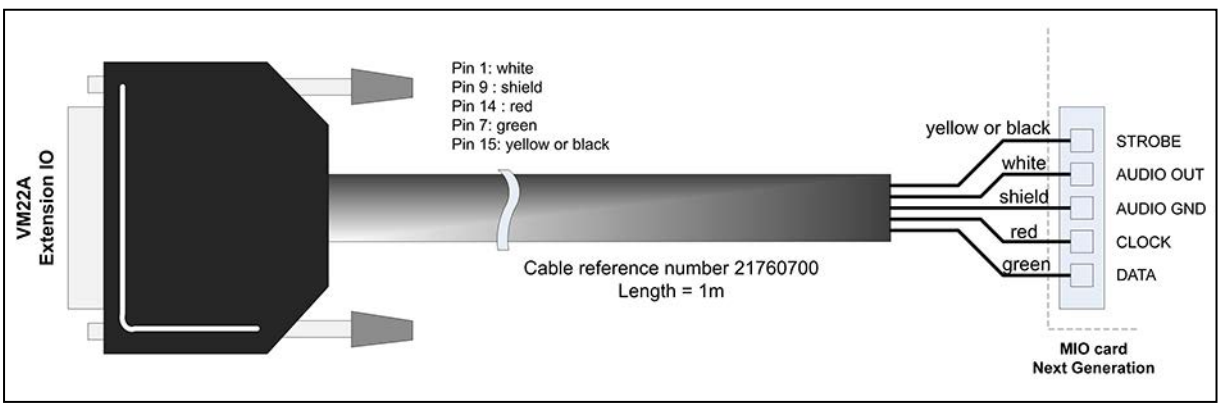
13.2.2 Setup for VM22A

Note

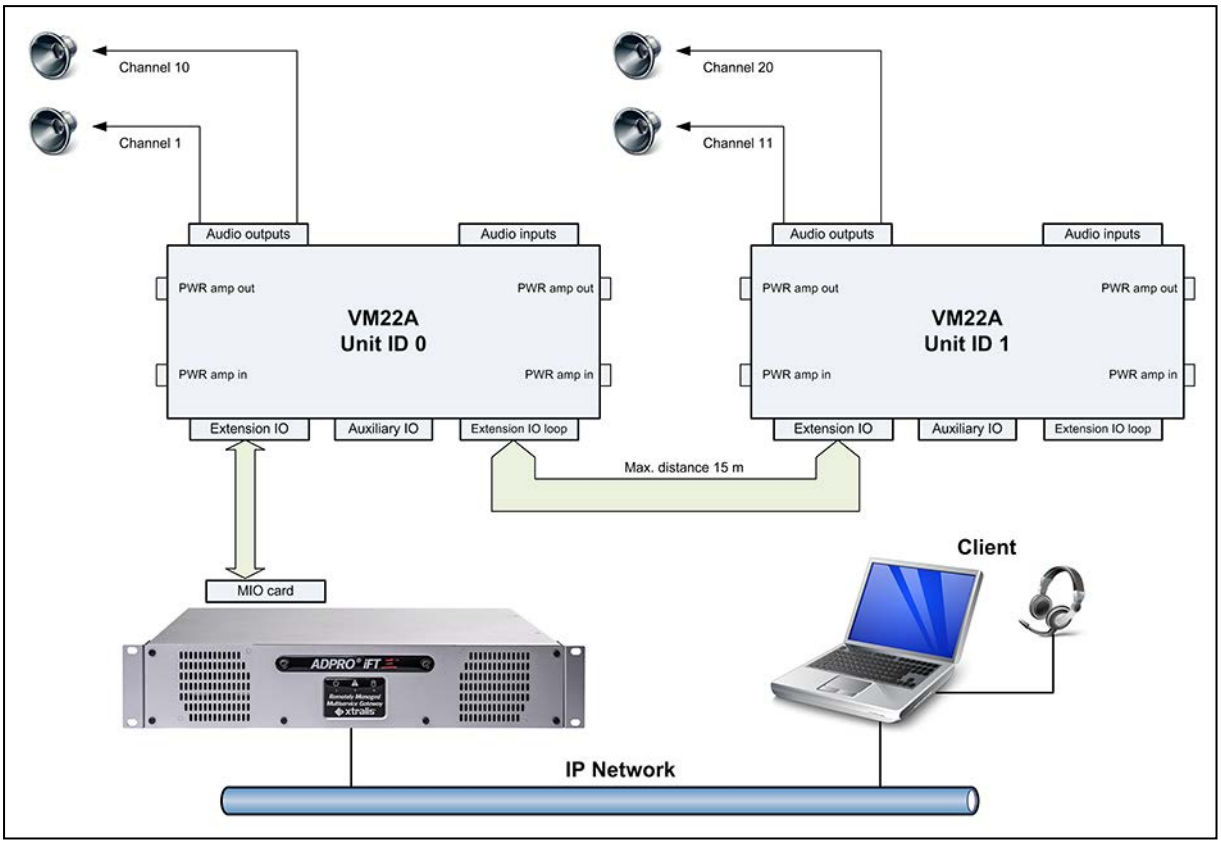
The VM22A audio switcher is only compatible with built-in MIO cards, not with the MIO cards in the external XO I/O Interface USB modules.

You need a specific cable to connect the VM22A to the XO device.

Connect the cable to the back of the device as illustrated below. Respect the colour code (yellow = STROBE; white = AUDIO OUT, shield = AUDIO GND, red = CLOCK, and green = DATA).



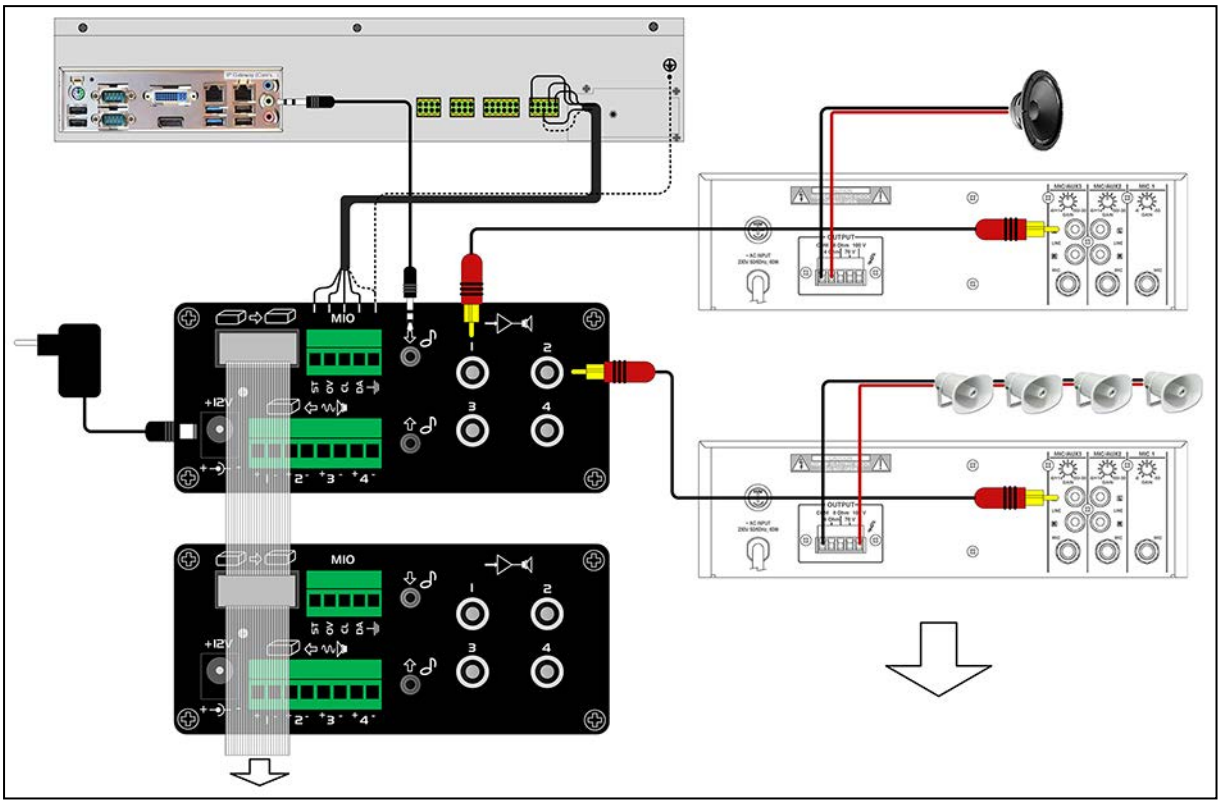
The diagram below shows a typical setup that allows talkback on the monitored site: it provides 20 audio outputs (loudspeakers) via two VM22A units in cascade. A headset connected to the client PC serves as the audio input (microphone).



For more information, see the *VM22A Audio Switcher – Installation and User Manual*.

13.2.3 Setup for VM22E

For the hardware installation of the VM22E, see the connection scheme below. The illustrations below show connections to the built-in MIO card, but you can also connect to a MIO card in an XO I/O Interface USB module.



The table below lists the correct connections between the VM22E module and the MIO card (built-in or external):

VM22E terminal	MIO card Next Generation	
	No.	Name
ST	30	STROBE
0V	33	GND
CL	36	CLOCK
DA	38	DATA
⏚	33	GND

For more information, see the *VM22E Technical Manual* (29541).

13.2.4 Troubleshooting Talkback

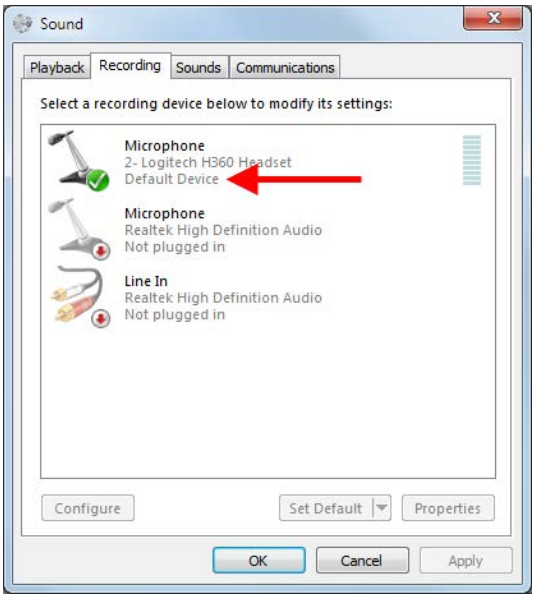
You can test talkback using the XO client. The audio out setup screen provides a test button to play a sound clip. For details, see the *XO Client Software User Manual* (21796).

