truVision

# TruVision NVR 71 User Manual

P/N 1073374-EN • REV I • ISS 19OCT22

**Copyright**

**Trademarks and patents**

TruVision and associated names and logos are a product brand of Aritech, a part of Carrier.

Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.

**Manufacturer**

PLACED ON THE MARKET BY:
Carrier Fire & Security Americas Corporation Inc.
13995 Pasteur Blvd, Palm Beach Gardens, FL 33418, USA

AUTHORIZED EU REPRENSENTATIVE:
Carrier Fire & Security B.V.
Kelvinstraat 7, 6003 DH Weert, Netherlands

**FCC compliance**

Class A: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

**FCC conditions**

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference.

(2) This Device must accept any interference received, including interference that may cause undesired operation.

**Canada**

This Class A digital apparatus complies with CAN ICES-003 (A)/NMB-3 (A).

Cet appareil numérique de la classe A est conforme à la norme CAN ICES-003 (A)/NMB-3 (A).

**cUL**

Safety Instruction:

Improper use or replacement of the battery may result in explosion hazard. Replace with the same or equivalent type only. Dispose of used batteries in conformance with the local codes.

Instructions de sécurité :

L'utilisation ou le remplacement inadéquats de la pile peuvent entraîner un risque d'explosion. Remplacez-la par le même type ou l'équivalent du même type seulement. Jetez les piles usagées conformément aux directives fournies par le fabricant de la pile.

**ACMA compliance**

**Notice!** This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

**Certification**

CE FC c UL us UK CA

**EU directives**

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, the RoHS Directive 2011/65/EU.

2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: recyclethis.info.

2013/56/EU & 2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: recyclethis.info.

**Product warnings and disclaimers**

THESE PRODUCTS ARE INTENDED FOR SALE TO AND INSTALLATION BY QUALIFIED PROFESSIONALS. CARRIER FIRE & SECURITY CANNOT PROVIDE ANY ASSURANCE THAT ANY PERSON OR ENTITY BUYING ITS PRODUCTS, INCLUDING ANY “AUTHORIZED DEALER” OR “AUTHORIZED RESELLER”, IS PROPERLY TRAINED OR EXPERIENCED TO CORRECTLY INSTALL FIRE AND SECURITY RELATED PRODUCTS.

For more information on warranty disclaimers and product safety information, please check https://firesecurityproducts.com/policy/product-warning/ or scan the following code:

**Contact information**

EMEA: https://firesecurityproducts.com

Australian/New Zealand: https://firesecurityproducts.com.au/

**Product documentation**

Please consult the following web link to retrieve the electronic version of the product documentation. The manuals are available in several languages.

# Content

# Important information

## Limitation of liability

To the maximum extent permitted by applicable law, in no event will Carrier be liable for any lost profits or business opportunities, loss of use, business interruption, loss of data, or any other indirect, special, incidental, or consequential damages under any theory of liability, whether based in contract, tort, negligence, product liability, or otherwise. Because some jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages the preceding limitation may not apply to you. In any event the total liability of Carrier shall not exceed the purchase price of the product. The foregoing limitation will apply to the maximum extent permitted by applicable law, regardless of whether Carrier has been advised of the possibility of such damages and regardless of whether any remedy fails of its essential purpose.

Installation in accordance with this manual, applicable codes, and the instructions of the authority having jurisdiction is mandatory.

While every precaution has been taken during the preparation of this manual to ensure the accuracy of its contents, Carrier assumes no responsibility for errors or omissions.

## Product Warnings

YOU UNDERSTAND THAT A PROPERLY INSTALLED AND MAINTAINED ALARM/SECURITY SYSTEM MAY ONLY REDUCE THE RISK OF EVENTS SUCH AS BURGLARY, ROBBERY, FIRE, OR SIMILAR EVENTS WITHOUT WARNING, BUT IT IS NOT INSURANCE OR A GUARANTEE THAT SUCH EVENTS WILL NOT OCCUR OR THAT THERE WILL BE NO DEATH, PERSONAL INJURY, AND/OR PROPERTY DAMAGE AS A RESULT.

THE ABILITY OF CARRIER PRODUCTS, SOFTWARE OR SERVICES TO WORK PROPERLY DEPENDS ON A NUMBER OF PRODUCTS AND SERVICES MADE AVAILABLE BY THIRD PARTIES OVER WHICH CARRIER HAS NO CONTROL AND FOR WHICH CARRIER SHALL NOT BE RESPONSIBLE INCLUDING, BUT NOT LIMITED TO, INTERNET, CELLULAR AND LANDLINE CONNECTIVITY; MOBILE DEVICE AND OPERATING SYSTEM COMPATIBILITY; MONITORING SERVICES; ELECTROMAGNETIC OR OTHER INTERFERENCE, AND PROPER INSTALLATION AND MAINTENANCE OF AUTHORIZED PRODUCTS (INCLUDING ALARM OR OTHER CONTROL PANEL AND SENSORS).

ANY PRODUCT, SOFTWARE, SERVICE OR OTHER OFFERING MANUFACTURED, SOLD OR LICENSED BY CARRIER, MAY BE HACKED, COMPROMISED AND/OR CIRCUMVENTED AND CARRIER MAKES NO REPRESENTATION, WARRANTY, COVENANT OR PROMISE THAT ITS PRODUCTS (INCLUDING SECURITY PRODUCTS), SOFTWARE, SERVICES OR OTHER OFFERINGS WILL NOT BE HACKED, COMPROMISED AND/OR CIRCUMVENTED.

CARRIER DOES NOT ENCRYPT COMMUNICATIONS BETWEEN ITS ALARM OR OTHER CONTROL PANELS AND THEIR WIRELESS OUTPUTS/INPUTS INCLUDING BUT NOT LIMITED TO, SENSORS OR DETECTORS UNLESS REQUIRED BY APPLICABLE LAW. AS

A RESULT THESE COMMUNICATIONS MAY BE INTERCEPTED AND COULD BE USED TO CIRCUMVENT YOUR ALARM/SECURITY SYSTEM.

THE EQUIPMENT SHOULD ONLY BE OPERATED WITH AN APPROVED POWER ADAPTER WITH INSULATED LIVE PINS.

DO NOT CONNECT TO A RECEPTACLE CONTROLLED BY A SWITCH.

THIS UNIT INCLUDES AN ALARM VERIFICATION FEATURE THAT WILL RESULT IN A DELAY OF THE SYSTEM ALARM SIGNAL FROM THE INDICATED CIRCUITS. THE TOTAL DELAY (CONTROL UNIT PLUS SMOKE DETECTORS) SHALL NOT EXCEED 60 SECONDS. NO OTHER SMOKE DETECTOR SHALL BE CONNECTED TO THESE CIRCUITS UNLESS APPROVED BY THE LOCAL AUTHORITY HAVING JURISDICTION.

**WARNING!** The equipment should only be operated with an approved power adapter with insulated live pins.

**Caution**: Risk of explosion if battery is replaced by an incorrect type. Dispose of batteries according to the instructions. Contact your supplier for replacement batteries.

## Warranty Disclaimers

CARRIER HEREBY DISCLAIMS ALL WARRANTIES AND REPRESENTATIONS, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING ANY IMPLIED WARRANTIES, THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

(USA only) SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. YOU MAY ALSO HAVE OTHER LEGAL RIGHTS THAT VARY FROM STATE TO STATE.

CARRIER DOES NOT MAKE ANY CLAIMS OR WARRANTIES TO YOU OF ANY KIND REGARDING ANY PRODUCT, SOFTWARE OR SERVICE’S POTENTIAL, ABILITY, OR EFFECTIVENESS TO DETECT, MINIMIZE, OR IN ANYWAY PREVENT DEATH, PERSONAL INJURY, PROPERTY DAMAGE, OR LOSS OF ANY KIND WHATSOEVER.

CARRIER DOES NOT REPRESENT TO YOU THAT ANY PRODUCT (INCLUDING SECURITY PRODUCTS), SOFTWARE, SERVICE OR OTHER OFFERING MAY NOT BE HACKED, COMPROMISED AND/OR CIRCUMVENTED.

CARRIER DOES NOT WARRANT THAT ANY PRODUCT (INCLUDING SECURITY PRODUCTS), SOFTWARE OR SERVICE MANUFACTURED, SOLD OR LICENSED BY CARRIER WILL PREVENT, OR IN ALL CASES PROVIDE ADEQUATE WARNING OF OR PROTECTION FROM, BREAK-INS, BURGLARY, ROBBERY, FIRE, OR OTHERWISE.

CARRIER DOES NOT WARRANT TO YOU THAT ITS SOFTWARE OR PRODUCTS WILL WORK PROPERLY IN ALL ENVIRONMENTS AND APPLICATIONS AND DOES NOT WARRANT ANY PRODUCTS AGAINST HARMFUL ELECTROMAGNETIC INTERFERENCE INDUCTION OR RADIATION (EMI, RFI, ETC.) EMITTED FROM EXTERNAL SOURCES

CARRIER DOES NOT PROVIDE MONITORING SERVICES FOR YOUR ALARM/SECURITY SYSTEM (“MONITORING SERVICES”). IF YOU ELECT TO HAVE MONITORING SERVICES YOU MUST OBTAIN SUCH SERVICE FROM A THIRD PARTY AND CARRIER MAKES NO REPRESENTATION OR WARRANTY WITH RESPECT TO SUCH SERVICES INCLUDING WHETHER OR NOT THEY WILL BE COMPATIBLE WITH THE PRODUCTS, SOFTWARE OR SERVICES MANUFACTURED, SOLD OR LICENSED BY CARRIER.

## Intended Use

Use this product only for the purpose it was designed for; refer to the data sheet and user documentation. For the latest product information, contact your local supplier or visit us online at firesecurityproducts.com.

The system should be checked by a qualified technician at least every 3 years and the backup battery replaced as required.

## Advisory messages

Advisory messages alert you to conditions or practices that can cause unwanted results. The advisory messages used in this document are shown and described below.

**WARNING:** Warning messages advise you of hazards that could result in injury or loss of life. They tell you which actions to take or to avoid in order to prevent the injury or loss of life.

**Caution:** Caution messages advise you of possible equipment damage. They tell you which actions to take or to avoid in order to prevent the damage.

**Note:** Note messages advise you of the possible loss of time or effort. They describe how to avoid the loss. Notes are also used to point out important information that you should read.

# Chapter 1
# Product introduction

## Product overview

This recorder is a high-performance network video recorder that can store, search, export and manage video from up to 576 Mbps of incoming camera bandwidth, or up to 128 IP cameras. There are many redundancy features to ensure system stability failure such as RAID (only available in dedicated RAID models), hot spare mode, network redundancy, and redundant power supplies. It provides integration with the Carrier portfolio of security solutions and offers a seamless product experience within the TruVision brand.

The recorder can fully integrate with the license-free TruVision Navigator software, which is ideal for most commercial applications. It features an easy-to-use and intuitive web browser interface that enables remote configuration and secure viewing, searching, and playing back of video.

## Contact information and manuals/tools/firmware

For contact information and to download the latest manuals, tools, and firmware, go to the web site of your region:

| | |
|---|---|
| EMEA: | https://firesecurityproducts.com<br>Manuals are available in several languages. |
| Australia/New Zealand: | https://firesecurityproducts.com.au/ |

## Firmware version

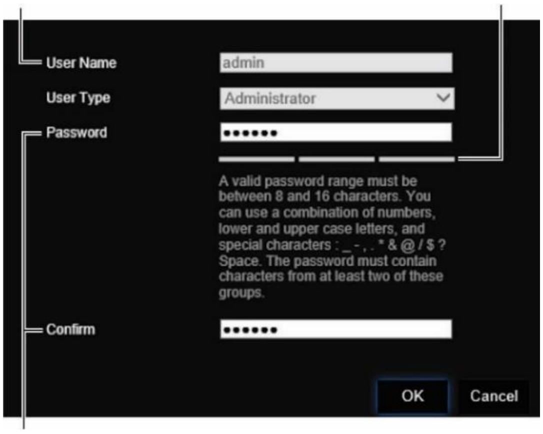
This manual applies to firmware version 1.5.

# Activate the admin password

When you first start up the unit, the *Activation* window appears. You must define a high-security admin password before you can access the unit. There is no default password provided.

A message will appear on-screen when the unit has been activated.

**Figure 1: Password activation window**



User Name: It is always “admin”. It cannot be changed.

The bar showing password strength

User Name: admin

User Type: Administrator

Password: ••••••

A valid password range must be between 8 and 16 characters. You can use a combination of numbers, lower and upper case letters, and special characters : _ - , . * & @ / $ ? Space. The password must contain characters from at least two of these groups.

Confirm: ••••••

Enter the new admin password and confirm it.

### Tips on creating a strong password:

- A valid password range must be between 8 and 16 characters. You must use at least one character from each of the following items: numbers, lower-case letters, upper-case letters, and special characters : _ - , .* & @ / $ ? Space. The maximum number of allowed attempts to enter a password is 3. Lockout is 30 minutes when in web mode and 10 minutes when in OSD mode.
- The password is case-sensitive.
- Do not use personal information or common words as “password”.
- The password cannot contain the username.
- We recommend that you do not use a space at the start or end of a password, and that you reset your password regularly. For high security systems, it is particularly recommended to reset the password monthly or weekly for better protection.

**Note**: If you should forget your admin password, please contact Technical Support to reactivate the unit with a new password.

Go to Chapter 16 “User management” on page 125 for further information on creating user passwords.

## Default network settings

The network settings are:

- IP address - 192.168.1.82
- Subnet mask - 255.255.255.0

- Gateway address - 192.168.1.1
- Ports:

| When using the browser: | When using TruNav: |
|---|---|
| RTSP port: 554 | RTSP port: 554 |
| HTTP port: 80 | Server/Client software port: 8000 |
| When using Chrome, Safari or Firefox, port in HTTP mode: 7681 | |

Go to “Web browser” on page 48 for further information.

**Note**: It is recommended that the recorder is placed behind a firewall and that only those ports that need to communicate with browsers and software can be accessed.

# Chapter 2
# Physical installation

This section describes how to install the recorder.

## Installation environment

When installing your product, consider these factors:

- Ventilation
- Temperature
- Humidity
- Chassis load

**Ventilation:** Do not block any ventilation openings. Install in accordance with the manufacturer's instructions. Ensure that the location planned for the installation of the unit is well ventilated.

**Temperature:** Consider the unit's operating temperature (-10 to +55 ºC, 14 to 131 °F) and noncondensing humidity specifications (10 to 90%) before choosing an installation location. Extremes of heat or cold beyond the specified operating temperature limits may reduce the life expectancy of the recorder. Do not install the unit on top of other hot equipment. Leave 44 mm (1.75 in.) of space between rack-mounted NVR units.

**Humidity:** Do not use the unit near water. Moisture can damage the internal components. To reduce the risk of fire or electric shock, do not expose this unit to rain or moisture.

**Chassis:** Equipment weighing less than 15.9 kg (35 lb.) may be placed on top of the unit.

## Unpacking the recorder and its accessories

When you receive the product, check the package and contents for damage, and verify that all items are included. There is an item list included in the package. If any of the items are damaged or missing, please contact your local supplier.

Items shipped with the product include:

- AC power cords
- Recorder
- Hard drive kits
- *TruVision NVR 71 Quick Start Guide*

You can download the software and the following manuals from our web site:

- *TruVision NVR 71 User Manual*
- *TruVision Recorder Operator Guide*

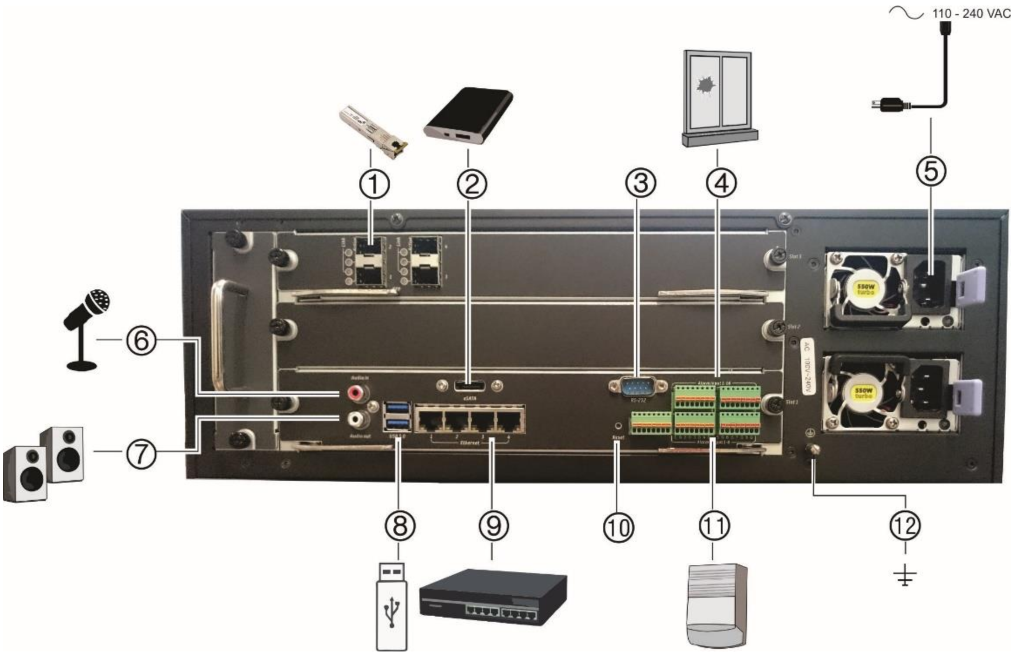
## Back panel description

The figure below shows the back panel connections and describes each connector on a typical TVN 71 network video recorder. Details may vary for specific models.

Once all required connections are done, enter the relevant data in the setup wizard (see page 14).

**Note**: For every hardwired alarm input, connect one wire to the input connection with the alarm number label and one wire to a Ground connection (labeled G).

**Figure 2: TVN 71 back panel connections**



| | Description | Use |
|---|---|---|
| 1. | SFP port (X4) | Plug a small form-factor pluggable transceiver into the port to connect fiber cables.(Optional) |
| 2. | eSATA | Connect an optional eSATA drive to extend the internal storage or to archive. |
| 3. | RS-232 input | Used by technical support.<br>See “Configure the RS-232 port” on page 115 for more information. |

| | Description | Use |
|---|---|---|
| 4. | Alarm inputs (X16) | Connect physical alarms such as detectors, push buttons, etc. |
| 5. | Redundant power supplies (X2) | Connect two PSUs.<br>The PSUs are shipped with the recorder. |
| 6. | Audio input (X1) | Connect a microphone for bi-directional audio (not recorded) (Optional)<br>Specification: RCA jack, 315 mV, 40 kohms. Unbalanced.  Line-level audio requires amplification. |
| 7. | Audio output (X1) | Connect to speakers for audio output.(Optional)<br>Specification: RCA jack, 315mV, 600 ohms. Unbalanced.  Line-level audio requires amplification. |
| 8. | USB 3.0 port (X2) | Connect an optional USB device, CD/DVD burner or HDD. |
| 9. | Ethernet ports | Connect to a network. |
| 10. | Reset pin hole | Access to the reset button using a paper clip.<br>Hold down the reset button for seven seconds to reset the network settings back to factory default.<br>**Note**: This might cause the cameras to stop recording and the software to be unable to connect to the recorder. |
| 11. | Alarm outputs (X8) | Connect physical alarm outputs such as a siren, flash, or relay. (Optional) |
| 12. | Ground | Connect to ground. |

# HDD slots

The recorder has four rows of four HDD (hard disk drive) slots. This allows up to 16 HDDs to be connected, depending on the model. The slots are accessed from the front panel for easy expansion or replacement of the hard drives.

Each HDD slot can support 4 or 6 TB HDDs. The total onboard storage capacity is between 16 and 96 TB in RAID or non- RAID configuration, depending on the model. The storage capacity can be further expanded by using the USB 3.0, eSATA, or NAS functionality.

# Rack mounting

The recorder is 3U rack mountable using a rack mount shelf. The rack mount ears included with the product are intended to fix the product in the rack, not to carry the full weight of the recorder. It can also be installed desk based.

# Chapter 3
# Getting started

## Power on the recorder

The recorder comes equipped with two universal power supplies that will auto-sense 110/240 V, 60/50 Hz.

**Note:** It is recommended that an uninterruptible power supply (UPS) is used in conjunction with the device.

**To turn on the recorder:**

Plug in both power cords on the back panel. Once it is powered up, the status LEDs on the front panel will light up.

**To reboot the recorder:**

Connect to the recorder through the web browser interface or TruVision Navigator and reboot the recorder, if needed. See “Restart the recorder” on page 113 for more information.

## The startup wizard

The recorder has an express installation wizard that lets you easily configure basic recorder settings when first used. It configures all cameras to default settings. The configuration of each camera and recorder can be customized as required later in the Configuration menu.

Any changes you make to a setup configuration page are saved when you exit the page and return to the main wizard page.

**Note**: If you want to set up the recorder with default settings only, click **Next** in each screen until the end.

**To use the Startup wizard:**

1. There are two ways to access the Startup wizard:

In Internet Explorer enter the IP address of the recorder. The browser will automatically launch the startup wizard.

**Note**: Use TruVision Device Manager 4.0 to locate the recorder on the LAN and, if required, to change the recorder's IP address.

- Or -

On the recorder's menu toolbar, click **Configuration** > **Device Management** > **General Settings** and select **Start wizard now** to immediately launch the startup wizard.

2. Enable or disable the option to start the wizard automatically when the recorder is turned on. Click **Next**.
3. In each setup configuration page, enter the desired information, click **OK** to save the changes, and then click **Next** to move to the next page. The setup configuration pages are:

| Wizard setup pages | Description |
|---|---|
| User configuration | You can change the admin password. Select the admin entry and click the Edit button. Change the desired admin information and then click OK to save and return to the *User configuration* window.<br>See Chapter 16 "User management" on page 125 for more information about users. |
| Time configuration | Select the desired time zone, date format, system time, and system date.<br>If Daylight saving time (DST) is required, select **Enable DST** and enter the start and end times of summer time.<br>Set the amount of time to move DST forward from the standard time. Default is 60 minutes.<br>**Note**: The system time and date are visible on screen. However, they do not appear in recordings.<br>See "Time and date settings" on page 111 for more information. |
| Hard drive initialization | The hard drives are initialized at the factory. However, if you wish to clear all data, click **Initialization** to initialize the HDD. |
| IP cameras | A list of cameras already added to the recorder is shown, if any. Their status is shown as Online or Offline. Click **Search/Add** to find any available IP cameras on the LAN.<br>There are two ways to add an IP camera to the recorder system:<br>*Manually*: Enter the IP address of the IP camera to be added. Select the appropriate protocol, stream number, and management port, and then enter User name, Admin password, and transfer protocol, and then click the **OK** button. Click, **Next** to move to the next page.<br>*Automatically*: Click **Search/Add** to get a list of all supported IP cameras that are located on the LAN. Select the desired IP cameras from the search results list to add to the recorder system and click **OK**. The camera information cannot be modified.  Click, **Next** to move to the next page |
| Recording schedule setup | Configure your default recording settings as required. The settings apply to all cameras connected to the recorder.<br>Select the desired time lapse check box**, TL-Hi** or **TL-Lo**. |

| Wizard setup pages | Description |
|---|---|
| | To enable motion detection recording in the recording schedule, select **Enable Motion Detection Plan**. However, no motion will be recorder until you set up a motion grid. The motion grid needs to be set up for each camera individually via the normal Configuration menu.<br>To enable alarm events recording, select **Enable Alarm Input Plan**.<br>**Note**: You can configure the recording parameters of each individual camera for the different recording schedules in the recording menu. |

4. When all the required changes have been entered, a summary page appears showing all the settings.

   Click **Finalize** to exit the Wizard. All changes made are saved. The recorder is now ready to use.

   **Note**: If you click **Exit Wizard**, you will exit the wizard and changes made to the language, alarm, password, IP camera, or date and time settings will be saved. However, all other changes will be lost.

   For a description of the recorder main menu, see “Web browser interface” on page 20.

# Chapter 4
# Operating instructions

## Control the recorder

You operate the recorder through a browser interface, which provides full functionality for viewing, playback, and recorder configuration.  You can also use TruVision Navigator or TVRMobile. Please refer to the TruVision Navigator and TVRMobile user manuals for more information.

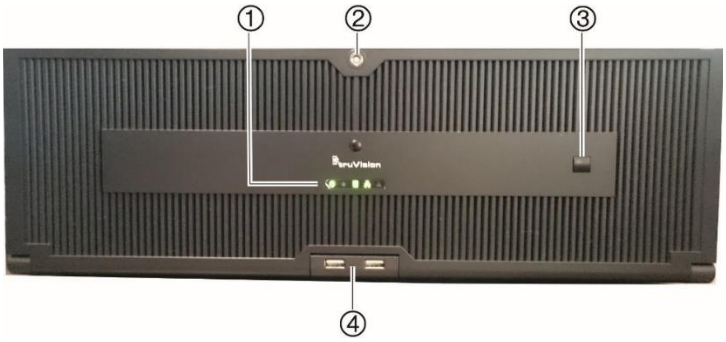
You can use your preferred control method for any procedure, but in most cases, we describe procedures using the browser.

## Front panel description

The function button on the front panel lets you easily export log files. You can also open the front panel to access the HDDs in the recorder. The front panel can be locked with a key to limit access.

The LED indicators light up to alert you of various conditions. See Figure 3 below for more information.

**Figure 3: TVN 71 front panel**



The controls on the front panel include:

**Table 1: Front Panel Elements**

| | Name | Description |
|---|---|---|
| 1. | Status LEDs | **Power**: A steady GREEN light indicates that the recorder is operating correctly. A RED light indicates a fault. |
| | | Event Alarm: A blinking RED light indicates that there is a sensor Alarm In or another alarm such as motion or tampering. No light indicates no alarm. |
| | | **HDD**: A blinking RED light indicates that the recorder is accessing the HDD in a read or write operation. A steady RED light indicates HDD failure. No light indicates that the unit is in idle state. |
| | | **Network**: A GREEN light indicates a normal network connection. A blinking RED light indicates a normal network connection when not all eight network ports are in multi-address mode. No light indicates that the recorder is not connected to any network. |
| | | **Technical Alarm**: A steady RED light indicates that there is a technical alarm from the recorder. No light indicates that there is no alarm. |
| 2. | Front panel lock | You can lock or unlock the front panel with a key. It provides access to the HDDs. |
| 3. | Export log button | **Export log** button: Insert a USB stick into one of the front panel USD ports. Press the button to export the log file of the recorder for all channels (format .txt). The download file has the log information for the past 24 hours from when you press the button. The name format is YYYYMMDDHHMM.txt.<br>**Note**: You cannot export files to a USB CD/DVD burner using this button. However, you can use a USD stick. |
| 4. | USB 3.0 port | There are two USB ports. They can be used for archiving video (setup via the webpage), upgrading the firmware, or exporting the log file (via the front panel button). |

# Access browsers

The recorder now works with the following browsers:

- Microsoft Internet Explorer (IE)
- Google Chrome (from version 45)
- Apple Safari (from version 10)
- Mozilla Firefox (from version 52)

The procedures described in the manual use the Microsoft Internet Explorer web browser.

**Note**: The recorder does not support Microsoft Edge.

The recorder can automatically detect if you are using IE, Chrome, Safari or Firefox.

The specifications of the plug-in free solution for Google Chrome, Mozilla Firefox and Apple Safari compared to IE are shown below:

| Mode | Function | Result | Remark |
|---|---|---|---|
| Live | Live view | Possible for resolution <= 1080p; bit rate<= 2048kbps | For viewing higher resolution/quality cameras, use the substream. |
| | Audio | Supported | |
| | Capture a snapshot | Supported | |
| | Digital zoom | Supported | |
| | Window division | Supported | |
| | Full screen view | Supported | |
| | Local record | Only supported for Google Chrome | |
| Playback | Playback | 1 channel @ 1080P (max.) | |
| | Fast forward | Not supported | |
| | Single frame | Not supported | |
| | Reverse playback | Not supported | |
| | Download a video clip | Supported | |
| Configuration | Export device parameters | Supported | |
| | Import device parameters | Supported | |
| | Firmware upgrade | Supported | |
| | Draw area (Motion/VCA) | Supported | |
| | Export log | Support for .TXT format | |
| | Local configuration | Not supported | |
| | File path setting | Only the file name can be displayed. The full path cannot be shown. | |

# Internet Explorer users

Internet Explorer for Windows operating systems have increased security measures to protect your PC from any malicious software being installed. When using the recorder web browser interface, you can install ActiveX controls to connect and view video using Internet Explorer.

To have complete functionality of the web browser interface and the recorder player with Internet Explorer, do the following:

- Run the Browser interface and the recorder player application as an administrator in your workstation
- Add the recorder’s IP address to your browser’s list of trusted sites

**To add the recorder's IP address to Internet Explorer's list of trusted sites:**

1. Open Internet Explorer.
2. Click **Tools**, and then **Internet Options**.
3. Click the Security tab, and then select the Trusted Sites icon.
4. Click **Sites**.
5. Clear the "Require server verification (https:) for all sites in this zone" box.
6. Enter the IP address or DDNS name in the "Add this website to the zone" field.
7. Click **Add**, and then click **Close**.
8. Click **OK** in the Internet Options dialog box.
9. Connect to the recorder for full browser functionality.

# Access the web browser

To access the recorder, open the Microsoft Internet Explorer web browser, and enter the IP address assigned to the recorder, as a web address. On the logon window, enter the user ID and password.

The default values for recorder network settings are:

- IP address - 192.168.1.82
- Subnet mask - 255.255.255.0
- Gateway address - 192.168.1.1
- Server port: 8000
- Ports:

| When using the browser: | When using TruNav: |
|---|---|
| RTSP port: 554 | RTSP port: 554 |
| HTTP port: 80 | Server/Client software port: 8000 |
| When using Chrome, Safari or Firefox, port in HTTP mode: 7681 | |

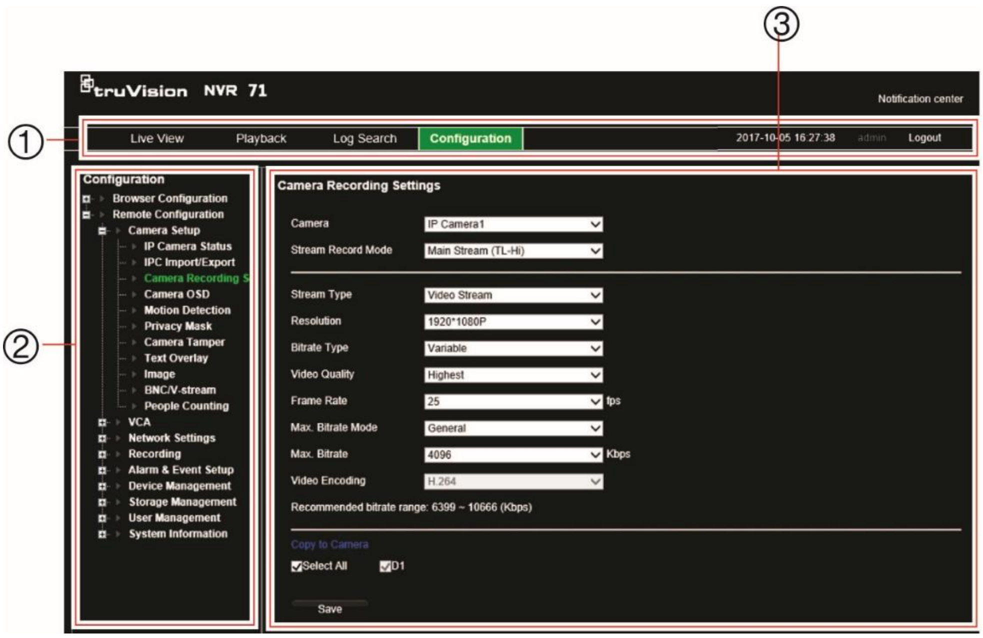
For more information on port forwarding, see Appendix B "Port forwarding information" on page 135.

# Web browser interface

The recorder's web browser interface has an intuitive structure that allows you to configure the unit's parameters quickly and efficiently. Each submenu item displays a setup menu that lets you edit a group of settings. Most menus are available only to system administrators.

The browser window is divided into three sections. The currently selected submenu is highlighted in green. See Figure 4 below.

**Figure 4: Browser window**



Camera Recording Settings

| | |
|---|---|
| Camera | IP Camera1 |
| Stream Record Mode | Main Stream (TL-Hi) |
| Stream Type | Video Stream |
| Resolution | 1920*1080P |
| Bitrate Type | Variable |
| Video Quality | Highest |
| Frame Rate | 25 fps |
| Max. Bitrate Mode | General |
| Max. Bitrate | 4096 Kbps |
| Video Encoding | H.264 |

Recommended bitrate range: 6399 ~ 10666 (Kbps)

☑Select All ☑D1

1. **Menu toolbar**: Setup options available for the selected menu function. Move the mouse over a menu function and click to select it. There are four menu modes: Live View, Playback, Log Search, and Configuration.
2. **Configuration panel**: Displays the configuration submenus for the selected menu function. Click an item to select it.
3. **Setup menu**: All the details for the selected submenu are displayed. Click a field to make changes.

# Chapter 5
# Live view

Live view mode is the normal operating mode of the unit where you watch live images from the cameras.

## Web browser live view

The recorder web browser lets you view, record, and play back videos as well as manage all aspects of the recorder from any PC with Internet access. The browser’s easy-to-use controls give you live view to all the recorder functions. See Figure 5 on page 23.

You can watch up to 16 cameras in live view simultaneously.

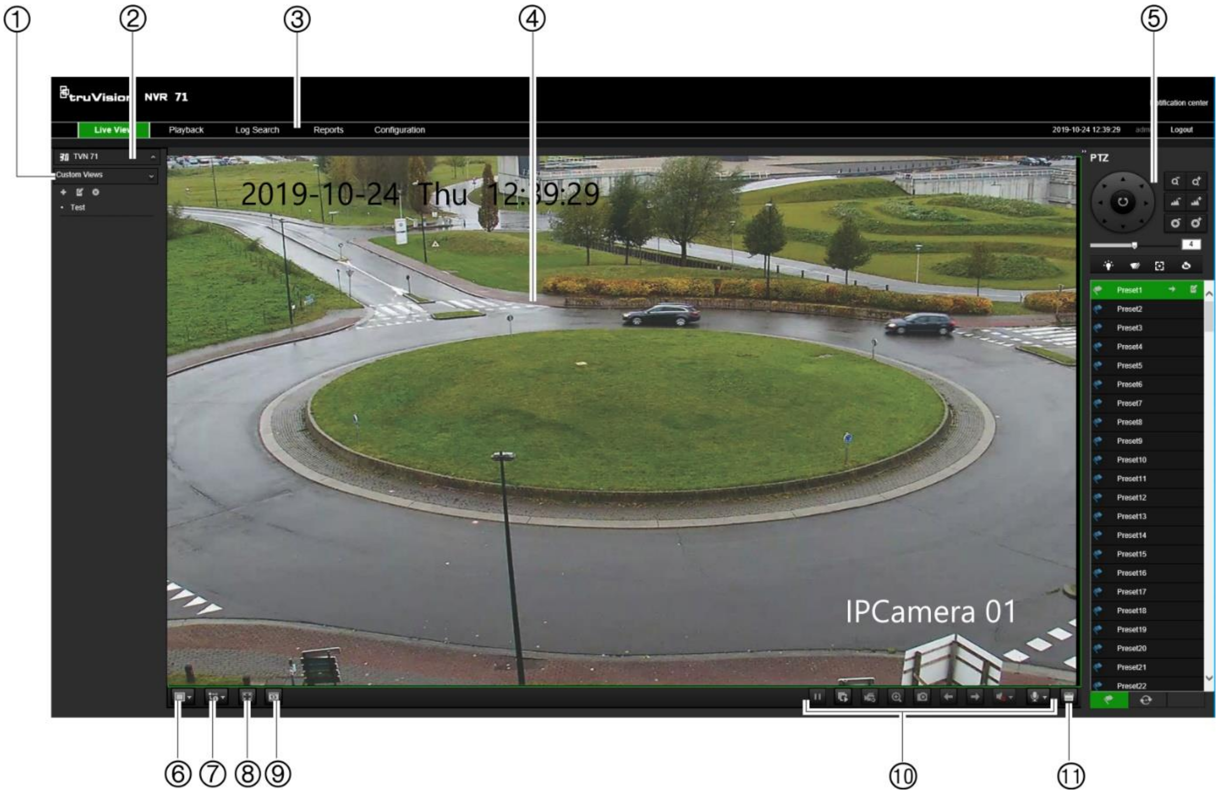
**Note**: You must run Microsoft Internet Explorer as administrator.

The recorder has three different stream types. You can select the best stream type to type your needs.

**Table 2: Stream types**

| Stream type | Description |
|---|---|
| Main stream | Use main stream for live viewing and recording with high resolutions and bandwidth. It delivers high resolution video for local HDD recording and storage. |
| Substream | Use substream when there is a bandwidth limitation in real time streaming. It delivers a low or standard resolution video for remote viewing, such as when using a smartphone application. |
| Transcoded stream | Use transcoded stream for remote live viewing and playback when there is a bandwidth limitation over the web client. You can reduce the resolution, bitrate, and frame rate of the original stream so that it better suits a low bandwidth.<br>The recorder transcodes the original stream before sending it over the web. In Auto Mode, if the original stream is 1080p or higher, the resolution of the transcoded stream will be 1080p. If original stream is less than 1080p, the resolution of the transcoded stream will not change. |

**Figure 5: Live view in the web browser interface**



| | Name | Description | |
|---|---|---|---|
| 1. | Custom view | Lets you group selected cameras together in live view. See “Custom views” on page 24 for more information. | |
| 2. | Camera live view and recording | Select the camera for live viewing and recording as well as the streaming type. | |
| | | / | Click the button to start/stop live view from the selected camera. |
| | | / | Click the button to start/stop local recording on your PC from the selected camera. |
| | | Main stream (1)<br>Substream (2)<br>Transcoded stream (3) | Position the mouse cursor on the streaming type button and select the desired stream from the pop-up menu: Main stream, Substream, or Transcoded stream. |
| 3. | Menu toolbar | Lets you navigate through the following menus:<br>• View live video<br>• Play back video<br>• Search for event logs<br>• Configure settings<br>• Log out of the interface | |
| 4. | Viewer | View live or playback video. | |
| 5. | PTZ/Video parameters panel | Hide/display the PTZ panel. See “Control a PTZ dome camera” on page 26 for more information. | |
| 6. | Display format | Define how you want video to be displayed in the viewer: Single or multiview. | |

| | Name | Description | |
|---|---|---|---|
| 7. | Streaming type | | Select main stream, substream, and transcoded stream for all the cameras. |
| 8. | Full screen | Display the video tiles only. Toolbars and panels not displayed. Press ESC button on the keyboard to view toolbars and panels. | |
| 9. | Transcoding play | Transcoded streaming is normally used when accessing the recorder via a web client. Modify the resolution, maximum bit rate, and frame rate of the transcoded stream. | |
| 10. | Video function toolbar | Lets you do the following in live view: | |
| | | ⏸ | Pause live viewing. |
| | | | Start/stop live streaming from all cameras. |
| | | | Start/stop local recording from all cameras. |
| | | 🔍 | Digital zoom. |
| | | 📷 | Take a snapshot. |
| | | ←<br>→ | View previous and next camera respectively.<br>If viewing in multiview format, live view moves to the next group of cameras for the selected number of video tiles. |
| | | 🔇 | Turn audio on/off |
| | | 🎤 | Turn microphone on/off |
| 11. | Alarm output | Shows the alarm outputs of the recorder and lets you trigger them on/off | |

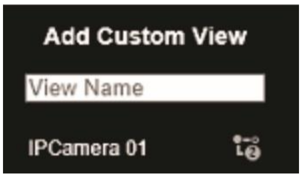
# Custom views

You can easily group cameras so that they appear in live view together. This allows you, for example, to quickly see all the cameras in a pre-defined part of the building such as a parking lot or different floors.

You can change the name of a custom view as well as select which cameras in a custom view group are main stream and substream. Not available for cameras with transcoded streaming.

**To create a custom view of cameras:**

1. Select the required multiscreen lay-out, depending on the number of cameras you want to show in the custom view.
2. Select a video tile for the camera that you want to appear in the custom view and click the camera button to enable live view (▣). The camera’s live view appears in the video tile.
3. Select another video tile and enable live view for the next camera to include in the custom view. Repeat for each camera to be included in the custom view.
4. Click the **Add Custom View** button ✚. The list of selected cameras appears. Enter the name of the custom view in the text box.



5. Select which cameras will be main stream and substream by clicking on each camera listed in the custom view. The camera button changes to show the streaming type:

   Main stream

   Substream

6. Click **Save**. The custom view is listed under “Custom Views”.

**To call up a custom view of cameras:**

1. In the custom view list, double-click the desired custom view. The selected name is highlighted in green. The cameras included in this custom view appear on screen.

**To edit a custom view of cameras:**

1. Double-click the desired custom view.
2. Click the **Edit Custom View** button .
3. To change the name of the custom view, enter a different name for selected custom view group.
4. To change a camera’s streaming type, click the desired camera’s streaming type icon. The number on the streaming type icon changes.

   **Note**: You cannot add a camera to an existing custom view. You need to create a new custom view and add all the desired cameras.
5. Click **Save** to save the changes.

**To delete a custom view of cameras:**

1. Double-click the desired custom view.
2. Click the **Delete Custom View** button . The selected custom view is deleted.

# Digital zoom

You can easily zoom in or out of a camera image in live view mode and playback using the digital zoom command. The zoom command magnifies the camera image four times.

**To quickly zoom in/out on a camera image:**

1. Click the digital-zoom button  in live view. When enabled, the digital zoom button has a green frame.
2. Use the scroll wheel on the mouse to zoom in/out.

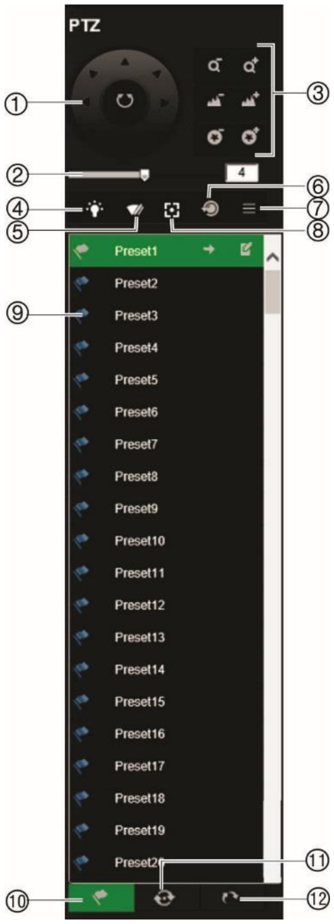
3. To exit digital zoom, click the digital zoom button again. The green frame on the button disappears.

