www.acornfiresecurity.com

truVision

TVN 23 (S/P) User Manual

P/N 1162-EN • REV A • ISS 11DEC23

www.acornfiresecurity.com

Copyright

© 2023 Carrier. All rights reserved. The information is subject to change without prior notice.

This document may not be copied in whole or in part or otherwise reproduced without prior written consent from Carrier, except where specifically permitted under US and international copyright law.

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 manufacturing representative:
Carrier Fire & Security B.V.,
Kelvinstraat 7, 6003 DH Weert, Netherlands.

Product warnings and disclaimers

THESE PRODUCTS ARE INTENDED FOR SALE TO AND INSTALLATION BY QUALIFIED PROFESSIONALS.
CARRIER FIRE & SECURITY B.V. 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 QR code.

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.

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.

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.

Canada

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

cUL

Safety Instructions:

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.

Compliance

European Union 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.

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 a designated collection point. For more information see recyclethis.info.

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.

www.acornfiresecurity.com

Content

Important information 5

Chapter 1 **Physical installation 8**
Installation environment 8
Firmware version 8
Unpacking the recorder and its accessories 9
Back panel 9
PoE ports 10
Monitor connections 10
Rack mounting 11
Front panel 11
Contact information and manuals/firmware 11

Chapter 2 **Getting started 12**
Powering up the recorder 13
Activate the admin password 13
Access via a web browser 14
Access via the OSD 16
Change the recorder's language 18

Chapter 3 **Browser configuration 19**

Chapter 4 **System management 22**
System settings 22
Maintenance 32
Security 40

Chapter 5 **Camera management 48**
Manage IP cameras in web mode 50
Manage IP cameras in OSD mode 51
PoE settings 54
Manage camera passwords 55
Add an IP camera 57
Change camera settings 60
Restrict viewing cameras on a VGA/HDMI monitor 62

Chapter 6 **User management 63**
Manage users 63
Double Verification permission for non-admin users 69

Chapter 7 **Network settings 72**
TCP/IP settings 72
DDNS settings 74
PPPoE settings 76
Port settings 76

www.acornfiresecurity.com

www.acornfiresecurity.com

NAT (UPnP) settings 78
Email settings 79
Network Service (web only) 81
802.1x 83
Other network settings 84
Integration protocol 86
Connect the recorder to UltraSync 86
Add the recorder to TVRMobile 92

Chapter 8 **Video and audio configuration 94**
Audio 94
Dual VCA 95
V-Stream encoding 95

Chapter 9 **Image settings 96**
Display settings 96
Camera OSD in web mode 98
Day/night switch 98
Privacy mask 99

Chapter 10 **Event setup 101**
Motion detection 101
Camera tamper 106
Video loss detection 109
Set up alarm inputs 110
Combined Alarm (OSD only) 112
Set up alarm outputs 113
Manually trigger an alarm output 115
Exception notification 116
Intrusion integration alarm reporting 118
Transparent Transmission Configuration (Web only) 122
Disable Actions 124
Smart event 127
Smart report (OSD only) 130
Behavior analysis (web only) 138
Face capture 143

Chapter 11 **Recording 145**
Recording schedule for video recording 145
Recording schedule for snapshot capturing 149
Search for snapshots 151
Camera encoding settings 153
Holiday recording schedules 156

Chapter 12 **Storage management 157**
Storage status information 157
Activate a new HDD 158
Initialize an HDD 158

www.acornfiresecurity.com

www.acornfiresecurity.com

Add a network storage system 158
S.M.A.R.T. settings 160
Bad sector detection 161
HDD sleep mode 162
Overwrite an HDD 163
Record file duration (web only) 163
Storage mode 164
Group HDDs 164
Redundancy in group mode 165
Repair HDD database 166
Manage eSATA (OSD only) 166
Auto backup 166
Dynamically Adjust Recording writing buffer (OSD only) 167
Hot spare device backup (OSD only) 167
Disk Array (P models only and with 4TB/disk or larger) 170
HDD clone (OSD only) 174
HDD health detection (OSD only) 174