If talkback does not work, check the following:

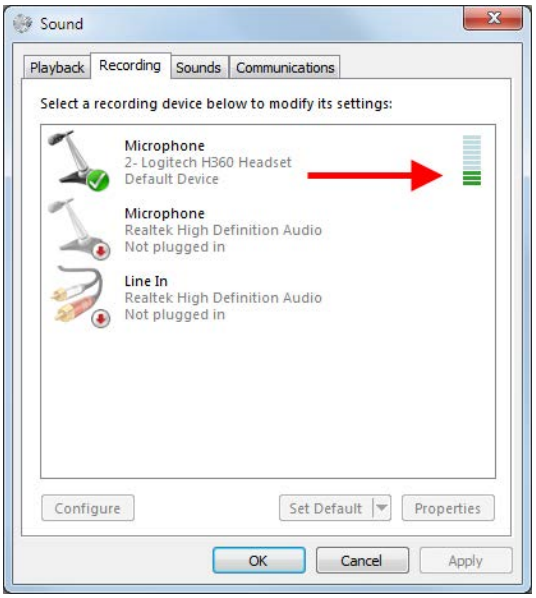
- In the XO client software, check the access rights of the user: **Audio talk** must be allowed.
- Routers may block UDP packets. In the audio setup in the XO client, specify TCP, or configure the router to allow UDP packets.
- Use the PC headphones plug instead of the PC microphone plug.
- Check the configuration of the microphone on your computer. For details, see below.

To configure the microphone on your computer in Windows 7, proceed as follows:

1. Click **Start**, and then click **Control Panel**.
2. Click **Sound**, and then click the **Recording** tab.
3. If you have more than one sound device, check if the device you want to use with the XO device is the default device. If not, right-click the desired device, and click **Set as Default Device**.



4. To test if the microphone works, tap it with your finger a few times. The blue lines next to the default microphone light up in green, indicating the volume.



5. Click **OK**, and close **Control Panel**.

13.3 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).

14 Connecting PIR Detectors

14.1 Required PIR Firmware

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 (e.g. alarm management).

14.2 Connecting PIR Detectors

To connect PIR detectors to the XO device, you have the following options:

Connection method	Max. no. of PIR detectors
RS-485 cable connected directly to the MIO card of the XO device	32 on the RS-485 bus
Via a USB-to-RS-485 8-channel distribution unit, connected to a USB port on the XO device	32 on the RS-485 bus
Via a USB-to-serial-port RS-485 converter, connected to a USB port on the XO device	32 on the RS-485 bus
Via the IFM-485-ST interface module, connected to a USB port on the XO device	32 on the RS-485 bus
Via IP modules, connecting the PIR detectors via the local network to the XO device (no RS-485 bus required)	34; with firmware version XOa 3.02.0001 or above

You can connect maximum 32 PIR detectors on an RS-485 bus. However, you can combine an RS-485 bus and IP modules to connect more PIR detectors to the XO device.
The maximum number of PIR detectors on an XO device is 34 (requires minimum firmware version XOa 3.02.0001).
The XO client will indicate how each PIR detector is connected: over RS-485 (**SER**) or over IP (**ETH**).

You can connect a PIR detector to only one XO device.

Note

You need a PIR-HLI application license to enable the PIR detectors. Use Xchange to install the license on the XO device. For more information, see the *Xchange Tool User Manual* (27816).

14.3 PIR Address Range

Regardless of the connection method, PIR detector addresses must be in the following ranges:

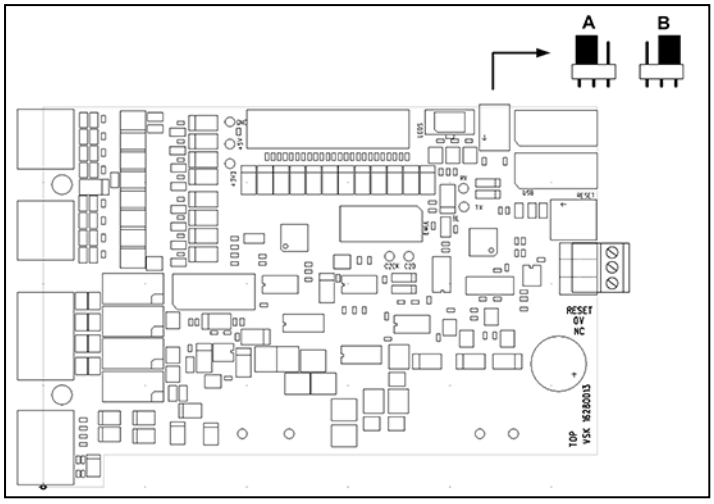
- Firmware version XOa 3.02.0001 and above: 1–34. The XO device will not discover PIR detectors with addresses above 34.
- Firmware versions below XOa 3.02.0001: 1–32. The XO device will not discover PIR detectors with addresses above 32.

Furthermore, each PIR detector must have a unique address, regardless of the connection method (RS-485 or IP). For instructions on setting PIR detector addresses, see the *ADPRO PRO E PIR System Setup Manual* (26571).

14.4 Direct Connection to the MIO Card

Connect the PIR detector(s) to the XO device by connecting the RS-485 cable of the PIR closest to the XO device to the MIO card of the XO device. You can connect up to 32 PIR detectors in cascade on the RS-485 bus.

On the internal MIO card, set the RS-485 jumper to the 2-wire position (**A**).

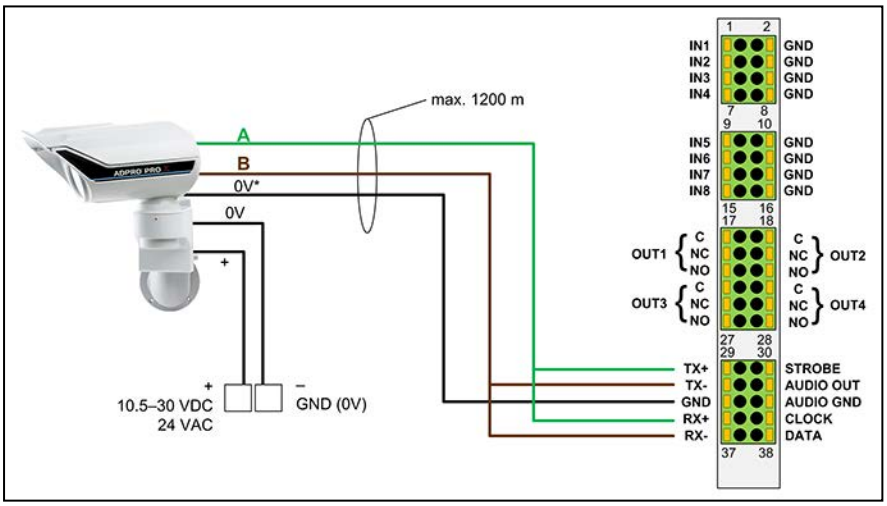


MIO card Next Generation	
A	RS-485 PTZ jumper: 2-wire setting (default setting – see Note below)
B	RS-485 PTZ jumper: 4-wire setting

Note

On systems produced from the end of April 2015, the default setting of the RS-485 PTZ jumper is 2-wire. On older systems, the 4-wire setting was default. If you experience any problems when connecting devices to the MIO card, check the RS-485 PTZ jumper setting. Change it if necessary.

Connect the wires as shown below:



(*) Some PIR models have separate 0V terminals for data and power; on other models there is only one common 0V terminal.

Make sure to bridge the following connections:

- TX+ with RX+
- TX– with RX–

The PIR detectors are powered locally by a power adapter.
You can place locally powered PIR detectors at the maximum distance of 1200 m for RS-485 cables. Make sure that there is no difference in earth potential between the XO device and the PIR detector.

14.5 Connection via the USB-to-RS-485 8-Channel Distribution Unit

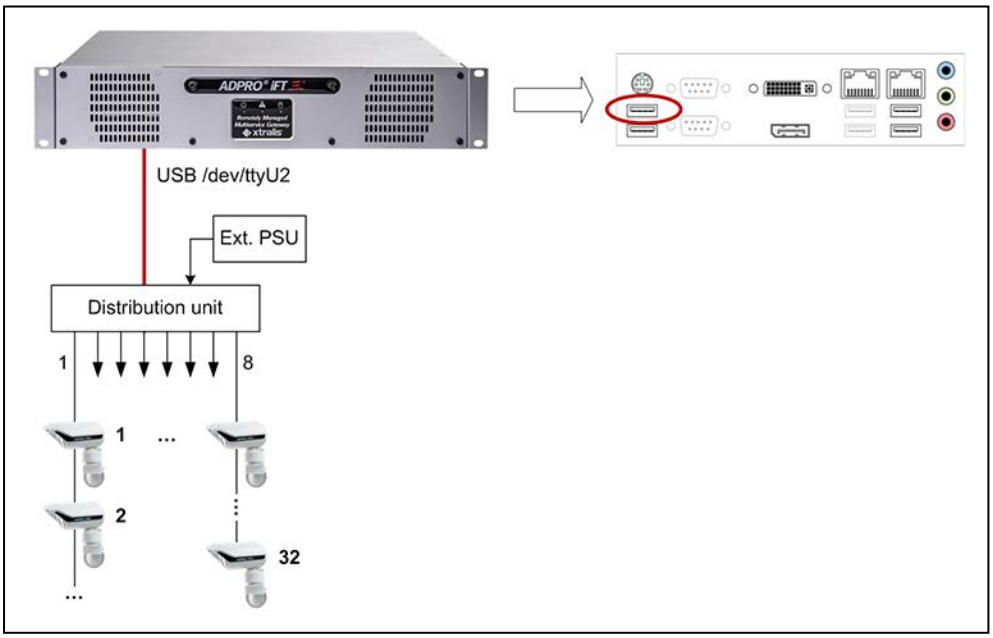
The USB-to-RS-485 distribution unit provides 8 channels to easily connect and configure the PIR detectors on the XO device.