# Control a PTZ dome camera

The web browser interface lets you control the PTZ functions of a dome camera. Click a PTZ dome camera and use the PTZ controls on the interface to control the PTZ functions.

See Figure 6 below for a description of the PTZ control panel. The PTZ control panel is always displayed in live view.

**Figure 6: PTZ controls panel**



1. Directional pan/auto-scan buttons: Controls the movements and directions of the PTZ. Center button is used to start auto-pan by the PTZ dome camera.
2. Adjust speed of PTZ dome camera.
3. Adjust zoom, focus, and iris.
4. Turn on or off the camera light (Not used).
5. Start or stop camera wiper (Not used).
6. Lens initialization: Initialize the lens of a camera with a motorized lens, such as PTZ or IP cameras. This function helps to maintain lens focus accuracy over prolong periods of time.
7. Auxiliary focus: Automatically focus the camera lens for the sharpest picture.
8. Menu: Not used.
9. Depending on function selected:

   - Call and set the selected preset

   - Run, stop, set, and delete the selected preset tour

   - Run, stop, start recording, stop recording, and delete the selected shadow tour
10. List of presets available.
11. List of preset tours available.
12. List of shadow tours available.

## Presets

Presets are previously defined locations of a PTZ dome camera. It allows you to quickly move the PTZ dome camera to a desired position. They are controlled from the PTZ panel in live view. You can set up to 255 presets for a camera.

Presets are saved on the camera and not on the recorder. The presets are identified on screen when they occur.

**To call up a preset:**

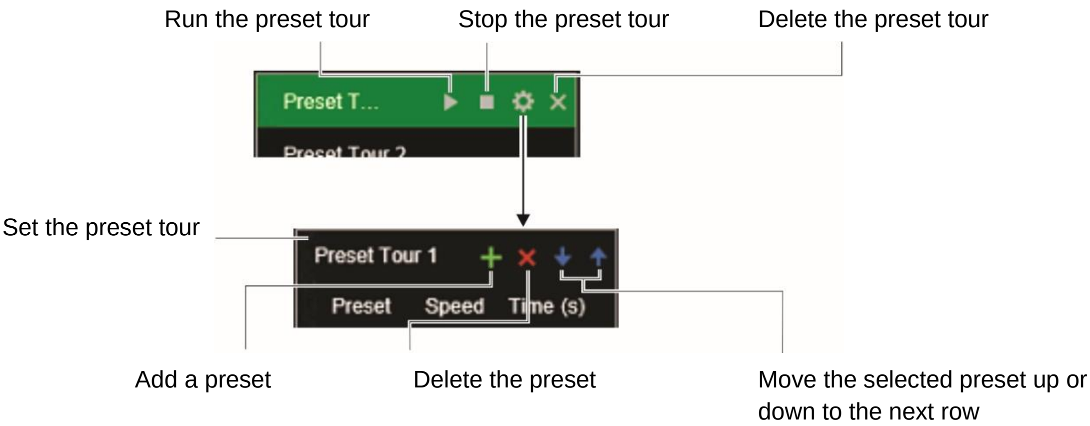
1. In live view, select the desired camera from the camera list.
2. Click the **Preset** button at the bottom of the PTZ panel to list all the presets.
3. Click the desired preset from the Preset list in the PTZ panel and click the ➡ button to call up the preset. The camera immediately jumps to the preset position.

## Preset tours

Preset tours are a series of presets. You can set up to eight preset tours for a camera.

Preset tours are saved on the camera and not on the recorder.

**Figure 7: Preset tour interface**



**To call up a preset tour:**

1. In live view, select the desired camera from the camera list.
2. Click the **Preset Tour** button at the bottom of the PTZ panel to list all the preset tours.
3. Click the desired preset tour from the Preset Tour list in the PTZ panel and click the run button to start the tour. The camera immediately moves through the preset tour.

**To add a preset tour:**

1. In live view, select the desired camera from the camera list.
2. Click the **Preset Tour** button at the bottom of the PTZ panel.
3. Select a preset tour from the list and click ⚙ to set a preset tour.
4. Click + to add a preset. The Step window appears. Select the preset number and enter the speed and dwell time (Time) in seconds of the preset.

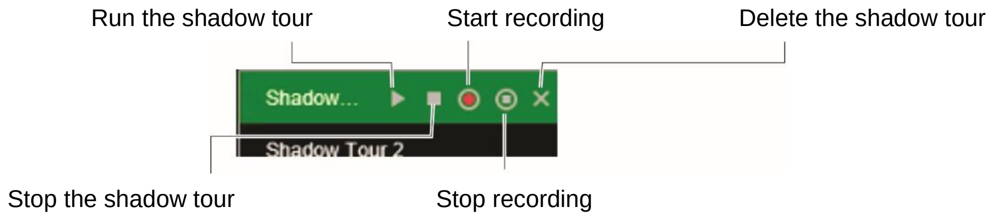
   **Note**: A preset tour should have at least two presets.
5. Repeat step 4 to add other presets to the preset tour.
6. Click **OK** to save the settings. The tour appears in the list.

## Shadow tours

Shadow tours allow you to record the manual movement of a PTZ and follow the same tour later. You can set up to eight shadow tours for a camera.

Shadow tours are saved on the camera and not on the recorder.

**Figure 8: Shadow tour interface**



### To call up a shadow tour:

1. In live view, select the desired camera from the camera list.
2. Click the Shadow Tour button at the bottom of the PTZ panel to list all the shadow tours.
3. Select the desired shadow tour and click the run button. The camera immediately carries out the shadow tour movement. Click the stop button to stop the tour.

### To set up a shadow tour:

1. In live view, select the desired camera from the camera list.
2. Click the Shadow Tour button at the bottom of the PTZ panel to list all the shadow tours.
3. Click the record button and, using the PTZ directional buttons, move the camera to follow the desired path. Click the save button to save the tour.

   **Note**: A shadow tour can be overwritten.

# Chapter 6
# Playback functionality

The recorder lets you quickly locate and play back recorded video. There are three ways to play back video:

- Web browser
- TruVision Navigator
- TVRMobile

You can search video by specific time, events, motion detection, bookmarks, or snapshots (see Chapter 7 “Searching for files” on page 36 for further information). Video can be played back from up to 16 cameras simultaneously.

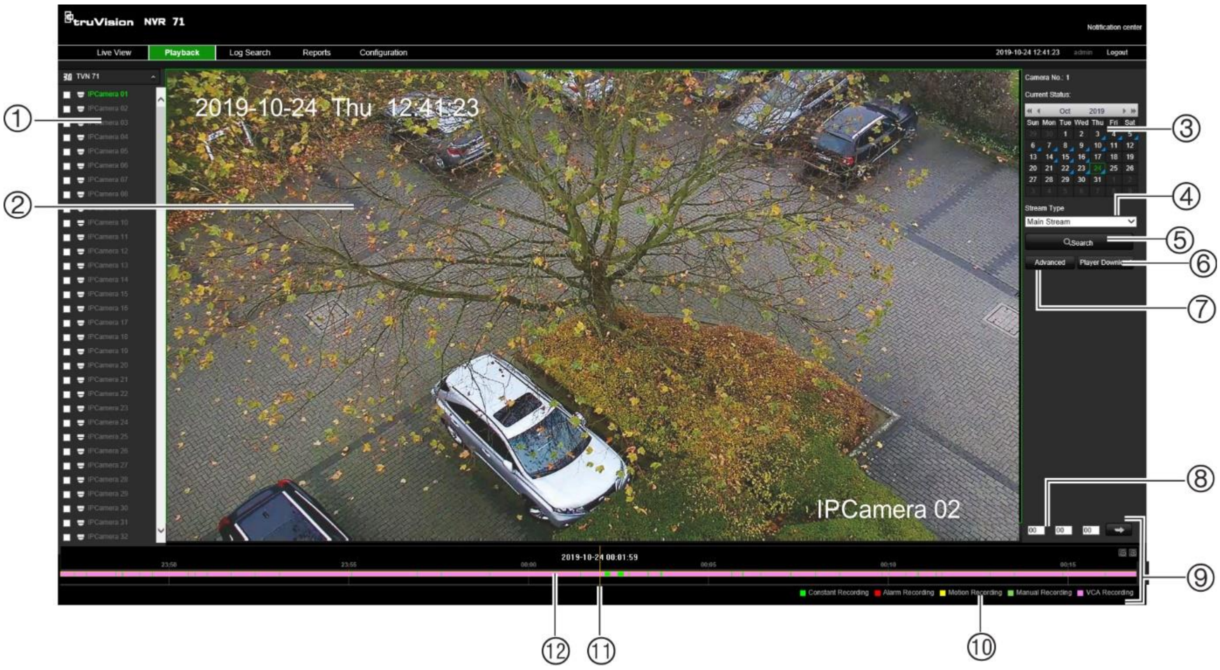
The recorder continues to record the live view from a camera while simultaneously playing back video on that camera display. You must have the access privilege to play back recordings (see “Customize a user’s access privileges” on page 126 for more information).

## Overview of the playback view

The playback video can be set up to display a time/date stamp for evidentiary purposes (see “Camera OSD” on page 58).

**Note**: Greyed out cameras are cameras that are not, or are no longer, connected to the recorder. As such, they may not contain recordings. However, every channel can be selected as channels that were connected in the past might still have associated video recordings.

### Figure 9: Playback window

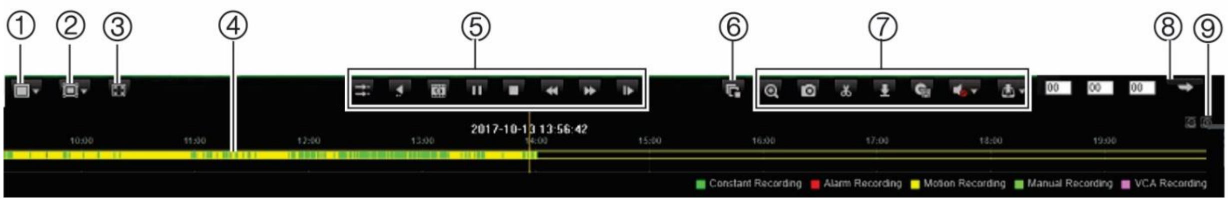


1. **Camera panel**. Select the cameras for playback. Move the mouse over the area to display the list of cameras available. Use the slide bar to see more cameras.
2. Playback viewer.
3. **Calendar panel**.
   Blue: Current selected date
   Green: Current date
   Blue triangle in the corner of a day: Recordings available for this day
4. **Streaming**. Select the streaming type: Main stream or substream.
5. **Search button**. Click to jump to the start of the selected day. Playback of the recording starts from the time set in the time field.
6. **Player Download button**. Click to download TruVision Player on to your PC to play back recordings.
7. **Advanced button**. Search the recordings of selected cameras by time/date as well as by events. Found recordings can then be played back and also locked to avoid being overwritten.
8. **Time field**. Enter the time from which to start playback of the recordings for all the selected cameras.
9. **Playback control toolbar**. See Figure 10 on page 31 for more information.
10. **Recording type**: Description of the color coding of recording types that appear in the playback progress bar.  Green indicates constant recording. Red indicates alarm recording. Yellow indicates motion recording. Pale green indicates manual recording. Magenta indicates VCA recording.
11. **Timeline**: Actual time of playback in progress.
12. **Recording progress bar**: This bar displays how much of the period has been recorded. It indicates in color the type of recording.

# Playback control toolbar

It is easy to manually control playback using the playback control toolbar. See Figure 10 below.

**Figure 10: Playback control toolbar**



| | Description | | | |
|---|---|---|---|---|
| 1. | Display playback on single screen or multiscreen mode. | | | |
| 2. | **Smart playback:**<br>Click one of these buttons to display when the following events occurred in the timeline. | | | |
| | 🗑 | Clear | ⟍ | Cross line detected |
| | 🏃 | Motion | ⚠ | Intrusion detected |
| 3. | **Full screen mode** | | | |
| 4. | **Recording progress bar**: This bar displays how much of the period has been recorded. It indicates in color the type of recording. | | | |
| 5. | **Playback control toolbar**: | | | |
| | ⇄ | **Synchronize playback**: Use to synchronize the playback time of several cameras when in multiscreen format. Select one of the video tiles in playback mode and click this button to synchronize all the other camera video tiles. Up to 16 channels can be simultaneously played back. | | |
| | ◀ | **Reverse**: Click to reverse playback. | | |
| | ▣ | **Transcode:** Click to play back transcoded video. See Table 2 on page 22 for more information. | | |
| | ▶ / ⏸ | **Play/pause playback**: Play or pause playback. | | |
| | ■ | **Stop playback**. Playback stops and the viewer goes black. | | |
| | ◀◀ | **Fast reverse**: Click to scroll through the different speeds available: -64X, -32X, -16X, -8X, -4X, -2X, single frame. Current speed is displayed under the camera name on top right of window.-For recorded video with audio, no audio is available during this function. | | |
| | ▶▶ | **Fast forward**: Click to scroll through the different speeds available: +64X, +32X, +16X, +8X, +4X, +2X, single frame. Current speed is displayed under the camera name on top right of window. For recorded video with audio, no audio is available during this function. | | |
| | ▮▶ | **Single frame**: Click to play back one frame at a time. | | |
| 6. | ⧉ / ⧉ | **Start/stop all playback**: Stop streaming playback from all cameras. | | |
| 7. | **Audio and video control toolbar:** | | | |
| | 🔍 | **Digital Zoom.** Click to enter the digital zoom function. Click again to exit. See “Digital zoom in playback” on page 34 for more information. | | |
| | 📷 | **Snapshot**: Capture a snapshot of the video. | | |
| | ✂ | **Video clips**: Start/stop video clip during playback. Sections of a recording can be saved to an external storage device. | | |
| | ⤓ | **Download**: Download video clips. | | |

| | Description | |
|---|---|---|
| | | **Backup**: Click to make back up of recorded files to save locally on the recorder. A list of the recorded files appears |
| | | **Audio**: Drag the scroll bar to the desired audio level. |
| | | **Bookmark management:** Manage bookmarks. |
| 8. | **Jump start**: Enter a precise time in the box and click the arrow button to jump start the playback to this selected time. | |
| 9. | **Zoom**: Zoom in and out of the time bar. | |

# Display order of cameras on screen

By default, playback is in full-screen mode. You can easily change the display mode to multiscreen using the single/multiscreen buttons at the bottom of the screen. You can play back up to 16 cameras at a time.

When using multiscreen mode, you can manually select the order in which the cameras appear on screen during play back. Camera 1 by default is always the camera displayed in video tile 1 and the other video tiles initially have no cameras allocated to them. The time bar underneath is located at midnight of the current day for the first video tile. The name of the camera associated with a selected video tile is displayed in the upper right of the screen under “Camera No

**To select the display order of cameras:**

1. Click **Playback** in the menu toolbar. The playback interface appears on screen.
2. Select the first video tile and click the name of the camera in the camera panel. The name turns green and appears under “Camera No.”.

   **Note**: A message is displayed if there is no recording associated with this camera,
3. Select the next video tile and click the camera name to be associated with this tile.
4. Repeat step 3 for each camera to be displayed.

# Play back by camera

See Figure 10 on page 31 for a description of the playback control toolbar.

Double-click a video tile to get full-screen mode. Double-click it again to return to the playback window.

**To search and play back recordings from specific cameras:**

1. Click **Playback** in the menu toolbar. The playback interface appears on screen.
2. In the camera panel on the left, select which cameras you want to play back. The camera recordings will be displayed in sequential order in the video tiles.

3. In the calendar, click the day of the week you want to play back. Days marked with a blue tab have recordings.
4. Click **Search** and then the **Play** ▶ button.

   Playback starts immediately in the video tiles. Playback of the recording starts from the time set in the time field for all the selected cameras. If you want a different start time for playback, slide the timeline to the desired time for each tile.

   The playback speed of the camera is displayed on the top right of the screen under “Current Status”.

   **Note:** A message appears if there are no recordings found in a video tile for the requested camera or time period.
5. Use the playback control toolbar to manually control playback.

# Synchronize play back across cameras

If several cameras are playing back simultaneously, you can synchronize their playback times so that it is easy to follow events across recordings.

**Note**: Up to 16 cameras can be played back simultaneously.

**To synchronize play back from several cameras:**

1. Click **Playback** in the menu toolbar. The playback interface appears on screen.
2. In the camera panel on the left, select which cameras you want to play back. The camera recordings will be displayed in sequential order in the video tiles.
3. In the calendar, click the day of the week you want to play back. Days marked with a blue tab have recordings.
4. Click **Search** and then the **Play** ▶ button.

   Play back starts immediately in the video tiles. Playback of the recording starts from the time set in the time field for all the selected cameras. If you want a different start time for play back, slide the timeline to the desired time for each tile.

   The playback speed of the camera is displayed on the top right of the screen under “Current Status”.

   **Note:** A message appears if there are no recordings found for the requested camera or period.
5. Select the video tile to which you want all the other cameras synchronized and click the **Synchronize Playback** ☰ button.
6. Use the playback control toolbar to manually control playback.

# Playback speed

You can play back a selected video at different speeds. This allows you to carefully examine an event frame-by-frame as it happens.

The current frame rate is shown as “Current Status” below the camera number on the top right of the screen.  The speed rates available are: -64X, -32X, -16X, -8X, -4X, -2X, single frame (normal speed). No audio is available when playing back in fast reverse or fast forward.

**To change the playback speed:**

Click ⏩ and ⏪ to speed up and slow down recorded video.

**To play back frame-by-frame:**

1. In playback mode, click the **Single Frame** ❙▶ button in the playback control toolbar. The speed changes to single frame.
2. Continue to click ❙▶ to watch the recording frame by frame.
3. Click the **Play** button return to normal speed.

# Digital zoom in playback

You can zoom in on an image during playback to see it in greater detail.

**To digitally zoom-in during playback:**

1. Click the **Digital Zoom** button in the playback control toolbar.
2. Use the scroll wheel of the mouse to zoom in/out. The selected area is magnified.
3. Click the **Digital Zoom** button again to stop digital zoom and return to normal view.

# Capture snapshots

You easily capture a snapshot of a video image for later reference. The image is saved on the unit in JPEG format.

**To capture a snapshot:**

1. In playback mode, when you see an image that you want to capture click the snapshot button 📷.

# Create video clips

You can save important scenes in a recorded file for later reference by creating video clips of selected portions of the file during playback. When an intruder, for example, crosses in front of several cameras, you can save the video clip of the intruder’s path across these cameras.

Up to 30 video clips can be made from a recording. Archived files can be played using the TruVision Player tool.

**To create video clips during playback:**

1. Search for the required files to play back. See “Advanced search video menu” on page 36.
2. Select the file or files to play back and click **Play**. Playback starts immediately.
3. Click the **Start Clipping** button to start the video clip click the **End Clipping** button to stop the video clip. The clip is automatically saved on your PC.

   **Note**: Go to Configuration > Browser Configuration to see where on your PC the clips have been saved.
4. Repeat for additional clips.

# Create bookmarks

You can bookmark the important scenes in a recorded file for later reference.

Bookmarks flag the start of a scene. Up to 64 bookmarks can be saved in a video file. There are two types of bookmarks:

- **Default bookmark** : All default bookmarks have the same generic name, “TAG”.
- **Customized bookmark** : You can give a name to a bookmark for easy identification. The time is automatically entered. The same name can be used for several bookmarks.

Bookmarks flag the start and end of a scene. Up to 64 bookmarks can be saved in a video file.

To search for existing bookmarks, see “Search bookmarked recordings” on page 40 for further information.

**To create a bookmark:**

1. In the playback mode, click the timeline bar where you want the bookmark to start or enter in the exact time of the desired playback start point in the jump start box. The yellow timeline jumps to this position.

   If there are multiple video tiles open, first select the desired tile.
2. Click the **Bookmark Management** button and select which bookmark type you want to create: Default or Customized.
3. Click the start bookmark button to start the recording clipping. The button turns green. When you want to end the clip, click the bookmark button again to end the clipping. A message will appear to say that the clipping was successful.

# Chapter 7
# Searching for files

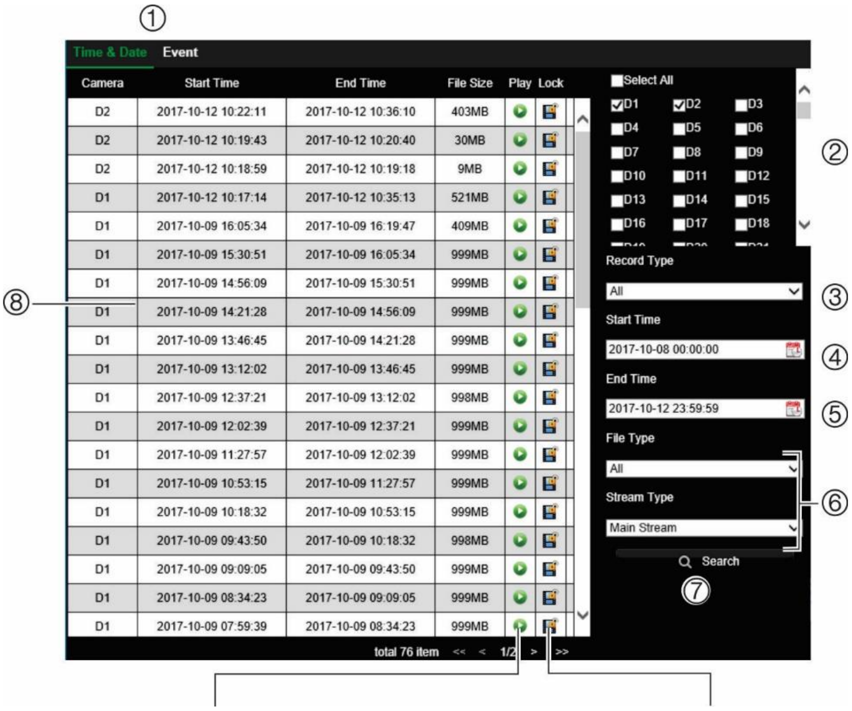
This chapter describes how to search and playback recorded videos as well as search them by time, events, bookmarks, and snapshots. It also describes searching for event logs.

## Advanced search video menu

You can easily search and play back recorded videos by time and date and events.

A search will usually produce a list of files, which may extend to several pages. The files are listed by date and time. The most recent file is listed first. You can then select a file to play it back. See Figure 11 below for an example of a search.

**Figure 11: Advanced Search: Time & Date menu**



| Camera | Start Time | End Time | File Size | Play | Lock |
|---|---|---|---|---|---|
| D2 | 2017-10-12 10:22:11 | 2017-10-12 10:36:10 | 403MB | ▶ | 🔒 |
| D2 | 2017-10-12 10:19:43 | 2017-10-12 10:20:40 | 30MB | ▶ | 🔒 |
| D2 | 2017-10-12 10:18:59 | 2017-10-12 10:19:18 | 9MB | ▶ | 🔒 |
| D1 | 2017-10-12 10:17:14 | 2017-10-12 10:35:13 | 521MB | ▶ | 🔒 |
| D1 | 2017-10-09 16:05:34 | 2017-10-09 16:19:47 | 409MB | ▶ | 🔒 |
| D1 | 2017-10-09 15:30:51 | 2017-10-09 16:05:34 | 999MB | ▶ | 🔒 |
| D1 | 2017-10-09 14:56:09 | 2017-10-09 15:30:51 | 999MB | ▶ | 🔒 |
| D1 | 2017-10-09 14:21:28 | 2017-10-09 14:56:09 | 999MB | ▶ | 🔒 |
| D1 | 2017-10-09 13:46:45 | 2017-10-09 14:21:28 | 999MB | ▶ | 🔒 |
| D1 | 2017-10-09 13:12:02 | 2017-10-09 13:46:45 | 999MB | ▶ | 🔒 |
| D1 | 2017-10-09 12:37:21 | 2017-10-09 13:12:02 | 998MB | ▶ | 🔒 |
| D1 | 2017-10-09 12:02:39 | 2017-10-09 12:37:21 | 999MB | ▶ | 🔒 |
| D1 | 2017-10-09 11:27:57 | 2017-10-09 12:02:39 | 999MB | ▶ | 🔒 |
| D1 | 2017-10-09 10:53:15 | 2017-10-09 11:27:57 | 999MB | ▶ | 🔒 |
| D1 | 2017-10-09 10:18:32 | 2017-10-09 10:53:15 | 999MB | ▶ | 🔒 |
| D1 | 2017-10-09 09:43:50 | 2017-10-09 10:18:32 | 998MB | ▶ | 🔒 |
| D1 | 2017-10-09 09:09:05 | 2017-10-09 09:43:50 | 999MB | ▶ | 🔒 |
| D1 | 2017-10-09 08:34:23 | 2017-10-09 09:09:05 | 999MB | ▶ | 🔒 |
| D1 | 2017-10-09 07:59:39 | 2017-10-09 08:34:23 | 999MB | ▶ | 🔒 |

total 76 item << < 1/2 > >>

□ Select All
☑ D1 ☑ D2 □ D3
□ D4 □ D5 □ D6
□ D7 □ D8 □ D9
□ D10 □ D11 □ D12
□ D13 □ D14 □ D15
□ D16 □ D17 □ D18

Record Type: All

Start Time: 2017-10-08 00:00:00

End Time: 2017-10-12 23:59:59

File Type: All

Stream Type: Main Stream

Click to playback the selected video.

Click to lock recording to prevent it from being overwritten.

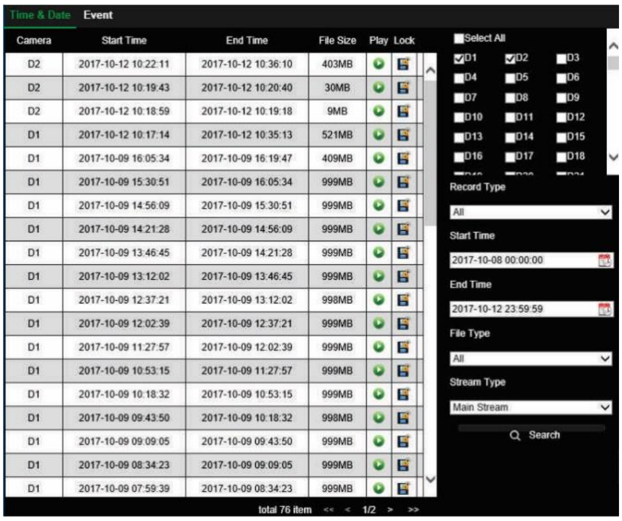
| | **Description** |
|---|---|
| 1. | The Advanced Search window has two submenus that allow you to carry out different searches by theme:<br>**Time and date:** Search all video by time and date of recording.<br>**Event**: Search only event recorded files. Files can be searched by event type: Alarm input, motion detection, VCA alarms, or intrusion alarms. |
| 2. | Select the desired camera or cameras to search. |
| 3. | **Record Type:** Select the type of recording: All, constant, motion, manual, or VCA alarms or alarms. |
| 4. | **File Type:** Select |
| 5. | **Stream Type**: Search for main stream or substream recordings. |
| 6. | **Start and end times**: immediately access archived footage for the start and end time shown. See “Search and play back recordings by time and video type” below for further information. |
| 7. | **Search**: Call up Search result list. See below for further information. |
| 8. | Search results. |

# Search and play back recordings by time and video type

You can search recorded video by date/time and video type, such as constant recordings, motion, manual recordings, VCA alarms, and alarm recordings.

### To search and play back recordings by time and type:

1. In playback, click the **Advanced** button and select the **Time & Date** tab**.**
2. Select the desired cameras, record type, file type, stream type as well as the start and end times of the desired period.
3. Click **Search**. The list of search results appears.



| Camera | Start Time | End Time | File Size | Play | Lock |
|---|---|---|---|---|---|
| D2 | 2017-10-12 10:22:11 | 2017-10-12 10:36:10 | 403MB | ● | 🔒 |
| D2 | 2017-10-12 10:19:43 | 2017-10-12 10:20:40 | 30MB | ● | 🔒 |
| D2 | 2017-10-12 10:18:59 | 2017-10-12 10:19:18 | 9MB | ● | 🔒 |
| D1 | 2017-10-12 10:17:14 | 2017-10-12 10:35:13 | 521MB | ● | 🔒 |
| D1 | 2017-10-09 16:05:34 | 2017-10-09 16:19:47 | 409MB | ● | 🔒 |
| D1 | 2017-10-09 15:30:51 | 2017-10-09 16:05:34 | 999MB | ● | 🔒 |
| D1 | 2017-10-09 14:56:09 | 2017-10-09 15:30:51 | 999MB | ● | 🔒 |
| D1 | 2017-10-09 14:21:28 | 2017-10-09 14:56:09 | 999MB | ● | 🔒 |
| D1 | 2017-10-09 13:46:45 | 2017-10-09 14:21:28 | 999MB | ● | 🔒 |
| D1 | 2017-10-09 13:12:02 | 2017-10-09 13:46:45 | 999MB | ● | 🔒 |
| D1 | 2017-10-09 12:37:21 | 2017-10-09 13:12:02 | 998MB | ● | 🔒 |
| D1 | 2017-10-09 12:02:39 | 2017-10-09 12:37:21 | 999MB | ● | 🔒 |
| D1 | 2017-10-09 11:27:57 | 2017-10-09 12:02:39 | 999MB | ● | 🔒 |
| D1 | 2017-10-09 10:53:15 | 2017-10-09 11:27:57 | 999MB | ● | 🔒 |
| D1 | 2017-10-09 10:18:32 | 2017-10-09 10:53:15 | 999MB | ● | 🔒 |
| D1 | 2017-10-09 09:43:50 | 2017-10-09 10:18:32 | 998MB | ● | 🔒 |
| D1 | 2017-10-09 09:09:05 | 2017-10-09 09:43:50 | 999MB | ● | 🔒 |
| D1 | 2017-10-09 08:34:23 | 2017-10-09 09:09:05 | 999MB | ● | 🔒 |
| D1 | 2017-10-09 07:59:39 | 2017-10-09 08:34:23 | 999MB | ● | 🔒 |

total 76 item << < 1/2 > >>

☑ D1 ☑ D2 □ D3
□ D4 □ D5 □ D6
□ D7 □ D8 □ D9
□ D10 □ D11 □ D12
□ D13 □ D14 □ D15
□ D16 □ D17 □ D18

Record Type: All

Start Time: 2017-10-08 00:00:00

End Time: 2017-10-12 23:59:59

File Type: All

Stream Type: Main Stream

4. Play back the search results:

Click the playback button ▶ of a desired recording. Only one result can be played back at a time. The playback recording appears in the playback viewer. Click the viewer screen to watch the recording. When the selected recording finishes, the viewer screen goes black.

To view another search result, click **Advanced** and select another file to watch.

**Note**: If you close the Search window, all search results will be lost.

5. To hide the playback control toolbar during play back, click the full-screen button. Press **Esc** button on your keyboard to return to the playback window with the toolbar displayed.
6. Use the playback control toolbar to manually control playback.
7. To do another search, click **Stop All Playback** ⧉ in the playback window and then click the **Advanced** button. Reselect the search criteria and click **Search**.
8. Click ☒ in the top corner of the advanced search window to close it.

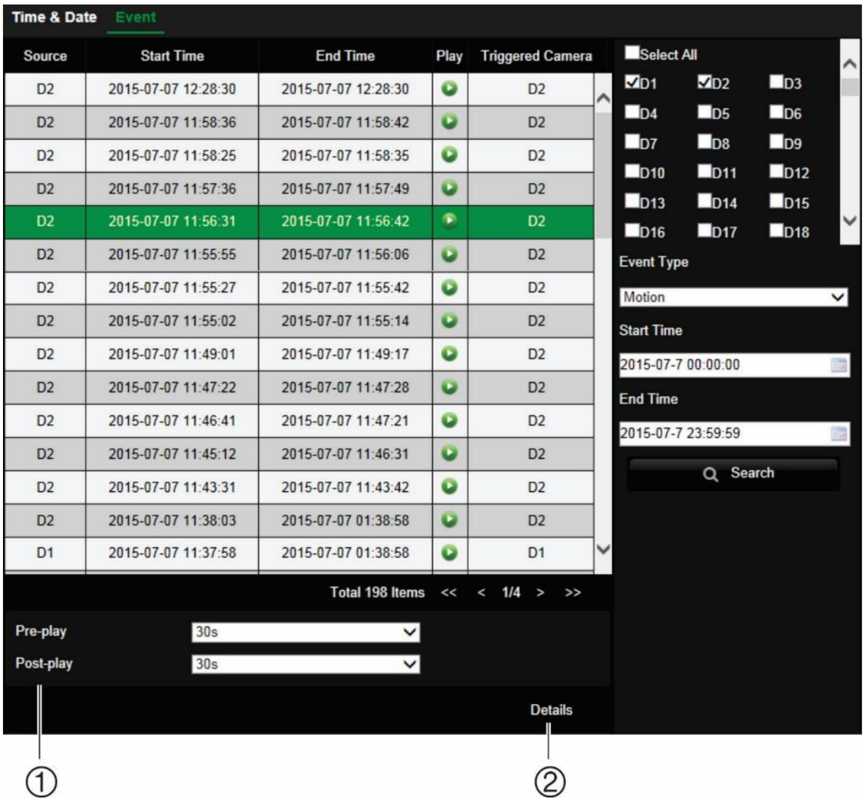
**To lock recordings to prevent overwriting:**

1. In playback, click the **Advanced** button and select the **Time & Date** tab.
2. Select the desired cameras, record type, file type, stream type as well as the start and end times of the desired recording.
3. Click **Search**. The list of search results appears.
4. Click the Lock button 🔒 of a desired camera. The selected file cannot be overwritten.

# Search and play back recordings by event

You can search recorded video by event type: Alarm Input, Motion, VCA Alarms, and Intrusion alarms. When you select a video to play back from an event search, you can add on to the beginning and end of the video pre-defined times. The pre-play and post-play times can help provide information to what happened just before and after an event. You can select one of seven time periods for the pre- and post-play times.

**Figure 12: Advanced Search: Event search menu**



Time & Date | Event

| Source | Start Time | End Time | Play | Triggered Camera |
|---|---|---|---|---|
| D2 | 2015-07-07 12:28:30 | 2015-07-07 12:28:30 | ▶ | D2 |
| D2 | 2015-07-07 11:58:36 | 2015-07-07 11:58:42 | ▶ | D2 |
| D2 | 2015-07-07 11:58:25 | 2015-07-07 11:58:35 | ▶ | D2 |
| D2 | 2015-07-07 11:57:36 | 2015-07-07 11:57:49 | ▶ | D2 |
| D2 | 2015-07-07 11:56:31 | 2015-07-07 11:56:42 | ▶ | D2 |
| D2 | 2015-07-07 11:55:55 | 2015-07-07 11:56:06 | ▶ | D2 |
| D2 | 2015-07-07 11:55:27 | 2015-07-07 11:55:42 | ▶ | D2 |
| D2 | 2015-07-07 11:55:02 | 2015-07-07 11:55:14 | ▶ | D2 |
| D2 | 2015-07-07 11:49:01 | 2015-07-07 11:49:17 | ▶ | D2 |
| D2 | 2015-07-07 11:47:22 | 2015-07-07 11:47:28 | ▶ | D2 |
| D2 | 2015-07-07 11:46:41 | 2015-07-07 11:47:21 | ▶ | D2 |
| D2 | 2015-07-07 11:45:12 | 2015-07-07 11:46:31 | ▶ | D2 |
| D2 | 2015-07-07 11:43:31 | 2015-07-07 11:43:42 | ▶ | D2 |
| D2 | 2015-07-07 11:38:03 | 2015-07-07 01:38:58 | ▶ | D2 |
| D1 | 2015-07-07 11:37:58 | 2015-07-07 01:38:58 | ▶ | D1 |

Total 198 Items << < 1/4 > >>

Pre-play: 30s

Post-play: 30s

Details

□ Select All

☑ D1 ☑ D2 □ D3
□ D4 □ D5 □ D6
□ D7 □ D8 □ D9
□ D10 □ D11 □ D12
□ D13 □ D14 □ D15
□ D16 □ D17 □ D18

Event Type: Motion

Start Time: 2015-07-7 00:00:00

End Time: 2015-07-7 23:59:59

Search

1. Pre- and post-play recording times: Extra time added pre and post the recording.
2. Details: Shows the different recording files associated with this event from the selected camera. These can be main and substream recordings.

### To search and play back event recordings:

1. In playback, click the **Advanced** button and select the **Event** tab.
2. Select the desired event type as well as start and end times of the desired period.
3. If you selected “Motion”, select the desired cameras.

   If you selected “Alarm Input”, select the desired alarm inputs.

   If you selected “VCA Alarms”, enter the event type from the drop-down list under Event and the cameras.

   If you selected “Intrusion Alarm”, enter the desired intrusion panel event.
4. Select the desired date and time to search.
5. For VCA alarms and intrusion alarms, select the desired alarm type.
6. Click **Search**. The list of search results appears.
7. Select the desired video from the list.
8. Select a pre-play and post-play time to add to the playback videos: 5 s, 10 s, 30 s, 60 s, 120 s, 300 s, or 600 s. By default, they are 30 s.
9. Play back the search results.

Click the playback button ▶ of a desired recording. Only one result can be played back at a time. The playback recording appears in the playback viewer. Click the viewer screen to watch the recording. When the selected recording finishes, the viewer screen goes black.

To view another search result, click **Advanced** and select another file from the results list to watch.

**Note**: If you close the Search window, all search results will be lost.

10. To hide the playback control toolbar during play back, click the full-screen button. Press **Esc** button on your keyboard to return to the playback window with the toolbar displayed.
11. Use the playback control toolbar to manually control playback.
12. To do another search, click **Stop All Playback** ⧉ in the playback window and then click the **Advanced** button. Reselect the search criteria and click **Search**.
13. Click ☒ in the top corner of the Advanced Search window to close it.

# Search bookmarked recordings

You can search bookmarks and then manage them. The manage function lets you rename, play back and delete bookmarks.

For information on creating bookmarks, see “Create bookmarks” on page 35.

**To manage bookmarks:**

1. In the playback mode, click the bookmark search button. The bookmark window appears.
2. Select the desired stream type, search type, as well as the start and end times of the bookmark clippings. Click **Search**.
3. The results are listed on screen.

   **Note**: A message appears if no bookmarks are found.
4. You can carry out several actions on the listed bookmarks:

   **To rename a bookmark**: Click on the **Edit** button or double-click on the name of the desired bookmark in the result list. Enter the new name in the edit box. Click on the green part of the bookmark entry for the name to be accepted.

   **To playback a bookmark**: Click the **Play** button of the desired bookmark in the result list.

   **To delete a bookmark**: Click the Delete button in the result list. Confirm that you want to delete the bookmark. It is deleted.

# Search snapshots

Snapshots are saved on your browser folder. You can select the folder in the Configuration > Browser Configuration > Save Snapshots when in Playback to. See “Capture snapshots” on page 34 for information on how to create snapshots.

# Search event logs

The recorder compiles a log of events, such as the start or end of video recording, recorder notifications, and alarms, through which you can easily search. Logs are categorized by the following event types:

- **Alarm:** Includes motion detection, tamper detection, video tampering, and other alarm events
- **Notification:** Includes system notifications such as video loss, HDD failures, and other system-related events
- **Operation:** Includes user access to the web interfaces and other operational events
- **Information:** Includes general information on the recorder actions, such as the start and end of video recording, etc.

Up to 2000 log files can be viewed at once.

Log files can also be exported onto a USB device. The exported file is named according to the time it was exported. For example: 20140729124841logBack.txt.