Chapter 13 Live view in web mode 176
Description of live view 176
PTZ control 177
Preset and preset tours 178

Chapter 14 Live view in OSD mode 180
Live view control toolbar 181
Live view mouse menu 182
Live view general setup menu 183
Single and multiview display modes 184
Custom layout configuration and usage (OSD) 185
Sequencing feature 186
Digital zoom 187
Target display details in live view 187
PTZ control 188

Chapter 15 Playback in web mode 193
Play back recordings 195
Synchronous playback 196
Smart search 196
Create snapshots 197
Create video clips 198
Digital zoom in playback 198

Chapter 16 Playback in OSD mode 199
Playback modes 201
Smart search 203
Custom playback (OSD only) 204
Thumbnail images to preview a recording 205
Instant playback 206

www.acornfiresecurity.com

www.acornfiresecurity.com

Create tags 206
Create video clips 207
Digital zoom in playback 207

Chapter 17 **Search recordings 208**
Search in web mode 208
Search recordings in OSD mode 209
Smart search 212

Chapter 18 **UltraSync related functions 216**
Introduction 216
Service levels and functionalities 216

Appendix A **Specifications 229**

Appendix B **Port forwarding info 233**
Seeking further assistance 233

www.acornfiresecurity.com

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

www.acornfiresecurity.com

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.

www.acornfiresecurity.com

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.

www.acornfiresecurity.com

Chapter 1
Physical installation

Installation environment

When installing your product, consider these factors:

- Ventilation
- Temperature
- Moisture
- 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 DVR units.

Moisture: 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.

Firmware version

This manual applies to firmware version 1.00.004 Build 231219.

www.acornfiresecurity.com

www.acornfiresecurity.com

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 cord
- Recorder including HDDs
- USB mouse
- Rack mounts
- *TruVision NVR 23 (S/P) Quick Start Guide*
- *TruVision NVR 23 (S/P) Operator Guide*

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

- *TruVision NVR 23 (S/P) Quick Start Guide*
- *TruVision NVR 23 (S/P) User Manual*
- *TruVision NVR 23 (S/P) Operator Guide*

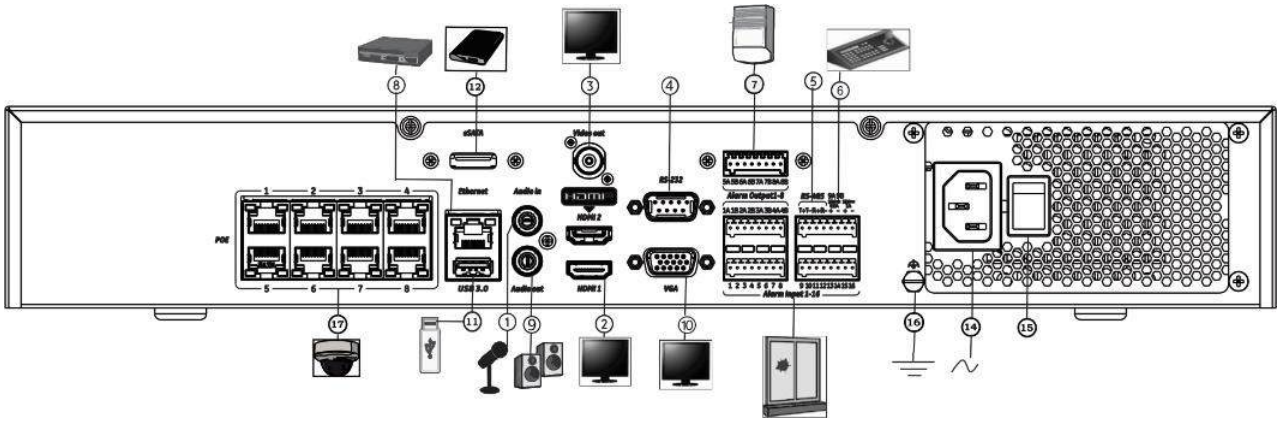
Back panel

The figures below show the back panel connections and describe each connector on a typical TVN 23 (S/P) digital video recorder. Details may vary for specific models.