Each PIR detector needs a unique address. For the appropriate address ranges, see *PIR Address Range* on page 65. You can use the unit, together with the ADPRO PIR software on your PC, to assign a unique address to the PIR detector. In this case, connect the distribution unit to your PC, and connect only 1 PIR detector per channel on the distribution unit. For details, see datasheet *USB-RS-485 distribution unit* (19532060).

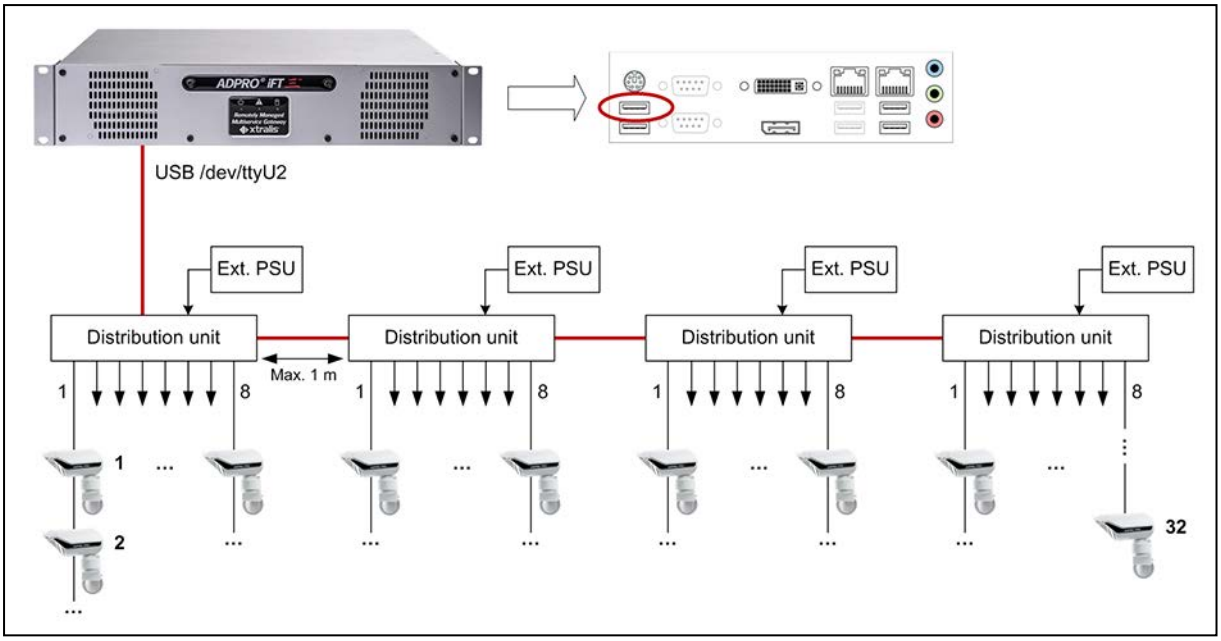
Once you have assigned unique addresses to the PIR detectors, you can connect multiple PIR detectors to the same channel on the distribution unit, allowing you to connect 32 PIR detectors to an XO device using only 1 distribution unit. Depending on the existing installation (see the restrictions on distances and cable lengths further below), you can determine which PIR detectors you connect to which channel. If necessary, you can connect up to 4 distribution units in cascade. In that case, you connect only one of the 4 distribution units directly to the XO device.

Keep the following in mind:

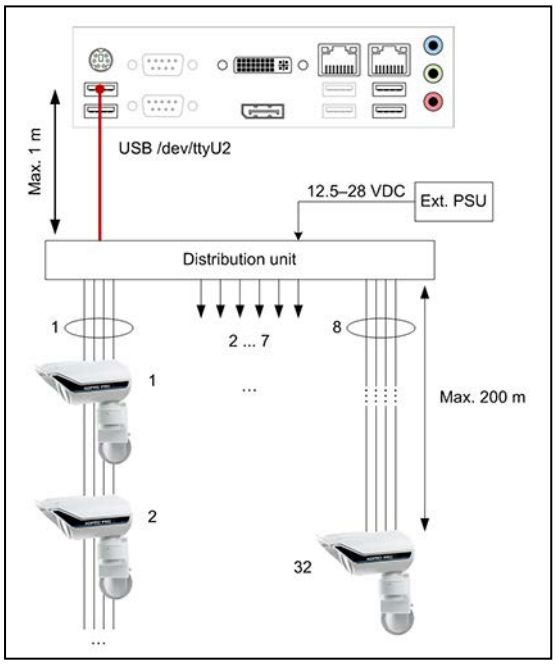
- Before connecting multiple PIR detectors to the same channel, you have to assign a **unique address** to each PIR detector.
- Connect the distribution unit to the **/dev/ttyU2** USB port on the XO device. Do not use any other ports.
- Restart the XO software after connecting the PIR detectors to the USB port.
- Only the 485 bidirectional communication of the PIR detectors is used, not the mechanical PIR tampers.
- The **maximum distance** between distribution unit and PIR detector is 200 m. If the distance is longer than 200 m, then the PIR detector needs a separate local power supply.
- With local power supplies, the **maximum distance** between distribution unit and PIR detector is 1200 m.
- The **maximum length** of the USB cable between the distribution unit and the XO device is 1 m.
- If you use several distribution units in cascade, the **maximum length** of the cables between the units is 1 m.



An example of distribution units in cascade:



A detailed view of a connected distribution unit:



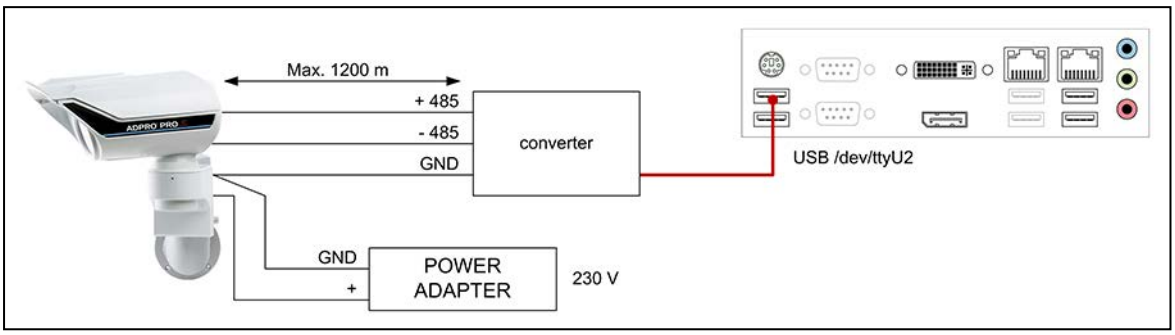
The maximum length of the USB cable between the XO device and the distribution unit is 1 m.

Four wires connect the PIR detector to the distribution unit (power supply and communication).

The maximum distance between distribution unit and PIR detector is 200 m. If the distance is longer than 200 m, then the PIR detector needs a separate local power supply.

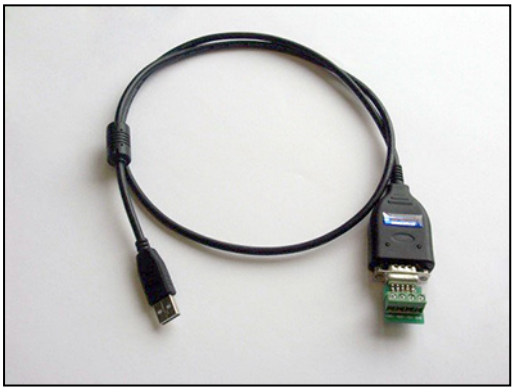
14.6 Connection via the USB-to-Serial-Port RS-485 Converter

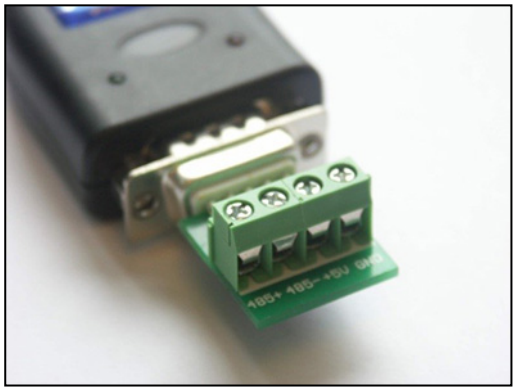
Connect the PIR detector to the converter and plug the USB cable of the converter in the /dev/ttyU2 USB port of the XO device.
Restart the XO client software after connecting the PIR detectors to the USB port.



You can place locally powered PIR detectors at a maximum distance of 1200 m with RS-485 cables. Make sure that there is no difference in earth potential between the XO device and the PIR detector.

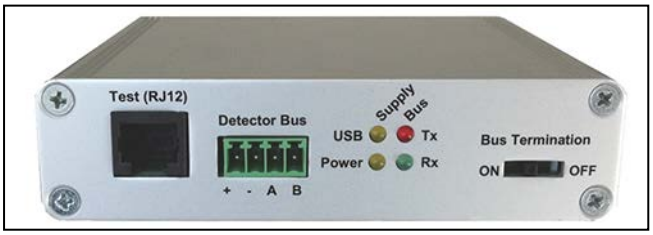
You need to order the USB to serial port RS-485 converter separately (reference number 20415490).





14.7 Connection via the IFM-485-ST Interface Module

The IFM-485-ST is an interface module which allows to conveniently connect the RS-485 bus of the PIR detector to the /dev/ttyU2 USB port of your XO device.



For detailed installation instructions, see the *ADPRO IFM-485-ST Legal Disclaimer & Intended Use of Product* (27178), and the *ADPRO PRO E PIR System Setup Manual* (26571).

14.8 Connection via IP Modules (PRO E-IPM)

14.8.1 Summary

IP modules allow you to connect PIR detectors via the local network, instead of via an RS-485 bus. The modules convert the signals from network to RS-485. They are powered via PoE.

You need to set up the IP modules so that they can communicate with the XO device: assign an IP address, and specify the correct communication settings. For this, you will use the Lantronix DeviceInstaller program. Honeywell recommends to use IP addresses in the same range as the local network of the XO device (eth0; not in eth1 which is the range of the IP camera network).