**Note**: Connect the backup device, such as a USB flash drive, to the recorder before commencing the log search.

**To search video from the system log:**

1. From the menu toolbar, click **Log Search**.
2. Under **Event**, select an option from the drop-down list: All, Alarm, Notification, Operation, or Information.
3. From the **Type** list, select one of the options:

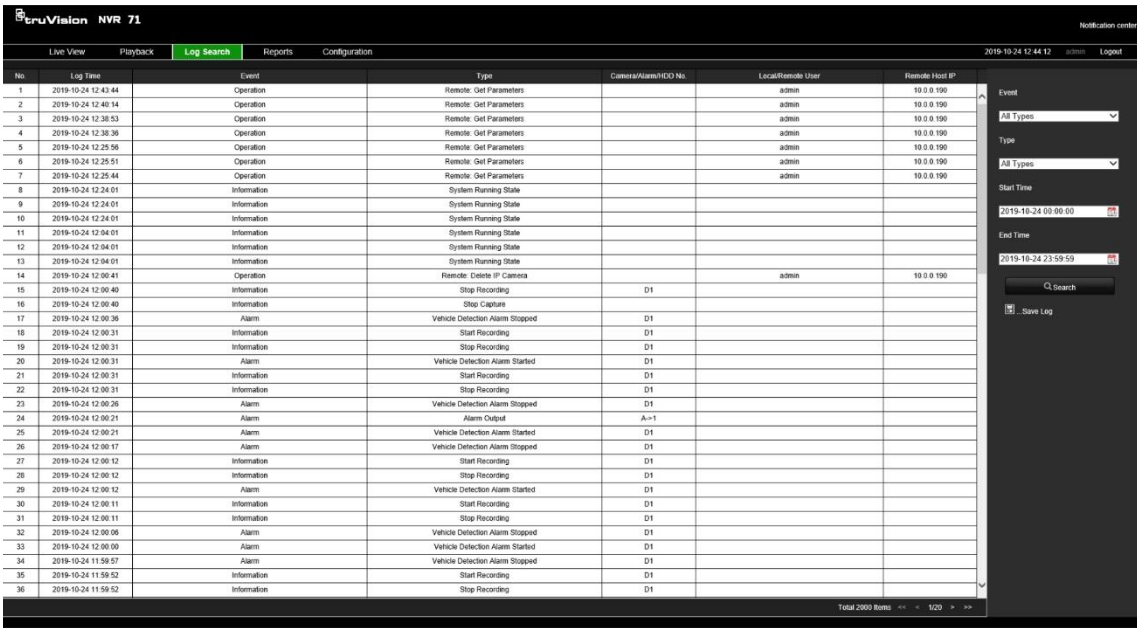
| Event | Type |
|---|---|
| All Types | All Types |
| Alarm | All Types, Alarm Input, Alarm Output, Start Motion Detection, Stop Motion Detection, Start Camera Tamper, Stop Camera Tamper, Cross Line Alarm Started, Cross Line Alarm Stopped, Intrusion Detected Alarm Started, Intrusion Detected Alarm Stopped, Audio Exception Alarm Started, Audio Exception Alarm Stopped, Sudden Change of Sound Intensity Alarm Started, Sudden Change of Sound Intensity Alarm Stopped, Face Detected Alarm Started, Face Detected Alarm Stopped, Defocus Detected Alarm Started, Defocus Detected Alarm Stopped, Sudden Scene Change Alarm Started, Sudden Scene Change Alarm Stopped, Enter Region Alarm Started, Enter Region Alarm Stopped, Exit Region Alarm Started, Exit Region Alarm Stopped, Object Left Behind Detection Alarm Started, Object Left Behind Detection Alarm Stopped, Object Removal Alarm Started, Object Removal Alarm Stopped, Intrusion Arming Event Stopped, Intrusion Disarming Event Started, Intrusion Event Alarm Started, Intrusion Heartbeat Alarm Started |
| Notification | All Types, Video Loss Alarm, Invalid Login, HDD Full, HDD Error, Duplicate IP Address Found, Network Disconnected, Abnormal Record, IP Camera Disconnected, IP Camera Address Conflicted, Hot Spare Exception, IP Camera Motion Analysis Exception, EFR Record Exception, Record Buffer Overflow, IP Camera Access Exception |

| | |
|---|---|
| Operation | All Types, Power Up, Abnormal Shutdown, Watchdog Reboot, Local: Export Record File, Remote: Reboot, Remote: Login, Remote: Logout, Remote: Configure Parameters, Remote: Upgrade, Remote: Start Manual Recording, Remote: Stop Manual Recording, Remote: PTZ Control, Remote: Lock File, Remote: Unlock File, Remote: Trigger Alarm Output, Remote: Initialize HDD, Remote: Add IP Camera, Remote: Delete IP Camera, Remote: Set IP Camera, Remote: Playback by File, Remote: Playback by Time, Remote: Download by File, Remote: Download by Time, Remote: Export Config File, Remote: Import Config File, Remote: Export Record File, Remote: Get Parameters, Remote: Get Working Status, Connect Transparent Data Chan, Disconnect Transparent Data Chan, Start Bi-directional Audio, Stop Bi-directional Audio, Remote: Alarm Arming, Remote: Alarm Disarming, Remote: Add Network Storage, Remote: Delete Network Storage, Remote: Set Network Storage, Export Snapshot File,  Configure SNMP, Operate Bookmark, Delete HDD, Load HDD, Unload HDD, Spare Operate, Upgrade IP Camera Firmware, Export IP Camera File, Import Camera File, Operation: Activation, Operation: Restore Defaults, Restore Default Settings |
| Information | All Types, Local HDD Information, HDD S.M.A.R.T., Start Recording, Stop Recording, Delete Expired Video File, Network Storage Information, System Running State, Spare Start Backup, Spare Stop Backup, EFR Record Start, EFR Record Stop, ADD IP Camera EFR Time Duration, Delete IP Camera EFR Time Duration, Spare Work Device Information |

4. Select the search start and end date and times.

5. Click the **Search** button. A list of results appears.

   The columns are: File number, Log time, Event, Type, Camera/Alarm/HDD Number, Local/Remote User, and Remote Host IP.



2019-10-24 12:44:12

| No. | Log Time | Event | Type | Camera/Alarm/HDD No. | Local/Remote User | Remote Host IP |
|---|---|---|---|---|---|---|
| 1 | 2019-10-24 12:43:44 | Operation | Remote: Get Parameters | | admin | 10.0.0.190 |
| 2 | 2019-10-24 12:40:14 | Operation | Remote: Get Parameters | | admin | 10.0.0.190 |
| 3 | 2019-10-24 12:38:53 | Operation | Remote: Get Parameters | | admin | 10.0.0.190 |
| 4 | 2019-10-24 12:38:36 | Operation | Remote: Get Parameters | | admin | 10.0.0.190 |
| 5 | 2019-10-24 12:25:56 | Operation | Remote: Get Parameters | | admin | 10.0.0.190 |
| 6 | 2019-10-24 12:25:51 | Operation | Remote: Get Parameters | | admin | 10.0.0.190 |
| 7 | 2019-10-24 12:25:44 | Operation | Remote: Get Parameters | | admin | 10.0.0.190 |
| 8 | 2019-10-24 12:24:01 | Information | System Running State | | | |
| 9 | 2019-10-24 12:24:01 | Information | System Running State | | | |
| 10 | 2019-10-24 12:24:01 | Information | System Running State | | | |
| 11 | 2019-10-24 12:04:01 | Information | System Running State | | | |
| 12 | 2019-10-24 12:04:01 | Information | System Running State | | | |
| 13 | 2019-10-24 12:04:01 | Information | System Running State | | | |
| 14 | 2019-10-24 12:00:41 | Operation | Remote: Delete IP Camera | | admin | 10.0.0.190 |
| 15 | 2019-10-24 12:00:40 | Information | Stop Recording | D1 | | |
| 16 | 2019-10-24 12:00:40 | Information | Stop Capture | | | |
| 17 | 2019-10-24 12:00:36 | Alarm | Vehicle Detection Alarm Stopped | D1 | | |
| 18 | 2019-10-24 12:00:31 | Information | Start Recording | D1 | | |
| 19 | 2019-10-24 12:00:31 | Information | Stop Recording | D1 | | |
| 20 | 2019-10-24 12:00:31 | Alarm | Vehicle Detection Alarm Started | D1 | | |
| 21 | 2019-10-24 12:00:31 | Information | Start Recording | D1 | | |
| 22 | 2019-10-24 12:00:31 | Information | Stop Recording | D1 | | |
| 23 | 2019-10-24 12:00:26 | Alarm | Vehicle Detection Alarm Stopped | D1 | | |
| 24 | 2019-10-24 12:00:21 | Alarm | Alarm Output | A->1 | | |
| 25 | 2019-10-24 12:00:21 | Alarm | Vehicle Detection Alarm Started | D1 | | |
| 26 | 2019-10-24 12:00:17 | Alarm | Vehicle Detection Alarm Stopped | D1 | | |
| 27 | 2019-10-24 12:00:12 | Information | Start Recording | D1 | | |
| 28 | 2019-10-24 12:00:12 | Information | Stop Recording | D1 | | |
| 29 | 2019-10-24 12:00:12 | Alarm | Vehicle Detection Alarm Started | D1 | | |
| 30 | 2019-10-24 12:00:11 | Information | Start Recording | D1 | | |
| 31 | 2019-10-24 12:00:11 | Information | Stop Recording | D1 | | |
| 32 | 2019-10-24 12:00:06 | Alarm | Vehicle Detection Alarm Stopped | D1 | | |
| 33 | 2019-10-24 12:00:00 | Alarm | Vehicle Detection Alarm Started | D1 | | |
| 34 | 2019-10-24 11:59:57 | Alarm | Vehicle Detection Alarm Stopped | D1 | | |
| 35 | 2019-10-24 11:59:52 | Information | Start Recording | D1 | | |
| 36 | 2019-10-24 11:59:52 | Information | Stop Recording | D1 | | |

Total 2000 Items 1/20

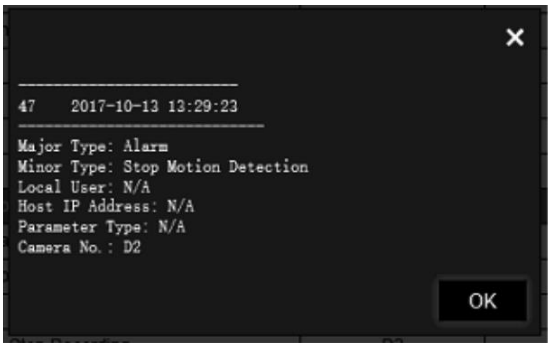
Event: All Types

Type: All Types

Start Time: 2019-10-24 00:00:00

End Time: 2019-10-24 23:59:59

6. Select a file and double-click it. The Details pop-up screen appears listing the information on the log or recording. For a recording it lists such information as start time, type of event, local user, host IP address, parameter type, and camera number. Click **OK** to close the Details pop-up window.



```
-------------------------
47    2017-10-13 13:29:23
----------------------------
Major Type: Alarm
Minor Type: Stop Motion Detection
Local User: N/A
Host IP Address: N/A
Parameter Type: N/A
Camera No.: D2
```

7. To save the selected log file to your PC or an external storage device, click **Save Log** in the log results list. In the “Save As” window that appears, enter the file name and select the location to save the file. It will be saved in *.txt format.
8. To archive the results of a log search, click **Save Log** and select the directory in which to save the file. The file is saved in *.txt format.

# Chapter 8
# Archiving files

Archive recorded files locally on your PC through the browser interface or software, or locally at the recorder on an external device such as USB flash drive, USB HDDs or a DVD burner. You must be in live view to archive video. Access to archive commands may require a password.

## Overview of archiving

You can configure the recorder to automatically archive files following a predefined schedule to the selected connected storage media.  See “Auto” below for more information.

## Auto archiving

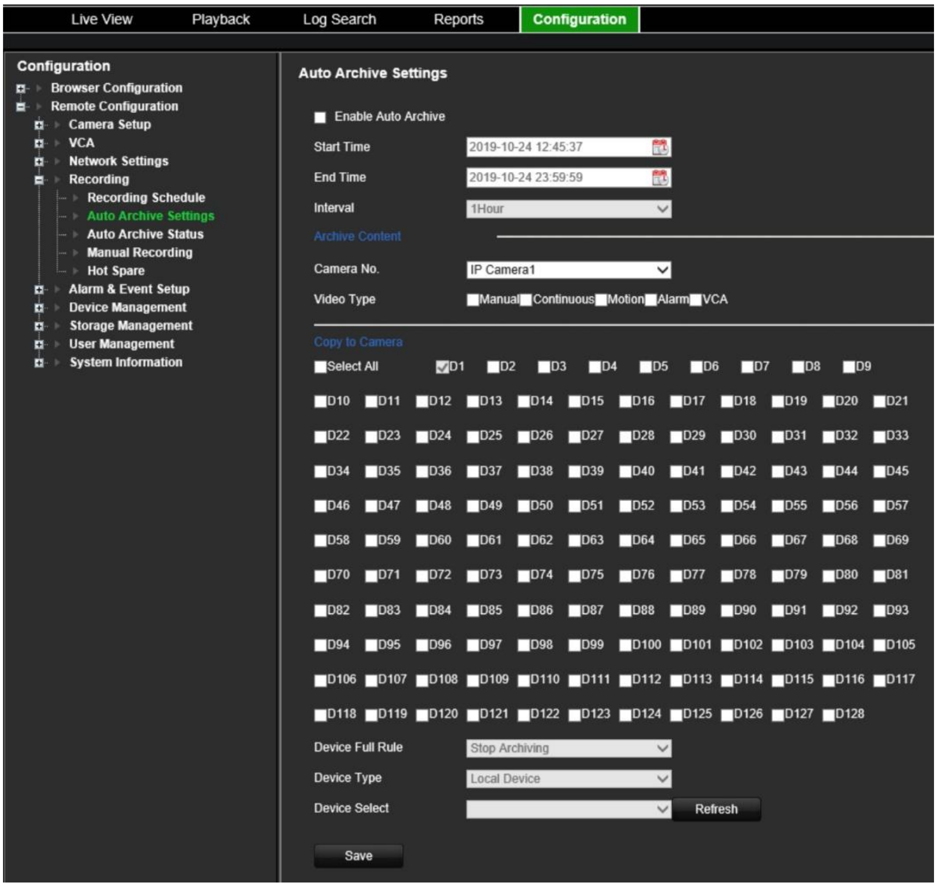
You can schedule the recorder to automatically archive recordings at set interval times to an external storage device. You can also select the cameras and recording types to auto archive as well as define how the system responds when the storage device becomes full.

It is easy to see the time of the most recent and next archive recording. Simply click the “Archive Status” menu and the information is displayed.

Archived files can be viewed using the TruVision Player tool.

**To schedule automatic archiving:**

1. Connect the backup device to the recorder.
2. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Recording** > **Auto Archive Settings**.



Auto Archive Settings

□ Enable Auto Archive

Start Time 2019-10-24 12:45:37

End Time 2019-10-24 23:59:59

Interval 1Hour

Archive Content

Camera No. IP Camera1

Video Type □Manual □Continuous □Motion □Alarm □VCA

Copy to Camera

□Select All ☑D1 □D2 □D3 □D4 □D5 □D6 □D7 □D8 □D9

□D10 □D11 □D12 □D13 □D14 □D15 □D16 □D17 □D18 □D19 □D20 □D21

□D22 □D23 □D24 □D25 □D26 □D27 □D28 □D29 □D30 □D31 □D32 □D33

□D34 □D35 □D36 □D37 □D38 □D39 □D40 □D41 □D42 □D43 □D44 □D45

□D46 □D47 □D48 □D49 □D50 □D51 □D52 □D53 □D54 □D55 □D56 □D57

□D58 □D59 □D60 □D61 □D62 □D63 □D64 □D65 □D66 □D67 □D68 □D69

□D70 □D71 □D72 □D73 □D74 □D75 □D76 □D77 □D78 □D79 □D80 □D81

□D82 □D83 □D84 □D85 □D86 □D87 □D88 □D89 □D90 □D91 □D92 □D93

□D94 □D95 □D96 □D97 □D98 □D99 □D100 □D101 □D102 □D103 □D104 □D105

□D106 □D107 □D108 □D109 □D110 □D111 □D112 □D113 □D114 □D115 □D116 □D117

□D118 □D119 □D120 □D121 □D122 □D123 □D124 □D125 □D126 □D127 □D128

Device Full Rule Stop Archiving

Device Type Local Device

Device Select

3. Select **Enable Auto Archive**.
4. Select the start and end date and time periods during which archiving can occur automatically.
5. Under **Interval Time**, select the desired interval time for archiving.

   The interval time options available are:  1 hour, 2 hours, 4 hours, 8 hours, 24 hours, or once only. Default is 1 hour.
6. Select the camera to auto archive.
7. Select the type of video files to be archived: Manual, Constant, Motion, Alarm, and VCA. More than one type can be selected.
8. You can copy these selected parameters to other cameras. Under the section “Copy to Camera, select the desired cameras.
9. Select how the recorder responds if the backup device becomes full. There are two options: Stop Archiving or Overwrite.

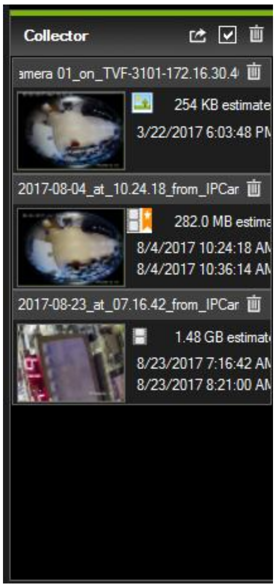
   If overwrite is selected, the oldest files are overwritten.
10. Under **Device Type**, select Local Device or Network Storage.
11. Under **Device Select**, select the backup device used.
12. If you change any options, click **Refresh**.
13. Click **Save**.

# Export video recordings and snapshots via TruVision Navigator

TruVision Navigator allows you to export a single recording file per camera. Exported video files from TruVision Navigator need to be viewed using the TruVision export file tool. For further information on exporting video and snapshots, please refer to the TruVision Navigator 7.1 User Manual.

**To export video and snapshots:**

1. In the playback window, search for the time frame of the desired video segment.
2. Click the **Video** button to move the selected video segment to the Collector.
3. Select each video or snapshot thumbnail for export in the Collector or use the Select/Deselect All button in the Collector header bar.



amera 01_on_TVF-3101-172.16.30.4
254 KB estimate
3/22/2017 6:03:48 PM

2017-08-04_at_10.24.18_from_IPCar
282.0 MB estima
8/4/2017 10:24:18 AM
8/4/2017 10:36:14 AM

2017-08-23_at_07.16.42_from_IPCar
1.48 GB estimat
8/23/2017 7:16:42 AM
8/23/2017 8:21:00 AM

4. Click the **Export** button at the top of the Collector panel.
5. Click **Browse** and select the destination of the export file.

   All selected video thumbnails will be exported as a single file.
6. Click the **Export Now** button.

**Note:** Make sure there is enough disk space at the destination location for the export. Use the file size estimate in the Collector as a guideline.

# Using TruVision Player

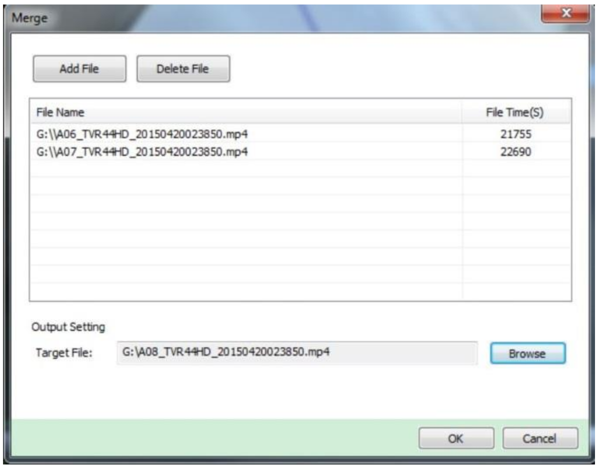
## Play back video using TruVision Player

Use the standard file player software, TruVision Player, to play back the archived video on your PC. It is downloaded from the Advanced Search menu in playback mode.

You can include multiple files in the TruVision Player playlist. Double-click the desired video file from the list and click the **Start** button. When the first file finishes, the next file will automatically start. Up to 16 files can be played synchronously from multiple cameras.

## Merge video files in TruVision Player

1. Add the exported video files to TruVision Player,
2. Click the menu button ⏷ and select **Tool** > **Merge**.
3. The Merge window appears. Click **Add File** to add the files you want to merge onto a selected video file. Under **Output Setting**, select the video file to which you want to add the files.



| File Name | File Time(S) |
|---|---|
| G:\\A06_TVR44HD_20150420023850.mp4 | 21755 |
| G:\\A07_TVR44HD_20150420023850.mp4 | 22690 |

Output Setting

Target File: G:\A08_TVR44HD_20150420023850.mp4

4. Click **OK**.

# Watermarking

You can display the digital watermark to authenticate images and protect them from alterations. Watermarking on an image is only visible during playback of exported video using the TruVision platform export video player.

The recorder supports watermarking from TruVision cameras and encoders.

Use the playback application to reveal the watermarking on archived video. Enable the Watermarking option in the player.

# Chapter 9
# Web browser configuration

This chapter describes how to configure the web browser locally. Use the local browser configuration to configure such settings as protocol type, stream type as well as where to save files on the system.

## Windows operating system

The recorder is compatible with Internet Explorer 9, 10 and 11 for Windows 8 and 10 operating systems. When using the recorder web browser interface, you can install ActiveX controls to connect and view video using Internet Explorer.

It is also compatible with Mozilla Firefox, Google Chrome and Apple Safari. See “Access the web browser” on page 20 for more information on the plug-in free solution to use these browsers.

To have complete functionality of the web browser interface and the recorder player with Windows 8 and above, do the following:

- Run the Browser interface and the recorder player application as an administrator in your workstation
- Add the recorder’s IP address to your browser’s list of trusted sites

**To add the recorder’s IP address to Internet Explorer’s list of trusted sites:**

1. Open Internet Explorer.
2. Click **Tools**, and then **Internet Options**.
3. Click the Security tab, and then select the **Trusted Sites** button.
4. Click **Sites**.
5. Clear the “Require server verification (https:) for all sites in this zone” box.
6. Enter the IP address or DDNS name in the “Add this website to the zone” field.
7. Click **Add**, and then click **Close**.
8. Click **OK** in the “Internet Options” dialog box.
9. Connect to the recorder for full browser functionality.

# Access the web browser

To access the recorder, open the Microsoft Internet Explorer web browser and enter the IP address assigned to the recorder, as a web address. On the logon window, enter the user name and password.

The default values for recorder network settings are:

- IP address - 192.168.1.82
- Subnet mask - 255.255.255.0
- Gateway address - 192.168.1.1
- Server port: 8000
- Ports:

| When using the browser: | When using TruNav: |
|---|---|
| RTSP port: 554 | RTSP port: 554 |
| HTTP port: 80 | Server/Client software port: 8000 |
| When using Chrome, Safari or Firefox, port in HTTP mode: 7681 | |

For more information on port forwarding, see Appendix B “Port forwarding information” on page 135.

Select a camera and a day to search from on the calendar displayed, and then click **Search**. The timeline below the page indicates video recorded for the specified day. The timeline also classifies by color the type of recording with each type.

Click and drag the marker across the timeline on where you want video playback to begin, and then click Play on the playback control toolbar. You can capture a snapshot of a video image, save the video playback, or download the recorded video.

# Configure the recorder via the browser

Click **Configuration** on the menu toolbar to display the configuration window. There are two ways to configure the recorder: Browser and Remote.

**Note**: You must run Microsoft Internet Explorer as administrator.

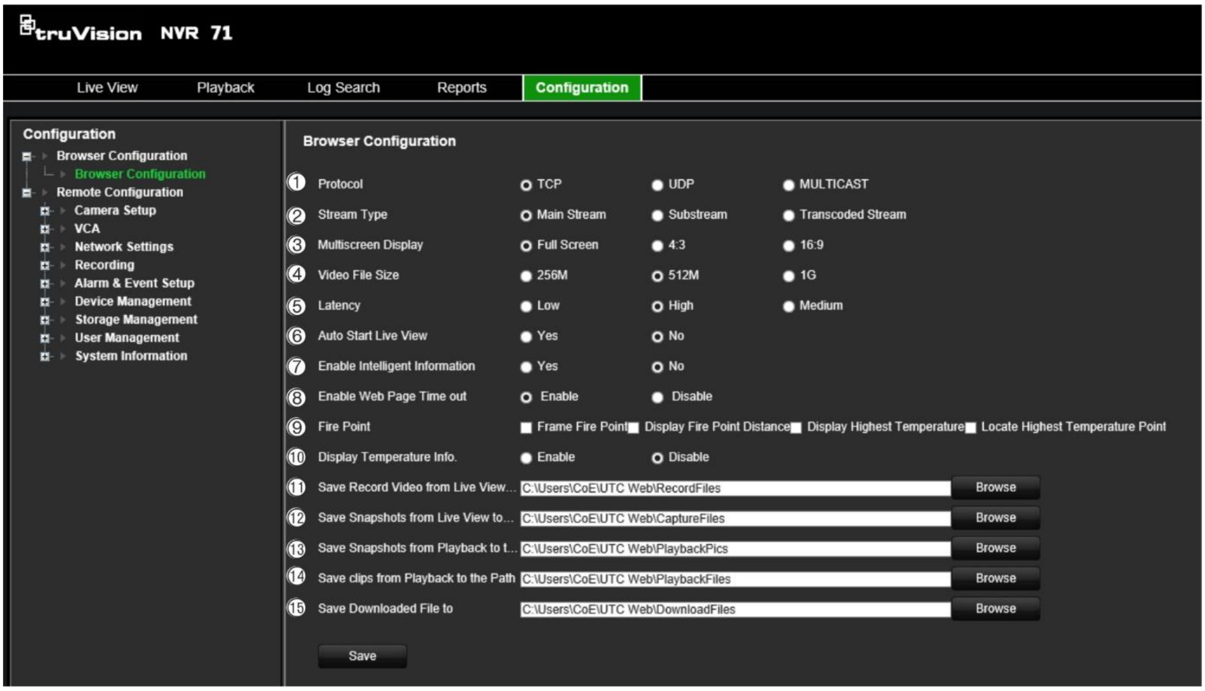
## Browser configuration

Browser configuration lets you define communication and network parameters such as protocol type, maximum file size, stream type and network transmission settings. You can also specify the directory locations for saving recorded and playback video, captured images, and downloaded files.

The browser interface settings are saved on your PC, not on the recorder.

See Figure 13 on page 50 for information on browser configuration settings.

## Figure 13: Browser configuration

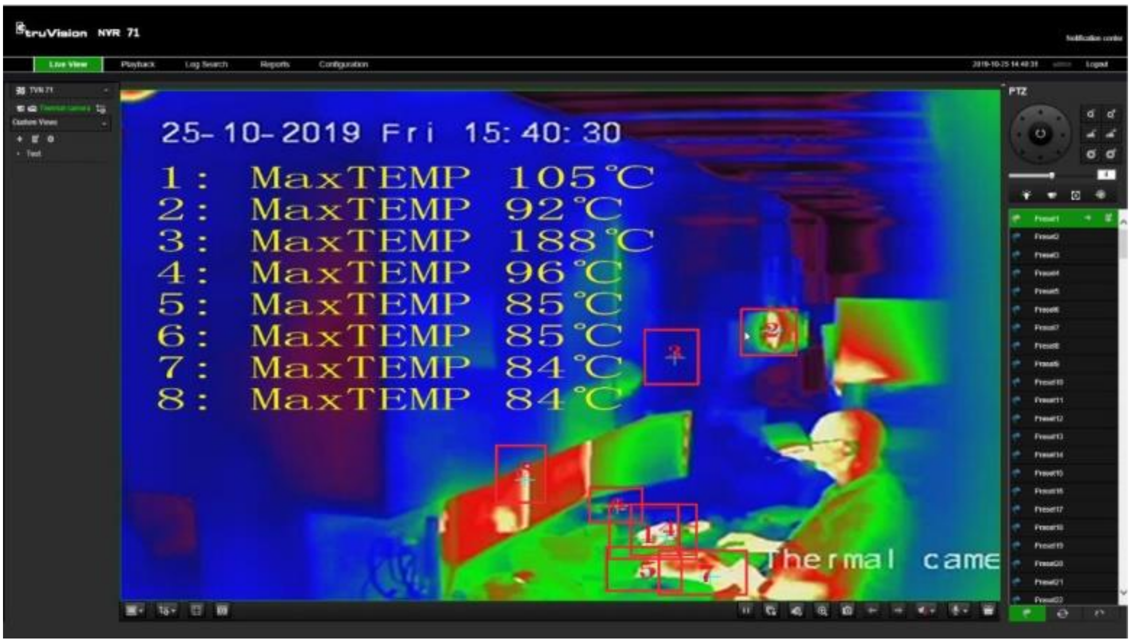


1 Protocol ○ TCP ● UDP ● MULTICAST
2 Stream Type ○ Main Stream ● Substream ● Transcoded Stream
3 Multiscreen Display ○ Full Screen ● 4:3 ● 16:9
4 Video File Size ● 256M ○ 512M ● 1G
5 Latency ● Low ○ High ● Medium
6 Auto Start Live View ● Yes ○ No
7 Enable Intelligent Information ● Yes ○ No
8 Enable Web Page Time out ○ Enable ● Disable
9 Fire Point □ Frame Fire Point □ Display Fire Point Distance □ Display Highest Temperature □ Locate Highest Temperature Point
10 Display Temperature Info. ● Enable ○ Disable
11 Save Record Video from Live View... C:\Users\CoE\UTC Web\RecordFiles
12 Save Snapshots from Live View to... C:\Users\CoE\UTC Web\CaptureFiles
13 Save Snapshots from Playback to t... C:\Users\CoE\UTC Web\PlaybackPics
14 Save clips from Playback to the Path C:\Users\CoE\UTC Web\PlaybackFiles
15 Save Downloaded File to C:\Users\CoE\UTC Web\DownloadFiles

| Option | | Description |
|---|---|---|
| 1. | Protocol Type | Specifies the network protocol used.  Options include: TCP, DUP, or MULTICAST. Default is TCP. |
| 2. | Stream Type | Specifies the streaming method used. Options include: Main Stream, Substream, or Transcoded Stream. Default is Main Stream.<br>Use main stream for live viewing and recording with high resolutions and bandwidth. Use substream when there is a bandwidth limitation, such as when using a mobile app.<br>Use transcoded stream for remote live viewing and playback when there is a bandwidth limitation. See Table 2 on page 22 for more information about stream types. |
| 3. | Window-division Mode | Specifies the image scale in a video tile. Options are Full Screen, 4:3, or 16:9. Default is full screen. |
| 4. | Video File Size | Specifies the maximum file size.  Options include: 256M, 512M, or 1G. Default is 512M. |
| 5. | Latency | Options include: Low, Medium or High. Default is High. |
| 6. | Auto Start Live View | Live view starts automatically when you login. Options are Yes or No. Default is No. |
| 7. | Enable Intelligent Information | Show/hide the IP camera motion or VCA metadata. Options are Yes or No. Default is No. |
| 8. | Enable Web Page Time-out | The web page times out after five minutes if there is no mouse movement by the user.<br>Options for time out are Enable and Disable. Default is Enabled. When disabled, the web page will not time out. |

| Option | Description |
|---|---|
| 9. Fire Point | This function is available when using the TruVision IP thermal camera. To be operational, the thermal camera function **Fire Source Detection** must be enabled under the *VCA Resource Configuration* menu.<br>It lets you visualize in live mode the temperature hot spots. The hot spots are displayed on screen with a list showing the temperature ranges of the hot spots. See Figure 14 below for an example.<br>You can select up to four options: Frame fire point, Display point distance, Display highest temperature, and Locate highest temperature point.<br>**IMPORTANT NOTICE**: This fire detection feature is not a substitute for a certified fire detection system. |

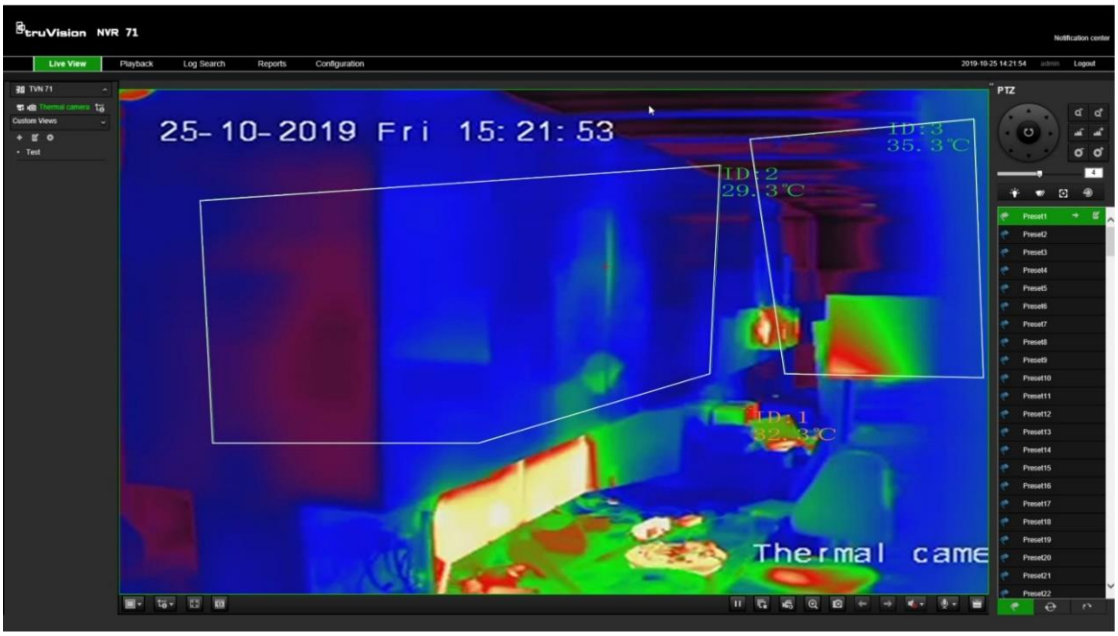
**Figure 14: Example of fire point results in a live view window**



25-10-2019 Fri 15:40:30

1 : MaxTEMP 105℃
2 : MaxTEMP 92℃
3 : MaxTEMP 188℃
4 : MaxTEMP 96℃
5 : MaxTEMP 85℃
6 : MaxTEMP 85℃
7 : MaxTEMP 84℃
8 : MaxTEMP 84℃

| Option | Description |
|---|---|
| 10. Display temperature info. | This function is available when using the TruVision IP thermal camera. To be operational, the thermal camera function **Temperature Measurement + Behavior Analysis + Standard VCA Functions must be** enabled under the *VCA Resource Configuration* menu.<br>It displays the temperature information in the frames that were set up in the thermal camera. See Figure 15 below for an example.<br>**IMPORTANT NOTICE**: This fire detection feature is not a substitute for a certified fire detection system. |

| Option | | Description |
|---|---|---|
| | **Figure 15: Example of temperature frames in a live view window**<br><br> truVision NVR 71<br>Notification center<br>Live View<br>Playback<br>Log Search<br>Reports<br>Configuration<br>2019-10-25 14:21:54<br>admin<br>Logout<br>TVN 71<br>Thermal camera<br>Custom Views<br>Test<br>25-10-2019 Fri 15:21:53<br>ID:3<br>35.3°C<br>ID:2<br>29.3°C<br>ID:1<br>32.3°C<br>Thermal came<br>PTZ<br>Preset1<br>Preset2<br>Preset3<br>Preset4<br>Preset5<br>Preset6<br>Preset7<br>Preset8<br>Preset9<br>Preset10<br>Preset11<br>Preset12<br>Preset13<br>Preset14<br>Preset15<br>Preset16<br>Preset17<br>Preset18<br>Preset19<br>Preset20<br>Preset21<br>Preset22 | |
| 11. | Save Record Video in Live View to | Specifies the directory for saving recorder video in live view mode. |
| 12. | Save Snapshots in Live View to | Specifies the directory for saving snapshots in live view mode. |
| 13. | Save Snapshots when in Playback to | Specifies the directory for saving snapshots in playback mode. |
| 14. | Save Clips when in Playback to | Specifies the directory for saving video clips in playback mode. |
| 15. | Save Downloaded File to | Specifies the directory for downloaded files. |

# Chapter 10
# Camera setup

Use the “Camera Setup” menu to configure IP cameras. You can also configure the camera OSD, snapshots, recording settings, motion detection, privacy masking, camera tampering, PTZ configurations and V-stream settings.

The camera configuration settings are saved on the recorder.

### Supported IP cameras

The recorder supports the following IP cameras:

- TruVision IP cameras with a maximum resolution of 12 MP
- ONVIF IP cameras
- Axis IP cameras

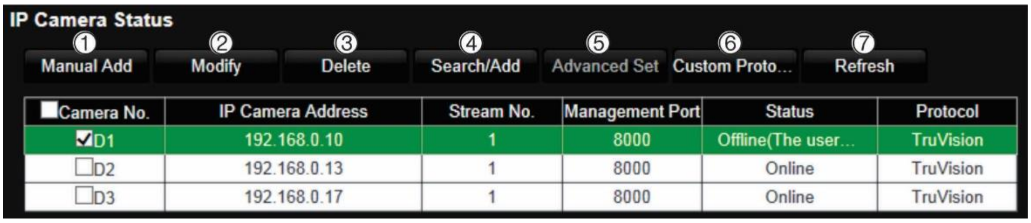
Please refer to the full IP camera compatibility chart for the latest validated IP camera models for TVN 71.

You can also add IP cameras that support RTSP streaming. See “RTSP Service Port” on page 137 for more information.

## IP camera status

The IP camera status menu allows you to add, edit, and remove cameras to the recorder as well as update the cameras’ firmware.

**Figure 16: IP camera window**



| ☐Camera No. | IP Camera Address | Stream No. | Management Port | Status | Protocol |
|---|---|---|---|---|---|
| ☑D1 | 192.168.0.10 | 1 | 8000 | Offline(The user... | TruVision |
| ☐D2 | 192.168.0.13 | 1 | 8000 | Online | TruVision |
| ☐D3 | 192.168.0.17 | 1 | 8000 | Online | TruVision |

| Option | | Description |
|---|---|---|
| 1. | Manual Add | Manually add an IP camera to the recorder without searching for it. Enter its parameters: IP Camera No., IP Camera Address, Protocol, Management Port, User Name, Password, and Transfer Protocol. |
| 2. | Modify | Change the parameters of a selected IP camera from the list. |
| 3. | Delete | Delete the selected IP camera from the list. |
| 4. | Search/Add | Search the network for available IP cameras and add an IP camera to the recorder. Select a camera, or cameras, from the list and click OK.<br>The camera parameters shown are: IP Camera Address, Channel Number, Protocol, Management Port, Subnet Mask, MAC Address, Serial No., and Firmware Version.<br>**Note**: When you add a camera automatically using the Search/Add feature, the system will check whether the camera password is 1234 or the same as the recorder. If the camera password is neither, the camera status is displayed as “Offline” (see Figure 16) and its password needs to be changed to be the same as the recorder. |
| 5. | Advanced Settings | Synchronize all supported TruVision and UltraView IP cameras passwords. |
| 6. | Custom Protocol | Configure custom RTSP streams. See “RTSP Service Port” on page 137 for more information. |
| 7. | **Refresh** | Update the information displayed on a camera in the recorder device list. |

### To search the network and add an IP camera:

1. From the menu toolbar, click **Configuration** > **IP Camera Status** > **Search/Add** to search for any supported IP cameras located in the recorder LAN.
2. In the list that appears, select the cameras that you want to add to the recorder.
3. Click **OK** to add the selected cameras to the list of devices in the recorder. The cameras are automatically added to the end of the list of devices.

   **Note**: If cameras still have default settings, they might have the same IP addresses. This creates an IP conflict. Use the **Modify** button to assign a different IP address to each camera.

### To manually add an IP camera:

1. From the menu toolbar, click **Camera Setup** > **IP Camera Status**.
2. Click **Manual Add**. In the pop-up window, enter the camera details such as the IP camera address/domain, protocol, management port, user name, and password. Click **OK**.

   The camera is added to the end of the list of devices.

**Note**: Only one camera can be manually added at a time.

# Import and export IP camera configuration settings

You can export and import the IP camera configuration settings from the recorder. This is useful if you want to copy the configuration settings to another recorder, if you want to edit a large list of camera settings in Excel, or if you want to make a backup of the camera settings.

Insert an external storage device in the recorder. Go to **Remote Configuration** > **IPC Import/Export** to import or export configuration settings. Click **Export** to export the recorder's configuration settings into an external storage device or click **Import** to import configuration settings after selecting a configuration file from the external storage device.

**Note**: If a setting is incorrect, the import function will not work for cameras that share the setting. An error message will appear on screen.

# RTSP custom protocols

Many IP cameras can stream video using RTSP. The recorder allows you to define RTSP custom protocols per camera type and to add cameras to the recorder via RTSP.

**To configure RTSP custom protocols:**

1. From the menu toolbar, click **Camera Setup** > **IP Camera Status**.
2. Click **Manual Add**. In the pop-up window, enter the camera details such as the IP camera address/domain, protocol, management port, user name, and password. Click **OK**.
3. Create a Custom Protocol by clicking **Protocol**. Select your parameters.
4. Click **Apply** to save the settings. Then click **OK** and **Add**.

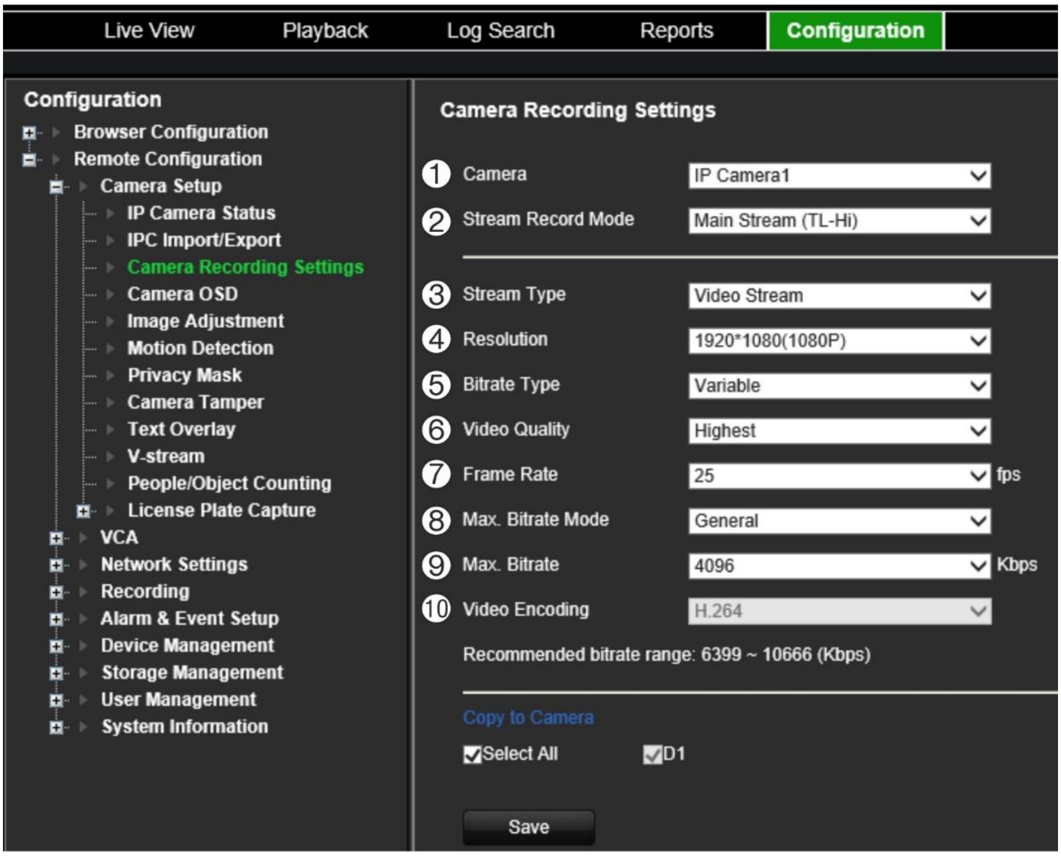
Note: When adding cameras via RTSP, only video streaming is available. No other functionality will be supported by the recorder.

**Note**: When a custom RTSP stream is used in the recorder, the user can create a camera name for it in the recorder. That camera name will be stored in the recorder and will be displayed in the OSD, webpage, and via the SDK it is possible to retrieve the name for use in a software. The camera name will not be pushed to the streaming device.

# Camera recording settings

You can set different resolution, frame rate, video quality, stream type, and maximum bit rate values for each camera. For each camera, you can also set different recording settings for each stream mode. For example, you can set different bit rate type, video quality and frame rate for event and alarm recordings for a selected camera.