Before powering up the recorder, insert the hard drives and connect a main monitor for basic operation.

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).

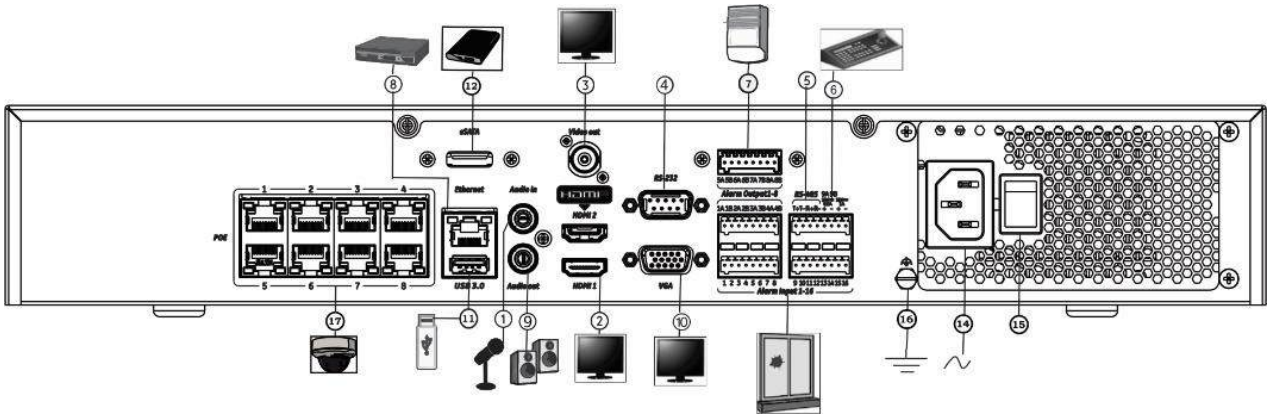
Figure 1: TVN 2316 S back panel connections



www.acornfiresecurity.com

www.acornfiresecurity.com

Figure 2: TVN 23 back panel connections



1. Connect one audio input to RCA connectors.
2. Connect to an HDTV. The HDMI connection supports both digital audio and video.
3. Connect one CCTV monitor (BNC-type connectors)
4. Connect to a RS-232 device.
5. RS-485 port not used.
6. Connect to a keypad via RS-485 (not used).
7. Alarm relay outputs.
8. Connect to a network (RJ45).
9. Connect to speakers for audio output.
10. Connect to a VGA monitor.
11. Universal Serial Bus (USB). Connect to an additional device such as a USB mouse, CD/DVD burner, or USB HDD.
12. Connect to an optional eSATA device such as HDD, CD/DVD-R
13. Connect up to 16 alarm inputs (depending on model).
14. Connect to a power cord.
15. Power button
16. Connect to ground.
17. 8/16 PoE ports (depending on model).

Default IP address - 192.168.1.82

Download the latest recorder firmware and TruVision Navigator software from www.firesecurityproducts.com

PoE ports

The S models of the recorder have PoE ports for camera connections. Connect up to 8 or 16 IP cameras to the embedded PoE ports on the TVN 23 S recorder.

Monitor connections

The recorder supports up to 1920 × 1080 / 60 Hz resolution in VGA and 8K (7680 x 4320) resolution in HDMI. The monitor resolution should be at least 1280 × 720. Adjust your monitor accordingly to this resolution.

The VGA or HDMI monitor can be used as the main monitor of the recorder.

For the TVN 2316 and TVN 2308S/2316S recorders, the HDM1 and VGA output show the same content. The HDMI2 output can show a different content.

www.acornfiresecurity.com

www.acornfiresecurity.com

For the TVN 23P recorders, HDMI 1 and VGA 1 provide the same video content, and work as the main output. HDMI 2 and VGA 2 provide the same video content, and work as the event monitor.