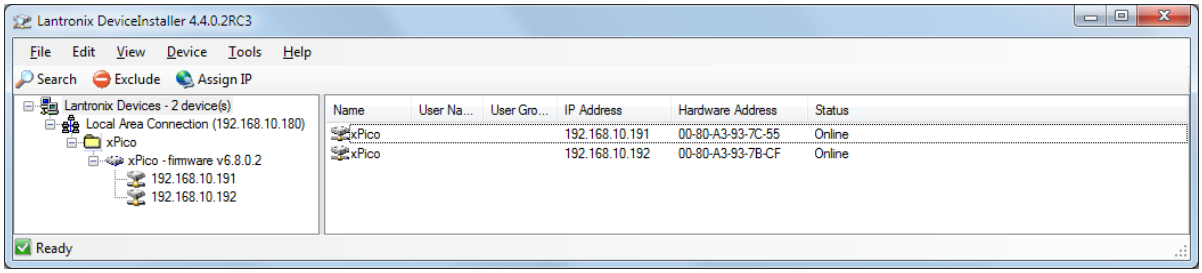
After the configuration, you can connect the IP modules to the PIR detectors, and finally add the IP modules to the XO client.

14.8.2 Setting up the IP Modules

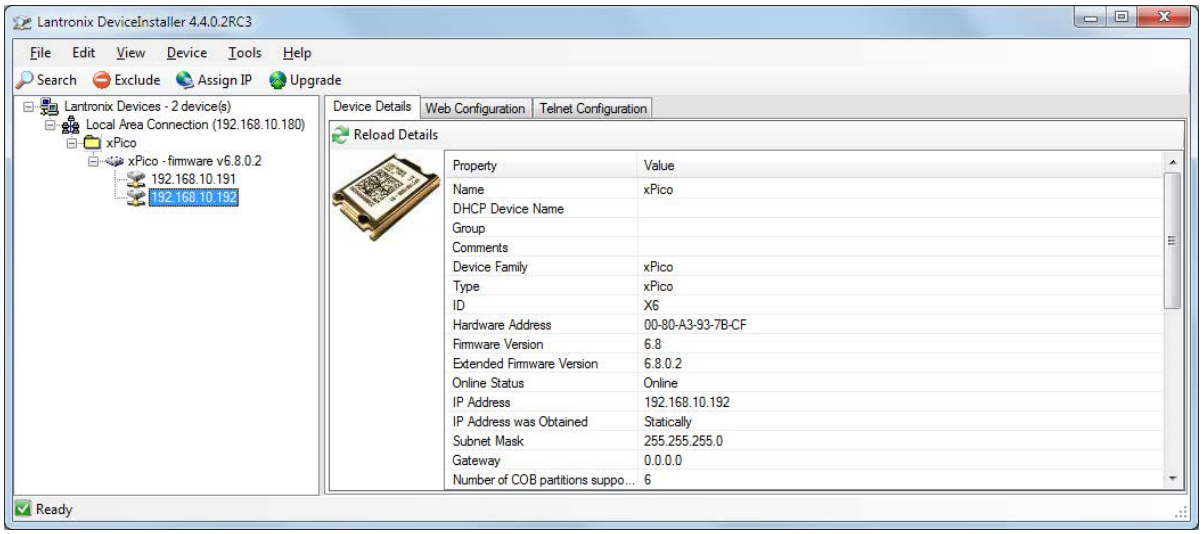
The IP modules only work with the XO client software if they have a static IP address and use the UDP communication protocol. Furthermore, you must set up the serial ports of the IP modules.

To set up the IP modules, proceed as follows:

1. Connect the IP modules to the network, and make sure that your PC is in the same network.
2. Download and install the Lantronix DeviceInstaller program (available from www.lantronix.com/products/deviceinstaller).
3. Launch DeviceInstaller. It automatically starts searching for the IP modules (xPico devices) on the network. If the search does not start automatically, click **Search**.



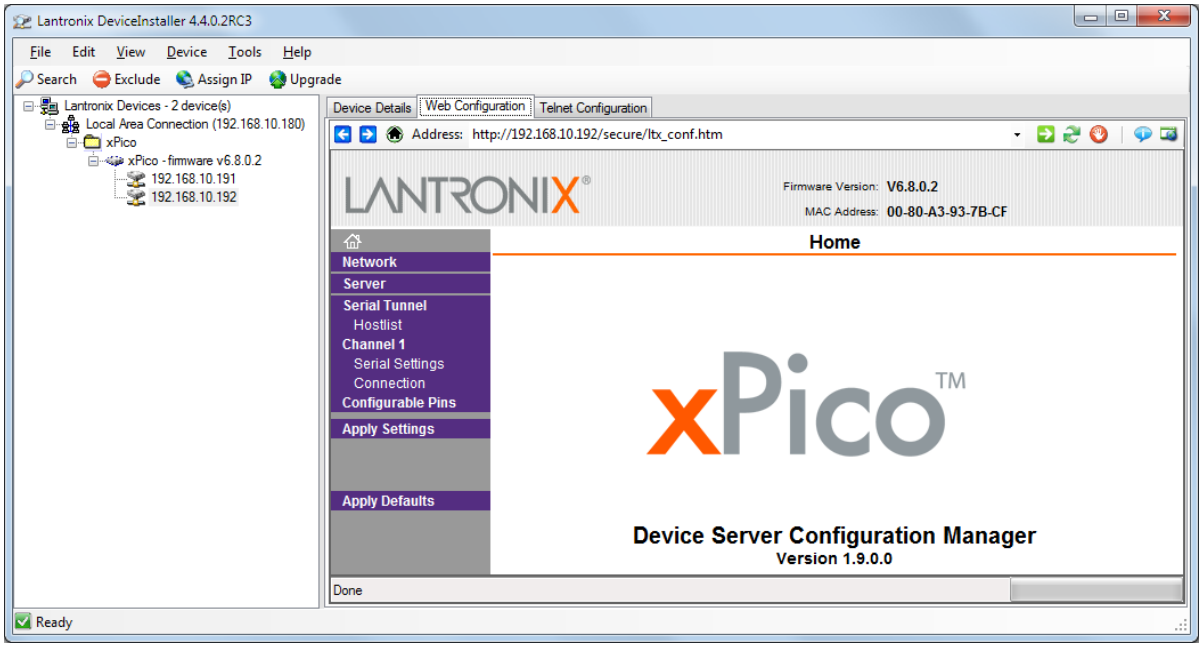
4. To configure a module, double-click it in the list.