### Figure 17: Camera recording settings



Camera Recording Settings

1 Camera: IP Camera1
2 Stream Record Mode: Main Stream (TL-Hi)
3 Stream Type: Video Stream
4 Resolution: 1920*1080(1080P)
5 Bitrate Type: Variable
6 Video Quality: Highest
7 Frame Rate: 25 fps
8 Max. Bitrate Mode: General
9 Max. Bitrate: 4096 Kbps
10 Video Encoding: H.264

Recommended bitrate range: 6399 ~ 10666 (Kbps)

☑Select All ☑D1

| Parameter | | Descriptions |
|---|---|---|
| 1. | Camera | Specifies the camera selected. |
| 2. | Stream Record Mode | Specifies the streaming method used.<br>Options include: Main Stream (TL-Hi), Main Stream (TL-Lo), Main Stream (Event), Main Stream (Alarm), Substream. |
| 3. | Stream Type | Specifies the stream type you wish to record.<br>Select Video Stream to record video stream only. Select Video&Audio to record both video and audio streams.<br>**Note**: Video&Audio is only available for those camera models that support audio. |
| 4. | Resolution | Specifies the recording resolution. A higher image resolution provides a higher image quality but also requires a higher bit rate. The resolution options listed depend on the type of camera and on whether main or sub stream is being used.<br>**Note**: Resolutions can vary depending on the camera model. |
| 5. | Bitrate Type | Specifies whether variable or fixed bit rate is used. Variable produces higher quality results suitable for video downloads and streaming. Default is Constant. |
| 6. | Video Quality | Specifies the quality level of the image. It can be set when variable bit rate is selected. Options include: Lowest, Lower, Medium, Higher, and Highest. |
| 7. | Frame Rate | Specifies the frame rate for the selected resolution.<br>The frame rate is the number of video frames that are shown or sent per second.<br>**Note**: The maximum frame rate depends on the camera model and selected resolution. Please check the camera specifications in its datasheet. |

| Parameter | | Descriptions |
|---|---|---|
| 8. | Max. Bitrate Mode | If “General” is selected, a list of predefined bit rates is displayed. If “Custom” is selected, any bit rate can be entered. |
| 9. | Max Bitrate | Specifies the maximum allowed bit rate. A high image resolution requires that a high bit rate must also be selected. |
| 10. | Video Encoding | Specifies the video encoding standard. Depending on the camera model, you can select H264 or H265. |

**To configure recording settings:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Camera Setup** > **Camera Recording Settings**.
2. Select the camera you want to configure.
3. Select one of the stream record modes: Mainstream (TL-Hi) (default), Mainstream (TL-Lo), Mainstream (Event), Mainstream (Alarm), or Substream.
4. Configure the following recording settings for the selected record stream mode and camera (options available depend on the camera model):
   - **Stream Type**: Select the type of stream to record, either video or video and audio.
   - **Resolution**: Select the resolution of the recording.
   - **Bitrate Type**: Select Variable (default) or Constant. If “Variable” is selected, the bandwidth can vary depending on video quality and the bandwidth required. If “Constant” is selected the video streaming is always at the maximum bit rate selected.
   - **Video Quality**: Select the quality at which to record. If “Constant” is selected as the bit rate type, this option is unavailable.

     If a low video quality is selected, the image quality is poorer, and the bandwidth required is reduced thereby allowing recording over a longer period.
   - **Frame Rate**: Select the recording frame rate.
   - **Max. Bitrate Mode**: Select the general (Default) or customized option.
   - **Max. Bitrate (kbps)**: If the customized maximum bit rate mode was selected, enter the value here. The recommended bit rate range to use is displayed.
   - **Video Encoding**: Select the desired video encoding standard.
5. Click **Save** to save the settings.
6. If you want to save these parameters to another camera, select the desired cameras under “Copy to Camera”.

   **Note**: When copying settings to cameras that do not support the settings, an error message will be displayed when trying to save. For example, it is not possible to set a Full HD resolution on a camera that does not support that resolution.
7. Click **Save** to save the settings.

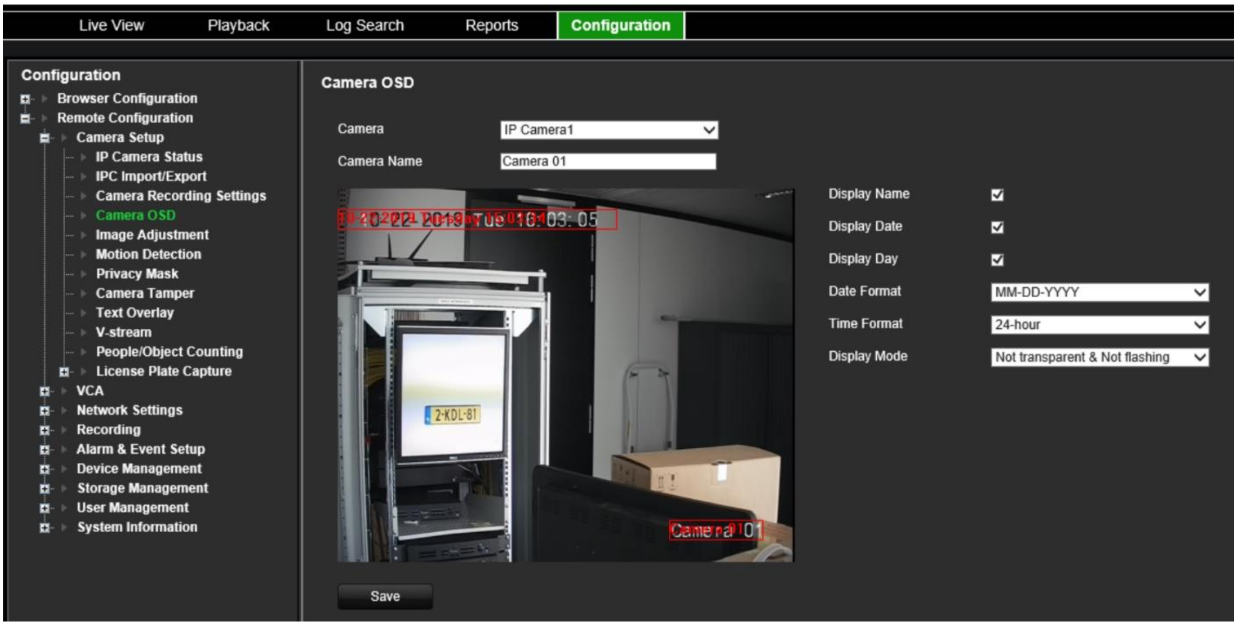
# Camera OSD

The recorder lets you configure which information is displayed on-screen for each individual camera.

The on-screen display (OSD) settings appear in live view mode and include the camera name, time and date. They are part of the image and are therefore also recorded.

**To configure the OSD settings:**

1. From the menu toolbar, click **Configuration** > **Camera Setup** > **Camera OSD**.



Camera OSD

Camera: IP Camera1

Camera Name: Camera 01

Display Name ☑

Display Date ☑

Display Day ☑

Date Format: MM-DD-YYYY

Time Format: 24-hour

Display Mode: Not transparent & Not flashing

2. Select the desired camera and enter a name for the camera, if required. The name can have up to 32 alphanumeric characters.
3. Select the **Display Name**, **Display Date**, and **Display Day** check boxes to display the camera name, date, and week.
4. Select date and time formats.
5. Select how you want the camera information displayed.

   Select one of the options from the drop-down list. Default is non-transparent & not flashing.

   - Transparent & Flashing
   - Transparent & Not flashing
   - Non-transparent & Flashing
   - Non-transparent & Not flashing
6. There are two red text boxes in the camera view window; one for the camera name and the other for the date/time. Using the mouse, click and drag a text box to the desired display position.
7. Click **Save** to save the settings.

# Image settings

The Image tab allows you to adjust image settings for each individual camera channel.

You may need to adjust the camera image depending on the location background to get the best image quality.

You can modify the digital noise reduction (DNR) value to improve image quality. This function removes image noise from a video signal, which can be more pronounced in low light conditions.

**To adjust display settings:**

1. From the menu toolbar, click **Camera Setup** > **Image Adjustment**.
2. Under **Camera**, select the desired camera.
3. Adjust the brightness, contrast, and saturation values by dragging each scroll bar.

   Click the **Default** button to return image setting values to the default position.
4. Select how you want the camera to rotate the image. There are two rotate functions:

| | |
|---|---|
| Enable Rotate | You can rotate the image 270°.<br>In a vertical-shaped scene, such as a hallway or corridor, the image is shown with a vertical (tall) rather than horizontal (wide) format. The video image is at a 9:16 aspect ratio.<br>Default is OFF. |
| Mirror Mode | You can flip the camera image three ways:<br>Left-Right: Flip the image horizontally.<br>Up-Down: Flip the image vertically.<br>Center: Flip both horizontally and vertically.<br>Default is OFF. |

   **Note**: This is only available for cameras that support the function.
5. Click **Save** to save the settings.

# Motion detection

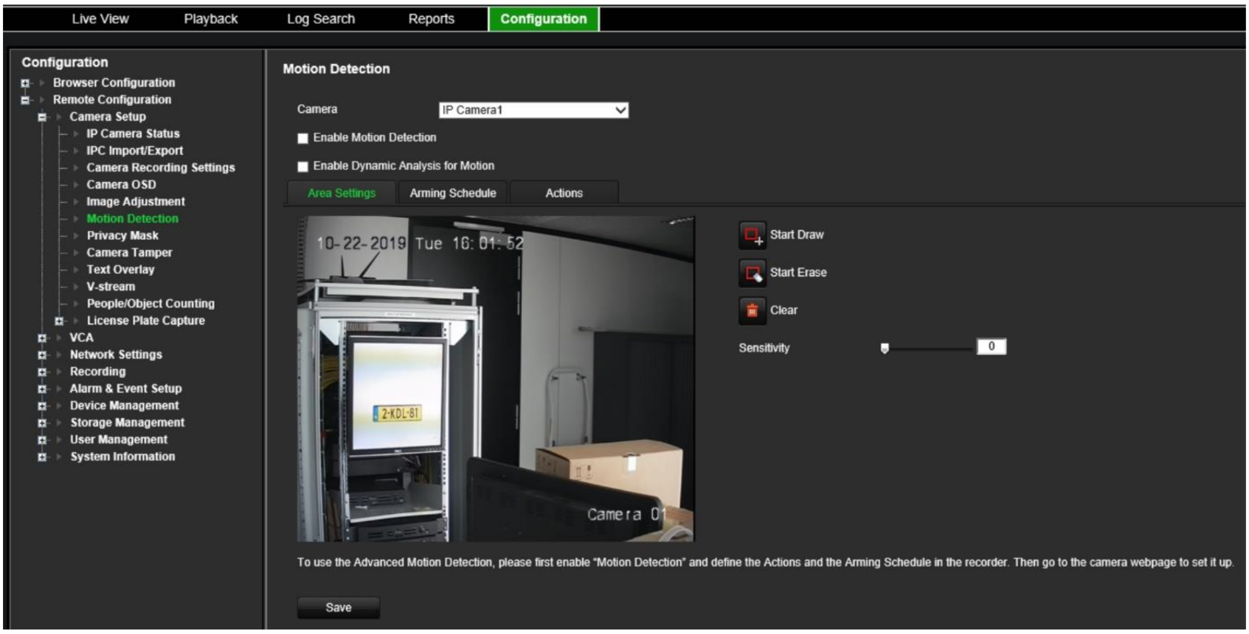
The motion detection menu allows you to enable or disable motion detection for each camera, as well as create motion grids, set the sensitivity of the motion detection, and link motion detection to a specific action. However, the motion alarm is only triggered if it occurs during a programmed time schedule.

**To set up motion detection:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Camera Setup** > **Motion Detection**.

2. Select the camera to detect motion. Each camera must be set up individually.
3. Select **Enable Motion Detection**. If this is not enabled, motion will not be recorded.
4. Select **Enable Dynamic Analysis for Motion**. Use this feature to display and store motion metadata. This metadata can also be used in TruVision Navigator and is also used for motion search.
5. Select the areas on-screen to be sensitive to motion.

   Click the **Area Settings** tab and then click the **Start Drawing** button. Drag the mouse cursor across the window to select an area sensitive to motion detection, which are shown as a red motion grid. Click the **Stop Drawing** button to stop selecting the area. Click **Clear** to clear the screen.



Camera: IP Camera1

□ Enable Motion Detection

□ Enable Dynamic Analysis for Motion

Sensitivity: 0

To use the Advanced Motion Detection, please first enable "Motion Detection" and define the Actions and the Arming Schedule in the recorder. Then go to the camera webpage to set it up.

   Set the sensitivity level. Drag the sensitivity scroll bar to the desired sensitivity level. Default is 50.

   **Note**: For information on advanced motion detection, see the section “Advanced motion detection” on page 61.

6. Select the arming schedules for motion detection.

   a) Click the **Arming Schedule** tab and then click the time bar of the desired day of the week. In the Time pop-up window, enter the start and end times during the day when motion can be recorded and click **Save** to save the change. You can schedule up to eight time periods in a day. Default is 24 hours.

   **Note**: Time periods defined cannot overlap.

   b) To copy the settings to other days of the week, place the mouse cursor at the end of the day time bar. A green icon appears. Click it to get the Copy to pop-up window. Select the desired days and click **Copy**.

7. Link the corresponding action to motion detection.

a) Click the **Actions** tab to open the Actions window. Select the linkage method by which you want the recorder to notify you of the event (see page 96 for the list of alarm notification types available). More than one option can be selected.

b) Under **Trigger Alarm Output**, select which external alarm outputs are triggered when an event occurs.

c) Under **Trigger Channel**, select which cameras will be recorded when an event occurs.

8. Click **Save** to save settings.

## Advanced motion detection

TruVision Series 6 IP cameras, and future TruVision cameras, have a function called “Advanced motion detection”, which allows you to fine tune the motion detection setup. Basic motion detection setup is available in the recorder, but advanced motion detection must be done from the camera.

**To set up advanced motion detection:**

1. Enable motion detection in the recorder and set up the actions and arming schedule.
2. Go to the camera’s webpage to set up advanced motion detection.

# Privacy mask

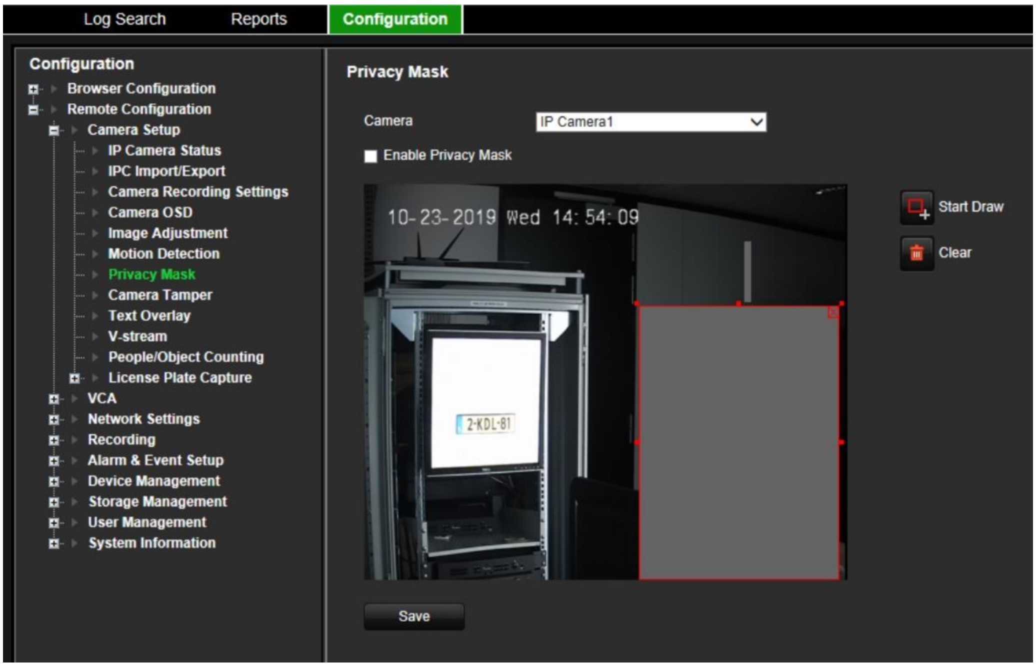
You can define an area on screen to remain hidden from view and recording. For example, you can choose to block the view of a camera when overlooking residential premises. This hidden area is referred to as privacy masking. Privacy masking cannot be viewed in live view or recorded mode and appears as a black area on the video image.

The number of privacy masks supported depends on the camera model.

**To setup a privacy mask:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Camera Setup** > **Privacy Mask**.
2. Select the camera for privacy masking.
3. Select **Enable Privacy Mask** to enable the feature.
4. Set up the mask area.

   Click the **Start Draw** button and, using the mouse, click and drag a privacy-mask box in the camera view window over the desired area. Click the **Stop Draw** button to stop drawing. If you want to draw another privacy mask, click **Start Draw** again.



To delete all masks, click **Clear All**. You cannot delete individual privacy masks.

5. Click **Save** to save the settings.

# Camera tamper

You can setup the recorder to alert you when the camera view has changed such as when someone has deliberately blocked the camera view by spraying paint on the lens or by moving the camera. You can select a specific area of the camera screen to detect tampering.

**Note:** It is strongly recommended not to configure for video tampering when using PTZ dome cameras.

**To set up video tampering detection:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Camera Setup** > **Camera Tamper**.
2. Select a camera to configure for video loss detection.
3. Select **Enable Camera Tamper** to enable the feature.
4. Select the area on-screen to be sensitive to tamper. By default, none of the screen is sensitive to tamper. Only one area can be drawn.

   Click the **Start Draw** button and drag the mouse cursor across the window to deselect areas sensitive to motion detection. Click the **Stop Draw** button to select areas. Click **Clear** to clear the screen.
5. Select the tamper detection sensitivity level by clicking the sensitivity scroll bar. Higher sensitivity is to the right of the bar.
6. Select the arming schedules for tamper.

Click the **Arming Schedule** tab and then click the **Edit** button. Select the day of the week and the time periods during the day when motion can be recorded. You can schedule up to eight time periods in a day. Default is 24 hours.

**Note:** Time periods defined cannot overlap.

7. Specify the linkage method when an event occurs.

   Click the **Actions** tab to open the Actions window. Select the method by which you want the recorder to notify you of the alarm (see page 96 for the list of alarm notification types available). “Notify Alarm Host” is the default selection. More than one option can be selected.

8. In the Actions window, specify which external alarm outputs are triggered when an event occurs.
9. Click **Save** to save settings.

# Text overlay

You can add up to four lines of text on screen via the browser. This option can be used, for example, to display emergency contact details. By default, these lines of text are positioned along the top of the screen. The strings follow each other consecutively.

**To add on-screen overlay text:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Camera Setup** > **Text Overlay**.
2. Select the desired camera.
3. Select the string check box **1** for the first line of text.
4. Enter the text for string 1 in the column alongside. Up to 44 alphanumeric characters can be used.
5. Repeat steps 3 and 4 for each extra line of text, selecting the next string number.
6. Click **Save** to save the settings.

# V-stream encoding

The V-stream shows all camera channels within one camera tile. V-stream is available for remote use with the browser interface, mobile application, TruVision Navigator or third-party software implementation.

This feature is particularly useful if you have limited bandwidth available on a remote location but still want to be able to view all camera tiles at once.

V-stream encoding can be set for up to 16 cameras.

**To enable V-streaming:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Camera Setup** > **V-stream Encoding**.
2. Select **Enable V-stream**.
3. Select the desired settings for frame rate (fps) and maximum bit rate (Kbps).
4. Select the screen mode. Select 1*1, 2*2, 1+5, 1+7, 3*3, or 4*4.
5. Select the screen order of the cameras.
6. Click **Save** to save the settings.

# Object counting

This function helps to calculate the number of objects entering or exiting a configured area and is primarily used with entrances or exits.

Set up the counting function from the camera itself. Please refer to the camera's configuration manual for further information.

**Note:** Only TruVision Series 4 cameras currently support counting. This function cannot distinguish between a moving person and a moving object.

**To set up counting statistics:**

**Note**: An SD card must be installed and configured in the camera to save count data and generate reports.

1. From the menu toolbar, click **Camera Setup** > **People/Object Counting**.
2. Select the camera from which you want to count objects.
3. Select the report type: Daily report, Weekly report, Monthly report, or Annual report.

   Daily report calculates the data on the selected date. Weekly report calculates for the week of the selected date. Monthly report calculates for the month of the selected date. Annual report calculates for the year of the selected date.
4. Under **Statistics Time**, select the desired day/month/year for the report.
5. Click **Counting** to list the people/object counting result.  The camera pushes the counting data to the recorder every 15 minutes. As a result, there might be differences between the counting data seen via the camera webpage and via the recorder.

# Video analytics

VCA (video content analysis) is the intelligent analysis of video to detect events of interest. When the function is enabled, the recorder can handle VCA alarms generated by Aritech cameras that support the VCA feature.

VCA is configured at the camera and not at the recorder. However, you can link actions to a VCA alarm from IP cameras that support this feature.

**Table 3: VCA types**

| | |
|---|---|
| Face Detected | When this function is enabled, the camera can detect a moving object that is moving towards it, triggering a configurable response. The camera can only detect a face looking directly into the camera, not side views. This feature is best suited when the camera is in front of a door or is in a narrow corridor. |
| Audio Input Exception | This function is used to detect when the camera detects sounds that are above a selected threshold. |
| Cross Line Detected | This function can be used to detect people, vehicles, and objects crossing a pre-defined line or an area on-screen. The line crossing direction can be set as unidirectional or bidirectional (A -> B, B -> A, or A<-> B). Unidirectional is crossing the line from left to right or from right to left. Bidirectional is crossing the line from both directions. |
| Intrusion Detected | You can set up an area in the surveillance scene to detect when intrusion occurs. If someone enters the area, a set of alarm actions can be triggered. This event type is different from the intrusion events that are reported to the recorder via the Aritech Alarm panel integration. |
| Defocus Detected | The camera can detect image blur caused by defocusing of the lens, triggering a series of alarm actions.<br>The sensitivity level determines how much blur is tolerated by the camera before triggering an alarm. When enabled, the camera regularly checks the level of image focus (to allow for variations in light during the day) and then compares the current image to that of the reference image to see if there is a difference. A high sensitivity level means that there cannot be a large variance between the reference and current image. |
| Sudden Scene Change | This function is used to detect when the camera detects a change in the scene caused by an intentional rotation of the camera. |
| Enter Region Detected | This function detects people, vehicles or other objects that enter a designated area from outside that area. |
| Exit Region Detected | This function detects people, vehicle or other objects that exit from a designated area, and certain actions can be configured to occur when the alarm is triggered. |
| Object Left Behind Detected | Unattended baggage detection function detects the objects left in the designated area such as baggage, a purse, dangerous materials, etc. |
| Object Removed Detected | Object removal detection function detects objects removed from a designated area, such as exhibits on display. |

### To setup VCA alarm actions:

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **VCA** and select the desired VCA type from the configuration panel.
2. Select the camera for which to set up the VCA alarm.

   **Note**: A pop-up message will appear when the camera does not support this VCA type.
3. Enable the VCA type.

   If *Face Detected* has been selected, also enable **Enable Dynamic Analysis for Face Detection**.

4. If you have selected *Face Detected or Defocus Detected*, set the sensitivity level.
5. If you have selected *Audio Input Exception*, enable **Audio Loss Detection**, **Sudden Increase of Sound Intensity Detection** and/or **Sudden Decrease of Sound Intensity Detection**.

   For **Sudden Increase of Sound Intensity Detection** set the levels for sensitivity and sound intensity threshold.

   For **Sudden Decrease of Sound Intensity Detection** set the sensitivity level.
6. If you have selected *Cross Line Detected, Intrusion Detected, Enter Region Detected, Exit Region Detected, Object Left Behind Detected, or Object Removed Detected*, click the **Area Settings** tab. Draw the areas on the image that will be sensitive to motion, and set the sensitivity and threshold values.
7. Click the **Arming Schedule** tab to set the schedule for the detection.

   Place the mouse cursor on the schedule start time for the desired day of the week and drag it to the end time to mark the schedule for that day. Repeat the process for the other days of the week.

   To copy a day's schedule to other days, place the mouse cursor on the day of the week to copy. A green icon appears at the end of the line. Click it and in the pop-up menu that appears, select the days of the week to which to copy this schedule and click **OK**.

   Repeat this step for each camera.
8. Click the **Actions** tab to define which actions are required with the VCA events from each camera.

   **Set the alarm linking method:**

   Select the method by which you want the recorder to notify you of the alarm: Enable Alarm Audio, Notify Alarm Host, and Send Email. See page 96 for the list of alarm notification types.

   **Set the alarm outputs to be triggered:**

   Set the external alarm outputs to be triggered when an event occurs. Select "Select All" or each individual alarm output.

   **Set the cameras to be recorded:**

   Set the channels to be recorded when an event occurs. Check "Select All" or select each individual channel.

   **Set the PTZ linking to be triggered:**

   Select the PTZ camera for linking and select the preset, preset tour, and/or a shadow tour to be triggered when the alarm is detected. Enable the preset, preset tour, and/or a shadow tour.
9. Click **Save** to save the settings.

# License plate identification

License plate recognition lets you identify, track and analyze vehicle license plates as they enter or leave your site. The recorder can be set up to automatically capture license plates for storage and later analysis. You can also create reports of the plates identified.

**Note**: The TruVision ANPR IP camera is only supported in certain regions. Refer to the camera datasheet for the list of countries in which is it supported.

## License plate capture

Use this function to set up the area on screen to be detected and to capture a vehicle's number plate information.

**Note**: This license plate functionality only applies to the EMEA region.

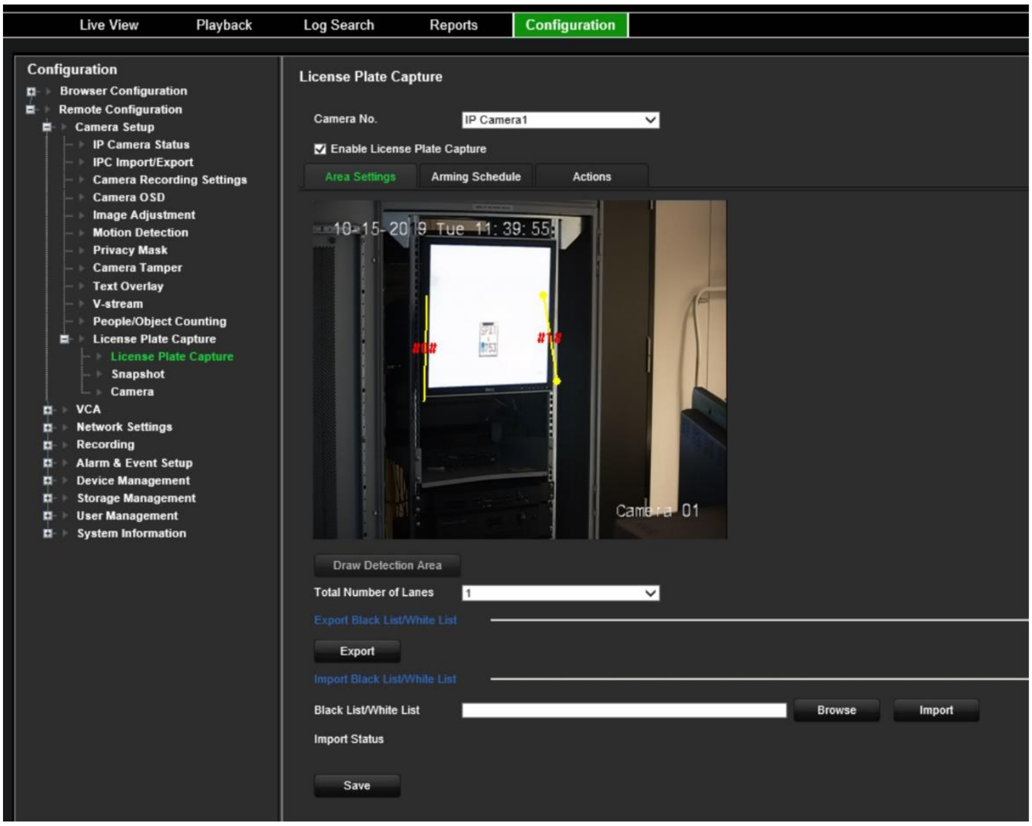
**To set up license plate capture:**

1. From the menu toolbar, click **Remote Configuration** > **Camera Setup > License Plate Capture > License Plate Capture**.
2. Import the desired list of license plates to the NVR. This is the list that will be used for all ANPR cameras.

   Under Import Black List/White List, click **Browse** to locate the file to upload and click **Import**.
3. Select the desired ANPR camera from the drop-down list.
4. Select the **Enable** check box to enable the license plate capture.
5. Set up the detection area.

   Under **Total Number of Lanes**, select the desired number of lanes from the drop-down list. Up to four lanes can be set up. For the best performance, we recommend using one camera for each lane.

   Click the **Area Settings** tab and then click the **Draw Detection Area** button to set up the lanes. Select the desired detection area on the image. Using the mouse, click and drag the yellow lane line to set the area.



License Plate Capture

Camera No. IP Camera1

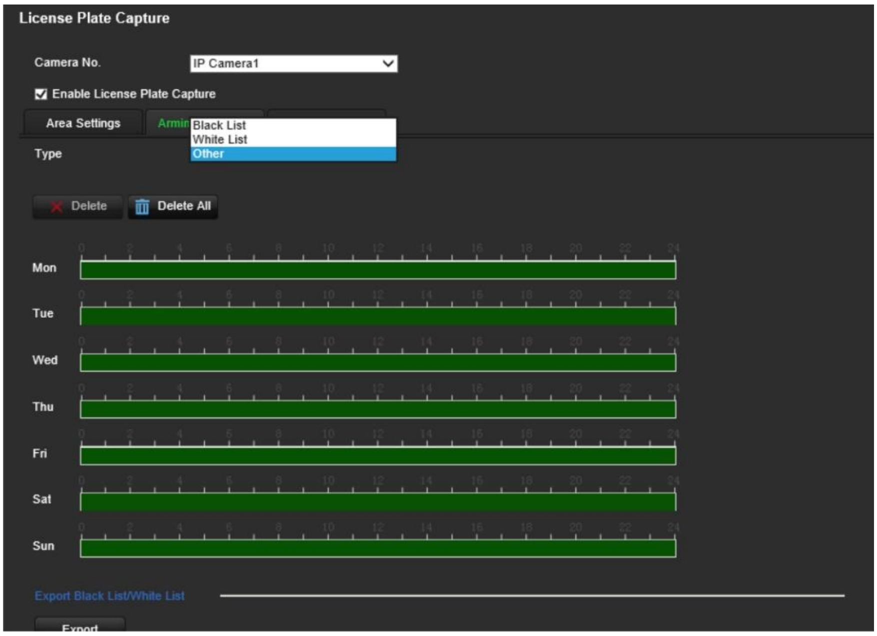
☑ Enable License Plate Capture

Total Number of Lanes 1

Black List/White List

Import Status

6. Select the **Arming Schedule** tab to set up the arming schedule and linking action for the white list, black list, and other list.



License Plate Capture

Camera No. IP Camera1

☑ Enable License Plate Capture

Type Other

Under **Type**, select the license plates group: **White List**, **Black List**, or **Other**.

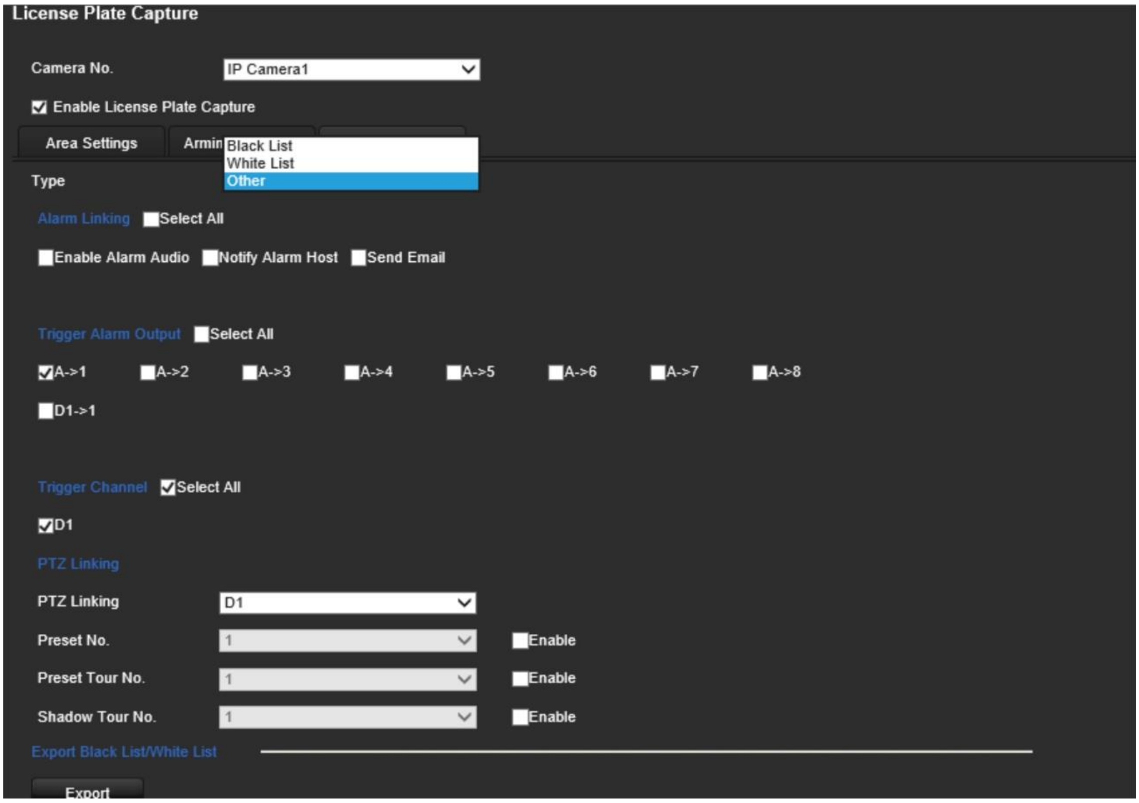
Click the timeline of the desired day of the week. The *Edit schedule* window pops up.  Enter the start and end times of the arming schedule. Click **Save**. Repeat for each type.

You can define up to eight different periods during a day, and a different schedule for each day of the week. Click **Delete** or **Delete All** to delete time periods.

**Note**: The time periods defined for a day cannot overlap.

7. Set up the linkage method when an event occurs.

   Click the **Actions** tab and then under **Type**, select the license plate group: **White List**, **Black List**, or **Other**.



License Plate Capture

Camera No. IP Camera1

☑ Enable License Plate Capture

Type: Black List / White List / Other (selected)

Alarm Linking □ Select All

□ Enable Alarm Audio □ Notify Alarm Host □ Send Email

Trigger Alarm Output □ Select All

☑ A->1 □ A->2 □ A->3 □ A->4 □ A->5 □ A->6 □ A->7 □ A->8

□ D1->1

Trigger Channel ☑ Select All

☑ D1

PTZ Linking

PTZ Linking D1

Preset No. 1 □ Enable

Preset Tour No. 1 □ Enable

Shadow Tour No. 1 □ Enable

Export Black List/White List

Select one or more response methods listed below for the system when number plate is detected.

| | |
|---|---|
| **Alarm Linking** | Set the alarm linking method. Select the method by which you want the recorder to notify you of the alarm: Enable Alarm Audio, Notify Alarm Host, and Send Email. See page 96 for the list of alarm notification types |
| **Trigger Alarm Output** | Set the alarm outputs to be triggered. Set the external alarm outputs to be triggered when an event occurs. Select “Select All” or each individual alarm output. |
| Trigger Channel | **Set the channels to be recorded when an event occurs. Check “Select All”.** |
| **PTZ Linking** | Set the PTZ linking to be triggered. Select the PTZ camera for linking and select the preset, preset tour, and/or a shadow tour to be triggered when the alarm is detected. Enable the preset, preset tour, and/or a shadow tour. |

8. Click **Save** to save changes.

## Black and white list

You can store a list of black and white entries on the recorder to match against when automatically analyzing the captured numbered plates. By default, a list of maximum 2,048 license plates can be loaded in the recorder. See Table 1 below for the description of the list types.

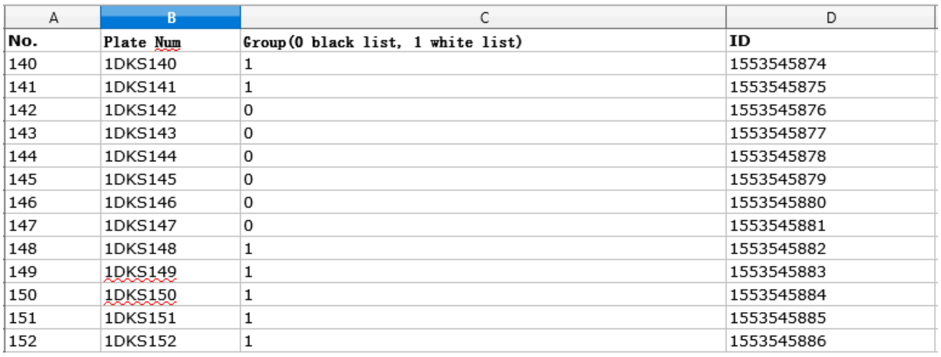
**Table 4: Description of Black list, White list, and Other**

| | |
|---|---|
| **Black listed** | These are license plates marked in the list as restricted vehicles. |
| **White listed** | These are license plates marked in the list as authorized vehicles. |
| **Other** | Captured license plates that are not part of the list are automatically marked as “Other”. |

If you do not already have a list of your black/white license plates, you can export the template to create one. It can then be imported back to the camera. It is one single list in which you mark your license plate as white or black listed. Captured license plates that are not part of the list will automatically be marked as “Other”.

The template format is shown below. When inputting the license plate number and ID, there should be no spaces between the letters and numbers. For example, if the actual license number plate is “1-DKS-140”, in the list it should be written as “1DKS140”. See Figure 13 below. When entering 0 in column C, the license plate will be marked as black listed. Entering 1 in column C marks the license plate as white listed.

**Figure 18: Example of a Black/White list**



| A | B | C | D |
|---|---|---|---|
| No. | Plate Num | Group(0 black list, 1 white list) | ID |
| 140 | 1DKS140 | 1 | 1553545874 |
| 141 | 1DKS141 | 1 | 1553545875 |
| 142 | 1DKS142 | 0 | 1553545876 |
| 143 | 1DKS143 | 0 | 1553545877 |
| 144 | 1DKS144 | 0 | 1553545878 |
| 145 | 1DKS145 | 0 | 1553545879 |
| 146 | 1DKS146 | 0 | 1553545880 |
| 147 | 1DKS147 | 0 | 1553545881 |
| 148 | 1DKS148 | 1 | 1553545882 |
| 149 | 1DKS149 | 1 | 1553545883 |
| 150 | 1DKS150 | 1 | 1553545884 |
| 151 | 1DKS151 | 1 | 1553545885 |
| 152 | 1DKS152 | 1 | 1553545886 |

### To import a black and white lists from a PC to the recorder:

1. From the menu toolbar, click **Remote Configuration** > **Camera Setup > License Plate Capture > License Plate Capture**. Under **Import Black List/White List**, click **Browse** to select a file from your library or online and click **Import** to import it to the recorder.

   Select the file name of the Black/White list file to upload to the camera; either use the existing name (Default) or give it new name (Custom).

2. Click **Save** to save changes.

### To export a black and white lists from the recorder to PC:

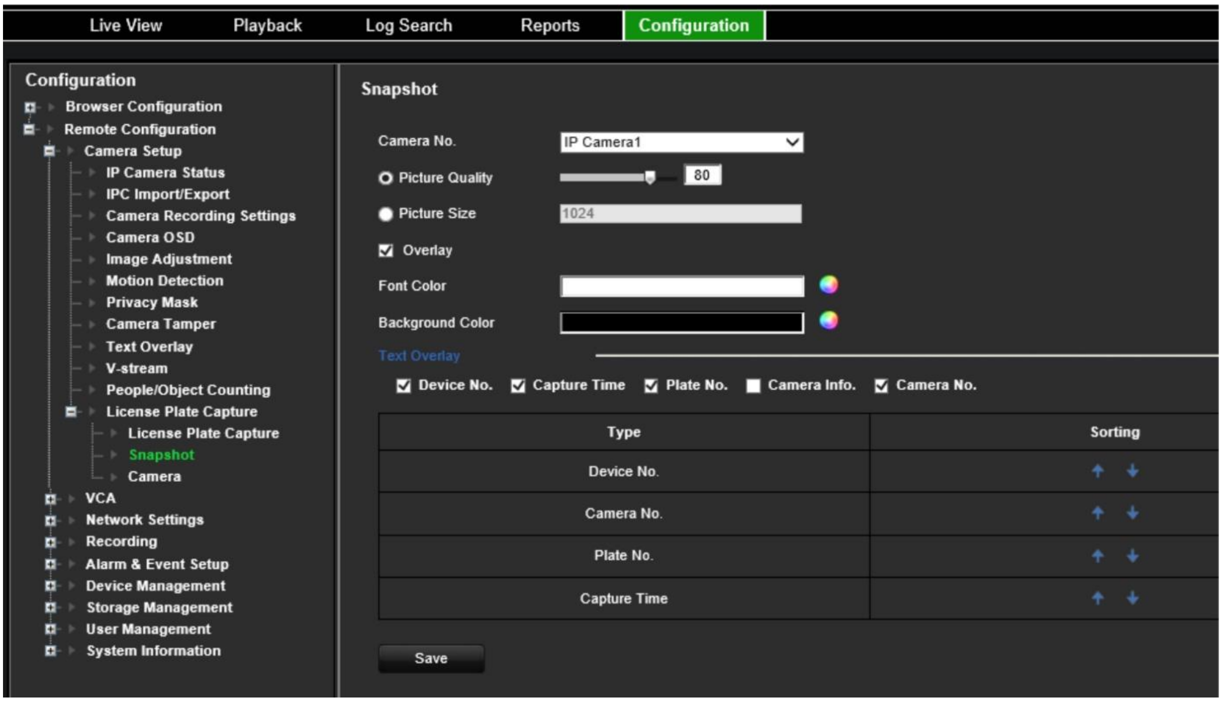
1. From the menu toolbar, click **Remote Configuration** > **Camera Setup > License Plate Capture > License Plate Capture**. Under **Export Black List/White List**, click **Export** and enter where you want to export the file.

## Text overlay on snapshots

You can have text appear on a snapshot of a license plate to provide context, such as the camera number, license plate number and time of capture.