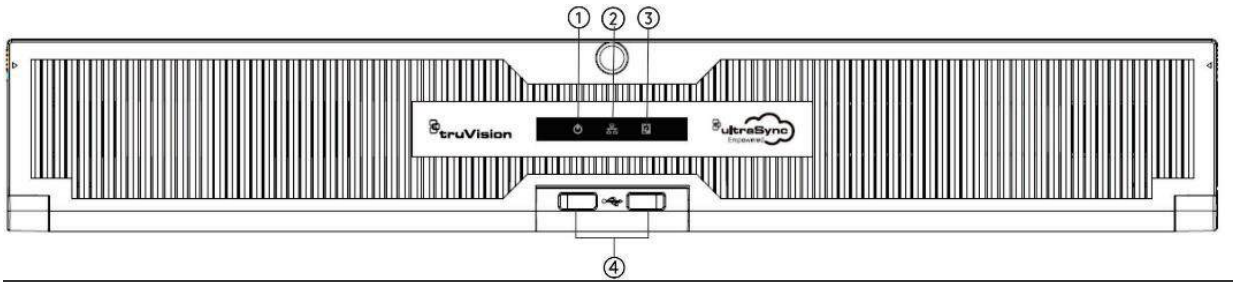
Rack mounting

The TVN 23 (S/P) recorders are shipped with rack ears.

Front panel

There are no buttons on the front panel to control recorder functions. There are status LEDs showing power, HDD data upload/download, and the network connection.

Figure 3: Front panel



	Name	Description
1.	Power	A steady green light indicates the recorder is working correctly. Red indicates a fault.
2.	Network	White light blinks fast when data is being transferred via the network
3.	HDD	The white LED blinks when data is being read from or written to the HDD.
4.	USB interface	Universal Serial Bus (USB) port for additional devices such as a USB mouse or USB Hard Disk Drive (HDD).

Contact information and manuals/firmware

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

EMEA: https://firesecurityproducts.com

Manuals are available in several languages.