5. Click the **Web Configuration** tab, and then click the button to connect to the module.

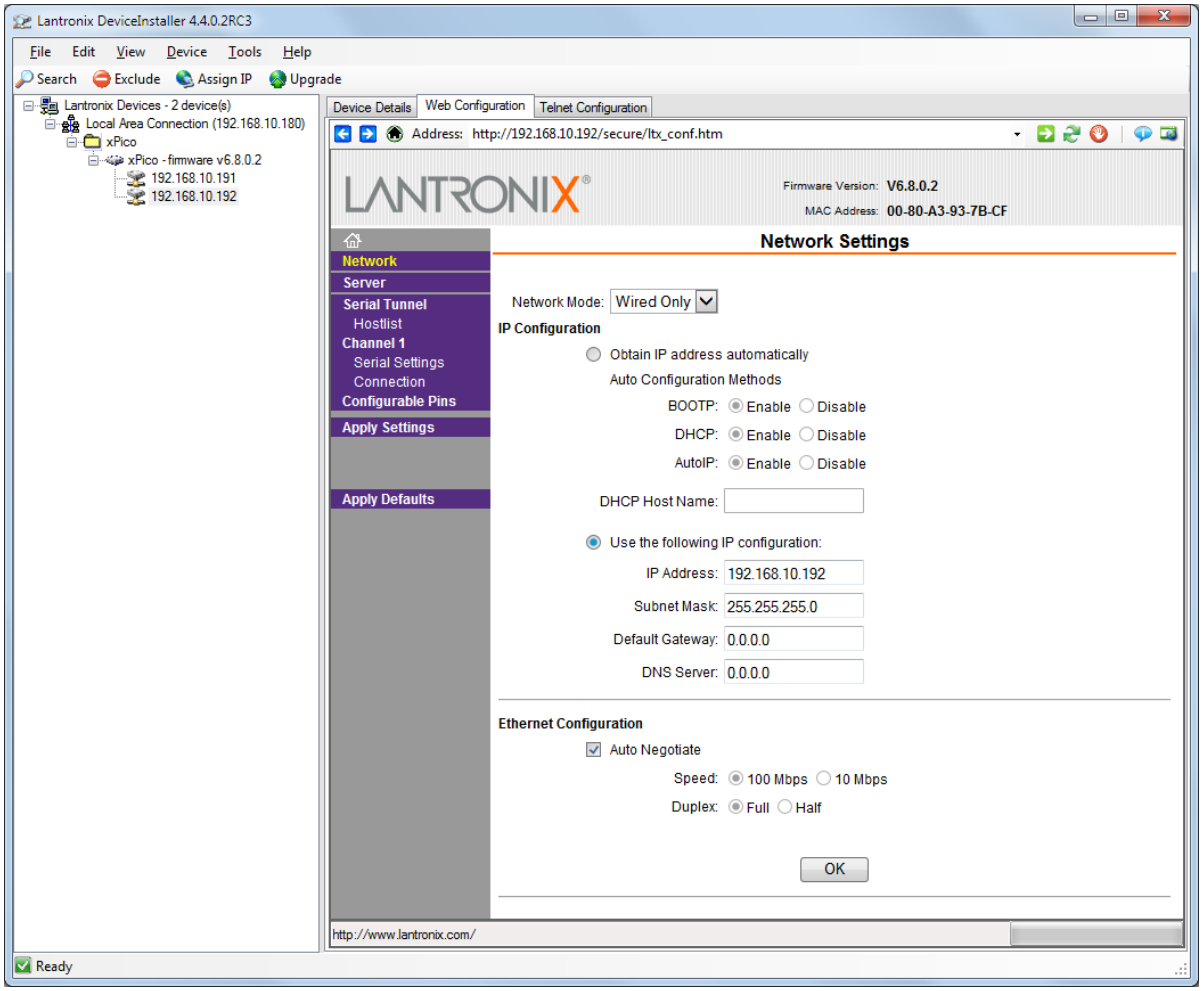


6. Leave the username and password blank; just click **OK** to continue.



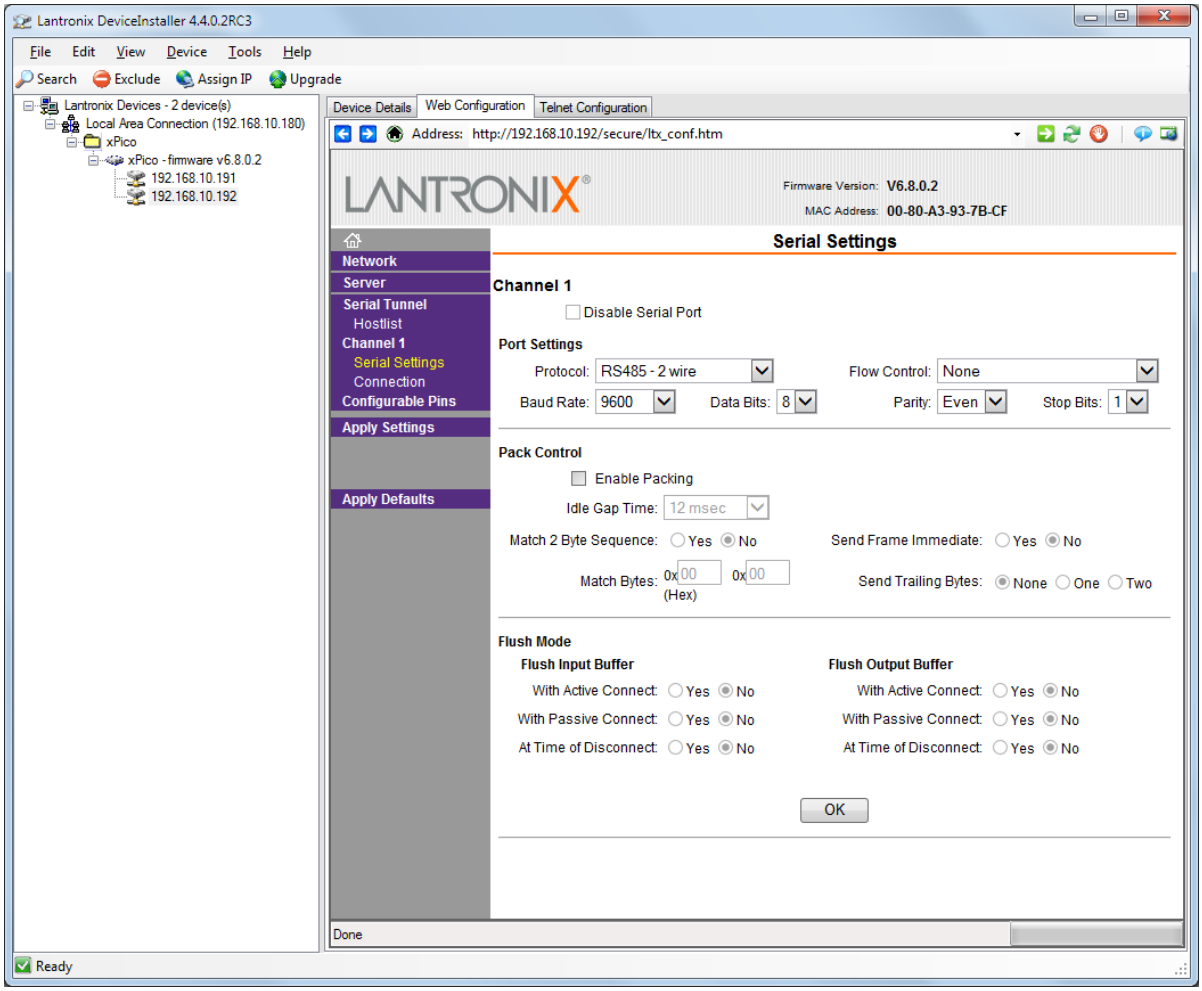
Next, you will make sure that the module uses a static IP address.

7. Click **Network**, and provide the correct network settings. The example screen above shows the settings for an IP module with IP address 192.168.10.192. Honeywell recommends to use IP addresses in the same range as the local network of the XO device (eth0; not in eth1 which is the range of the IP camera network).



8. Click **OK** to save the settings.
Next, you will set up the serial port communication.

9. Click **Serial Settings**, and set the parameters as shown in the screen below.

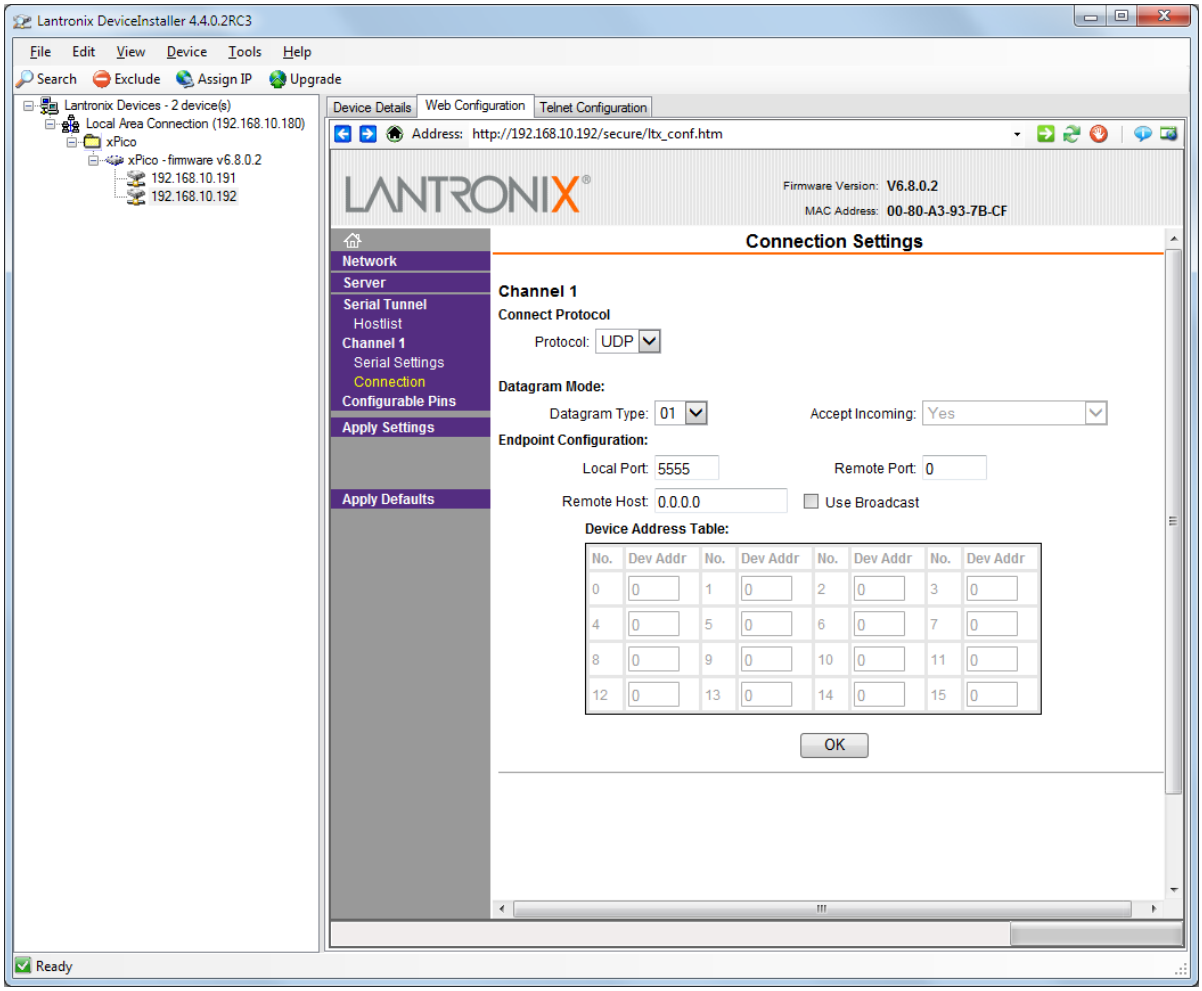


Make sure that the **Port Settings** are as follows:

Item	Description
Protocol	RS485 - 2 wire
Flow control	None
Baud rate	9600
Data Bits	8
Parity	Even
Stop Bits	1

10. Click **OK** to save the settings.
Next, you will set up the module to use UDP communication.

11. Click **Connection**, and set the parameters as shown in the screen below:

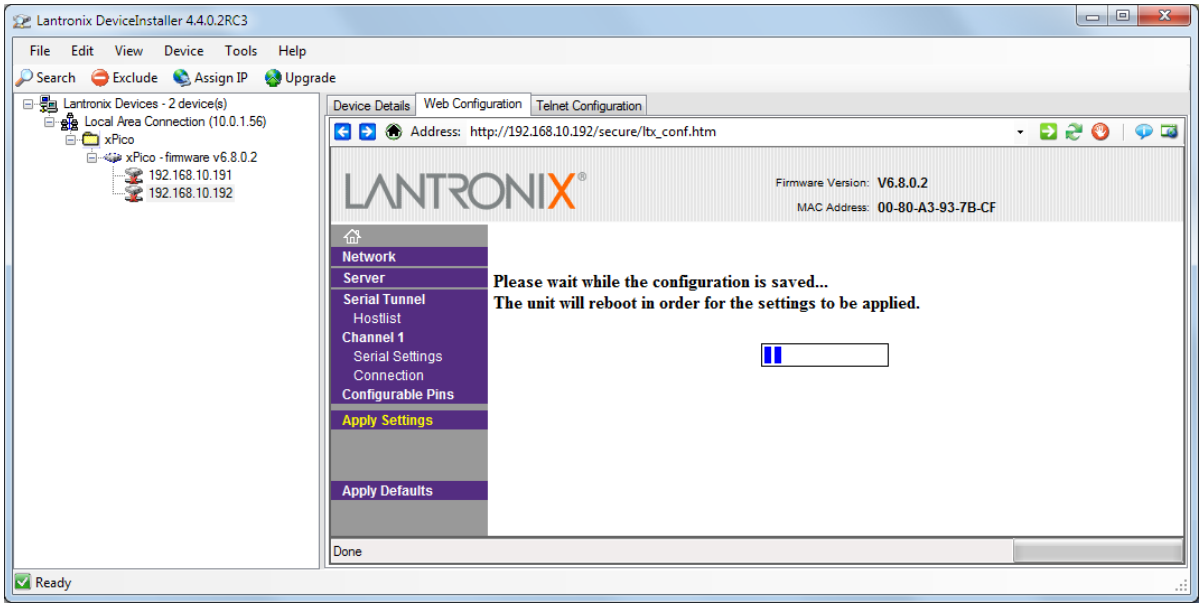


Make sure to set the following parameters correctly:

Item	Description
Protocol	UDP
Datagram Type	01
Local Port	5555

12. Click **OK** to save the settings.
Next, you will apply all the settings to the module.

13. Click **Apply Settings**.



The module will restart, and will then become available with the new IP settings. You can change the IP address in the address bar, or you can use the search function as before.