**To set up the snapshot text overlay:**

1. From the menu toolbar, click **Remote Configuration** > **Camera Setup > License Plate Capture > Snapshot**.



Snapshot

Camera No. IP Camera1

○ Picture Quality 80

● Picture Size 1024

☑ Overlay

Font Color

Background Color

Text Overlay

☑ Device No. ☑ Capture Time ☑ Plate No. □ Camera Info. ☑ Camera No.

| Type | Sorting |
|---|---|
| Device No. | ↑ ↓ |
| Camera No. | ↑ ↓ |
| Plate No. | ↑ ↓ |
| Capture Time | ↑ ↓ |

2. Select the camera from the drop-down list from which you want to place text overlay on the snapshots.
3. Select the picture quality and picture size. You can also select the font and background color.
4. Select the text to overlay on the snapshot. The five options are: device number, camera number, plate number, camera information, and capture time. You can change the order in which the selected overlay text of the selected items appears on the snapshot from the *Sorting* column.
5. Click **Save** to save changes.

## Camera information

You can identify the TruVision ANPR IP camera so that its information appears in any report as well as on snapshots.

**To set up the camera information displayed on the snapshot:**

1. From the menu toolbar, click **Remote Configuration** > **Camera Setup > License Plate Capture > Camera**.
2. Enter the camera details.
3. Click **Save** to save changes.

# Create reports

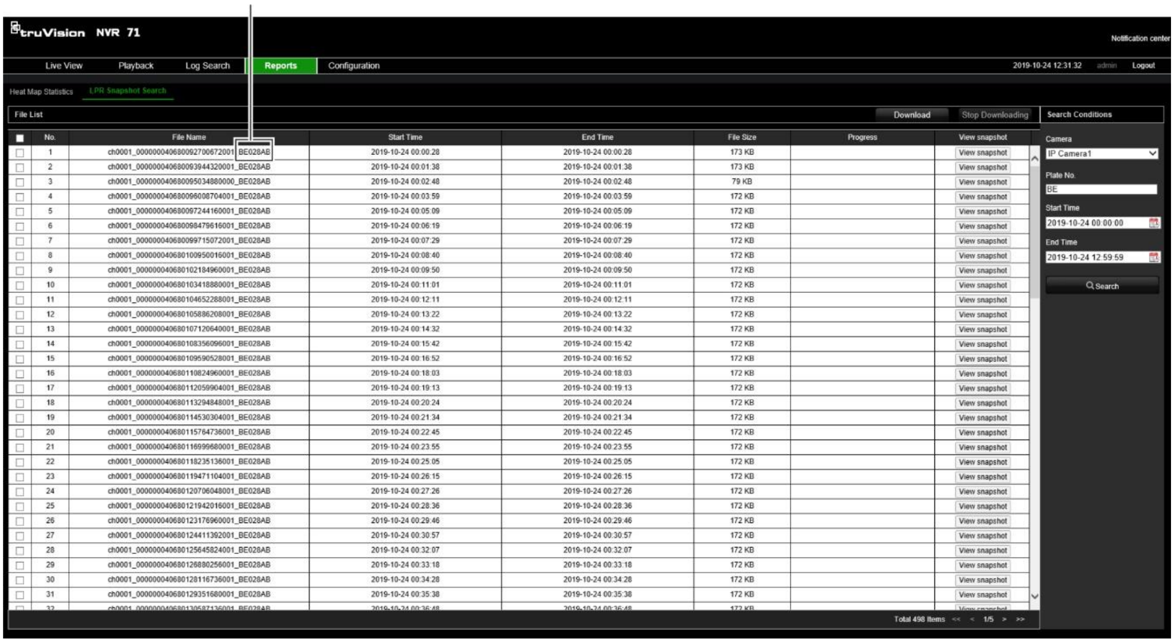
You can create and download reports on the license plates captured using TruVision ANPR IP cameras as well as the heat map statistics generated by TruVision 360° cameras.

**Notes**:

- Ensure that the TruVision 360° camera has a SD card installed before creating reports.
- The license plate functionality only applies to the EMEA region.

**To create a report on captured license plates:**

1. Click **Reports** in the menu toolbar. The reports interface appears on screen.
2. Select the **LPR Snapshot Search** tab.
3. Select the desired camera as well as start and end times for the search. You can leave the **Plate No.** field empty to list all the license plates captured found or enter the letters/numbers to search for specific license plates starting with those characters. See the figure below for an example of the results of a search for license plates starting with the letters “BE”.



License plate number

Camera: IP Camera1

Plate No.: BE

Start Time: 2019-10-24 00:00:00

End Time: 2019-10-24 12:59:59

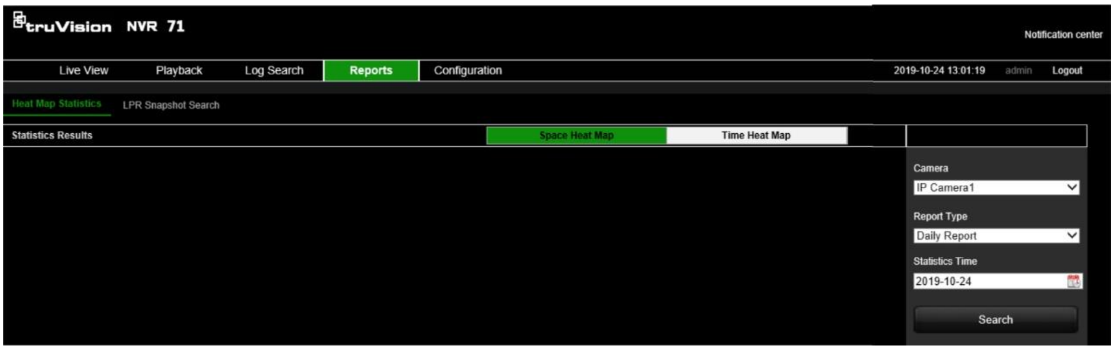
| ■ | No. | File Name | Start Time | End Time | File Size | Progress | View snapshot |
|---|---|---|---|---|---|---|---|
| ☐ | 1 | ch0001_00000004068009270067200 1_BE028AB | 2019-10-24 00:00:28 | 2019-10-24 00:00:28 | 173 KB | | View snapshot |
| ☐ | 2 | ch0001_00000004068009394432000 1_BE028AB | 2019-10-24 00:01:38 | 2019-10-24 00:01:38 | 173 KB | | View snapshot |
| ☐ | 3 | ch0001_00000004068009503488000 0_BE028AB | 2019-10-24 00:02:48 | 2019-10-24 00:02:48 | 79 KB | | View snapshot |
| ☐ | 4 | ch0001_00000004068009600870400 1_BE028AB | 2019-10-24 00:03:59 | 2019-10-24 00:03:59 | 172 KB | | View snapshot |
| ☐ | 5 | ch0001_00000004068009724416000 1_BE028AB | 2019-10-24 00:05:09 | 2019-10-24 00:05:09 | 172 KB | | View snapshot |
| ☐ | 6 | ch0001_00000004068009847961600 1_BE028AB | 2019-10-24 00:06:19 | 2019-10-24 00:06:19 | 172 KB | | View snapshot |
| ☐ | 7 | ch0001_00000004068009971507200 1_BE028AB | 2019-10-24 00:07:29 | 2019-10-24 00:07:29 | 172 KB | | View snapshot |
| ☐ | 8 | ch0001_00000004068010095001600 1_BE028AB | 2019-10-24 00:08:40 | 2019-10-24 00:08:40 | 172 KB | | View snapshot |
| ☐ | 9 | ch0001_00000004068010218496000 1_BE028AB | 2019-10-24 00:09:50 | 2019-10-24 00:09:50 | 172 KB | | View snapshot |
| ☐ | 10 | ch0001_00000004068010341888000 1_BE028AB | 2019-10-24 00:11:01 | 2019-10-24 00:11:01 | 172 KB | | View snapshot |
| ☐ | 11 | ch0001_00000004068010465228800 1_BE028AB | 2019-10-24 00:12:11 | 2019-10-24 00:12:11 | 172 KB | | View snapshot |
| ☐ | 12 | ch0001_00000004068010588620800 1_BE028AB | 2019-10-24 00:13:22 | 2019-10-24 00:13:22 | 172 KB | | View snapshot |
| ☐ | 13 | ch0001_00000004068010712064000 1_BE028AB | 2019-10-24 00:14:32 | 2019-10-24 00:14:32 | 172 KB | | View snapshot |
| ☐ | 14 | ch0001_00000004068010835609600 1_BE028AB | 2019-10-24 00:15:42 | 2019-10-24 00:15:42 | 172 KB | | View snapshot |
| ☐ | 15 | ch0001_00000004068010959052800 1_BE028AB | 2019-10-24 00:16:52 | 2019-10-24 00:16:52 | 172 KB | | View snapshot |
| ☐ | 16 | ch0001_00000004068011082496000 1_BE028AB | 2019-10-24 00:18:03 | 2019-10-24 00:18:03 | 172 KB | | View snapshot |
| ☐ | 17 | ch0001_00000004068011205990400 1_BE028AB | 2019-10-24 00:19:13 | 2019-10-24 00:19:13 | 172 KB | | View snapshot |
| ☐ | 18 | ch0001_00000004068011329484800 1_BE028AB | 2019-10-24 00:20:24 | 2019-10-24 00:20:24 | 172 KB | | View snapshot |
| ☐ | 19 | ch0001_00000004068011453030400 1_BE028AB | 2019-10-24 00:21:34 | 2019-10-24 00:21:34 | 172 KB | | View snapshot |
| ☐ | 20 | ch0001_00000004068011576473600 1_BE028AB | 2019-10-24 00:22:45 | 2019-10-24 00:22:45 | 172 KB | | View snapshot |
| ☐ | 21 | ch0001_00000004068011699968000 1_BE028AB | 2019-10-24 00:23:55 | 2019-10-24 00:23:55 | 172 KB | | View snapshot |
| ☐ | 22 | ch0001_00000004068011823513600 1_BE028AB | 2019-10-24 00:25:05 | 2019-10-24 00:25:05 | 172 KB | | View snapshot |
| ☐ | 23 | ch0001_00000004068011947110400 1_BE028AB | 2019-10-24 00:26:15 | 2019-10-24 00:26:15 | 172 KB | | View snapshot |
| ☐ | 24 | ch0001_00000004068012070604800 1_BE028AB | 2019-10-24 00:27:26 | 2019-10-24 00:27:26 | 172 KB | | View snapshot |
| ☐ | 25 | ch0001_00000004068012194201600 1_BE028AB | 2019-10-24 00:28:36 | 2019-10-24 00:28:36 | 172 KB | | View snapshot |
| ☐ | 26 | ch0001_00000004068012317696000 1_BE028AB | 2019-10-24 00:29:46 | 2019-10-24 00:29:46 | 172 KB | | View snapshot |
| ☐ | 27 | ch0001_00000004068012441139200 1_BE028AB | 2019-10-24 00:30:57 | 2019-10-24 00:30:57 | 172 KB | | View snapshot |
| ☐ | 28 | ch0001_00000004068012564582400 1_BE028AB | 2019-10-24 00:32:07 | 2019-10-24 00:32:07 | 172 KB | | View snapshot |
| ☐ | 29 | ch0001_00000004068012688025600 1_BE028AB | 2019-10-24 00:33:18 | 2019-10-24 00:33:18 | 172 KB | | View snapshot |
| ☐ | 30 | ch0001_00000004068012811673600 1_BE028AB | 2019-10-24 00:34:28 | 2019-10-24 00:34:28 | 172 KB | | View snapshot |
| ☐ | 31 | ch0001_00000004068012935168000 1_BE028AB | 2019-10-24 00:35:38 | 2019-10-24 00:35:38 | 172 KB | | View snapshot |
| ☐ | 32 | ch0001_00000004068013058713600 1_BE028AB | 2019-10-24 00:36:48 | 2019-10-24 00:36:48 | 172 KB | | View snapshot |

Total 498 Items << < 1/5 > >>

4. If you want to see the snapshot of a captured license plate, click **View snapshot** of the desired license plate, which opens. Click **OK** to close the image.
5. Select the entries to download and then click **Download**. The file is downloaded to the directory specified in the browser setup (see “Browser configuration” on page 49). You can stop the download, if desired by clicking **Stop Downloading**.

**To create a report on heat map statistics:**

1. Click **Reports** in the menu toolbar. The reports interface appears on screen.



Camera: IP Camera1

Report Type: Daily Report

Statistics Time: 2019-10-24

2. Select the **Heat Map Statistics** tab.
3. Select the tab **Space Heat Map** or **Time heat Map**.

   A space heat map displays in a color spectrum the frequency of visits by people in the area. A time heat map shows a flow chart of the number of people visiting the area.
4. Select the camera and report type.
5. Click **Search**. The results appear on screen.

   In the time heat map screen, click **Export** to export the result. However, the space heat map cannot be exported.

# Chapter 11
# Network settings

The Network settings menu allows you to manage all network related aspects of the recorder including general network settings, DDNS, NTP synchronization, email setup, FTP server, and HTTPS setup.

Additionally, the Network statistics menu provides you with a useful and efficient tool to analyze the behavior of the recorder on the network.

You must correctly configure your recorder’s network settings before using it over the networking order to:

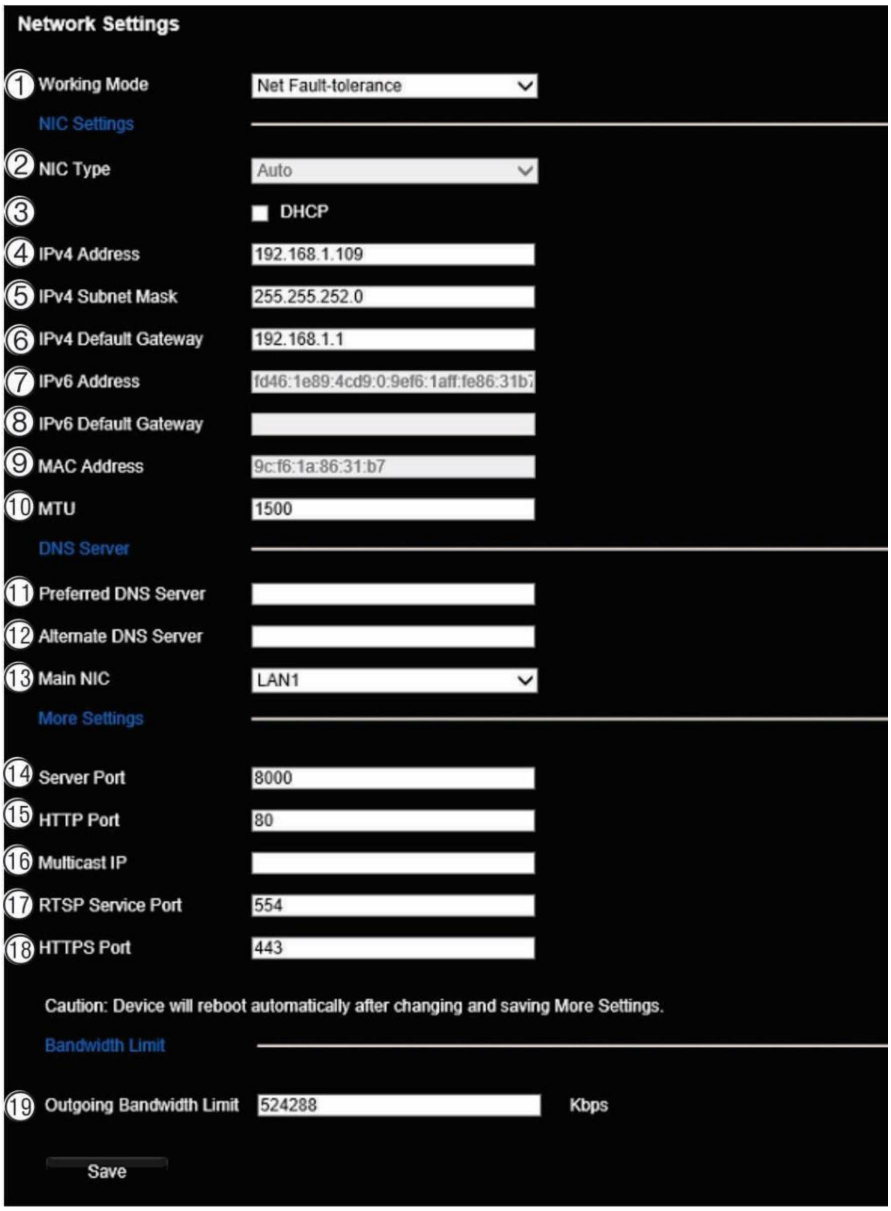
- Connect IP cameras to it
- Connect to the recorder over the LAN
- Connect to the recorder over the internet

## Network settings

**Note**: As every network configuration may differ, please contact your Network Administrator or ISP to see if your recorder requires specific IP addresses or port numbers.

**To configure general network settings:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Network Settings** > **Network Settings**.



Network Settings

| | | |
|---|---|---|
| 1 | Working Mode | Net Fault-tolerance |
| | NIC Settings | |
| 2 | NIC Type | Auto |
| 3 | | □ DHCP |
| 4 | IPv4 Address | 192.168.1.109 |
| 5 | IPv4 Subnet Mask | 255.255.252.0 |
| 6 | IPv4 Default Gateway | 192.168.1.1 |
| 7 | IPv6 Address | fd46:1e89:4cd9:0:9ef6:1aff:fe86:31b |
| 8 | IPv6 Default Gateway | |
| 9 | MAC Address | 9c:f6:1a:86:31:b7 |
| 10 | MTU | 1500 |
| | DNS Server | |
| 11 | Preferred DNS Server | |
| 12 | Alternate DNS Server | |
| 13 | Main NIC | LAN1 |
| | More Settings | |
| 14 | Server Port | 8000 |
| 15 | HTTP Port | 80 |
| 16 | Multicast IP | |
| 17 | RTSP Service Port | 554 |
| 18 | HTTPS Port | 443 |

Caution: Device will reboot automatically after changing and saving More Settings.

Bandwidth Limit

| | | |
|---|---|---|
| 19 | Outgoing Bandwidth Limit | 524288 Kbps |

2. Enter the required settings:

| Parameter | Description |
|---|---|
| 1. Working Mode | The recorder has eight 10M/100M/1000M NIC cards that support net fault tolerance, load balance, and multi-address modes.<br>The default mode is Net fault-tolerance.<br>There are four RJ45 NIC cards and four NIC cards with a fiber connector (SFP).<br>Select one of the options:<br>**Net Fault-tolerance**: When one LAN port fails, the other one takes over. This is the default option.<br>**Load Balance**: The bandwidth is divided over the LAN ports with one IP address.<br>**Multi-address**: Each LAN port is separate with its own IP address. This allows a LAN port for the IP cameras and another for client PCs, such as TruNav. |

| Parameter | | Description |
|---|---|---|
| 2. | NIC Type | Network interface card (NIC) is a device used to connect the recorder to a network. Select the NIC type used from the drop-down list.<br>Default value is 10/100/1000M self-adaptive. |
| 3. | DHCP | Select **Enable DHCP**. It is disabled by default.<br>Dynamic Host Configuration Protocol (DHCP) is a network application protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network. |
| 4. | IPv4 Address | Enter the IP address for the recorder. This is the LAN IP address of the recorder.<br>Default value is 192.168.1.82. |
| 5. | IPv4 Subnet Mask | Enter the subnet mask for your network so the recorder will be recognized within the network.<br>Default value is 255.255.255.0. |
| 6. | IPv4 Default Gateway | Enter the IP address of your network gateway so the recorder will be recognized within the network. This is typically the IP address of your router. Consult your router user manual or contact your ISP to get the required information on your gateway.<br>Default value is 192.168.1.1. |
| 7. | IPv6 Address | Enter the IPv6 address for the recorder. This is the IP address of the local network to which the recorder is connected.<br>Default value is fe80::240:3dff:fe7e:926f/64 |
| 8. | IPv6 Default Gateway | Enter the IPv6 address of your network gateway so the recorder will be recognized within the network. This is typically the IP address of your router. |
| 9. | MAC Address | Displays the MAC address. The MAC address is a unique identifier of your recorder. It cannot be changed. |
| 10. | MTU (bytes) | Enter a value between 500 and 9676. Default is 1500. |
| 11. | Preferred DNS Server | Enter the preferred domain name server to use with the recorder. It must match the DNS server information of your router. Check your router’s browser interface or contact your ISP for the information. |
| 12. | Alternate DNS Server | Enter the alternate domain name server to use with the recorder. It must match the DNS server information of your router. Check your router’s browser interface or contact your ISP for the information. |
| 13. | Main NIC | Select the main LAN port when net fault tolerance or load balance mode is selected. LAN 1 is default.<br>Select which LAN is the main route when multi-address mode is selected. |
| 14. | Server Port | Use the server port for remote client software access. The port range is between 1024 and 65535.<br>Enter the server port value. The default value is 8000. |
| 15. | HTTP Port | Use the HTTP port for remote internet browser access.<br>Enter the HTTP port value, which can be any port number that is not occupied. The default value is 80. |
| 16. | Multicast IP | Enter a D-class IP address between 224.0.0.0 to 239.255.255.255. Only specify this option if you are using the multicast function. Some routers prohibit the use of multicast function in case of a network storm. |

| Parameter | | Description |
|---|---|---|
| 17. | RTSP Service Port | The RTSP (Real Time Streaming Protocol) is a network control protocol designed for use in entertainment and communications systems to control streaming media servers.<br>Enter the RTSP port value, which can be between1 to 65535. The default value is 554. |
| 18. | HTTPS Port | HTTPS (Hyper Text Transfer Protocol Secure) allows a secure access to the browser. Enter the HTTPS port value. The default port number is 443. |
| 19. | Outgoing Bandwidth Limit (Kbps) | The outgoing bandwidth limit is a threshold you can set to limit the amount of outgoing bandwidth that is being handled by the recorder. You can also increase the outgoing bandwidth, though this will negatively impact the incoming bandwidth of the recorder. |

20. Click **Save** to save the settings.

# PPPoE settings

Although not usually used, you can connect the recorder directly to a DSL modem. To do this, you need to select the PPPoE option in the network settings. Contact your ISP to get the user name and password.

**To configure PPPoE settings:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Network Settings** > **PPPOE**.
2. Select **Enable PPPoE**. It is disabled by default.
3. Enter your user name and password and confirm the password.
4. Click **Save** and manually reboot the recorder to save the settings.

# DDNS settings

DDNS servers allow you to connect to your recorder using a fixed address. This fixed address needs to be registered with a DNS service. The DDNS setup menu allows you to enable or disable DDNS and to configure it using ezDDNS, No-IP or DynDNS.

**Note**: Some service providers block the default RTSP streaming port 554 used for video streaming, so if you are not receiving video images over the internet, you may need to change it to another value.  See Appendix B “Port forwarding information” on page 135 for more information.

There are three DDNS providers to choose from:

- **ezDDNS:** A free-of-charge service included with your recorder and fully managed within the recorder interface

- **DynDNS:** A third-party service where users need to apply for a DynDNS account on the Dyn.com website
- **No-IP:** A third-party service where users need to apply for a no-IP account on the no-ip.com website

**Note**: You cannot have two recorders with the same host name.

**To set up DDNS:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Network Settings** > **DDNS**.
2. Select **Enable DDNS**. It is disabled by default.
3. Select one of the DDNS types listed:

   **ezDDNS**: Click the **Get URL** button. The URL address to access the unit is displayed. If no host name is specified, the DDNS will allocate one automatically.

   The maximum length for the host name field is 64 characters. This limit does not include tvn-ddns.net. An example of a host name could be *max64chars.tvr-ddns.net*.

   - Or -

   **DynDNS**: Select **DynDNS** and enter the server address for DynDNS. In the recorder domain name field, enter the domain name obtained from the DynDNS web site. Then enter your user name and password registered in the DynDNS network.

   For example:

      Server address: members.dyndns.org

      Domain: mycompanydvr.dyndns.org

      User name: myname

      Password: mypassword

   - Or -

   **NO-IP:** Enter server address (for example, dynupdate.no-ip.com). In the host name field, enter the host obtained from the NO-IP web site. Then enter the user name and password that are registered with the No-IP network.
4. Ask your ISP service provider for your DNS server address or look it up in the browser interface settings of your router.

   Go to **Network Settings** and enter the preferred and alternate DNS server addresses as well as the default gateway address.
5. Click **Save** to save the settings.

# NTP server settings

A Network Time Protocol (NTP) server can also be configured on your recorder to keep the date and time current and accurate.

**Note**: If the device is connected to a public network, you should use a NTP server that has a time synchronization function, such as the server at the National Time Center (IP Address: 210.72.145.44) or europe.ntp.pool.org. If the device is setup in a more customized network, NTP software can be used to establish a NTP server used for time synchronization.

**To set up an NTP server:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Network Settings** > **NTP**.
2. Select **Enable NTP**. It is disabled by default.
3. Enter the NTP settings:

- Interval (min): Time in minutes to synchronize with the NTP server. The value can be between 1 and 10080 minutes. Default is 60 minutes.
- NTP Server: IP address of the NTP server.
- **NTP Port:** Port of the NTP server.

4. Click **Save** to save the settings.

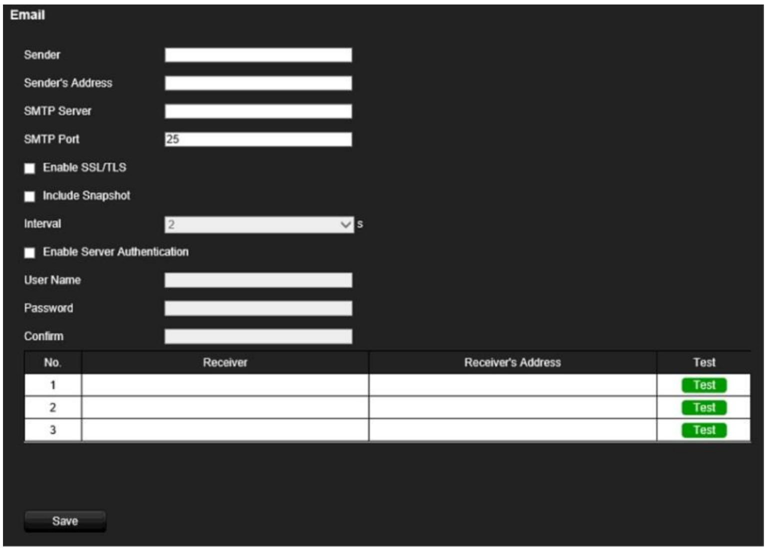
## Email settings

The recorder can send email notifications of alarms or notifications through the network.

**Note:** Ensure that the DNS address has been set up correctly beforehand.

**To configure email settings:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Network Settings** > **Email**.



Email

Sender:
Sender's Address:
SMTP Server:
SMTP Port: 25
□ Enable SSL/TLS
□ Include Snapshot
Interval: 2 s
□ Enable Server Authentication
User Name:
Password:
Confirm:

| No. | Receiver | Receiver's Address | Test |
|---|---|---|---|
| 1 | | | Test |
| 2 | | | Test |
| 3 | | | Test |

2. Enter the required settings.

| Option | Description |
|---|---|
| Sender | Enter the name of the sender of the email. |
| Sender’s Address | Enter the sender’s email address. |
| SMTP Server | Enter the SMTP server’s IP address. |
| SMTP Port | Enter the SMTP port. The default TCP/IP port for SMTP is 25. |
| Enable SSL/TLS | Select the check box to enable the SSL or TLS cryptographic protocol required by the SMTP server. The recorder will auto-detect which encryption method is being used.<br>SSL/TLS is an encryption method that is used to increase the security level of data transfer via email. |
| Include Snapshot | Select if you want to send an email with attached alarm images. |
| Interval | Select an interval range. Default is two seconds.<br>The interval range represents the time range in between the alarm images being sent. For example, if you set the interval range at two seconds, the second alarm image will be sent two seconds after the first alarm image |
| Enable Server Authentication | Select the check box if your mail server requires authentication and enter the login user name and password. |
| User Name | If the mail server requires authentication, enter the login user name. |
| Password | If the mail server requires authentication, enter the login password. |
| Receiver | Enter an email recipient. Up to three receivers can be entered. |
| Receiver’s Address | Enter the email address of the selected receiver. |
| Test | Click the Test button to confirm that the settings have been correctly configured. |

3. Click **Test** to the test email settings for each email address.

   **Note:** We recommend that you test the email settings after entering values in the email window.

4. Click **Save** to save the settings.

# Configure an FTP server to store snapshots

You can upload your snapshots to an FTP server for storage.

Note: It is not possible to stream video to an FTP site.

### To configure the FTP server settings:

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Network Settings** > **FTP**.
2. Select the **Enable FTP** box.
3. Enter the FTP server information.

4. Select the directory to use (root, parent, or secondary). If Parent or Child were selected, select the desired options for them.
5. Click **Save** to save the settings.

# SNMP settings

SNMP is a protocol for managing devices on networks. When you enable SNMP in the menu, network management systems can retrieve recorder status information from the recorder via SNMP.

When you set the trap address and trap port in the recorder  menu to the network management system’s IP address and port number and set up the network management system as trap receiver, trap notifications (such as startup) are sent from the recorder to the network management system.

Before configuring this function, you must first install the SNMP software.

**Note**:

SNMP v2c has some known vulnerabilities. Take care when enabling it on a public network. Contact your network team and follow best practices before enabling it.

Never use default community strings; only use unique community strings.

Make sure that all security measures have been taken at your end.

**To configure SNMP protocol settings:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Network Settings** > **SNMP**.
2. Select the **Enable SNMP** box.
3. Enter the required settings.
4. Click **Save** to save the settings.

# Add a network storage system

You can use multiple network storage systems (NAS) or IP SAN devices to remotely store recordings.

The recommended brands of storage system to use are:

- Iomega StorCenter ix2-dl
- QNAP TS-219 II Turbo NAS
- QNAP TS-220/221

**To set up a network storage system:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Network Settings** > **Network Storage**.
2. Under **Server IP**, enter the IP address of the desired remote storage system.
3. Under **File Path**, enter the file path name to define where on the remote storage system you want to store the files.

   **Note**: If using the NAS storage system Iomega StorCenter ix2-dl, you must add the prefix “/nfs” to the NAS path.
4. Under **Type**, select type of storage system to be used: NAS or IP SAN. Default is NAS.
5. Up to eight remote storage systems can be set up.
6. Click **Save** to save the settings.

# UPnP settings

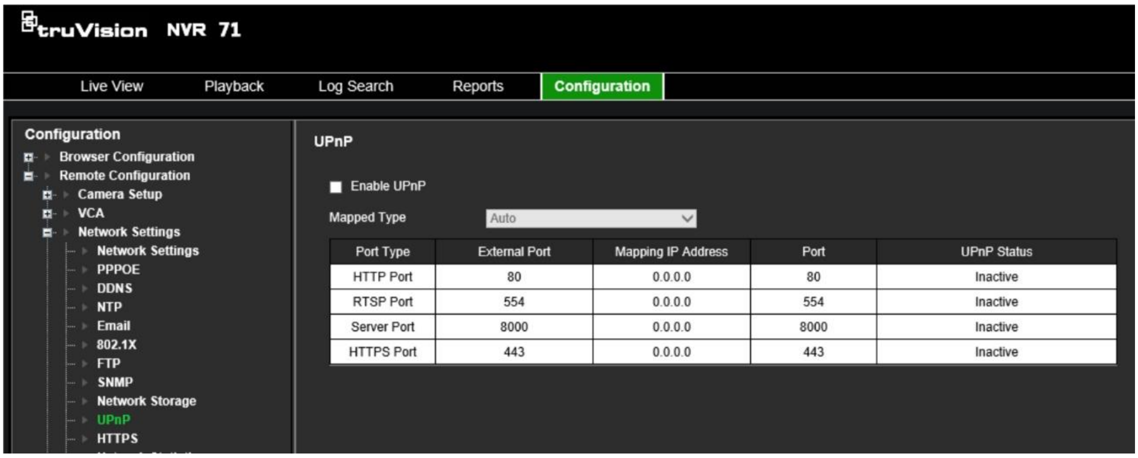
The recorder supports UPnP (Universal Plug and Play). This feature lets the recorder automatically configure its own port forwarding if this feature is also enabled in the router.

You can select one of two methods to set up UPnP:

**Automatic mapped type**: The recorder automatically uses the free ports available that were set up in the Network Settings menu.

**Manual mapped type**: You enter the specific external port settings and IP addresses required to connect to the desired router (see Figure 19 below).

**Figure 19: UPnP manual configuration screen**



UPnP

□ Enable UPnP

Mapped Type: Auto

| Port Type | External Port | Mapping IP Address | Port | UPnP Status |
|---|---|---|---|---|
| HTTP Port | 80 | 0.0.0.0 | 80 | Inactive |
| RTSP Port | 554 | 0.0.0.0 | 554 | Inactive |
| Server Port | 8000 | 0.0.0.0 | 8000 | Inactive |
| HTTPS Port | 443 | 0.0.0.0 | 443 | Inactive |

**To enable UPnP:**

1. Connect the recorder to the router.

   **Note**: The router must support UPnP and this option must be enabled.

2. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Network Settings** > **UPnP**.
3. Check the **Enable UPnP** box.
4. From **Mapped Type,** select Auto or Manual.
5. Click **Save** to save the settings.

# HTTPS settings

Using HTTPS (Hypertext Transfer Protocol Secure) is a secure protocol that provides authenticated and encrypted communication. It ensures that there is a secure private channel between the recorder and cameras.

You can create self-signed server certificates as well as request certified server certificates to ensure your network security. For larger companies, a corporate certificate might be available with the IT department.

The HTTPS port can only be configured through the web browser.

**Note**: You must run Microsoft Internet Explorer as administrator.

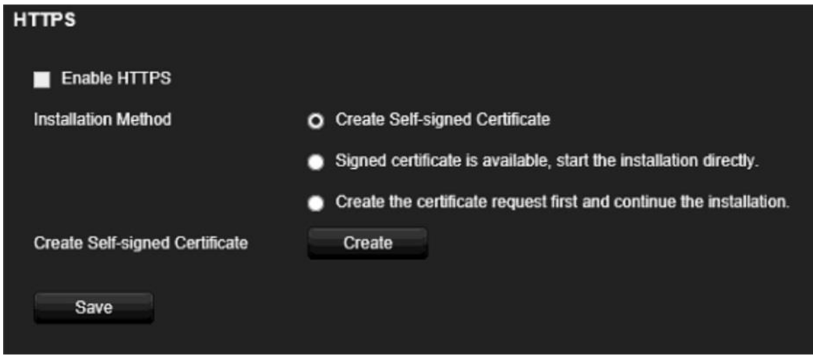
**Create a certificate:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Network Settings** > **HTTPS**.
2. Check **Enable HTTPS**.

   **Note**: This only works if you have entered the address in the browser as HTTPS (as in https://192.168.1.70)
3. Select the type of certificate you want:

   - **Create a self-signed certificate:**

   a) Select **Create Self-Signed certificate**.



HTTPS

□ Enable HTTPS

Installation Method
◉ Create Self-signed Certificate
○ Signed certificate is available, start the installation directly.
○ Create the certificate request first and continue the installation.

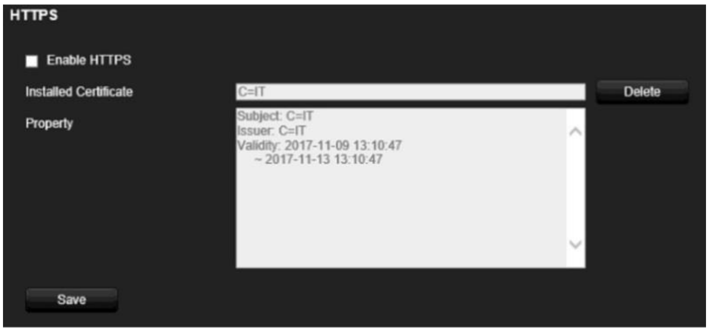
Create Self-signed Certificate [Create]

[Save]

   b) Click **Create**. The Create pop-up window appears.

   c) Enter the country, hostname/IP address, and days of validity (there are more parameters, but you do not need to add anything to them) and click **OK.**

   d) A screen appears showing certificate information. Click **Save**.



HTTPS

□ Enable HTTPS

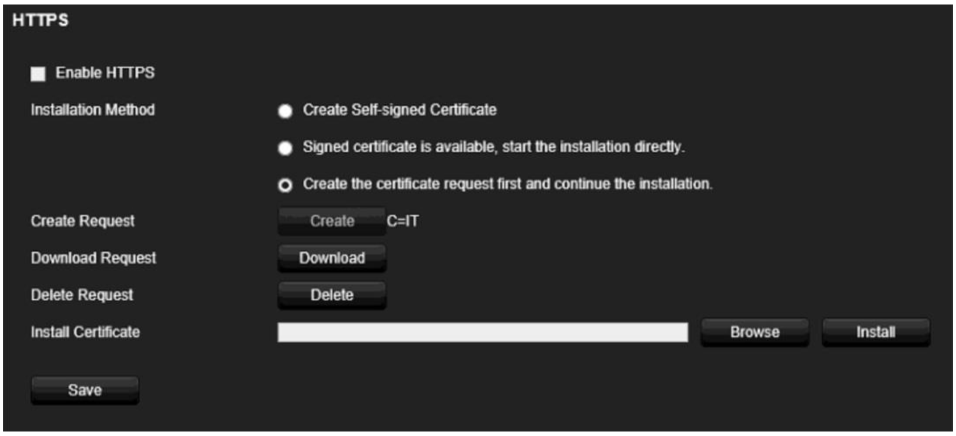
Installed Certificate: C=IT

Property:
Subject: C=IT
Issuer: C=IT
Validity: 2017-11-09 13:10:47
~ 2017-11-13 13:10:47

- Or -

- **Create a certificate request and continue with the installation**

a) Select **Create the certificate request first and continue the installation**.



HTTPS

□ Enable HTTPS

Installation Method: ● Create Self-signed Certificate
● Signed certificate is available, start the installation directly.
○ Create the certificate request first and continue the installation.

Create Request: Create C=IT

Download Request: Download

Delete Request: Delete

Install Certificate: Browse Install

b) Click **Create** to create the certificate request and then click **Download**. Click **Save** to save the certificate in the desired folder and then submit it to a trusted certificate authority for signature.

c) When you receive the signed certificate, upload it to the recorder. Click **Browse** to locate the certificate file and then click **Install**.

- Or -

- **If you already have a certified certificate:**

a) Select **Signed certificate is available, start the installation directly**.

b) Click **Browse** to locate the certificate file and then click **Install**.

4. Click **Save** to save the settings.

# Network statistics

You can easily check the bandwidth that is being used by remote live view and playback.

**To check network statistics:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Network Settings** > **Network Statistics**.

2. The latest information is displayed on the bandwidth used by remote live view and playback as well by Net Receive Idle and Net Send Idle. Click **Refresh** to update the information.

# Filter IP addresses

You can define the list of forbidden or allowed IP addresses that can be accessed by the recorder. This lets you select who can access the system, increasing the system’s security. The function is disabled by default.

**To define forbidden or allowed IP addresses:**

1. From the menu toolbar, click **Configuration** > **Network Settings** > **IP Address Filter**.
2. Select the **Enable IP Filter** check box.
3. Under **IP Filter Type**, select Forbidden or Allowed.
4. Click **Manually Add**. In the “Add IP Address” pop-up dialog box, enter the IP address to be controlled and click **OK**.

   Click **Delete** to remove IP addresses from the list.
5. If required, you can modify a saved IP address. Click **Modify** and enter the changes.
6. Click **Save** to save the settings.

# 802.1x authentication

802.1X is a standard for port-based access control. It provides an authentication mechanism to devices wishing to attach to a LAN (or WLAN).

802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client device (such as a recorder) that wishes to attach to the LAN (WLAN)

The authenticator is a network device, such as an Ethernet switch or wireless access point. The authentication server is typically a host running software supporting the RADIUS and EAP protocols. In some cases, the authentication server software may be running on the authenticator hardware.

The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant’s identity has been validated and authorized by the authentication server. With 802.1X port-based authentication, the supplicant provides credentials, such as user name/password or digital certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device) can access resources located on the protected side of the network.

To use 802.1X with the recorder, the network switch needs to also to support 802.1X.

**To define the 802.1X parameters:**

1. From the menu toolbar, click **Configuration** > **Network Settings** > **802.1X**.
2. Select **Enable IEEE 802.1X** to enable the feature.
3. Configure the 802.1X settings. Select **EAP-PEAP** or **EAP-TLS**.

   **If EAP-PEAP is selected:**

   PEAP (Protected Extensible Authentication Protocol) fully encapsulates EAP and is designed to work within a TLS (Transport Layer Security) tunnel that may be encrypted but is authenticated. The primary motivation behind the creation of PEAP was to help correct the deficiencies discovered within EAP since that protocol assumes that the communication channels are protected.

   For each option shown below, enter or select a value as required:

| Option | Description |
|---|---|
| Protocol | Select EAP-PEAP. |
| EAPOL version | Version 2 is supported. Affects the format of the exchange with the RADIUS server. |
| User Name | This is a valid user name for the authentication server (usually a RADIUS server). |
| Password | This is a valid password for the user name specified in the previous field. |
| CA certificate | This should be obtained from the network administrator, as network policies may differ. |

# Chapter 12
# Recording

Use the Recording menu to define the camera recording schedules, configure auto archiving and hot spare mode, and select the cameras for manual recording.

## Recording schedule

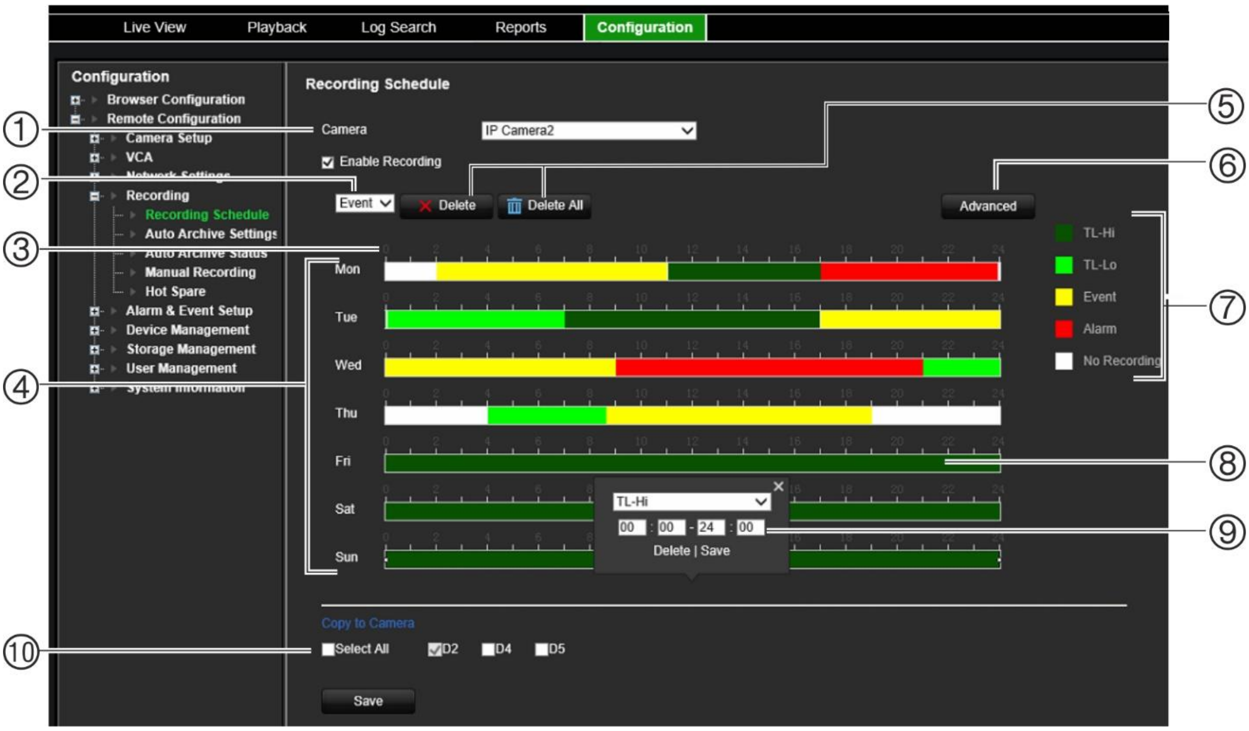
Defining a recording schedule lets you specify when the recorder records video and which pre-defined settings are used. Each camera can be configured to have its own recording schedule.

The schedules are visually presented on a map for easy reference. See Figure 20 on page 88 for a description of the recording schedule window.

**Note**: If a camera is set up for continuous recording (called “constant recording”), it will still switch to event recording or alarm recording if motion events are triggered or to alarm recording when alarms are triggered. This can be turned off in the individual action settings for each individual alarm if needed.

See Figure 20 on page 88 for a description of the recording schedule window.

**Figure 20: Description of the recording schedule window**



1. Camera: Select a camera.
2. **Recording type for a time period**: Select the recording type for a new recording period.
3. Schedule time: Represents the 24-hour cycle during which a schedule is selected.
4. Schedule map: There are seven days to select: Monday (Mon), Tuesday (Tue), Wednesday (Wed), Thursday, (Thu), Friday (Fri), Saturday (Sat), and Sunday (Sun).
5. **Delete/Delete All**: Select a recording period on a camera's day and click **Delete** to delete it. Click **Delete All** to delete all recording schedules for the selected camera.
6. **Advanced settings:** Click to modify the following parameters:

- **Record Audio**: Enable to record sound with the images. Default is Enable.
- **Enable EFR**: Enable the EFR function (Edge Failover Recording) to save video to the SD card in the selected camera when the network is offline. This video will then be synchronized to the recorder HDD when the network becomes online again.
- **Pre Event**: This is the time the camera starts recording before the event. Select the time in seconds from the list to start pre-recording before the event. Default is 5 seconds.

  The maximum pre-recording times available depend on the constant bit rate. See "Maximum storage times" in the appendix.
- **Post Event**: This is the time the camera continues to record after the event. Select the time in seconds from the list to stop post-recording after the event. Default is 5 seconds.
- **Auto Delete (day)**: Select the number of days after which recorded video from the specified camera is permanently deleted from the HDD. A "day" is defined as the 24-hour period from when the auto delete mode (ADM) was set.

  The maximum number of days that can be set is 365. However, the actual number of days permitted depends on the HDD capacity. If the value is set to '0', the option is disabled. Default is Disable.

7. **Recording type:** There are five types of recording to select, which are color-coded:

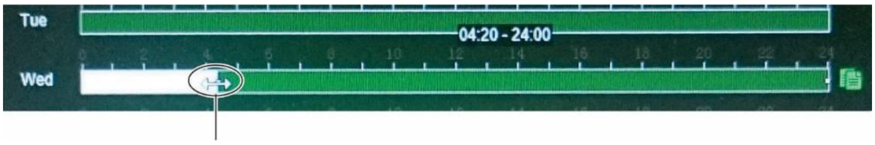
- **TL-Hi** (Dark green): High quality time lapse. It records high quality continuous video. This is the default recording type.

- **TL-Lo** (Bright green): Low quality time lapse. It records low quality continuous video. This could be used, for example, for night recordings when few events or alarms are expected. Saving the video in low quality helps save resources on the HDD.
- **Event** (Yellow): It records only events, such as motion detection.
- **Alarm** (Red): It records only alarms. It has priority over constant and event recording.
- **None** (White): No recording during this period.

8. Timeline: There is a 24-hour timeline for each day. Up to eight recording periods can be scheduled during the 24-hour period.
9. **Edit schedule window**: Enter the recording type, and time for the recording period.
10. **Copy to Camera:** Click to copy recording schedules between cameras.

## Define a recording schedule

There are a couple of ways to define the recording schedule. You can use the *Edit schedule* pop-up window, which appears when you click a schedule period on a timeline. You can also drag the start or end of the schedule period bar and move it to the desired time. The time period of the bar appears above so it is easy to adjust it to a specific time period.



Drag the start or end of the schedule period bar and move it to the desired time.

The Edit schedule pop-up menu does not appear if you click a “No Recording” time period. However, you can drag the mouse along the white “No recording” zone on the timeline to create a new recording period. Before creating the new recording period on a timeline, select the recording type from the drop-down list (see item 2, Figure 20).

**To set up a daily recording schedule:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Recording** > **Recording Schedule**.
2. Select a camera.
3. Check the **Enable Recording** box.
4. Click the timeline of the desired day of the week. The *Edit schedule* window pops up. Select the desired recording type and enter the start and end times of the recording schedule. Click **Save**.

   You can define up to eight different periods during a day, and a different schedule for each day of the week.

   **Note**: The time periods defined cannot overlap.
5. To copy a day’s schedule to another day of the week click 📋 , which appears at the end of the day’s timeline. The *Copy to* pop-up menu appears. Select the day or days of the week to which to copy this day’s schedule and click **OK**.
6. To copy a camera’s recording schedule to another camera, or several cameras, select the desired cameras under “Copy to Camera”.

7. Click **Save** to save the settings.

# Manual recording

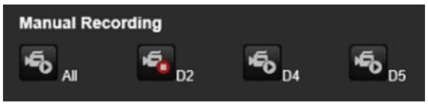
The recorder lets you manually record video during live view. This can be useful if you know that the recorder is not currently recording, and you see something of interest on a camera screen that should be recorded.

Once a manual recording is started, the recording continues until it is manually stopped. If an alarm occurs during a manual recording, the alarm recording has priority over the manual recording. If a scheduled recording is already in progress when a manual recording is started, it continues to record as scheduled.

Alternatively, the manual recording menu shows the current state of manual recording for each camera. In this menu you can enable or disable the current manual recording for any given camera.

**To start and stop manual recording:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Recording** > **Manual Recording**.
2. Check the boxes of the cameras to start or stop manual recording. The button is red when manually recording. Default is off.



# Hot spare

You can set up a spare recorder to act as a slave unit (hot spare) for up to four master recorders. This slave unit will continually monitor the master recorders and if one of the master recorders should fail, it can then take over recording until the failed recorder comes back online. Once the failed recorder is back operating normally again, the slave recorder will send its recordings to the HDDs of the recovered master so that no recordings are missing.

The hot spare recorder can only backup one master recorder at a time. If more than one recorder should fail, the hot spare recorder will only backup the recorder that failed first.

All recorders must have the same number of channels.

Once the failed master recorder is back online, the slave unit will return to its normal monitoring state.

**Note**: When the hot spare recorder records the cameras of another recorder, it will record the cameras continuously. So, any event settings such as motion and VCA are not considered by the hot spare recorder.

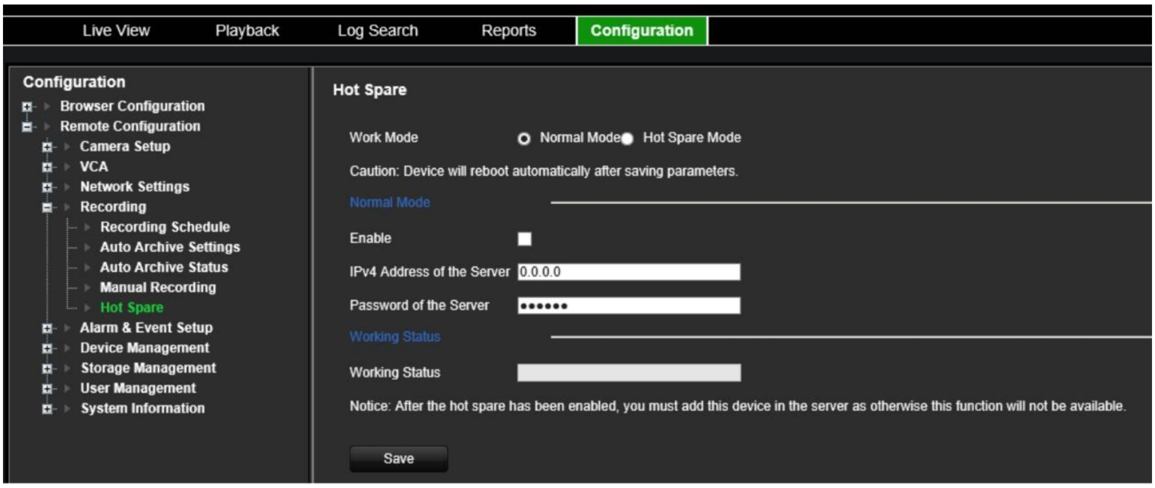
For the failover functionality to work properly, the following points must be taken into account:

- A stable network connection is required.
- There must be at least 10 Mbps of unallocated bandwidth available with the main recorder.
- This unallocated bandwidth is used for streaming the video footage from spare unit to master unit during the recovery process.
- Ideally the failover recorder must have equal storage capacity to the main recorder to accommodate for long outage times of the main recorder.

**To set up a hot spare recorder:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Recording** > **Hot Spare**.
2. First set up the master recorders.

   For each master recorder, select the **Normal Mode** button and **Enable** check box. Enter the IP address and password of the hot spare recorder.



Hot Spare

Work Mode ○ Normal Mode ● Hot Spare Mode

Caution: Device will reboot automatically after saving parameters.

Normal Mode

Enable □

IPv4 Address of the Server 0.0.0.0

Password of the Server ••••••

Working Status

Working Status

Notice: After the hot spare has been enabled, you must add this device in the server as otherwise this function will not be available.

Save

3. Set up the hot spare recorder.

   Check the **Hot Spare Mode** box.
4. The **Working Status** field displays whether the hot spare is in stand-by mode or busy.
5. Click **Save** to save the settings. The recorder will automatically reboot.

# Chapter 13
# Alarm and event setup

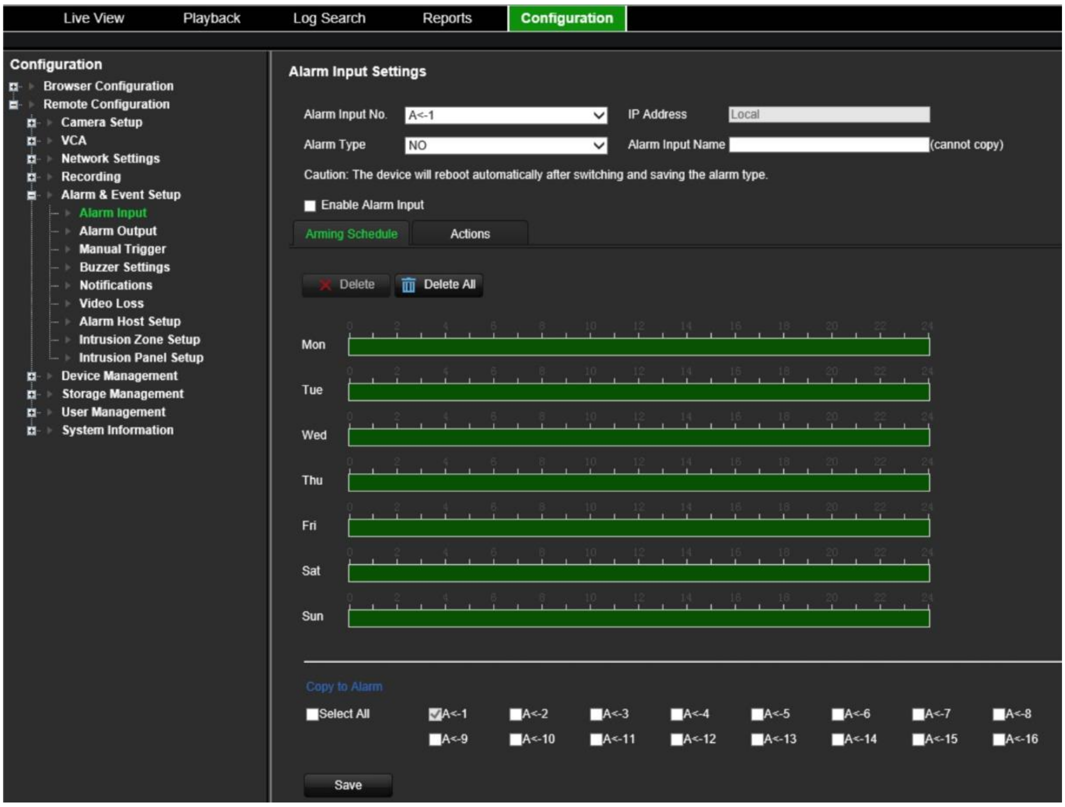
This chapter describes the alarm and event setup menu and provides more information on the different types of alarms and connected responses. Alarms are all notifications related to either physical alarm inputs on recorders and cameras or anything that does not work as expected: device errors, network issues, and video loss.

## Set up alarm inputs

You can configure the recorder to record when an alarm is triggered by an external alarm device (for example, PIR detector, dry contacts…). “A” inputs are marked A for analog and are physical inputs of the recorder. “D” inputs are marked as D for digital and are physical inputs on the IP cameras.

**To set up external alarms:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Alarm & Event Setup** > **Alarm Input**.



Alarm Input Settings

Alarm Input No. A<-1 IP Address Local

Alarm Type NO Alarm Input Name (cannot copy)

Caution: The device will reboot automatically after switching and saving the alarm type.

□ Enable Alarm Input

□ Select All ☑ A<-1 □ A<-2 □ A<-3 □ A<-4 □ A<-5 □ A<-6 □ A<-7 □ A<-8
□ A<-9 □ A<-10 □ A<-11 □ A<-12 □ A<-13 □ A<-14 □ A<-15 □ A<-16

2. Select the alarm input number of a camera, which corresponds to the connector on the back panel of the recorder, and enter a name for it, if desired (the name cannot be copied).

3. Select the alarm input type, NO (normally open) or NC (normally closed). Default is NO.

4. Check the **Enable Alarm Input** box.

5. Select the arming schedule for the external alarm.

   a) Click the **Arming Schedule** tab. Click the timeline of the desired day of the week. The *Edit schedule* window pops up. Enter the start and end times of the arming schedule. Click **Save**.

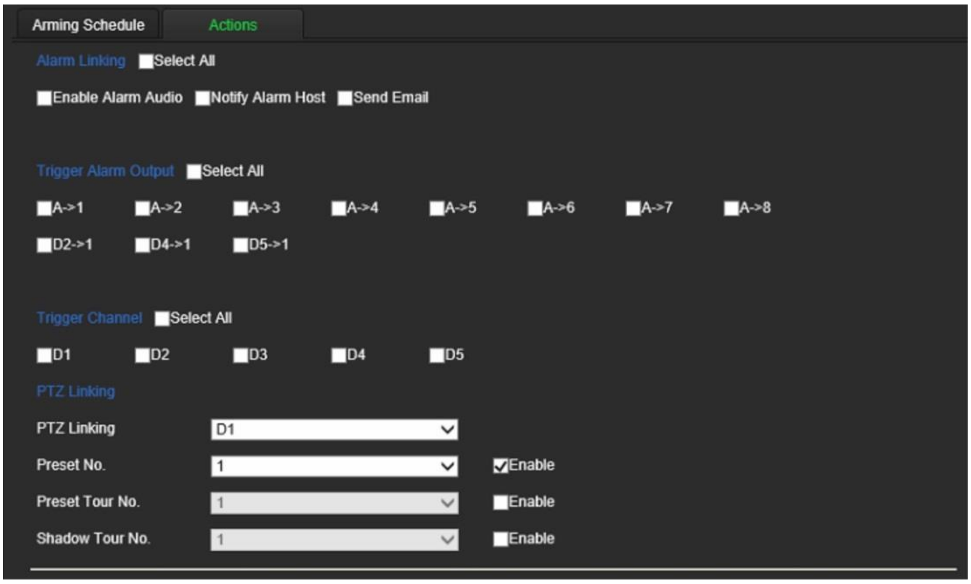
   You can define up to eight different periods during a day, and a different schedule for each day of the week.

   Note: The time periods defined cannot overlap.

   b) To copy a day's schedule to another day of the week click 📋 , which appears at the end of the day's timeline. The *Copy to* pop-up menu appears. Select the day or days of the week to which to copy this day's arming schedule and click **OK**.

6. Specify the linkage method when an event occurs.

   a) Click the **Actions** tab. Select the method by which you want the recorder to notify you of the alarm: Enable Alarm Audio, Notify Alarm Host, Send Email (see page 96 for the description of these alarm response types).



Arming Schedule | Actions

Alarm Linking □ Select All

□ Enable Alarm Audio □ Notify Alarm Host □ Send Email

Trigger Alarm Output □ Select All

□ A->1 □ A->2 □ A->3 □ A->4 □ A->5 □ A->6 □ A->7 □ A->8

□ D2->1 □ D4->1 □ D5->1

Trigger Channel □ Select All

□ D1 □ D2 □ D3 □ D4 □ D5

PTZ Linking

PTZ Linking: D1

Preset No.: 1 ☑ Enable

Preset Tour No.: 1 □ Enable

Shadow Tour No.: 1 □ Enable

b) Specify which alarm outputs are triggered when an event occurs.

c) Select the cameras to be triggered when an external alarm is detected.

d) Select the PTZ camera function required in response to an external alarm.

   Under **PTZ Linking**, enable the preset, preset tour or shadow tour to be triggered when the alarm is detected and enter the preset, preset tour or shadow tour number.

7. If you want to copy the settings to other alarm inputs, select the desired alarm inputs under “Copy to alarm”.

8. Click **Save** to save the settings.

## Set up alarm outputs

You can connect the recorder to an alarm system, such as a siren or intrusion system, which is then activated when an alarm is triggered. You can select how long the alarm signal remains active as well as schedule when alarm outputs can be triggered.

“A” outputs are marked A for analog and are physical outputs of the recorder. “D” outputs are marked as D for digital and are physical outputs on the IP cameras.

**To set up an alarm output:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Alarm & Event Setup** > **Alarm Output**.

2. Select the alarm output. Enter a name for it, if desired (the name cannot be copied).

3. Select a time out option between 5 seconds and 10 minutes or select “Manual”.

   The timeout setting lets you define how long an alarm signal remains active after the alarm has ended. If you select **Manual**, the alarm signal remains active until it is acknowledged (see “Manual trigger” on page 95).

4. Select the arming schedule for the alarm output.

a) Under the **Arming Schedule** tab click the timeline of the desired day of the week. The *Edit schedule* window pops up. Enter the start and end times of the arming schedule. Click **Save**.

   You can define up to eight different periods during a day, and a different schedule for each day of the week.

   Note: The time periods defined cannot overlap.

b) To copy a day's schedule to another day of the week click 📋, which appears at the end of the day's timeline. The *Copy to* pop-up menu appears. Select the day or days of the week to which to copy this day's arming schedule and click **OK**.

5. If you want to copy the settings to other alarm outputs, select the desired alarm outputs under "Copy to alarm".
6. Click **Save** to save the changes.

# Manual trigger

The manual trigger menu allows you to manually trigger outputs of the recorder.

**To trigger or clear alarm outputs manually:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Alarm & Event Setup** > **Manual Trigger**.
2. Select the desired alarm output and click the following buttons:

   **Trigger**: Trigger an alarm output or stop an alarm output.

   **Trigger All**: Trigger all alarm outputs or stop all alarm outputs.

   **Clear All**: Stop all alarm outputs at once.

   **Note**: The alarm output name can be entered in the Alarm Output menu.

# Buzzer settings

When an alarm is triggered by the system or a camera, the recorder can be set up to respond with a warning buzzer. The buzzer time is the time that it takes for the recorder to time-out the buzzer when a continuous alarm occurs. For example, when a physical alarm input is continuously triggered, the buzzer will time out after the time specified.

**To set up alarm notifications:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Alarm & Event Setup** > **Buzzer Settings**.
2. Under **System buzzer timeout time** select a buzzer time limit: 5 s, 10 s, 20 s, 30 s, 60 s, 120 s, 240 s, or Constant. Default is Constant.

3. Under **Camera buzzer timeout time** select a buzzer time limit: 5 s, 10 s, 20 s, 30 s, 60 s, 120 s, 240 s, or Constant. Default is Constant.
4. Click **Save** to save the settings.

# Alarm notification

When setting up the rules for alarm detection, you can specify how you want the recorder to notify you about an alarm or event. You can select more than one notification type.

Not all notification types are available for all types of alarms.

You can quickly check the system status by looking at the status LEDs on the front panel.

The alarm response methods are:

- **Enable Alarm Audio:** Triggers an audible *beep* when a notification or alarm is detected by the system or a camera.
- **Notify Alarm Host:** Sends a signal to TruVision Navigator or other software applications when an alarm or notification is detected.
- **Send Email:** Sends an email when an alarm or notification is detected. See “Email settings” on page 79 for information on how to configure the recorder to send an email.

**To set up alarm notifications:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Alarm & Event Setup** > **Notifications**.
2. Select the **Display Event Icon** check box so that the event icon appears in the OSD in live view when an alarm or event is triggered (default is enabled).
3. Select an alarm notification type. Under **Notification Type**, select the desired technical event notification:
   - **HDD Full**: All installed HDDs are full and will not record any more video.
   - **HDD Error**: Errors occurred while files were being written to the HDD, there is no HDD installed, or the HDD had failed to initialize.
   - **Network Disconnected**: Disconnected network cable.
   - **Duplicate IP Address Found**: There is an IP address conflict with another system on the network.
   - **Invalid Login**: Wrong user name or password used.
   - **Record/Capture Exception**: No space for saving recorded files or captured images.
   - **Hot Spare Exception**: Errors occurred with hot spare HDD.
4. Check one or more response method: Enable Alarm Audio, Notify Alarm Host, and Send Email

   **Note**: The list of options available depends on the alarm notification type selected.
5. Select the alarm outputs to be triggered when an alarm notification detected.

6. Repeat steps 2 and 6 for other alarm notification types.
7. Click **Save** to save the settings.

## Event notifications

Event notifications appear in the Notification Center.

The different types of events notifications are:

- **HDD Full**: All installed HDDs are full and will not record any more video.
- **HDD Error**: Errors occurred while files were being written to the HDD, there is no HDD installed, or the HDD had failed to initialize.
- **Network Disconnected**: Disconnected network cable.
- **Duplicate IP Address Found**: There is an IP address conflict with another system on the network.
- **Invalid Login**: Wrong user name or password used.
- **Video Loss**: The video image is lost. Video may be lost if the camera develops a fault, is disconnected, or is damaged.
- **Video Loss**: The video image is lost. Video may be lost if the camera develops a fault, is disconnected, or is damaged.
- **Alarm Input**: An alarm triggered by an external alarm device (for example, PIR detector, dry contacts…)
- **Camera Tamper Detected**: The camera view has changed. For example, someone has deliberately blocked the camera view by spraying paint on the lens or by moving the camera
- **Motion Detected**: Motion is detected.
- **Abnormal Record**: HDD cannot record any more files. This could be due to the overwrite option being disabled so recorded files are locked and cannot be deleted.
- **IP Camera Address Conflicted**: Conflict in IP address setting.
- **Abnormal Array**: Errors occurred with the array.
- **Motherboard Temperature Anomaly**:
- **Hot Spare Exception**: Errors occurred with hot spare HDD.
- **Resolution or Bitrate of Substream Not Supported**
- **Cross Line Detected**: People, vehicles and objects have been detected crossing a pre-defined line or an area on screen.
- **Intrusion Detected**: Someone has been detected entering a pre-defined area in the surveillance scene.
- **Audio Input Exception**: A camera has detected sounds that are above a selected threshold.
- **Sudden Change of Sound Intensity**: A camera has detected a change in the scene caused by an intentional rotation of the camera.

- **Face Detected**: A camera has detected that a human face is moving towards it.
- **Defocus Detected**: There is image blur caused by defocusing the lens.
- **Scene Change**: A camera has detected a change in the scene caused by an intentional rotation of the camera.
- **Enter Region Detected**: A camera has detected that an object, such a vehicle, people or other objects, has entered a designated region.
- **Exit Region Detected**: A camera has detected that an object, such a vehicle, people or other objects, has exited a designated region.
- **Object Left Leave Behind**:  A camera has detected that an object has been left in a designated region, such as baggage.
- **Object Removed**: A camera has detected that an object has been removed from a designated region, such as exhibits on display.
- **Enter Region Detected**: A camera has detected that an object, such a vehicle, people or other objects, has entered a designated region.
- **Exit Region Detected**: A camera has detected that an object, such a vehicle, people or other objects, has exited a designated region.
- **Leave Behind**:  A camera has detected that an object has been left in a designated region, such as baggage.
- **Object Removed**: A camera has detected that an object has been removed from a designated region, such as exhibits on display.

**To view events in the notification center**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Alarm & Event Setup** > **Notifications**.
2. Click the **Event Hint Settings** button. Check those required. All event items selected will be listed in the Notification Center if triggered. All notifications are selected by default.

# Detect video loss

Video may be lost if the camera develops a fault, is disconnected, or is damaged. You can set up the recorder to detect video loss and trigger a system notification.

**To setup video loss detection:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Alarm & Event Setup** > **Video Loss**.
2. Select a camera to configure for video loss detection.
3. Check the **Enable Video Loss Alarm** box to enable the feature.
4. Select the arming schedule for video loss.

a) Under the **Arming Schedule** tab click the timeline of the desired day of the week. The *Edit schedule* window pops up.  Enter the start and end times of the arming schedule. Click **Save**.

You can define up to eight different periods during a day, and a different schedule for each day of the week.

**Note**: The time periods defined cannot overlap.

b) To copy a day’s schedule to another day of the week click 📋, which appears at the end of the day’s timeline. The *Copy to* pop-up menu appears. Select the day or days of the week to which to copy this day’s arming schedule and click **OK**.

5. Specify the linkage method when video loss occurs.

   a) Click the **Actions** tab. Select the method by which you want the recorder to notify you of the alarm: Enable Alarm Audio, Notify Alarm Host, Send Email, and Upload to FTP.

   b) Specify which alarm outputs are triggered when an event occurs.

6. Repeat steps 2 to 5 for another camera.

7. Click **Save** to save the settings.

# Alarm host setup

If an alarm host is set, the recorder sends a signal to the host when an alarm is triggered. An example of an alarm host is the TruVision Navigator server. Note that alarm host applications need to have the TruVision recorder SDK implemented to successfully receive notifications from the recorder.

**To set up an alarm host:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Alarm & Event Setup** > **Alarm Host Setup**.

2. Enter Alarm Host IP and Alarm Host Port values.

   Alarm host IP represents the IP of the remote PC where the Network Video Surveillance software installed. The alarm host port value must be the same as software’s alarm monitor port. Up to three alarm hosts can be set. For each alarm host, the default port is 5001, 5002, and 5003.

3. Click **Save** to save the settings.

# Intrusion integration alarm reporting

The recorder includes an alarm receiver software module for intrusion integration. This permits SIA and XSIA events to be reported to the recorder from Aritech intrusion panels via IP and to be linked to recorder actions.

The following Aritech panels are supported:

- ATS Master (EMEA only)
- Advisor Advanced (EMEA only)
- NetworX panels

Up to three intrusion panels can be set up in the recorder. Each panel can report up to 32 intrusion zones (a zone is an intrusion panel input).

The panels must support the SIA or XSIA reporting protocol. They can report the following alarm types to the recorder:

- An arming event
- A disarming event
- An alarm event that has an “A” as a second character in the SIA/XSIA code as well as codes BV and HV.

| | |
|---|---|
| Intrusion Alarm_BA (Burglary alarm) | Intrusion Alarm_TA (Tamper alarm) |
| Intrusion Alarm_EA (Exit alarm) | Intrusion Alarm_UA (Technical alarm (General)) |
| Intrusion Alarm_FA (Fire alarm) | Intrusion Alarm_WA (Technical alarm (Water)) |
| Intrusion Alarm_GA (Technical alarm (gas)) | Intrusion Alarm_ZA (Technical alarm (Low temperature)) |
| Intrusion Alarm_HA (Hold-up alarm) | Panel Heartbeat Alarm |
| Intrusion Alarm_JA (User code tamper) | Arming Panel Alarm |
| Intrusion Alarm_KA (Technical alarm (High temperature) | Disarming Panel Alarm |
| Intrusion Alarm_MA (Medical alarm) | Intrusion Alarm_HV (Hold-up verified) |
| Intrusion Alarm_PA (Panic alarm | Intrusion Alarm_BV (Burglary verified) |
| Intrusion Alarm_QA (Emergency alarm) | |

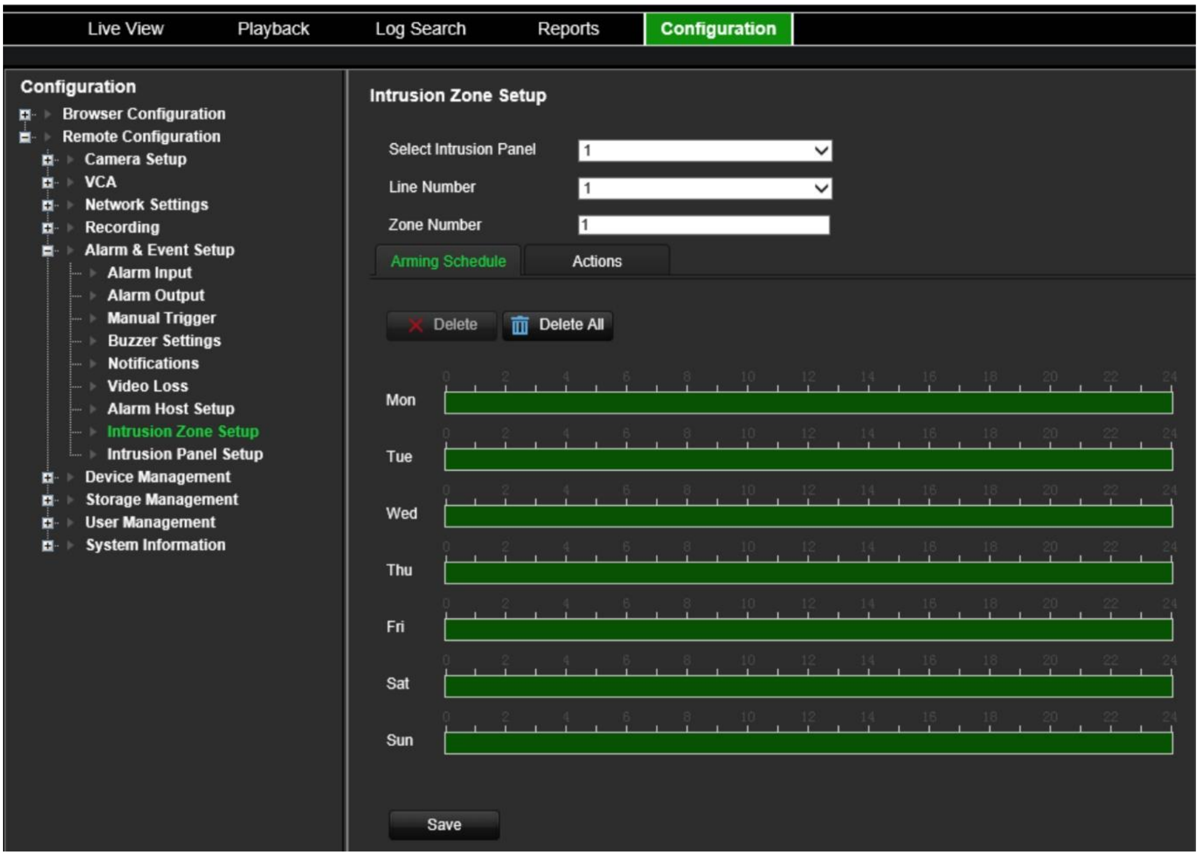
- A heartbeat alarm

In the intrusion panel, set up the recorder as a normal monitoring station. Use OH version 3 so that the data format is understood by the recorder.

For NX panels, polling must be enabled in the NX-590E.

**To set up the zones in an alarm panel:**

1. From the menu toolbar, click **Alarm & Event Setup** > **Intrusion Zone Setup**.



Intrusion Zone Setup

Select Intrusion Panel: 1

Line Number: 1

Zone Number: 1

2. Under **Select Intrusion Panel**, select intrusion panel 1, 2 or 3.
3. Under **Line Number**, select the desired ID of a zone. The maximum is 32. The number does not have to match the zone number.
4. Under **Zone Number**, select the desired zone number. The zone number can be any valid number of the panel, which does not need to match the zone number.
5. Select the arming schedule for the intrusion alarm.

   a) Click the **Arming Schedule** tab. Click the timeline of the desired day of the week. The *Edit schedule* window pops up. Enter the start and end times of the arming schedule. Click **Save**.

   You can define up to eight different periods during a day, and a different schedule for each day of the week.

   **Note**: The time periods defined cannot overlap.

   b) To copy a day's schedule to another day of the week click 📋, which appears at the end of the day's timeline. The *Copy to* pop-up menu appears. Select the day or days of the week to which to copy this day's arming schedule and click **OK**.

6. Specify the linkage method when an alarm occurs.

   a) Click the **Actions** tab. Select the method by which you want the recorder to notify you of the intrusion panel alarm: Enable Alarm Audio, Notify Alarm Host, Send Email (see page 96 for the description of these alarm response types).

   b) Specify which alarm outputs are triggered when an alarm occurs.

c) Select the cameras to be triggered when an intrusion panel alarm is detected.

d) Select the PTZ camera function required in response to an alarm.

Under **PTZ Linking**, enable the preset, preset tour or shadow tour to be triggered when the alarm is detected and enter the preset, preset tour or shadow tour number.

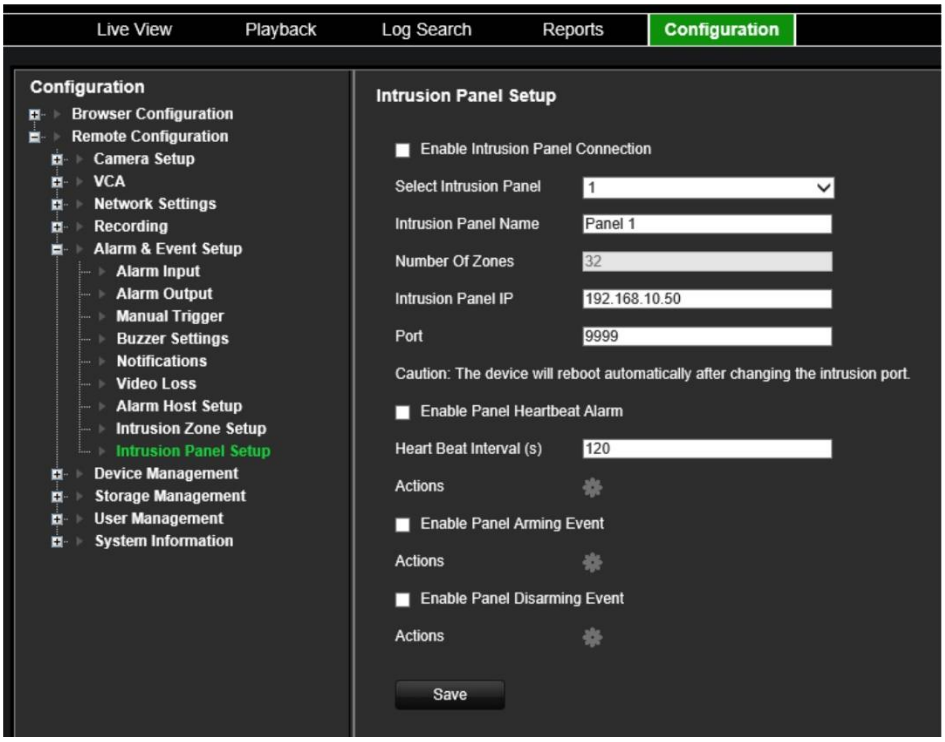
e) Click **OK** to save the changes and return to the *Intrusion Zone Setup* window.

7. To copy the intrusion panel's arming schedule to up to three other intrusion panels, select the desired intrusion panels and zones under "Copy to" at the bottom of the window.

8. Click **Save** to save the intrusion zone setup parameters.

**To set up an alarm panel in the recorder:**

1. From the menu toolbar, click **Alarm & Event Setup** > **Intrusion Panel Setup**.



Intrusion Panel Setup

□ Enable Intrusion Panel Connection

Select Intrusion Panel: 1

Intrusion Panel Name: Panel 1

Number Of Zones: 32

Intrusion Panel IP: 192.168.10.50

Port: 9999

Caution: The device will reboot automatically after changing the intrusion port.

□ Enable Panel Heartbeat Alarm

Heart Beat Interval (s): 120

Actions

□ Enable Panel Arming Event

Actions

□ Enable Panel Disarming Event

Actions

2. Select the **Enable Intrusion Panel Connection** check box to enable the intrusion panel connection.

3. Set up the intrusion panel connection parameters.

a) Select which panel you want to set-up. Up to three panels can be set up.

b) Enter a name for the panel.

c) Enter the number of zones. Up to 32 panel zones can report to the recorder. The number cannot be increased but you can allocate a different ID for each zone under the "Intrusion Zone Setup" menu.

d) Enter the panel's IP address. The IP address must be in the same LAN as the recorder.

e) Enter the port that is used to report the events. Default is 9999. This port number must match the port number set up in the intrusion panel.

**Caution**: The recorder will reboot automatically when the intrusion panel port number is changed.

4. Set up the heartbeat alarm parameters.

   a) Select **Enable Panel Heartbeat Alarm** check box to enable the panel heartbeat alarm. The heartbeat alarm will then be reported to the recorder.

   b) Enter the interval between two heartbeats. It is measured in seconds. Default is 120 s. This interval is valid even if the “Enable Panel Heartbeat Alarm” check box is disabled.

   To be able to trigger a heartbeat alarm when the heartbeat is not received within this interval, enable the “Enable Panel Heartbeat Alarm” check box.

   The recorder heartbeat interval must always be higher than that of the intrusion panel.

   c) Click the ⚙ button to set up the actions linked to the panel heartbeat alarm. Go to step 7 for further information.

5. Set up the panel arming alarm parameters.

   a) Select the **Enable Panel Arming Event** check box to enable the panel arming event. When the panel is armed, it will be reported to the recorder.

   b) Click the ⚙ button to set up the actions linked to the panel arming event. Go to step 7 for further information.

6. Set up the panel disarming alarm parameters.

   a) Select the **Enable Panel Disarming Event** check box to enable the panel disarming event. When the panel is armed, it will be reported to the recorder.

   b) Click the ⚙ button to set up the actions linked to the panel disarming event. Go to step 7 for further information.

7. To define the actions for the heartbeat, panel arm and panel disarm alarms that are reported by the intrusion panel, click ⚙ and do the following:

   a) Click the **Arming Schedule** tab. Click the timeline of the desired day of the week. The *Edit schedule* window pops up. Enter the start and end times of the arming schedule and click **Save**.

   You can define up to eight different periods during a day, and a different schedule for each day of the week.

   **Note**: The time periods defined cannot overlap.

   b) Click the **Actions** tab. Select the method by which you want the recorder to notify you of the intrusion panel alarm: Enable Alarm Audio, Notify Alarm Host, Send Email (see page 96 for the description of these alarm response types).

   c) Specify which alarm outputs are triggered when an alarm occurs.

   d) Select the cameras to be triggered (recorded) when an intrusion panel alarm is detected.

   Under **PTZ Linking**, enable the preset, preset tour or shadow tour to be triggered when the alarm is detected and enter the preset, preset tour or shadow tour number.

e) Click **OK** to save the changes and return to the *Intrusion Panel Setup* window.

8. Click **Save** to save the intrusion panel setup parameters.

# TVRMobile push notifications

TVRMobile 3.0 (and higher) can receive events from the recorder.

The ‘Push notifications’ feature lets TVRMobile notify a user of new messages or events even when the user is not actively using TVRMobile.

In TVRMobile, events can be received from the recorder and these events can be shown as a push notification to the user.