14. Repeat steps 4 to 13 for other IP modules.

Now you can connect the IP modules to the PIR detectors.

14.8.3 Connecting the IP Modules to the PIR Detectors

For details on connecting the IP modules to the PIR detectors, see the document *ADPRO PRO E-IPM Legal Disclaimer & Intended Use of Product* (27556).

Take into account that the wire colours may be different:

A	Blue	Red
B	Black	Orange
+	Brown	Yellow
GND	Red	Green

After connecting the IP modules to the PIR detectors, you can add the IP modules in the XO client. For details, see the *XO Client Software User Manual* (21796).

15 Power Consumption

The estimated power consumption depends on the installed components and on the system load:

Motherboard	12 W
Processor	65 W max.
Seagate 10 TB hard disk	7 W
MIO card	1 W

Example for a 2-disk device (with maximum values):

Motherboard	13 W
Processor	65 W (PH10LU with Core i7/4770-S microprocessor)
2 Seagate hard disks	14 W
MIO card	1 W
TOTAL on secondary circuit: on primary circuit: (total power consumption divided by 0.78 – this is the efficiency of the power supply)	 93 W 119 W (0.56 A / 230 VAC)



Note

Measurement on an iFT-E* device (with PH10LU motherboard and i7 microprocessor) produced the following results: 0.2 A at 230 VAC → 46 W (idle state).

(*) configuration = iFT-E with 2 hard disks (4 TB per disk).

16 Retrieving the IP Address

The XO client displays the XO device's IP address in the title bar. However, if you cannot connect to the XO device, you can find the IP address as follows:

1. Connect a monitor/screen and a keyboard to the XO device.
2. If the monitor displays the video matrix, press Ctrl+Alt+F1. The XO welcome screen appears:

```
ADPRO XO 4.05.0001

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 XO welcome screen displays the following information:

   - XO device (server) software version
   - IP address, subnet mask, and gateway
   - HTTP, control, and RTSP port numbers.

3. To return to the video matrix view, press Ctrl+Alt+F7.

17 Diagnostics

17.1 Log Files and Reports

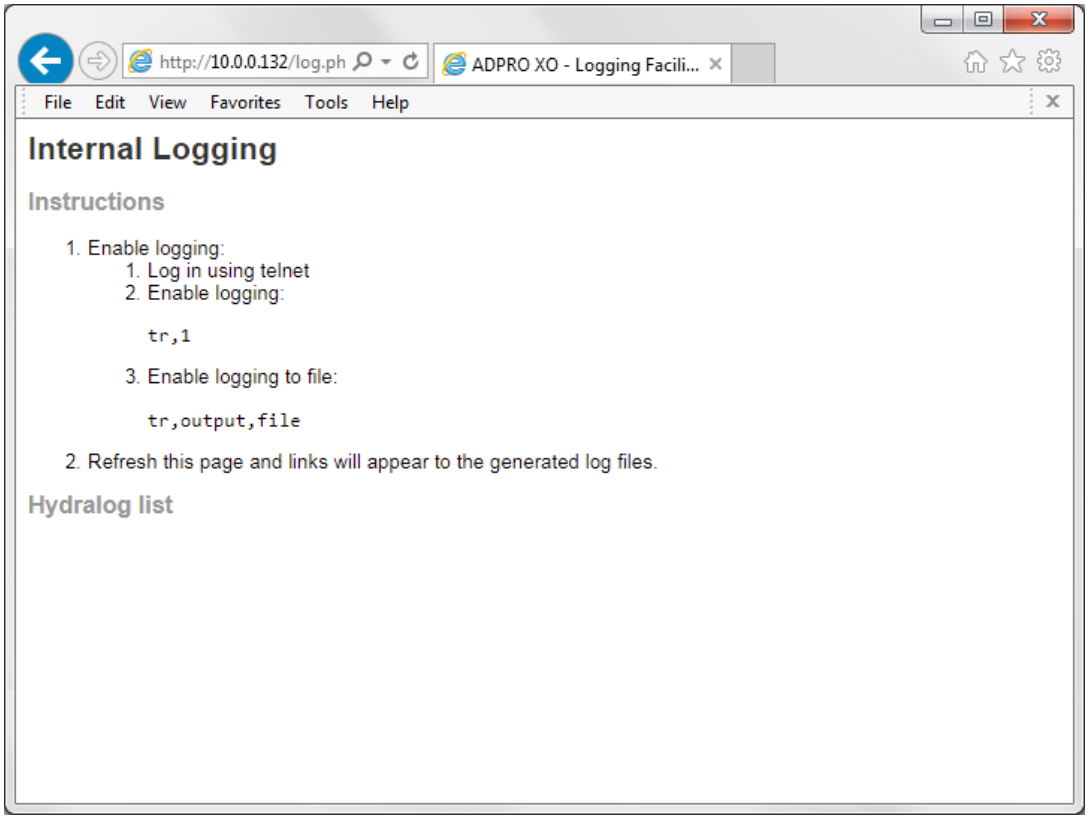
In case of major troubles with the XO device, the system allows to generate a number of log files and reports. In some cases, the Honeywell Support Division may ask you to activate and capture some log files and reports that can be helpful to resolve technical issues.

17.2 Retrieving Log Files

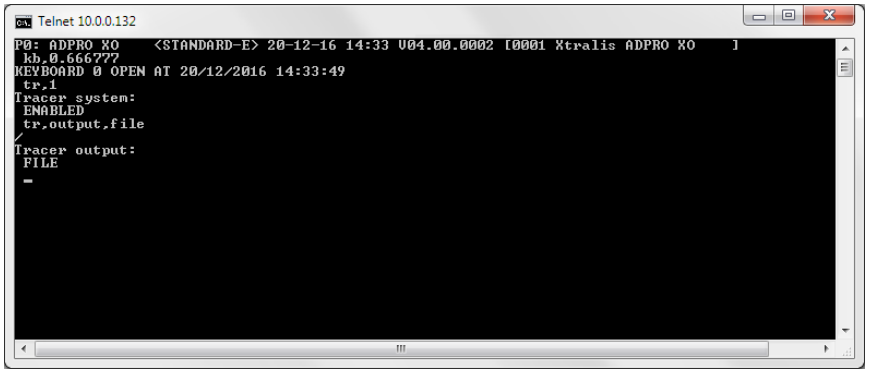
The XO device can output its internal trace buffer to hard disk to allow logging for longer periods without losing the data. You need to enable logging first.

To enable logging and retrieve log files, proceed as follows:

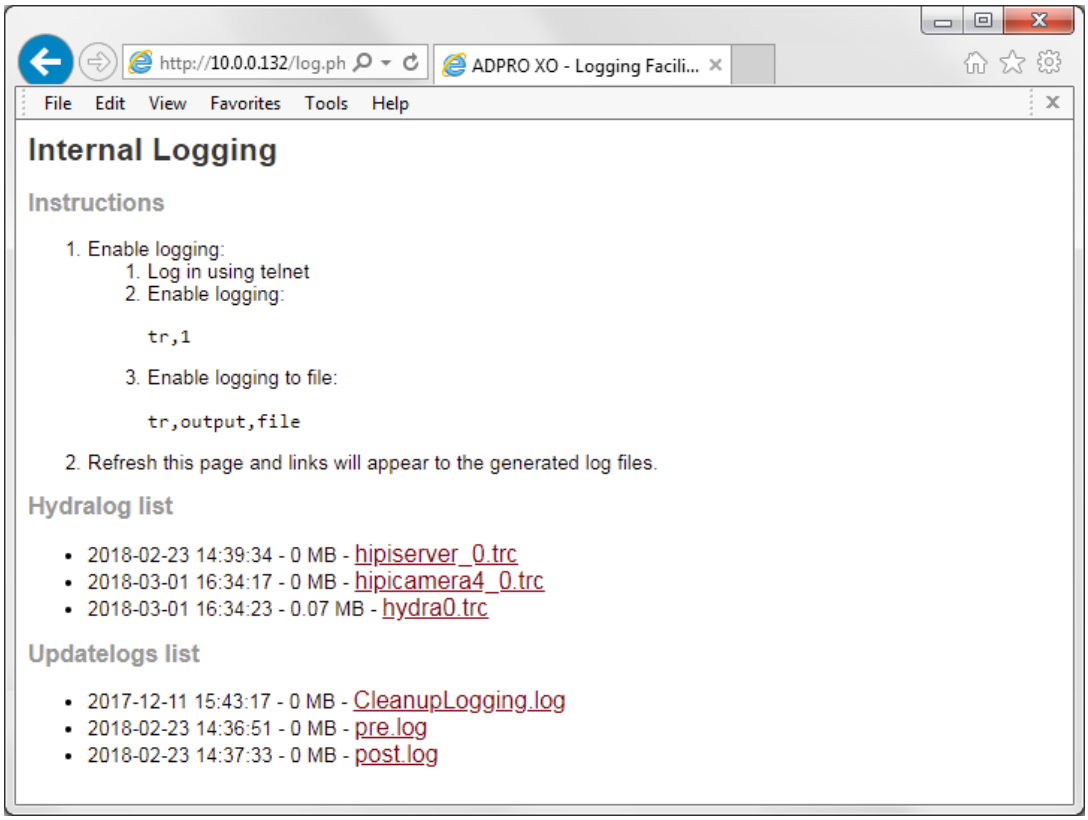
1. Type the device's IP address in the address bar of your internet browser, and add /log.php to the address. For example:
   http://10.0.0.10/log.php.
   The **Internal Logging** page appears. It displays instructions to enable logging. If logging is not yet enabled, the **Log list** at the bottom of the page is empty.



2. To enable logging, connect to the device via Telnet and enter the following Telnet commands:
   tr,1
   tr,output,file

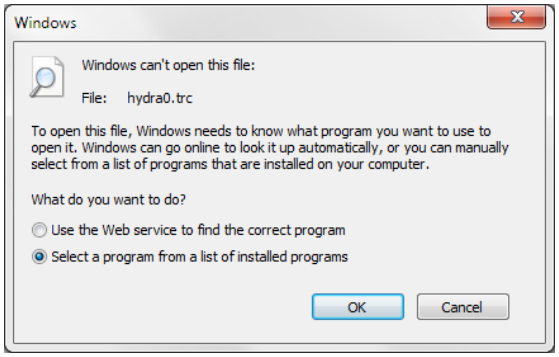


   After you have enabled logging, links to the log files appear on the web page in the **Log list**:



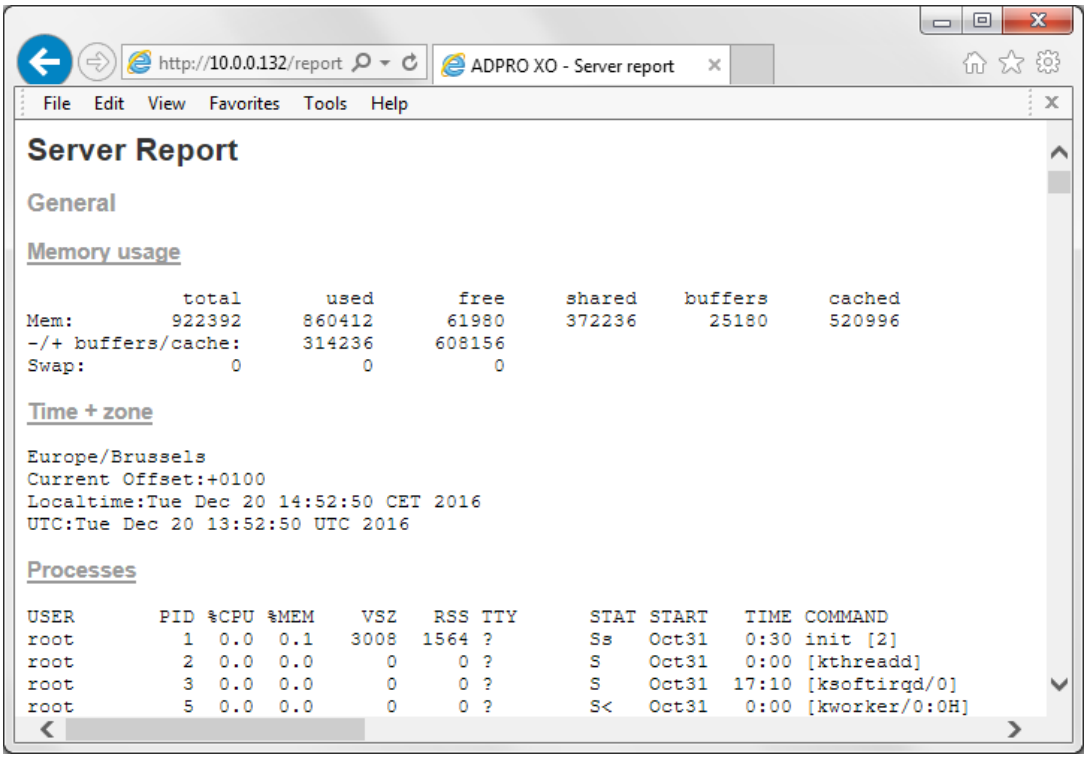
3. To retrieve a log file, click the link on the web page.
   Depending on your system settings, the system will open the file in the browser, or will (ask to) download the file.

4. If you have downloaded the file, double-click it to open it. If the following message appears, choose **Select a program from a list of installed programs**, and then set **Notepad** as default application.



17.3 Retrieving Reports

The XO device also generates reports. You can view these reports via the internet browser. Type the IP address of the XO device in the address bar of the browser and add /report.php to the IP address.
Example: http://10.0.0.10/report.php



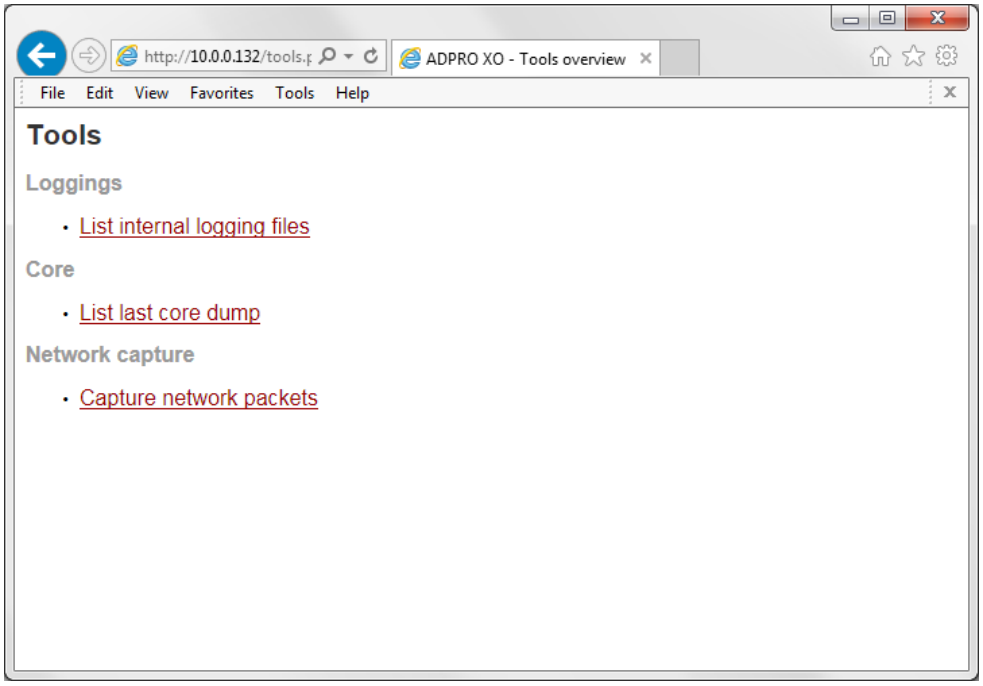
The Server Report contains the following information:

General	Memory usage
	Time + zone
	Processes
	Uptime
Performance	Vmstat
	I/O stat
	PID stat
	MP stat

Network	Interfaces – available
	Interfaces – enabled
	Routes
	Listen ports
	Netstat – all
	DEV stats
	Sockstat
	ARP cache
Filesystem	Mounts
	S.M.A.R.T
	Fsck
	Open files
	Free disk space
Hardware	CPU
	Memory
	Mainboard
	PCI
	Udev database
Server	Server version
	Server process memory usage
	Files
	Active config

18 Web Pages

There are several web pages to consult with the XO device. To open these web pages in your internet browser: type the IP address in the address bar, followed by the extensions as described in the table below.

Web page	Description
index.php	This is the main page of the XO device. If the XO client has been installed, this page automatically opens the XO client application. If the application has not yet been installed, you will be redirected to the setup page (setup.php).
setup.php	On this page you can download the XO client application.
tools.php	This page contains the links to the internal logging, the core dump and the network trace: 
log.php	Here you can download the log files (see *Retrieving Log Files* on page 78).
report.php	Here you can consult essential information on the configuration (see *Retrieving Reports* on page 80).
core.php	Here you can download the core dump (crash info) and watch dump (hang info) when you encounter these specific problems. The Honeywell Support Division may ask you to send these files to them for further investigation. Always mention the version when providing a core dump!
phpshell.php	This is a Linux console through a web browser. You need a username and password to use this tool. This is by default only accessible for the Honeywell Development Team.
net.php	Here you find a network sniffer for network tracing. You can use it for checking why a certain client cannot connect to the XO device.

19 Maintenance

The iFT Series devices require almost no maintenance.

Keep the device dust-free. Make sure to clean the ventilation grids at the front and back, to assure proper airflow in the device.

Caution!

Do NOT clean the device with water or any corrosive products. Use only dust cloths and wipes to clean the outside.

20 Full Reset by Flashing the DOM

20.1 Flashing the Image File to the DOM

You can perform a full reset of the device by flashing the iFT image file straight to the DOM (disk-on-a-module) using the ImageFlash tool.

When you perform a full reset using the ImageFlash tool, the system:

- Resets the IP address to 10.0.0.10.
- Deletes all configurations and restores the default values in all configurations.
- Restores the default values for the configuration of MIO card and Net I/O units (NO/NC, failsafe, and watchdog).
- Deletes all users and restores the default users.
- Deletes the calibration pictures.
- Deletes all licenses: system license and application licenses.

There are other options for full or partial resets. For more information, see *Tech Tip #06 Resetting to Defaults* (27986).

> ***Caution!***
>
> **Before** performing a full reset, back up any data that you need to keep and restore. At the very least, back up the system license. You can back up the system license via the XO client software. For instructions, see the *XO Client Software User Manual* (21796).
>
> You can easily reinstall your application licenses via Xchange (synchronise). For instructions, see the *Xchange Tool User Manual* (27816).

To perform a full reset using the ImageFlash tool, you need the following:

- the ImageFlash tool
- the iFT image file to flash on the DOM
- a SATA-to-USB cable.

You can find the tool and image file on the Security Solutions Support site www.xtralissecurity.com.

> ***Caution!***
>
> If you perform a full reset using the ImageFlash tool, the XO 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 perform a full reset using the ImageFlash tool, proceed as follows:

1. If you do not have the ImageFlash tool yet, go to the Security Solutions Support site www.xtralissecurity.com and log on.
2. In the **Keywords** box, type **imageflash** (one word) and press Enter to search for the tool.
3. Download and unzip the FT2ImageFlash.zip file on your PC.
4. To download the iFT Series XO 4 image file: in the **Keywords** box, type **32692** and press Enter to search for the file (or filter on **Product** = **XO** and **File Type** = **Firmware** (download the **image** file, not the upgrade file).
5. Download and unzip the **ADPROXO_04_03_000x_x64.img.zip** file.
6. In the XO client software, choose **System** > **Maintenance** > **Configuration Management**.

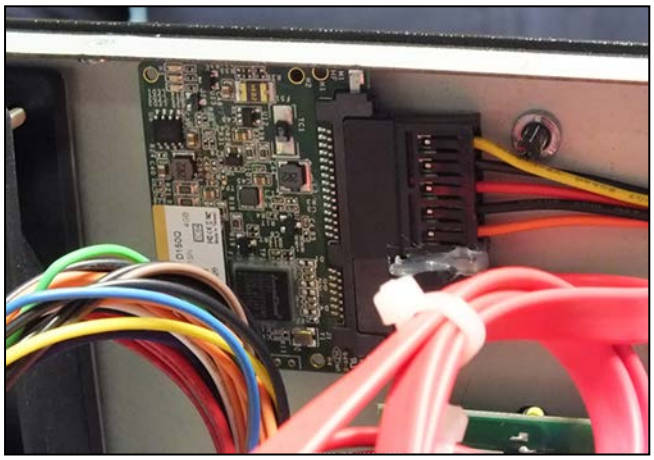
7. Click **System halt**.



8. Click **Yes** to confirm. The system shuts down all processes and connections. This may take a minute.
9. Wait for all the LEDs on the front panel to go out.
10. 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.

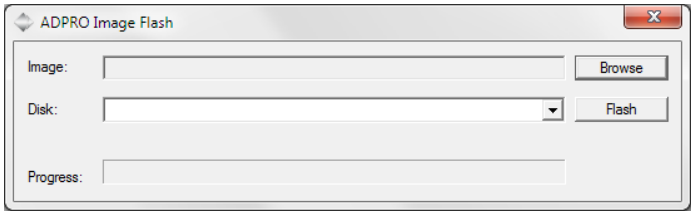
11. Unplug the power cord, and open the cover. The DOM is located at the back of the front panel:



12. Unplug the SATA cable that connects the DOM to the motherboard.
13. Unplug the DOM's power cable.
14. Insert the SATA-to-USB cable into the DOM, and plug the other end into your PC.

> **Note**
>
> If you are using a new, unused DOM, you must format it first. When you connect the DOM to your PC, the system will display a message, asking to format the DOM: click **Yes** or **OK** to format the DOM.

15. On your PC, double-click the FastTrace2ImageFlash.exe file to start the ImageFlash tool. The following screen appears:



16. Click **Browse** and browse to the folder where the iFT image file is located.
17. Select the image file and click **Open**.
18. In the **Disk** box, select the DOM.
19. Click **Flash**.
20. Wait for the tool to complete the flash process.
21. Unplug the SATA-to-USB cable from the DOM.

22. Re-insert the SATA cable to connect the DOM to the motherboard.
23. Re-insert the DOM's power cable.
24. Put the cover back in place and switch on the power supply. The XO device restarts.
25. Reconnect the XO client to the XO device using the default IP address (10.0.0.10) and the username/password of a default user.

20.2 After a Full Reset

After a full reset, the system contains no more licenses. The system license is no longer available either. 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 restore the system license immediately to have access to full functionality.

You can restore your system license via the **Transfer** function in the XO client. In some cases, you can also try to restore the system license using Xchange. For details, see the *Xchange Tool User Manual* (27816).

You can restore:

- the system license: via the XO client from the backup that you made before resetting, or via Xchange (if available).
- the application licenses: via Xchange.
- other files (configurations, calibration pictures…): via the XO client from the backup that you made before resetting.

You will need to reconfigure the MIO card and Net I/O units manually.

21 Product Labelling

21.1 Product Number Structure

Each ADPRO device has an 8-digit product number, indicating the installed options. The product number layout for iFT Series devices is as follows: PP CC HH 1 D

<table>
<tr><td>PP</td><td colspan="3">The iFT model number:
60 = iFT model
61 = iFT-E model (max. 2 HDDs)
63 = iFT-E model 4 HDD ready</td></tr>
<tr><td rowspan="2">CC</td><td colspan="3">The number of included IP channels:</td></tr>
<tr><td colspan="2">01 = 4 IP
02 = 8 IP
03 = 12 IP
04 = 16 IP</td><td>05 = 20 IP
06 = 24 IP
07 = 28 IP
08 = 32 IP</td></tr>
<tr><td rowspan="3">HH</td><td colspan="3">The hard disk size:</td></tr>
<tr><td>Single disk</td><td>RAID 1 Ready</td><td>2 x RAID 1 Ready</td></tr>
<tr><td>10 = device without hard disk, prepared for 1st disk
11 = 1 x 500 GB
12 = 1 x 1 TB
13 = 1 x 2 TB
14 = not used
15 = 1 x 4 TB
16 = 1 x 6 TB
17 = 1 x 8 TB
…
19 = 1 x “X” TB*</td><td>20 = for future use
21 = 2 x 500 GB
22 = 2 x 1 TB
23 = 2 x 2 TB
24 = not used
25 = 2 x 4 TB
26 = 2 x 6 TB
27 = 2 x 8 TB
…
29 = 2 x “X” TB*</td><td>40 = for future use
41 = 4 x 500 GB
42 = 4 x 1 TB
43 = 4 x 2 TB
44 = not used
45 = 4 x 4 TB
46 = 4 x 6 TB
47 = 4 x 8 TB
…
49 = 4 x “X” TB*</td></tr>
<tr><td colspan="3">00 = Transmission only (1 TB)
* X is to be defined in the future.</td></tr>
<tr><td>1</td><td colspan="3">1 = 1 built-in MIO card.</td></tr>
<tr><td>D</td><td colspan="3">Special options:
0 = no special options
2 = Bundle (+ 2 IntrusionTrace licenses)</td></tr>
</table>

For example:

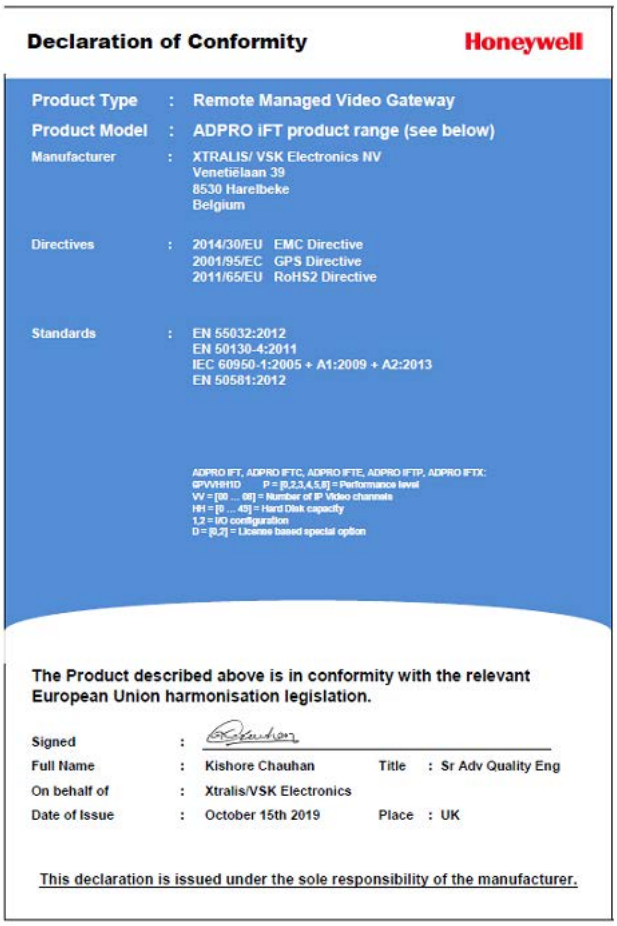
- 60021310 = iFT model, 8 IP channels included, 2 TB HDD, built-in MIO card
- 63041610 = iFT-E model, ready for 4 HDDs, 16 IP channels included, 6 TB HDD, built-in MIO card.

> ***Caution!***
>
> The product number on the label on your device indicates the device model and configuration **as it was originally delivered** by your supplier. If you have added, removed, or replaced items (HDDs, IP channel licenses…), the product number on the label **may no longer correspond with the actual configuration** of your device.

Note

Honeywell provides a broad range of iFT Series configurations, suitable for a wide variety of security system requirements.
For an overview of the available configurations, and for advice on selecting the one that best suits your needs, please contact your Honeywell Sales Representative.

21.2 Declaration of Conformity



Declaration of Conformity Honeywell

Product Type	:	Remote Managed Video Gateway
Product Model	:	ADPRO iFT product range (see below)
Manufacturer	:	XTRALIS/ VSK Electronics NV Venetiëlaan 39 8530 Harelbeke Belgium
Directives	:	2014/30/EU EMC Directive 2001/95/EC GPS Directive 2011/65/EU RoHS2 Directive
Standards	:	EN 55032:2012 EN 50130-4:2011 IEC 60950-1:2005 + A1:2009 + A2:2013 EN 50581:2012

ADPRO iFT, ADPRO iFTC, ADPRO iFTE, ADPRO iFTP, ADPRO iFTX:
GPVWHHD P = [0,2,3,4,5,8] = Performance level
VV = [00 ... 08] = Number of IP Video channels
HH = [0 ... 45] = Hard Disk capacity
1,2 = I/O configuration
D = [0,7] = License based special option

The Product described above is in conformity with the relevant European Union harmonisation legislation.

Signed	:			
Full Name	:	Kishore Chauhan	Title	: Sr Adv Quality Eng
On behalf of	:	Xtralis/VSK Electronics		
Date of Issue	:	October 15th 2019	Place	: UK

This declaration is issued under the sole responsibility of the manufacturer.

Appendix A – 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