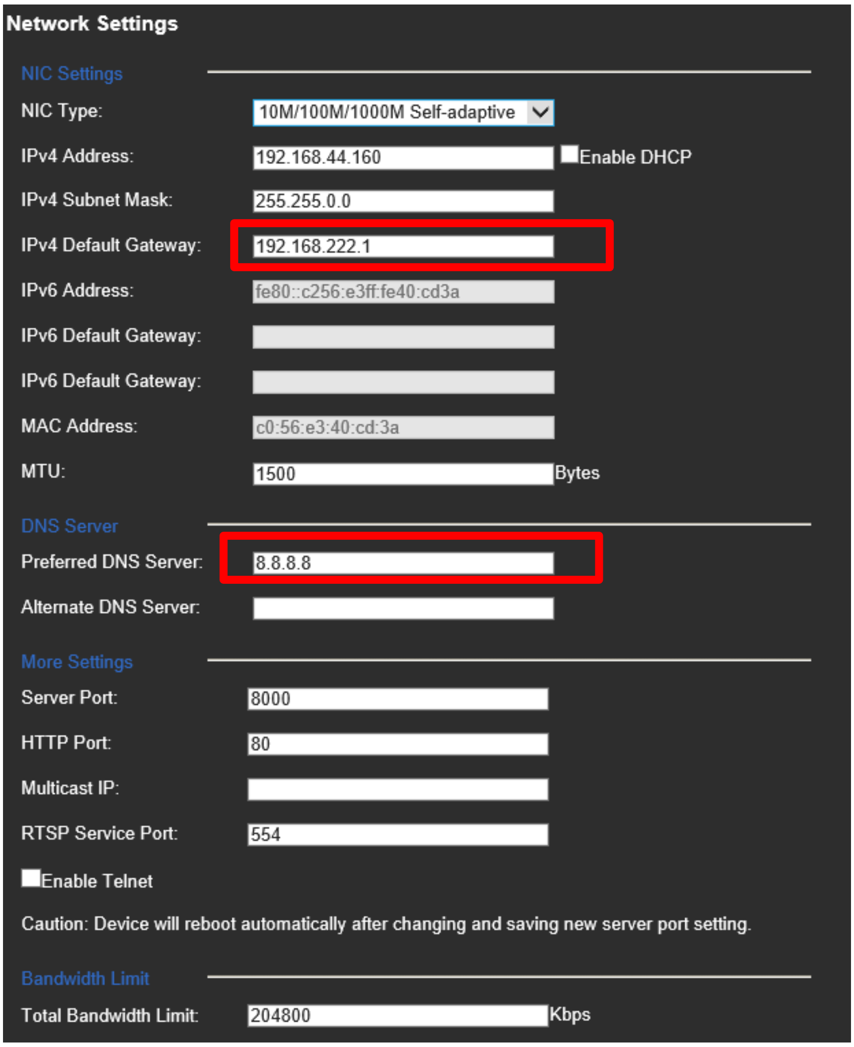
The recorder needs to be connected to the internet to be able to use push notifications. Even when the phone or tablet is used via Wi-Fi on the same LAN as the recorder, an internet connection is required.

## Which network settings are needed in the recorder and the local network?

In the recorder a user needs to set up the default gateway address and the DNS address.

The default gateway address can be the IP address of the router.

The DNS address can be the DNS of the ISP or you can also use the Google DNS address (8.8.8.8).



Network Settings

NIC Settings

NIC Type: 10M/100M/1000M Self-adaptive

IPv4 Address: 192.168.44.160 □ Enable DHCP

IPv4 Subnet Mask: 255.255.0.0

IPv4 Default Gateway: 192.168.222.1

IPv6 Address: fe80::c256:e3ff:fe40:cd3a

IPv6 Default Gateway:

IPv6 Default Gateway:

MAC Address: c0:56:e3:40:cd:3a

MTU: 1500 Bytes

DNS Server

Preferred DNS Server: 8.8.8.8

Alternate DNS Server:

More Settings

Server Port: 8000

HTTP Port: 80

Multicast IP:

RTSP Service Port: 554

□ Enable Telnet

Caution: Device will reboot automatically after changing and saving new server port setting.

Bandwidth Limit

Total Bandwidth Limit: 204800 Kbps

As well as the DNS and default gateway settings, the user will need to also set up port forwarding for the following ports:

- HTTP port (default: 80) (*)
- RTSP port (default: 554) (*)
- Server port (default: 8000)

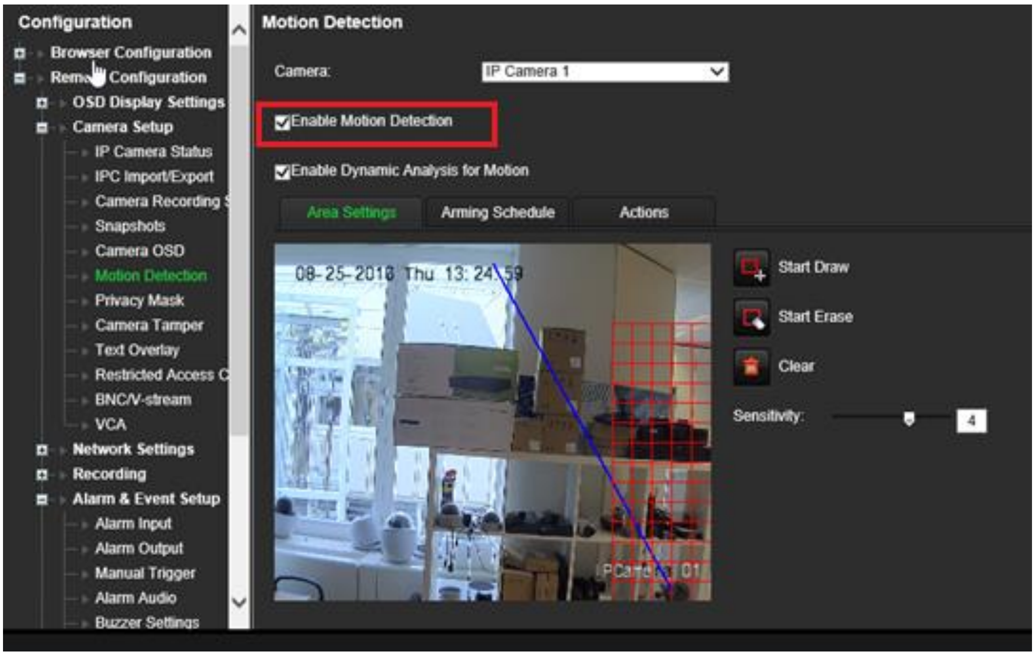
(*) Some ISPs block the use of port 80 and/or 554. When these ports are blocked, use a port number higher than 1024.

## How to set up push notifications in the recorder

As an example, we will set up push notifications for motion detection.

Steps to follow:

1. Set up motion detection for a camera



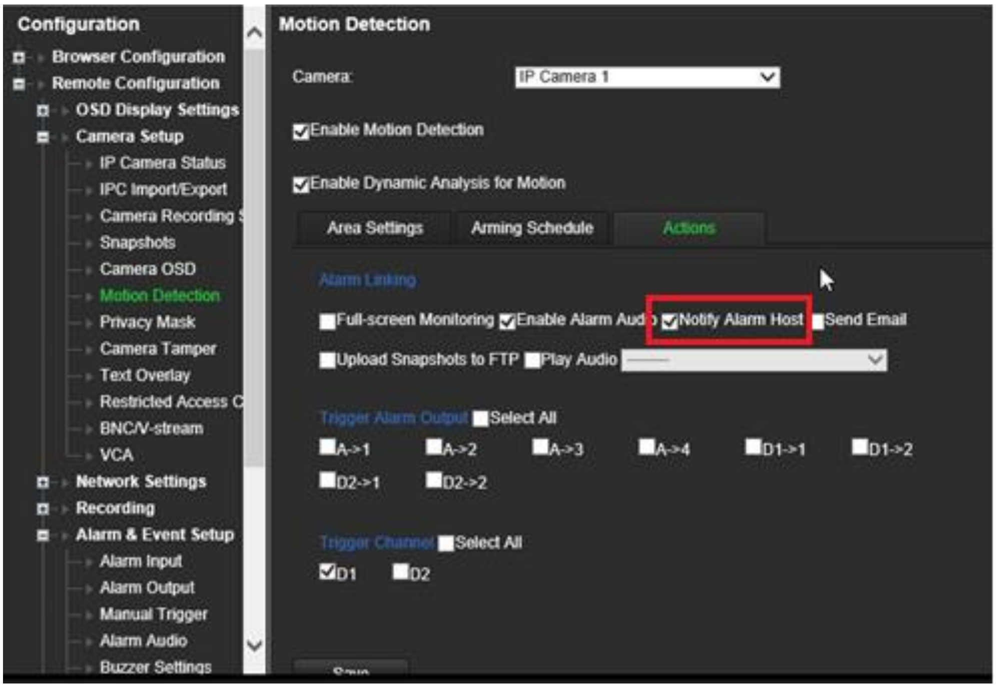
Camera: IP Camera 1

☑ Enable Motion Detection

☑ Enable Dynamic Analysis for Motion

Sensitivity: 4

2. Select **Notify Alarm Host** as an action for motion detection.



Camera: IP Camera 1

☑ Enable Motion Detection

☑ Enable Dynamic Analysis for Motion

Alarm Linking

□ Full-screen Monitoring ☑ Enable Alarm Aud ☑ Notify Alarm Host □ Send Email

□ Upload Snapshots to FTP □ Play Audio

Trigger Alarm Output □ Select All

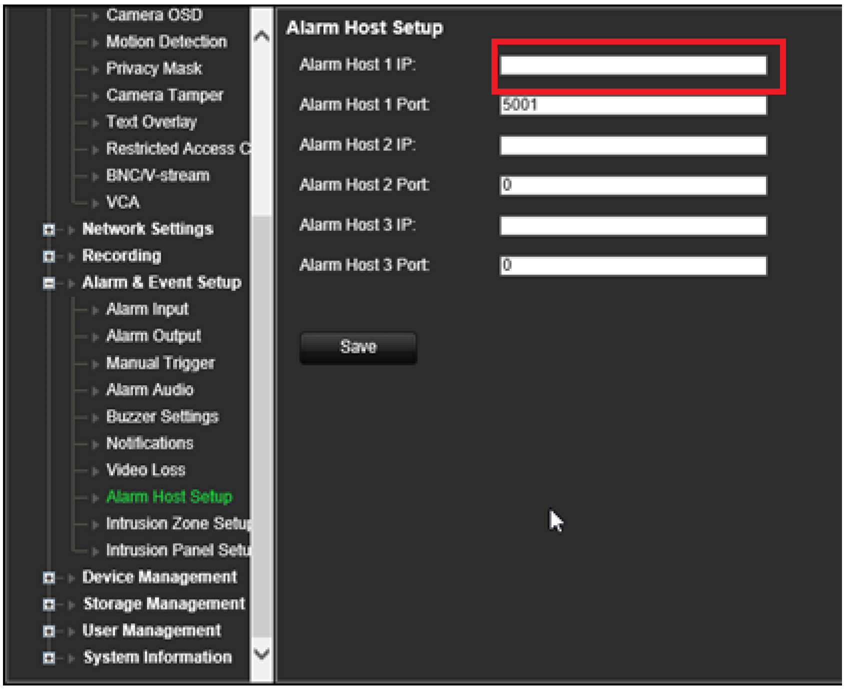
□ A->1 □ A->2 □ A->3 □ A->4 □ D1->1 □ D1->2

□ D2->1 □ D2->2

Trigger Channel □ Select All

☑ D1 □ D2

3. The user does not need to enter a destination address in the *Alarm Host* setup window.



Alarm Host Setup

Alarm Host 1 IP:

Alarm Host 1 Port: 5001

Alarm Host 2 IP:

Alarm Host 2 Port: 0

Alarm Host 3 IP:

Alarm Host 3 Port: 0

**Note:** For information on setting up TVRMobile and displaying information on the app, please refer to the TVRMobile user manual.

# Disable Actions

The *Disable Actions* feature allows you to disable the execution of the event/alarm actions and to influence the recording behavior, based on the arming status of an alarm panel.

The actions associated with motion detection, VCA, and alarms (alarm inputs or intrusion panel events) can be disabled when the alarm panel is disarmed. This will avoid users receiving unnecessary notifications (push notifications, emails, events in TruVision Navigator) or triggering actions (alarm output, PTZ preset, ...).

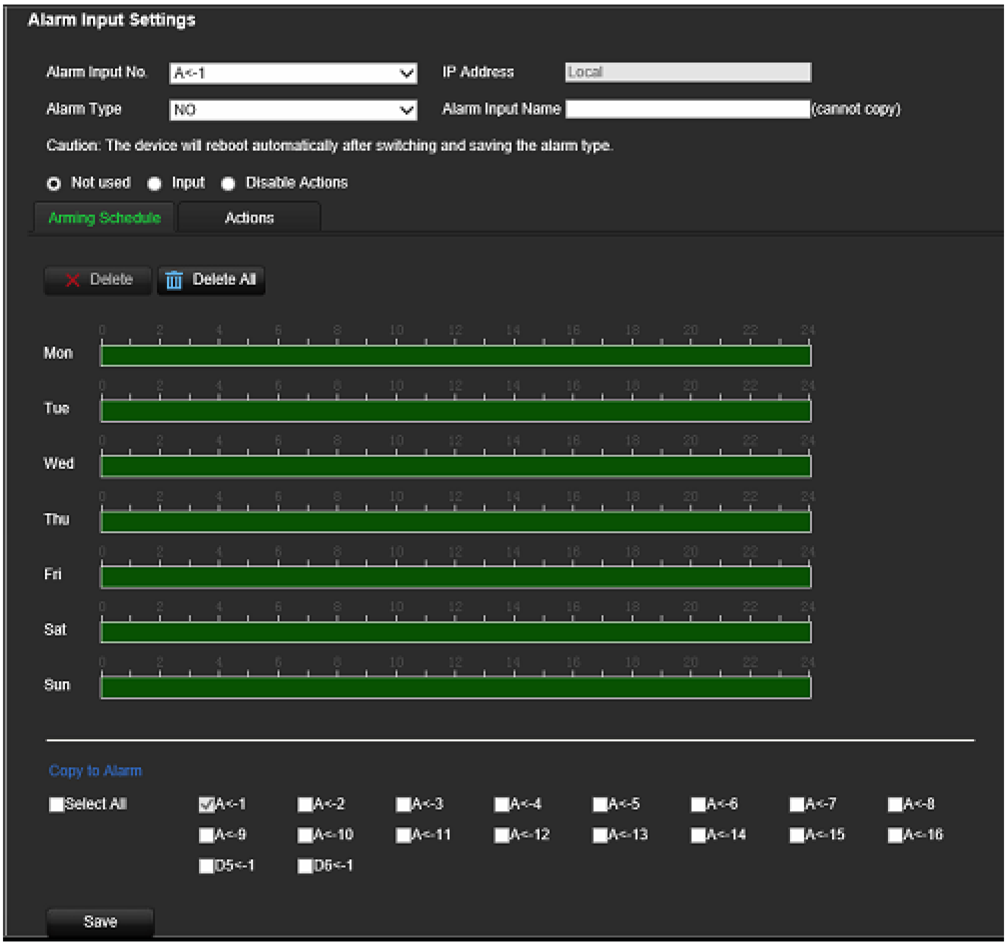
When the panel is armed again, the recorder will resume its scheduled operation and execute the configured actions and recordings.

The Disable Actions function can be used via alarm input one or via the OH integration.

The function can also be used with non-Aritech alarm panels.

**To set-up Disable Actions via alarm input 1:**

1. From the menu toolbar, click **Alarm & Event Setup** > **Alarm Input Settings**.



Alarm Input Settings

Alarm Input No. A<-1

IP Address Local

Alarm Type NO

Alarm Input Name (cannot copy)

Caution: The device will reboot automatically after switching and saving the alarm type.

○ Not used ● Input ● Disable Actions

☐ Select All ☑ A<-1 ☐ A<-2 ☐ A<-3 ☐ A<-4 ☐ A<-5 ☐ A<-6 ☐ A<-7 ☐ A<-8
☐ A<-9 ☐ A<-10 ☐ A<-11 ☐ A<-12 ☐ A<-13 ☐ A<-14 ☐ A<-15 ☐ A<-16
☐ D5<-1 ☐ D6<-1

2. Select **Disable Actions** for alarm input 1. The Disable Actions function is only available for alarm input 1.

   **Note**: Although there is a copy function foreseen when you enable the feature, Disable Actions can only be used for alarm input 1.

3. Make sure the alarm panel has a relay contact to connect it to the recorder. Connect one wire to alarm input 1 and connect the other wire to one of the Ground (‘G’) connections.

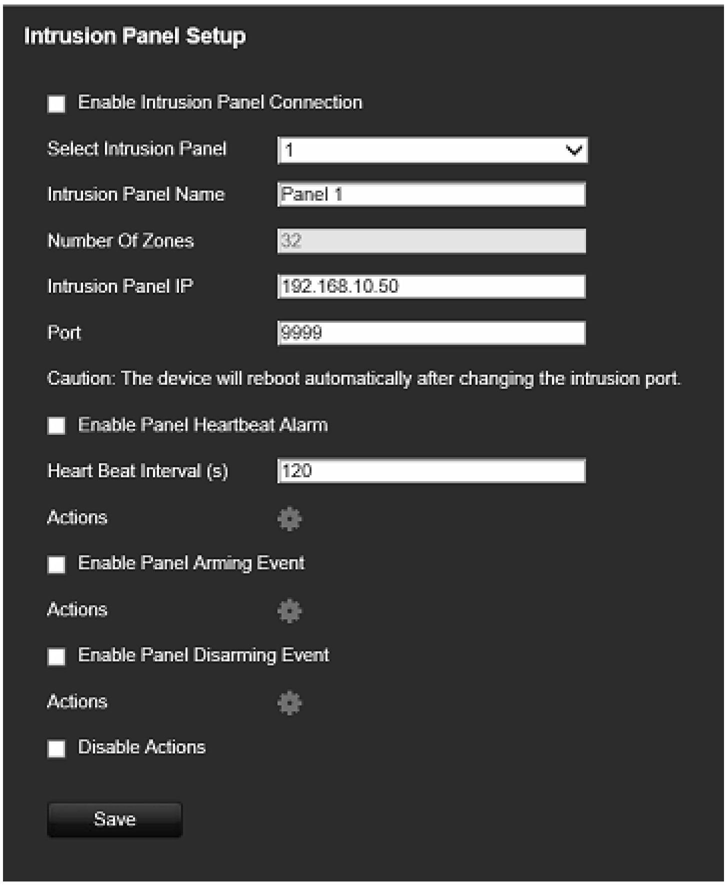
4. Select the alarm input type, NO (normally open) or NC (normally closed). Default is NO.

5. When the alarm input is triggered, the actions for motion detection and VCA will be disabled.

6. Click **Save** to save the changes.

**To set-up Disabled Actions via the alarm panel (OH integration):**

1. From the menu toolbar, click **Alarm & Event Setup** > **Intrusion Panel Setup**.



**Intrusion Panel Setup**

□ Enable Intrusion Panel Connection

Select Intrusion Panel: 1

Intrusion Panel Name: Panel 1

Number Of Zones: 32

Intrusion Panel IP: 192.168.10.50

Port: 9999

Caution: The device will reboot automatically after changing the intrusion port.

□ Enable Panel Heartbeat Alarm

Heart Beat Interval (s): 120

Actions ⚙

□ Enable Panel Arming Event

Actions ⚙

□ Enable Panel Disarming Event

Actions ⚙

□ Disable Actions

Save

2. Select **Disable Actions** for the desired alarm panel connection. Three alarm panels can be linked to the recorder. You can enable Disable Actions for each panel.

   Make sure that you also set up the other parameters for the alarm panel. See “Intrusion integration alarm reporting” on page 99 for further information.

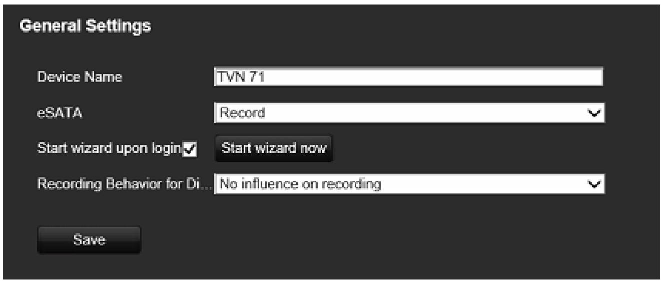
3. Click **Save** to save the changes.

4. When the alarm panel sends a SIA/XSIA event for disarming (OP message), the recorder will not execute the actions anymore for motion detection and VCA or for alarms (alarm inputs or intrusion panel events).

   **Note**: the actions that are set-up for the disarming event will also no longer be executed. This is a known limitation.

**To define the recording behavior when Disable Actions is used:**

1. From the menu toolbar, click **Device Management** > **General Settings**.



**General Settings**

Device Name: TVN 71

eSATA: Record

Start wizard upon login ☑ Start wizard now

Recording Behavior for Di...: No influence on recording

Save

2. Select one of the options for **Recording Behavior for Disable Actions**. The options are:

**No influence on recording**: Disable Actions will have no influence on the recordings. Recording of all cameras will continue as scheduled.

**Disable event/alarm recordings**: Disable Actions will stop the scheduled recordings for events (motion, VCA) and alarms (alarm inputs, intrusion panel alarms). Cameras that are scheduled for continuous recording will not stop the recording.

**Disable all recordings**: Disable Actions will stop all recordings for all cameras, regardless of the schedule or recording type.

3. Click **Save** to save the changes.

## Alarm output behavior for Disable Actions

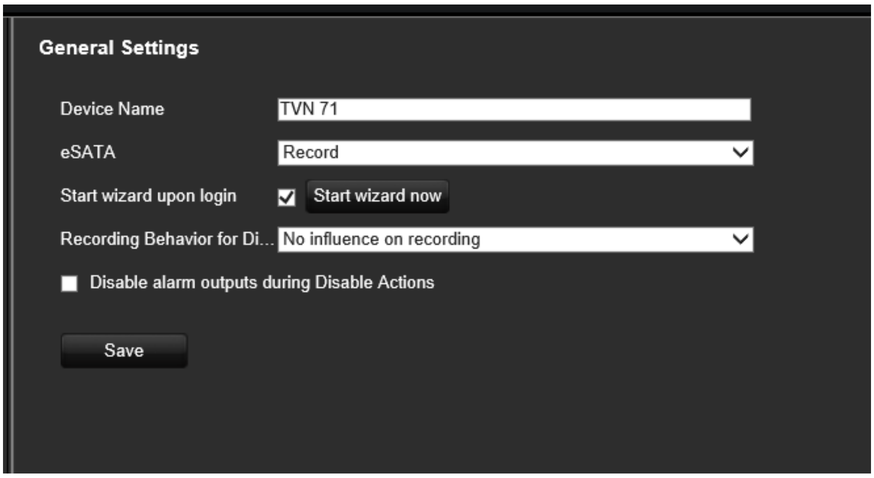
You can select the behavior of the alarm outputs when Disable Actions is active.

This feature is only available in web mode.

For further information on Disable Actions, see “Disable Actions” on page 107.

### To disable the use of alarm outputs when Disable Actions is active:

1. From the menu toolbar, click **Configuration** > **Device Management** > **General Settings**.
2. Select **Disable alarm outputs during Disable Actions** check box.



General Settings

Device Name: TVN 71

eSATA: Record

Start wizard upon login: ☑

Recording Behavior for Di...: No influence on recording

□ Disable alarm outputs during Disable Actions

This function is disabled by default, which allows the alarm outputs to be used when Disable Actions is enabled.

3. Click **Save**.

# Chapter 14
# Device management

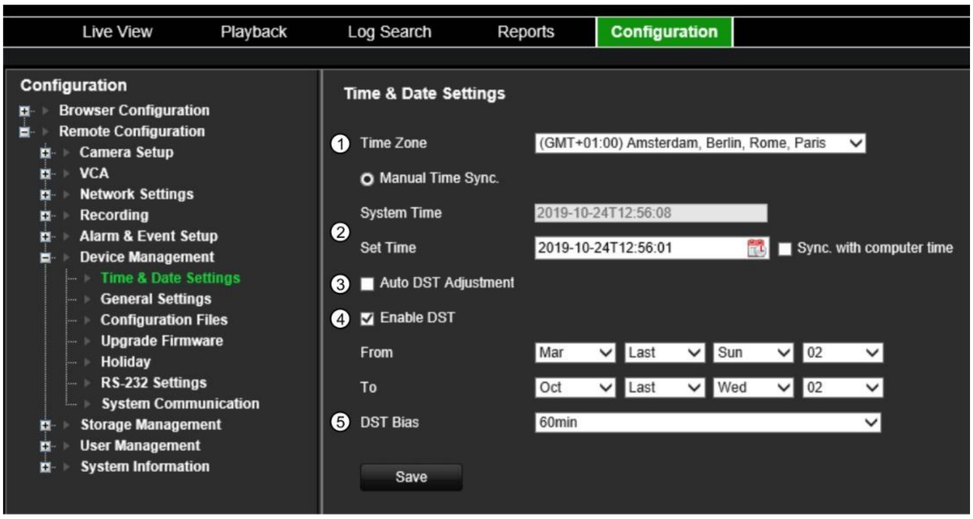
This chapter describes how to:

- Set up the time and date of the recorder
- Set up general system parameters such as the device name and eSATA as well as enable the wizard to start upon login
- Import/export configuration files
- Upgrade the firmware
- Set up holiday periods
- Configure RS-232 settings

## Time and date settings

You can set up the date and time that will appear on-screen as well as on time stamped recordings. The start and end time of daylight-saving time (DST) in the year can also be set. DST is deactivated by default. See Figure 21 below for the Time settings screen.

**Figure 21: Time and date settings window**



Time & Date Settings

1 Time Zone: (GMT+01:00) Amsterdam, Berlin, Rome, Paris

○ Manual Time Sync.

System Time: 2019-10-24T12:56:08

2 Set Time: 2019-10-24T12:56:01 □ Sync. with computer time

3 □ Auto DST Adjustment

4 ☑ Enable DST

From: Mar, Last, Sun, 02

To: Oct, Last, Wed, 02

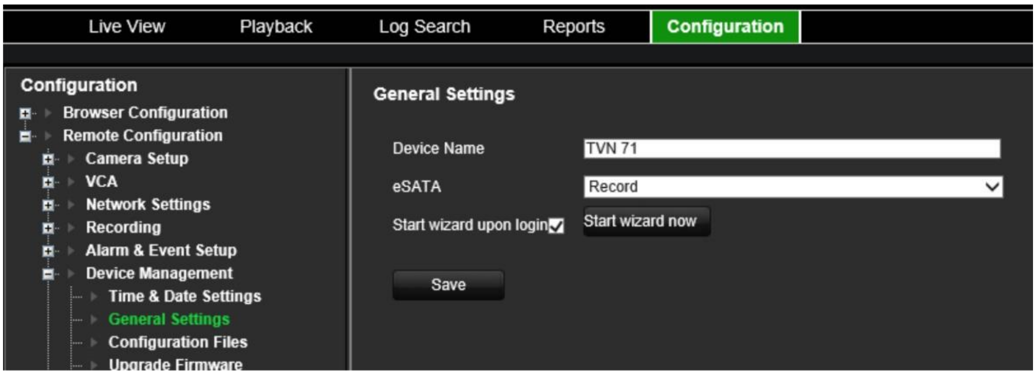
5 DST Bias: 60min

| Option | Description |
|---|---|
| 1. Time Zone | Select a time zone from the list. |
| 2. System Time | The system time is set up in the Wizard or can be set up via the **Set Time** field |
| Set Time | Enter the system date and time. Default is the current date and time. Time is always in 24-hour format. |
| 3. Auto DST Adjustment | Enable to activate DST is automatically.  It depends on the time zone selected. Default is Disable. |
| 4. Enable DST | Manually define DST. If this option is selected, the *Auto DST adjustment* option is disabled. Default is Disable.<br>Click the check box to enable or disable daylight savings time (DST). |
| From | Enter the start date and time for daylight savings. |
| To | Enter the end date and time for daylight savings. |
| 5. DST Bias | Set the amount of time to move DST forward from the standard time. Default is 60 minutes. |

# General recorder settings

Use the Device Management menu to configure the recorder name, manage an external eSATA device, and to start the wizard at login.

**Figure 22: General settings of the recorder**



General Settings

Device Name: TVN 71

eSATA: Record

Start wizard upon login ☑

| Option | Description |
|---|---|
| 1. Device Name | Define the recorder name. The default name is TVN 71.<br>Click the edit box and enter the new name from the soft keyboard. |
| 2. eSATA | Configure the e-SATA device to record or archive video. |
| 3. Start Wizard upon login | This will immediately start the wizard.   The system is not rebooted. Default is Disable. |

### Using an eSATA recording device

You can use an external storage device, such as an eSATA HDD, to backup video or to add its recording capacity to that of the recorder itself. If you change this option, you must reboot the recorder to implement the change.

**To define how the eSATA device is used:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** >**Device Management** > **General Settings**.
2. Under eSATA, select one of the two options:

   **Record**: Extend the recording capacity of the recorder.

   **Archive**: Backup data onto an eSATA backup device.

   **Note**: If the external storage device is part of the total internal capacity of the recorder, then it is no longer available for backing up video.
3. Click **Save** to save the settings.

## Configuration files

You can export and import configuration settings from the recorder. This is useful if you want to copy the configuration settings to another recorder, or if you want to make a backup of the settings.

This menu also allows you to reboot the unit, and restore default factory settings

### Restart the recorder

**To restart the recorder:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Device Management** > **Configuration Files**.
2. Click the **Restart** button.

   **Note**: Only the administrator can reboot the unit.
3. In the pop-up window, enter your admin password and click **OK**.

   The system reboots.

### Restore default settings

The administrator can reset the recorder to the factory default settings. Network information such as IP address, subnet mask, gateway, MTU, NIC working mode, server port, and default route are not restored to factory default settings

**Note**: Only the administrator can restore factory default settings.

**To restore parameters to default factory settings:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Device Management** > **Configuration Files**.
2. To restore all parameters, except network settings, to default factory settings: Click the **Restore** button. Enter the Admin password, click **OK**, and then click **Yes** to confirm that you want to restore all parameters except network settings to default.

   — Or —

   To restore all parameters to default factory settings: Click the **Default** button. Enter the Admin password, click **OK**, and then click **Yes** to confirm that you want to restore all parameters to default.

   The changes are immediately implemented.

## Import and export files

Insert an external storage device in the recorder. Go to the **Configuration** > **Remote Configuration** > **Device Management** > **Configuration Files** to import or export configuration settings.

To export the recorder’s configuration parameters into an external storage device, click the **Export** button**.**

To import configuration parameters from an external storage device, enter the location of the file to select it and click **Import**.

# Upgrade system firmware

The firmware on the recorder can be updated using three methods:

- Via a USB device
- Via the recorder web browser
- Using TruVision Navigator. For further information, refer to the TruVision Navigator user manual.

The firmware upgrade file is labeled *TVN71.dav*.

**To update the system firmware using the browser:**

1. Download the latest firmware from our web site at:

   https://firesecurityproducts.com/products/video/recorders
2. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Device Management** > **Upgrade Firmware**.
3. Select the firmware file and click **Upgrade**. Click **Yes** to begin the upgrade process.
4. When the upgrade process is completed, the recorder will reboot automatically.

# Holiday schedules

It is possible to indicate holidays for which you can create a separate recording schedule. Once one or more holidays are created, a separate entry for holiday will be included in the recording schedule (refer to “Recording schedule” on page 87 of the manual)

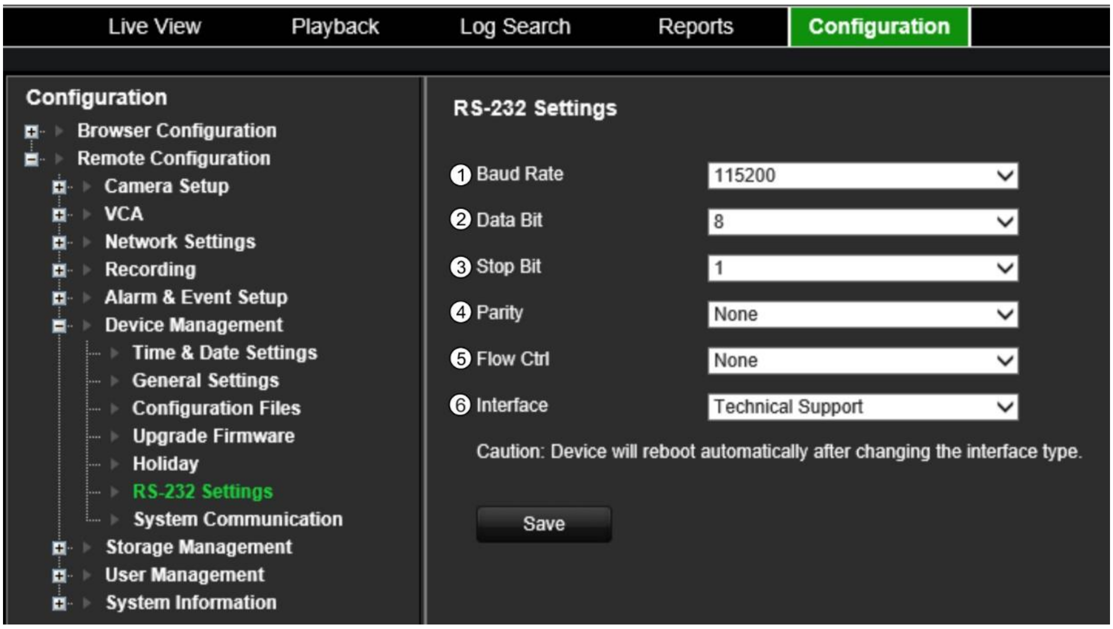
**To set up a holiday recording schedule:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Device Management** > **Holiday**.
2. Select a holiday period from the list and click its **Edit** button to modify the settings. The Edit window appears.
3. Enter the name of the holiday period and click **Enable Holiday**.
4. Select whether the holiday period will be categorized by date, week, or month and then enter the start and end dates.
5. Click **OK** to save the settings and return to the Holiday window.
6. Repeat steps 2 to 5 for other holiday periods.
7. Click **Save** to save the settings.

# Configure the RS-232 port

Use the RS-232 menu under **Device Management** to configure the RS-232 parameters such as baud rate, data bit, stop bit, parity, flow control, and interface.

**Figure 23: RS-232 setup window**



RS-232 Settings

1 Baud Rate: 115200

2 Data Bit: 8

3 Stop Bit: 1

4 Parity: None

5 Flow Ctrl: None

6 Interface: Technical Support

Caution: Device will reboot automatically after changing the interface type.

| Option | | Description |
|---|---|---|
| 1. | Baud Rate | This is a measure of the speed of data transmission. Default is 115200. |
| 2. | Data Bit | A bit is the smallest unit of data in a serial communication message. A data bit is the bit carrying the information, as opposed to the start bit and the stop bit. Default is 8. |
| 3. | Stop Bit | Stop bits mark the end of a transmission of a serial communication message.<br>Default is 1. |
| 4. | Parity | The method used to detect errors in the number of bits being transmitted. Default is None. |
| 5. | Flow Ctrl | Flow control is the process by which data transfer is regulated so that it does not arrive too quickly for the receiving process. Default is None. |
| 6. | Interface | This shows how the RS-232 port can be used. It is used by Technical Support only.<br>**Technical Support**: Console mode. |

# Chapter 15
# Storage management

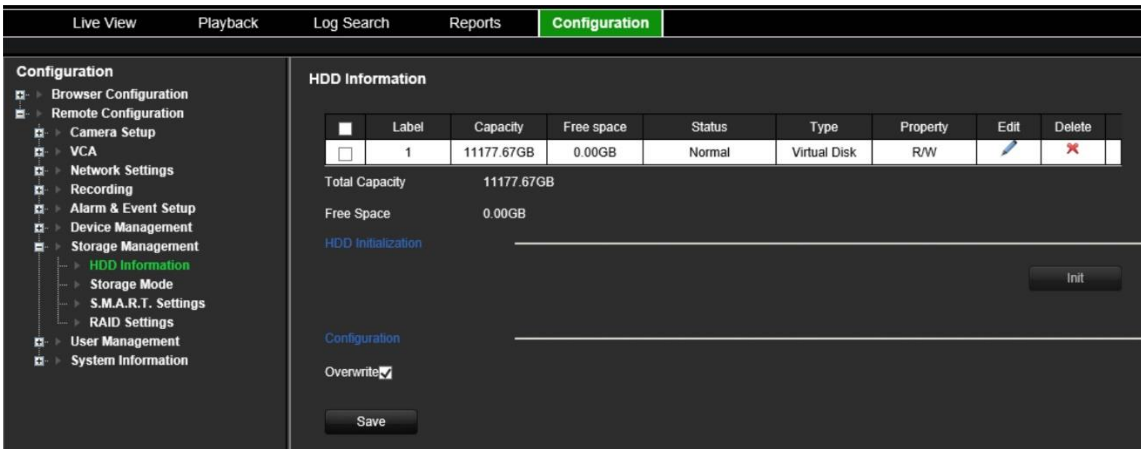
This chapter describes the content of the Storage Management menu, including HDD information, Storage Mode, S.M.A.R.T. settings as well as RAID settings.

## HDD information

You can check the status of any of the installed HDDs on the recorder at any time.

**To check the status of a HDD:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Storage Management** > **HDD Information**.



HDD Information

| □ | Label | Capacity | Free space | Status | Type | Property | Edit | Delete |
|---|---|---|---|---|---|---|---|---|
| □ | 1 | 11177.67GB | 0.00GB | Normal | Virtual Disk | R/W | ✎ | ✖ |

Total Capacity 11177.67GB

Free Space 0.00GB

Overwrite ☑

2. Note the status of the HDDs listed under the Status column.

   If the status is listed as Normal or Sleeping, the HDD is in working order. If it is listed as Abnormal and has already been initialized, the HDD needs to be replaced. If the HDD is Uninitialized, you need to initialize it before it can be used in the recorder. Refer to “Initialize a HDD” below for more information.

**Note**: The status information is also shown in the **System Information > HDD** window.

## Initialize a HDD

The HDDs delivered with the unit do not need to be initialized before they can be used. When reusing HDDs, you can also re-initialize the HDD. However, all data on the HDD will be erased.

**To initialize a HDD:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Storage Management** > **HDD Information**.
2. Click **Select All** to select all the HDDs.
3. Click the **Init** button to begin initialization.

   After the HDD has been initialized, the status of the HDDs changes from Abnormal to Normal.

## Overwrite a HDD

You can select how the recorder responds when the HDDs become full and there is no longer enough space to save new data. The overwrite option is enabled by default.

**To enable overwrite when the HDDs are full:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Storage Management** > **HDD Information**.
2. Enable **Overwrite**.

**Caution**: If the overwrite option is disabled and the quota management capacity for a channel is set to zero, the recordings on that channel can still be overwritten. To avoid this happening, set a quota level for the channel or use the group management mode.

3. Click **Save** to save the settings.

# Install HDDs

You can install up to 16 HDDs in the recorder.

**Caution:** Do not insert or remove HDDs with the recorder powered up.

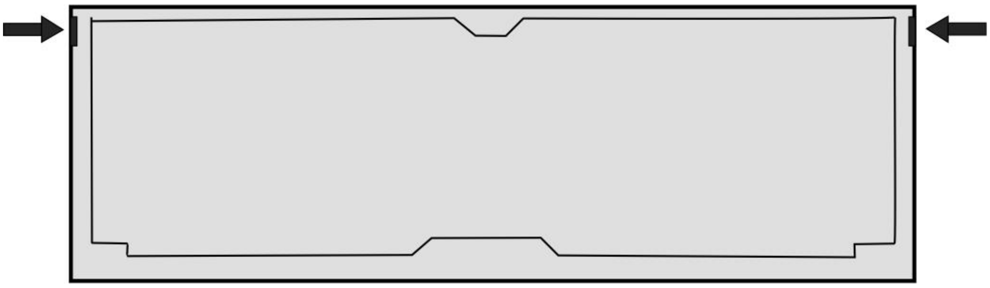
**Note:** This unit contains electrostatic-sensitive components. Before handling the HDDs, make sure you are properly grounded to avoid ESD damage.

**To install a HDD:**

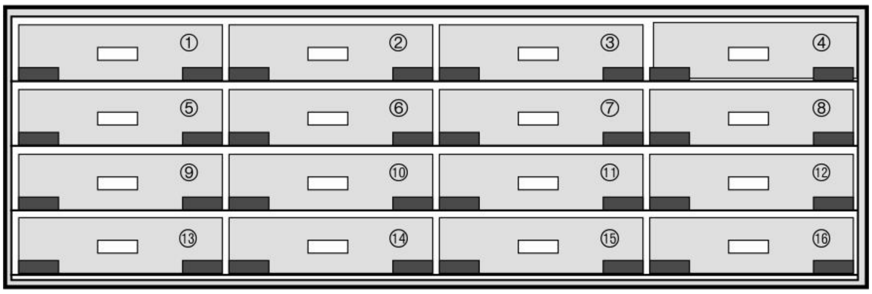
1. Unpack the recorder box.
2. Unpack the recorder HDD box.

   **Note:** HDDs for the TVN 71 are delivered separately from the chassis box due to shipping weight.

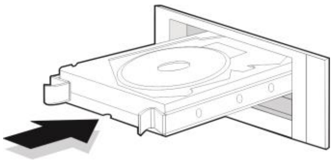
3. Use the key provided in the accessories box to unlock the recorder front panel.
4. Press the latches on both sides of the front panel to open it.



5. Install the HDDs as shown below. The first drive in position number 1, the second drive in position number 2, etc. Continue to install all the hard drives in numerical order.



6. Insert a HDD into one of the HDD bays until it has fully seated into position. Repeat with the rest of the HDDs.



7. Close and re-lock the front panel.

   **Note:** The HDDs must be installed BEFORE powering up the unit. The drives are defaulted to a single HDD group that is automatically ready to record once cameras are added and configured with recording schedules.

8. Apply the supplied label to the recorder chassis. Place it next to the original label without covering it.

   **Note**: Failure to install the label will affect the warranty of the recorder.

9. Initialize the new HDDs, if needed. See “Initialize a HDD” on page 118.

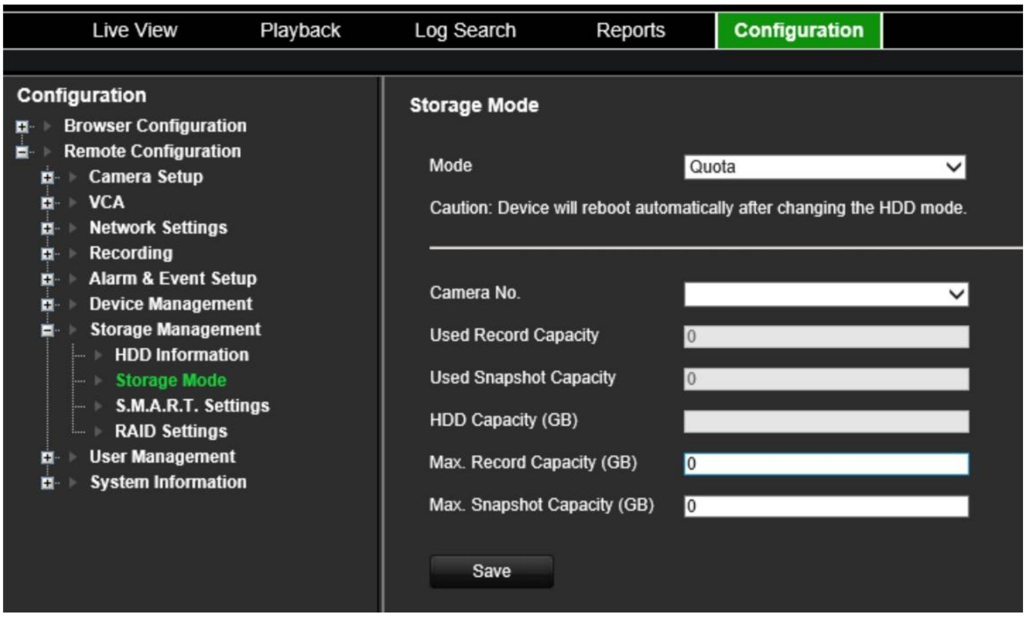
## Storage mode

To ensure an efficient use of the storage space available on HDDs, you can control an individual camera’s storage capacity using HDD quota management. This function lets you allocate different storage capacities for both recordings and snapshots to each camera.

**Note**: If the overwrite function is enabled, the maximum capacity for both recordings and snapshots is set to zero by default.

**To set the HDD quota for a camera:**

1. From the menu toolbar, click **Configuration** > **Storage Management** > **Storage Mode**.



Storage Mode

| | |
|---|---|
| Mode | Quota |

Caution: Device will reboot automatically after changing the HDD mode.

| | |
|---|---|
| Camera No. | |
| Used Record Capacity | 0 |
| Used Snapshot Capacity | 0 |
| HDD Capacity (GB) | |
| Max. Record Capacity (GB) | 0 |
| Max. Snapshot Capacity (GB) | 0 |

2. Under the Mode option, select **Quota**.

   **Note**: The recorder will reboot automatically if you change the HDD mode.

3. Select a camera whose storage capacity you want to change and enter the values in GB for the maximum record capacity and snapshot capacities. The available quota space available is displayed on screen.

4. If you want to copy these values to other cameras, select each camera individually.

5. Click **Save** to save the settings.

## Group HDDs

Your recorder can organize multiple HDDs into groups. Videos from specified channels can be set to be recorded onto a HDD group. You could, for example, save the records from a couple of high priority cameras to one HDD, and save the recordings from all the other cameras to another HDD.

**To set up an HDD group:**

1. From the menu toolbar, click **Configuration** > **Storage Management** > **Storage Mode**.

2. Under **Mode**, select **Group**.

   **Note**: The recorder will reboot automatically if you change the HDD mode.

3. Under **Record on HDD Group**, select a number for the HDD group.

4. Check the channels to be added to this group.

   **Note:** By default, all channels belong to HDD group 1.

5. Click **Save** to save the settings.

**Important**: You can add the same camera to more than one group. However, there is no parallel recording across HDDs. When a camera is in more than one group and the first HDD fails, the second HDD only then takes over the recording of that camera.

## Dual streaming capacity

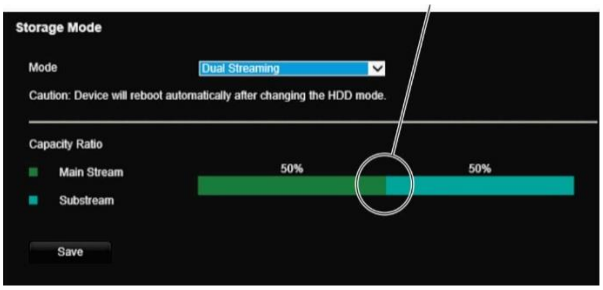
You can set up the recorder so that it records both main stream and substream. Doing so will allow you to, via the browser or TruVision Navigator, get access to the substream in both live & playback. You are also able to set the dual stream ratio. This can be useful, for example, if you have bandwidth limitations as you can then adjust the ratio to record more substream than main stream.

### To set up dual streaming mode:

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Storage Management** > **Storage Mode**.
2. Under the **Mode** option, select **Dual Streaming**.

   **Note**: The recorder will reboot automatically if you change the HDD mode.
3. Under **Capacity Ratio**, use the mouse to adjust the main stream/substream storage ratio. By default, the ratio is 50:50.

Move the slider left/right to adjust the capacity ratios



Storage Mode

Mode: Dual Streaming

Caution: Device will reboot automatically after changing the HDD mode.

Capacity Ratio

Main Stream: 50%

Substream: 50%

4. Click **Save** to save the settings.

# S.M.A.R.T. settings

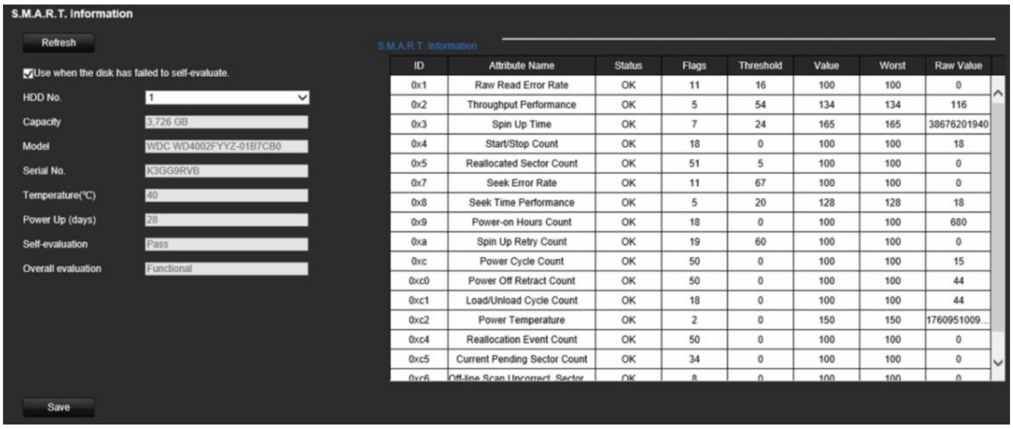
S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology) reports on a variety of hard drive attributes. It helps ensure that the HDD always functions correctly while protecting video stored on the hard drive.

**Note**: A recorder with RAID functionality does not support S.M.A.R.T.

### To view the S.M.A.R.T. information of a HDD:

1. From the menu toolbar, click **Configuration** > **Storage Management** > **S.M.A.R.T. Settings.**

2. Select the HDD whose data you want to see. A detail listing of S.M.A.R.T. information is displayed.



S.M.A.R.T. Information

☑ Use when the disk has failed to self-evaluate.

HDD No.: 1

Capacity: 3,726 GB

Model: WDC WD4002FYYZ-01B7CB0

Serial No.: K3GG9RVB

Temperature(°C): 40

Power Up (days): 28

Self-evaluation: Pass

Overall evaluation: Functional

S.M.A.R.T. Information

| ID | Attribute Name | Status | Flags | Threshold | Value | Worst | Raw Value |
|---|---|---|---|---|---|---|---|
| 0x1 | Raw Read Error Rate | OK | 11 | 16 | 100 | 100 | 0 |
| 0x2 | Throughput Performance | OK | 5 | 54 | 134 | 134 | 116 |
| 0x3 | Spin Up Time | OK | 7 | 24 | 165 | 165 | 38676201940 |
| 0x4 | Start/Stop Count | OK | 18 | 0 | 100 | 100 | 18 |
| 0x5 | Reallocated Sector Count | OK | 51 | 5 | 100 | 100 | 0 |
| 0x7 | Seek Error Rate | OK | 11 | 67 | 100 | 100 | 0 |
| 0x8 | Seek Time Performance | OK | 5 | 20 | 128 | 128 | 18 |
| 0x9 | Power-on Hours Count | OK | 18 | 0 | 100 | 100 | 680 |
| 0xa | Spin Up Retry Count | OK | 19 | 60 | 100 | 100 | 0 |
| 0xc | Power Cycle Count | OK | 50 | 0 | 100 | 100 | 15 |
| 0xc0 | Power Off Retract Count | OK | 50 | 0 | 100 | 100 | 44 |
| 0xc1 | Load/Unload Cycle Count | OK | 18 | 0 | 100 | 100 | 44 |
| 0xc2 | Power Temperature | OK | 2 | 0 | 150 | 150 | 1760951009... |
| 0xc4 | Reallocation Event Count | OK | 50 | 0 | 100 | 100 | 0 |
| 0xc5 | Current Pending Sector Count | OK | 34 | 0 | 100 | 100 | 0 |
| 0xc6 | Off-line Scan Uncorrect. Sector | OK | 8 | 0 | 100 | 100 | 0 |

3. If you want to continue to use a HDD when the S.M.A.R.T. test has failed, check the box **Use when the disk has failed to self-evaluate**.

4. Click **Save** to save the settings.

# RAID settings

RAID is data storage technology. It combines multiple HDDs into a single logical unit for the purposes of data redundancy or performance improvement.

**Note:** RAID settings are only available when using a TVN 71 RAID model (TVN-7101R-xxT).

## Data recovery and manual rebuild

You can recover the data when a HDD fails depending on the RAID level.

See Table 5 below for a description of the different RAID levels and data recovery.

**Table 5: Data recovery by RAID level**

| RAID level | Number of HDDs | What it does | Recovery in case of a HDD failure |
|---|---|---|---|
| 0 | Minimum 2 | Data is split across two or more HDDs. Each HDD contains a part of the data. Multiple HDDs can deal with simultaneous data writing, which increases the writing speed. | Replace the failed HDD. The failure of one disk will result in total data loss. There is no backup method available for RAID 0. |
| 1 | 2 | RAID 1 creates an exact copy of a data set (data mirroring) on two HDDs. The array will continue to operate as long as at least one HDD is operational. | Replace the failed HDD and manually rebuild. |

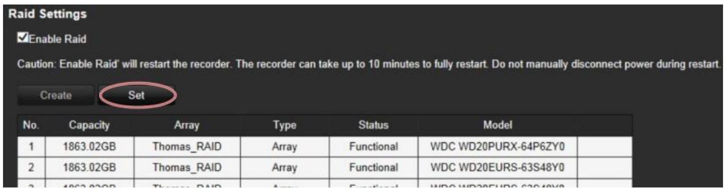
| RAID level | Number of HDDs | What it does | Recovery in case of a HDD failure |
|---|---|---|---|
| 5 | Minimum 3 | The parity information is divided over all HDDs in the array. For every HDD position, the parity information will be on one disk and the corresponding data will be on the other disk for the same position. | In a RAID 5 setup, one HDD can fail but the data will be OK.<br>When one HDD fails, the data can be restored via the parity information on the other disks. Replace the failed HDD and manually restart the rebuild process. To do this, select the new hard drive and click the **Rebuild** button. |
| 6 | Minimum 4 | RAID6 is almost the same as RAID5, but there are two parity blocks per disk. This allows a quicker rebuild process than RAID 5. | In a RAID 6 setup, two HDDs can fail, but still the data will be OK.<br>When a HDD fails, the data can be restored via the parity information of the other disks. Replace the failed HDD and manually restart the rebuild process. To do this, select the new HDD and click the **Rebuild** button. |
| 10 | Minimum 4 | It is the same as RAID 0 but in combination with RAID 1 (data mirroring) | Replace the failed HDD and manually restart the rebuild process. |

## Automatic rebuild

You can also automatically rebuild RAID 1, 5, 6, and 10.

To automatically rebuild, add an extra drive in the recorder that is not assigned to the RAID array. Configure this HDD as a backup disk (hot-spare disk). To do this, select this extra disk in the RAID settings and click the **SET** button.

**Figure 24: RAID Set button**



Raid Settings

☑ Enable Raid

Caution: Enable Raid' will restart the recorder. The recorder can take up to 10 minutes to fully restart. Do not manually disconnect power during restart.

| No. | Capacity | Array | Type | Status | Model | |
|---|---|---|---|---|---|---|
| 1 | 1863.02GB | Thomas_RAID | Array | Functional | WDC WD20PURX-64P6ZY0 | |
| 2 | 1863.02GB | Thomas_RAID | Array | Functional | WDC WD20EURS-63S48Y0 | |

Whenever a HDD fails in the RAID array, the backup/hot-spare disk will be automatically used to rebuild the array.

You can then replace the faulty hard disk and configure that new disk as the hot-spare/backup disk.

## Create a RAID array

### To create a RAID array:

1. From the menu toolbar, click **Configuration** > **Storage Management** > **RAID Settings**.

2. Click the **Enable RAID** checkbox.

   The system will automatically reboot.

**Caution**: The system can take up to 10 minutes to fully restart. Do not manually disconnect power during restart.

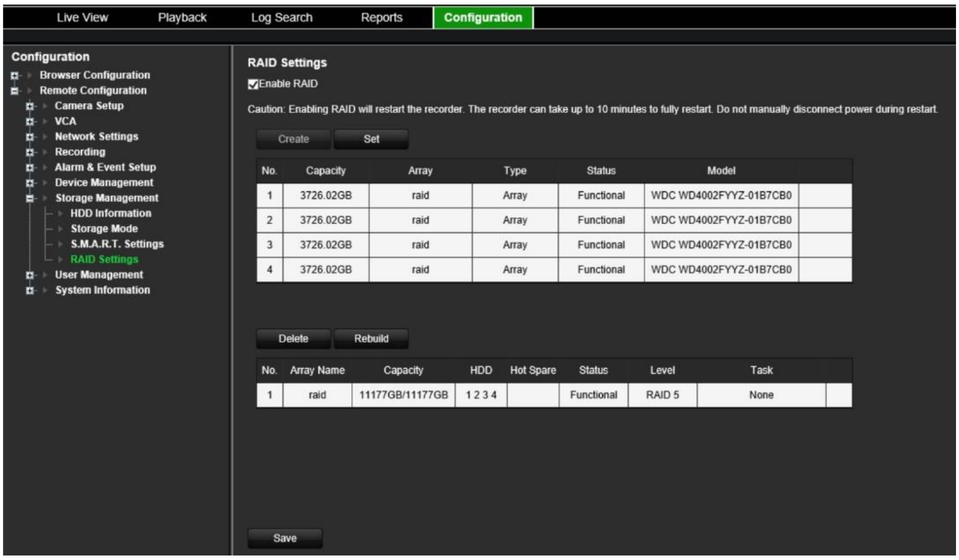
3. Once the system has restarted, go to the **Raid Settings** menu.
4. Click the **Create** button to open the “Create Array” window.
5. Enter a name for the array and select the RAID level and the drives to be included.
6. Click **OK** to start the process. When the process is complete, data on the RAID group is displayed.

   **Note:** You can create a RAID array of RAID 0, RAID 1, RAID 5, RAID 6, and RAID 10.

   - If you choose RAID 0, at least 2 HDDs must be installed.
   - If you choose RAID 1, 2 HDDs need to be configured for RAID 1.
   - If you choose RAID 5, at least 3 HDDs must be installed.
   - If you choose RAID 6, at least 4 HDDs must be installed.
   - If you choose RAID 10, 4/6/8 HDDs need to be configured for RAID 10.

**To rebuild a RAID array:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **Storage Management** > **RAID Settings**.
2. Ensure the **Enable RAID** checkbox is checked.
3. Click the **Rebuild** button to open the “Rebuild Array” window.
4. Select the HDD to include.
5. Click **Save** to start the process. When the process is complete, data on the RAID group is displayed.



RAID Settings

☑ Enable RAID

Caution: Enabling RAID will restart the recorder. The recorder can take up to 10 minutes to fully restart. Do not manually disconnect power during restart.

| No. | Capacity | Array | Type | Status | Model |
|---|---|---|---|---|---|
| 1 | 3726.02GB | raid | Array | Functional | WDC WD4002FYYZ-01B7CB0 |
| 2 | 3726.02GB | raid | Array | Functional | WDC WD4002FYYZ-01B7CB0 |
| 3 | 3726.02GB | raid | Array | Functional | WDC WD4002FYYZ-01B7CB0 |
| 4 | 3726.02GB | raid | Array | Functional | WDC WD4002FYYZ-01B7CB0 |

| No. | Array Name | Capacity | HDD | Hot Spare | Status | Level | Task |
|---|---|---|---|---|---|---|---|
| 1 | raid | 11177GB/11177GB | 1 2 3 4 |  | Functional | RAID 5 | None |

# Chapter 16
# User management

By default, the recorder comes with one user account, an Administrator account. See Table 6 below for a description of the different user accounts.

**Table 6: User accounts**

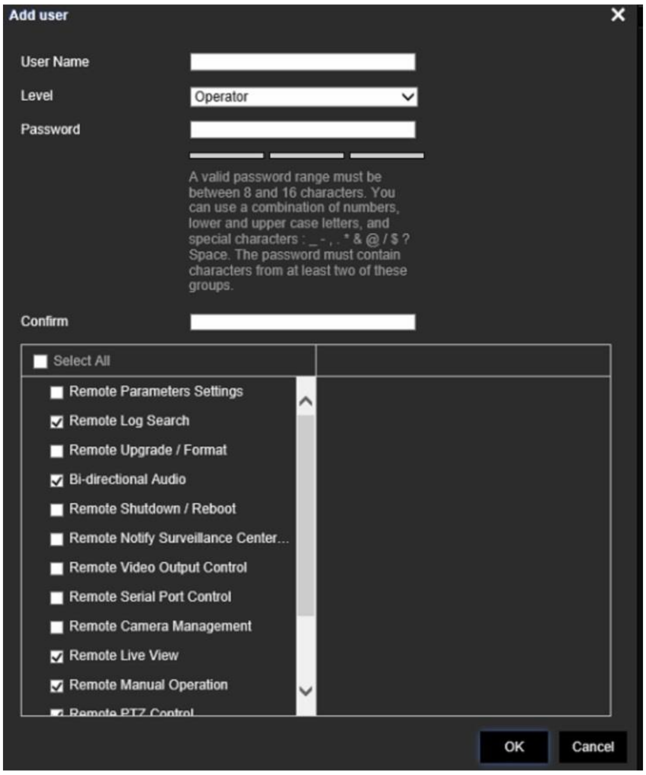
| User | Description |
|---|---|
| **Administrator** | The administrator account includes extended menu with full access to all settings. The Administrator has the authority to add, delete, or configure parameters for many of the system functions.<br>There can only be one administrator.<br>The user name is "admin". The name cannot be modified. You must define a high-security password. There is no default password provided. |

## Add a new user

Only a system administrator can create a user. You can add up to 16 new users.

**To add new users:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **User Management** > **Users**.
2. Click **Add** to enter the *Add User* window.



Add user

User Name

Level: Operator

Password

A valid password range must be between 8 and 16 characters. You can use a combination of numbers, lower and upper case letters, and special characters : _ - , . * & @ / $ ? Space. The password must contain characters from at least two of these groups.

Confirm

- ☐ Select All
- ☐ Remote Parameters Settings
- ☑ Remote Log Search
- ☐ Remote Upgrade / Format
- ☑ Bi-directional Audio
- ☐ Remote Shutdown / Reboot
- ☐ Remote Notify Surveillance Center...
- ☐ Remote Video Output Control
- ☐ Remote Serial Port Control
- ☐ Remote Camera Management
- ☑ Remote Live View
- ☑ Remote Manual Operation
- ☑ Remote PTZ Control

3. Select the new user's access level: Operator or Guest. Default is Operator.
4. Enter the new user's name and password. Both the user name and password can have up to 16 alphanumeric characters. See "Activate the admin password" on page 9 for information on the rules to set up a password. You will be shown the security level of the new password: Low, Medium or High. Confirm the new password.
5. Define the user's permissions.

   Check the required access privileges for basic permissions and camera operation. See "Customizing a user's access privileges" below for the permission descriptions for each permission group.
6. Click **OK** to save the settings and return to the previous window.
7. The list of users is displayed.

# Customize a user's access privileges

Only an administrator can allocate access privileges to Operator and Guest users. The access privileges can be customized for each user's needs. The administrator's access privileges cannot be changed.

There are two types of privilege settings: Basic Permission and Camera Operation.

## Basic permission settings

By default, only remote log search and bi-directional audio are enabled for operators, and only the remote log search is enabled for guests.

- **Remote Parameter Settings:** Remotely configure parameters and import configuration.
- **Remote Log Search:** Remotely view logs that are saved on the recorder.
- **Remote Upgrade/Format:** Remotely upgrade and format the recorder.
- **Bi-directional Audio:** Use bi-directional audio between the remote client and the recorder.
- **Remote Shutdown/Reboot:** Remotely shutdown or reboot the recorder.
- **Remote Surveillance Center/Trigger Alarm Output:** Remotely notify alarm and exception messages to the remote client and control the alarm output.
- **Remote Video Output Control:** For future use.
- **Remote Serial Port Control:** Remotely configure the RS-232 port.
- **Remote Camera Management:** Remotely enable and disable channels.

## Camera operation settings

By default, all IP cameras are enabled for operators for each of these settings. By default, the IP cameras are only enabled for local playback and remote playback for guests.

- **Remote Live View:** Remotely select and view live video over the network.
- **Remote Manual Operation**: Remotely start/stop manual recording on any of the channel.
- **Remote Playback:** Remotely play and download recorded files that are on the recorder.
- **Remote PTZ Control:** Remotely control PTZ dome cameras.
- **Remote Video Export**: Remotely backup recorded files from any channel.
- **Remote Video Download**: Remotely download video files.

**To customize a user’s access privileges:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **User Management** > **Users**.
2. Select the user to edit from the list and click the **Edit** button. The “Edit user” window opens.
3. Check the required access privileges for basic permissions and camera operation.
4. Click **OK** to save the settings and return to the previous window.

# Delete a user

Only a system administrator can delete a user.

**To delete a user from the recorder:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **User Management** > **Users**.
2. Select the user to delete from the list and click the **Delete** button.
3. Click **OK** in the pop-up window to confirm deletion. The user is immediately deleted.

# Modify a user

A user’s name, password, and access level can be changed. Only a system administrator can modify a user.

**To modify a user:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **User Management** > **Users**.
2. Select the user to edit from the list and click the **Edit** button. The “Edit user” window opens.
3. Edit the user information and click **OK** to save the settings and return to the previous window.

# Change the Administrator’s password

The administrator’s password can be changed in the **User Management** menu.

**To change the admin password:**

1. From the menu toolbar, click **Configuration** > **Remote Configuration** > **User Management** > **Users**.
2. Select “admin” in the list of users and click the Edit button. The “Edit user” window opens.
3. Enter the new admin password. Both the user name and password can have up to 16 alphanumeric characters. See “Activate the admin password for information on the rules to set up a password. You will be shown the security level of the new password: Low, Medium or High. Confirm the new password.
4. Enter the new admin password and confirm it. Change the admin MAC address, if required. Click **OK** to save the settings and return to the previous window.

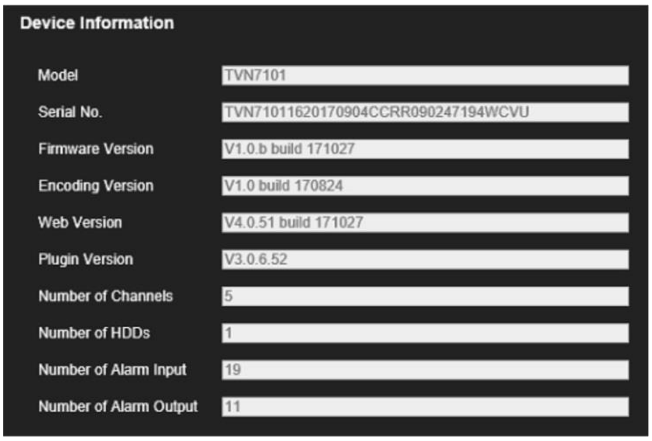
# Chapter 17
# System information

## View system information

**To view system information:**

1. From the menu toolbar, click **Configuration** > **System Information**.
2. To view device information, click **Device Info**.

   You can view the model, device name, serial number, firmware version, and encoding version, number of channels, number of HDDs, number of alarm inputs, and number of alarm outputs.

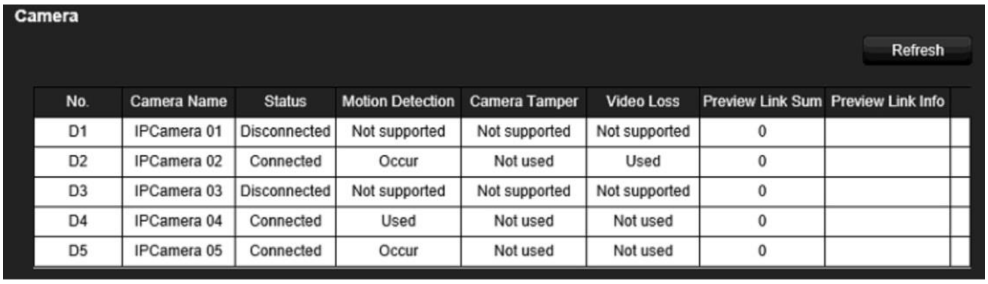
   Device Information

   | | |
   |---|---|
   | Model | TVN7101 |
   | Serial No. | TVN71011620170904CCRR090247194WCVU |
   | Firmware Version | V1.0.b build 171027 |
   | Encoding Version | V1.0 build 170824 |
   | Web Version | V4.0.51 build 171027 |
   | Plugin Version | V3.0.6.52 |
   | Number of Channels | 5 |
   | Number of HDDs | 1 |
   | Number of Alarm Input | 19 |
   | Number of Alarm Output | 11 |

3. To view camera information, click **Camera**.

   You can view the information on each camera: camera number, camera name, status, motion detection, camera tamper, video loss, preview link sum, and preview link information.

   Preview link sum shows the number of remote applications that are streaming video from this video channel. Preview link information shows you the IP addresses that are currently connected to this channel.

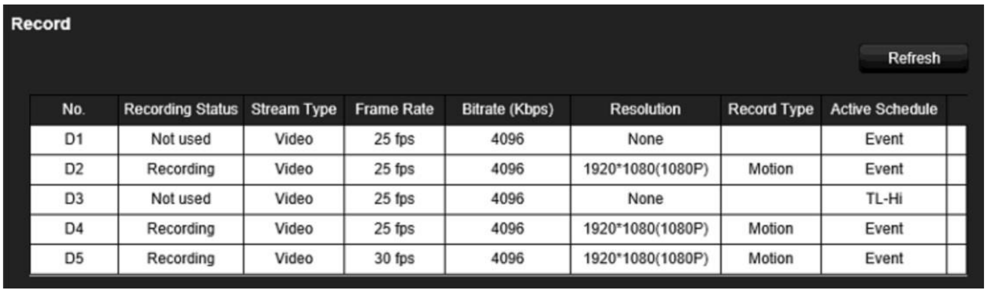


Camera

| No. | Camera Name | Status | Motion Detection | Camera Tamper | Video Loss | Preview Link Sum | Preview Link Info |
|---|---|---|---|---|---|---|---|
| D1 | IPCamera 01 | Disconnected | Not supported | Not supported | Not supported | 0 | |
| D2 | IPCamera 02 | Connected | Occur | Not used | Used | 0 | |
| D3 | IPCamera 03 | Disconnected | Not supported | Not supported | Not supported | 0 | |
| D4 | IPCamera 04 | Connected | Used | Not used | Not used | 0 | |
| D5 | IPCamera 05 | Connected | Occur | Not used | Not used | 0 | |

4. To view record information, click **Record**.

   You can view the camera number, recording status, stream type, frame rate, bit rate (Kbps), resolution, record type, and active schedule.

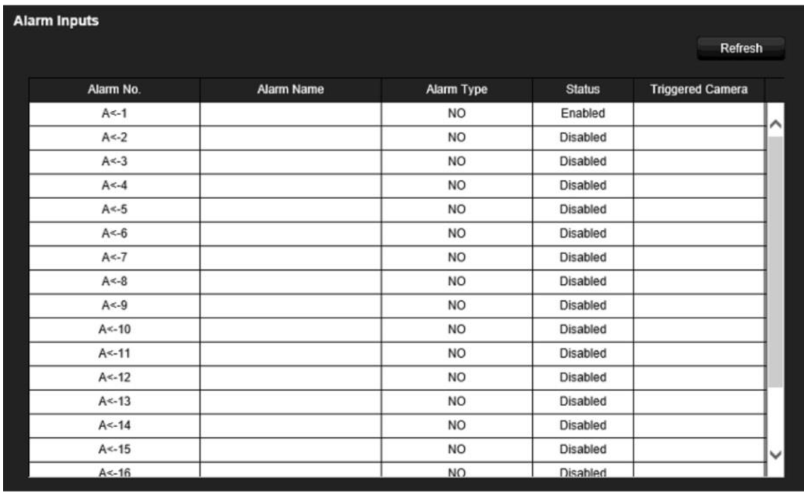


Record

| No. | Recording Status | Stream Type | Frame Rate | Bitrate (Kbps) | Resolution | Record Type | Active Schedule |
|---|---|---|---|---|---|---|---|
| D1 | Not used | Video | 25 fps | 4096 | None | | Event |
| D2 | Recording | Video | 25 fps | 4096 | 1920*1080(1080P) | Motion | Event |
| D3 | Not used | Video | 25 fps | 4096 | None | | TL-Hi |
| D4 | Recording | Video | 25 fps | 4096 | 1920*1080(1080P) | Motion | Event |
| D5 | Recording | Video | 30 fps | 4096 | 1920*1080(1080P) | Motion | Event |

5. To view alarm input information, click **Alarm Inputs**.

   You can view the alarm input number, alarm name, alarm type, alarm status, and triggered camera.

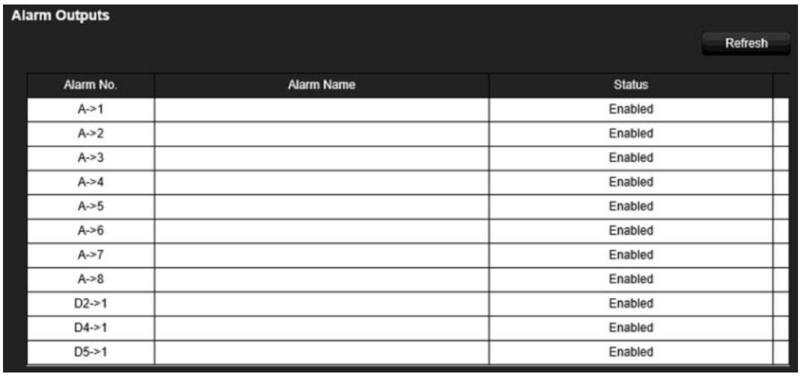


Alarm Inputs

| Alarm No. | Alarm Name | Alarm Type | Status | Triggered Camera |
|---|---|---|---|---|
| A<-1 | | NO | Enabled | |
| A<-2 | | NO | Disabled | |
| A<-3 | | NO | Disabled | |
| A<-4 | | NO | Disabled | |
| A<-5 | | NO | Disabled | |
| A<-6 | | NO | Disabled | |
| A<-7 | | NO | Disabled | |
| A<-8 | | NO | Disabled | |
| A<-9 | | NO | Disabled | |
| A<-10 | | NO | Disabled | |
| A<-11 | | NO | Disabled | |
| A<-12 | | NO | Disabled | |
| A<-13 | | NO | Disabled | |
| A<-14 | | NO | Disabled | |
| A<-15 | | NO | Disabled | |
| A<-16 | | NO | Disabled | |

6. To view alarm output information, click **Alarm Outputs**.

   You can view the alarm output number, alarm name, and alarm status.

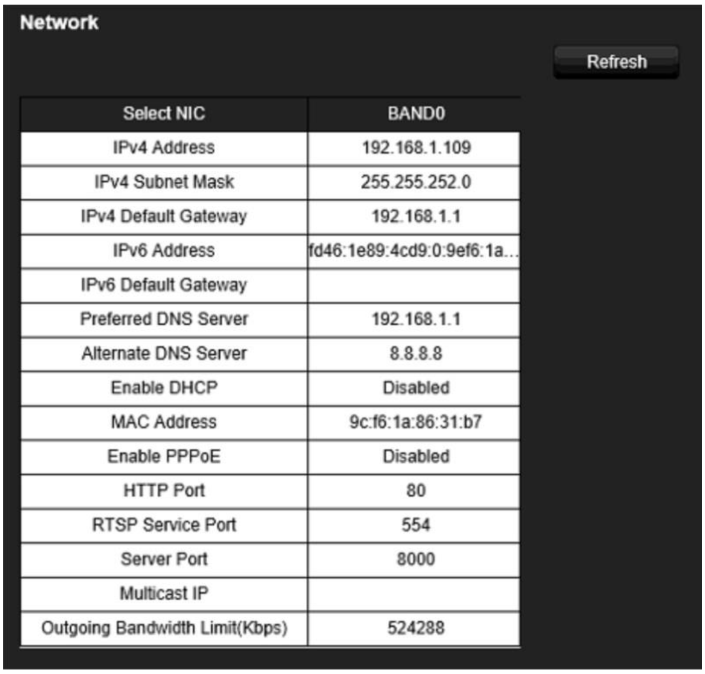


Alarm Outputs

| Alarm No. | Alarm Name | Status |
|---|---|---|
| A->1 | | Enabled |
| A->2 | | Enabled |
| A->3 | | Enabled |
| A->4 | | Enabled |
| A->5 | | Enabled |
| A->6 | | Enabled |
| A->7 | | Enabled |
| A->8 | | Enabled |
| D2->1 | | Enabled |
| D4->1 | | Enabled |
| D5->1 | | Enabled |

7. To view network information, click **Network**.

   You can view the IPv4 address, IPv4 subnet mask, IPv4 default gateway, IPv6 address, IPv6 default gateway, preferred DNS server, alternate DNS server, enable DHCP, MAC address, enable PPPoE, HTTP port, RTSP service port, multicast IP, and outgoing bandwidth limit (Kbps).

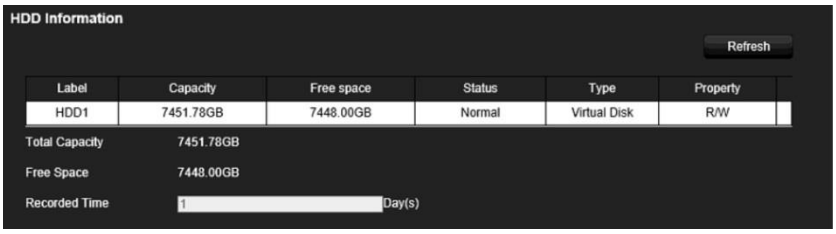


Network

| Select NIC | BAND0 |
|---|---|
| IPv4 Address | 192.168.1.109 |
| IPv4 Subnet Mask | 255.255.252.0 |
| IPv4 Default Gateway | 192.168.1.1 |
| IPv6 Address | fd46:1e89:4cd9:0:9ef6:1a… |
| IPv6 Default Gateway | |
| Preferred DNS Server | 192.168.1.1 |
| Alternate DNS Server | 8.8.8.8 |
| Enable DHCP | Disabled |
| MAC Address | 9c:f6:1a:86:31:b7 |
| Enable PPPoE | Disabled |
| HTTP Port | 80 |
| RTSP Service Port | 554 |
| Server Port | 8000 |
| Multicast IP | |
| Outgoing Bandwidth Limit(Kbps) | 524288 |

8. To view HDD information, click **HDD**.

   You can view the HDD label, status, capacity, free space, property, type, and group.



HDD Information

| Label | Capacity | Free space | Status | Type | Property |
|---|---|---|---|---|---|
| HDD1 | 7451.78GB | 7448.00GB | Normal | Virtual Disk | R/W |

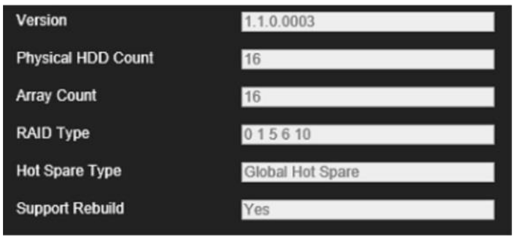
Total Capacity 7451.78GB

Free Space 7448.00GB

Recorded Time 1 Day(s)

9. To view RAID information, click **Raid Info**.

   You can view the version, physical HDD count, array count, RAID type, hot spare type, and support rebuild.



| | |
|---|---|
| Version | 1.1.0.0003 |
| Physical HDD Count | 16 |
| Array Count | 16 |
| RAID Type | 0 1 5 6 10 |
| Hot Spare Type | Global Hot Spare |
| Support Rebuild | Yes |

10. Click **Live View** on the menu toolbar to return to live view.

# Appendix A
# Specifications

| | TVN 71 |
|---|---|
| **Video & audio input** | |
| Video compression standards supported | H.264, H.265, RTSP custom protocol, ONVIF |
| Max. IP camera input | 128 |
| Max. bandwidth per channel | 16 Mbps |
| Audio input | 1-ch, RCA (2.0 Vp-p, 1 kΩ) |
| Total recording bandwidth available | Up to 576 Mbps |
| Bi-directional audio | 1-ch (reduplicated with audio input 1), RCA (2.0 Vp-p, 1 kΩ) |
| **Video & audio output** | |
| Recording resolution | 8 MP / 6 MP / 5 MP / 4 MP / 3 MP / 1080P / UXGA / 720P / VGA / 4CIF / DCIF / 2CIF / CIF / QCIF |
| Audio output | 1-ch, RCA (2.0 Vp-p, 1 kΩ) |
| Dual-stream recording | Up to 16 channels |
| Auto archiving | Yes |
| Stream type | Video, Video & Audio |
| Recording modes | Time lapse High, Time lapse Low, Event, Alarm, Manual |
| **Networking** | |
| Network interface | 8 × 10M / 100M / 1000M self-adaptive Ethernet interface (4x RJ45; 4x SFP (Fiber)) |
| Total connections to recorder (non-viewing) | 256 |
| Total viewing streams available per camera channel | 128 |
| Total viewing bandwidth available | 512Mbps |
| **Hard disk** | |
| SATA | 16 SATA interfaces |
| Max. onboard storage capacity | 96 TB (non-RAID or RAID) |
| Capacity per HDD | 6 TB |
| RAID | 0/1/5/6/10 |

| | TVN 71 |
|---|---|
| **External interface** | |
| Serial interface | 1 RS-232 interface (for Technical Support) |
| USB interface | Front panel: 2 × USB 2.0 (front), Back panel: 2 × USB 3.0 (back) |
| Alarm in | 16 |
| Alarm out | 8 |
| **Miscellaneous** | |
| Power supply | 2 × 100 to 240 VAC, 6.3 A, 50 to 60 Hz |
| Power consumption (without HDD) | ≤ 140 W |
| Power consumption (with 16 × 2TB RAID HDDs) | 150 W |
| Operating temperature | -10 to +50ºC (14 to 122°F) |
| Relative humidity | 10 to 90% |
| Chassis | 3U rack-mountable or desk-based chassis |
| Dimensions (W x H x D) | 442 × 494 × 146 mm (17.4 × 19.4 × 5.7 in.) |
| Weight | ≤ 16 kg (35.3 lb.) (without HDD) |

# Appendix B
# Port forwarding information

A router is a device that lets you share your internet connection between multiple computers. Most routers will not allow incoming traffic to the device unless you have configured them to forward the necessary ports to that device. By default, our software and recorders require the following ports to be forwarded:

**Note**: Port forwarding may reduce the security of the computers on your network. Please contact your network administrator or a qualified network technician for further information.

**Note**:  It is recommended that the recorder is placed behind a firewall and that only those ports that need to communicate with browsers and software can be accessed.

| | | |
|---|---|---|
| Port: 80 | HTTP protocol | Used to connect via IE browser. |
| Port: 8000 | Client Software Port | Used to connect to video streams. |
| Port: 554 | RTSP Port | Real time streaming protocol.<br>Used to record video remotely. |
| Port 7681 | Websocket Port | Used for live view on non-IE browsers. |
| Port: 1024 | RTSP Port for 3G/4G | Use with mobile apps.<br>Used for 3G/4G connection. |

**Note**: It is recommended that the RTSP port 1024 should only be used when experiencing connection issues over a 3G/4G connection.

## Seeking further assistance

Third-party assistance on configuring popular routers can be found at:

http://www.portforward.com/

http://canyouseeme.org/

http://yougetsignal.com

**Note**: These links are not affiliated with nor supported by Aritech technical support.

Many router manufacturers also offer guides on their websites as well as including documentation with the product.

On most routers the brand and model number are located on or near the serial number sticker on the bottom of the device.

If you cannot find any information for your specific router, please contact your router manufacturer or internet service provider for further assistance.

# Appendix C Guidelines when using a high camera count (>32 cameras)

## Introduction

When working with a large number (>32) of cameras per recorder, specific guidelines are advised for hard drives, network settings, and event linking features to ensure optimal performance of the TruVision recorder. Not following these guidelines may result in loss of frames.

## Hard drive configuration

The hard drives that we use in our recorders are especially designed for video surveillance purposes and/or enterprise class installations.

However, every hard drive has specific limitations.

Due to the read/write speed limitations of the hard drive, the maximum advised number of cameras per hard drive is 32 cameras with a maximum bit rate of 4Mbps/camera or a total bit rate of 128Mbps.

The number of cameras will decrease if the camera resolution requires a higher bit rate.

Going above these limitations may result in sporadic video recording gaps.

We advise to use HDD Group Mode for non-RAID configurations or RAID 5 or 6 for RAID configurations.

### A. For non-RAID configurations

The recorder a feature called **HDD Group Mode**.

Use the **HDD Group Mode** and use at least four hard drives.

When there are more than 32 cameras on the recorder, we advise to assign not more than 32 cameras per group. Every camera can only be part of one group.

### B. For RAID configurations

The recorder supports different RAID levels but with high camera numbers (>32), we recommend using RAID 5 or 6 only.

Using RAID 5 or 6 will distribute the recording load over the different hard drives.

Use at least three (RAID 5) or four (RAID 6) hard drives in a recorder when using RAID 5 or 6.

See the “HDD information” on page 117 for more information about how to configure HDD grouping or RAID.

## Network configuration

It is essential that a stable network environment is used.

A poor-quality network will result in data loss, offline cameras, and will equally impact the recorder’s performance.

A qualitative network will increase the recording stability and viewing performance of the recorder.

We recommend the following settings:

- Connect two or more network ports. Make sure the ports on the switches are 1 Gigabit ports.
- In the *Network* settings of the recorder, choose the working mode **Load Balance** and connect all the network ports to the same switch. The ports of the switch also need to be configured in load balance mode.

For the connection between cameras and the recorder it is better to spread the cameras over multiple switches as well.

It is also important to ensure the use of qualitative non-blocking switches, such as those available within the Aritech IFS product range.

## Event recording triggers

The process of activating event or alarm recording requires intelligence from the recorder. When triggering a high number of alarm/event recordings simultaneously, the recorder’s performance can be impacted.

We advise to limit the maximum number of cameras that will be recorded for an event to four. This will minimize the risk of impacting the recorder’s performance.

# Index