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

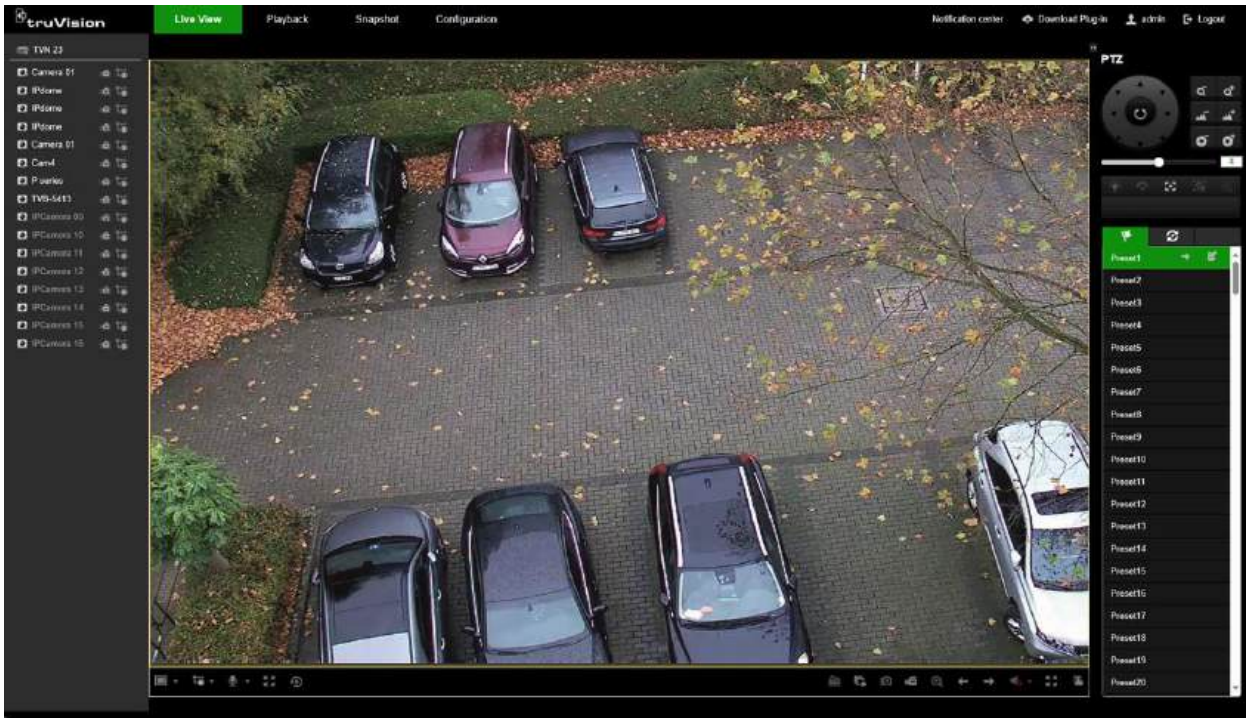
www.acornfiresecurity.com

Chapter 2
Getting started

The recorder can be configured through the OSD (On Screen Display) shown on a monitor connected to the recorder, web browser, TruVision Navigator, and the SDK.

You can access the recorder through the OSD and web interfaces. They let you view, record, and play back videos as well as manage many aspects of the recorder from any PC with internet access. See Figure 4.

Figure 4: Web browser interface (live view with menu options shown)



The recorder can fully integrate with the license-free TruVision Navigator software, which is ideal for most commercial applications. TVN 23 (S/P)'s easy and intuitive-to-use web browser interface enables remote configuration and secure viewing, searching, and playing back of video from computers connected via the Internet.

www.acornfiresecurity.com

Powering up the recorder

Before starting the recorder, connect at least one monitor (VGA or HDMI). Otherwise, you will not be able to see the user interface and operate the device.

It comes equipped with a universal power supply that will auto-sense 110/240 V, 60/50 Hz. Models are shipped with power cords for their region.

Note: It is recommended to use an uninterruptible power supply (UPS) in conjunction with the device.

To turn on/off the recorder:

Turn on or off the recorder using the power switch on the back panel. Once it is powered up, the status LEDs on the front panel will light up.

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.

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 our Technical Support to reactivate the unit with a new password.

For UltraSync connected recorders: the password reset is also possible via the UltraSync portal when the recorder is subscribed to the Core Video Plus Video service for UltraSync.

See chapter 18 for more details.

Go to Chapter 6 “User management” on page 63 for further information on creating user passwords.

You can also set up the camera password when starting up the recorder.

www.acornfiresecurity.com

www.acornfiresecurity.com

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 a browser:

RTSP port: 554

HTTP port: 80

When using Google Chrome, Apple Safari, Opera, or Mozilla Firefox, port in HTTP mode: port 7681

When using TruNav:

RTSP port: 554

Server/Client software port: 8000

Access via a web browser

To access the unit via the browser, open a web browser and enter the IP address assigned to the recorder as a web address. In the login screen, enter the user ID and password.

You can also access the recorder interface using its OSD display. The user manual explains how to use the recorder via the browser and OSD modes.

The recorder can automatically detect which browser you are using.

Microsoft Internet Explorer plug-in

When using Microsoft Internet Explorer, install the recorder web plug-in to see live camera images. You are requested to install this plug-in the first time you use the recorder via Internet Explorer.

Google Chrome, Apple Safari, and Mozilla Firefox plug-in

There is another plug-in tool available for use with Microsoft Edge, Google Chrome, Apple Safari, and Mozilla Firefox, which can be downloaded via the webpage of the recorder. Click “Download plug-in” on the top right of the recorder window when using one of these browsers. This plug-in solves the limitations of the plugin-free solution.

The recorder must be connected to the internet to download the plug-in.

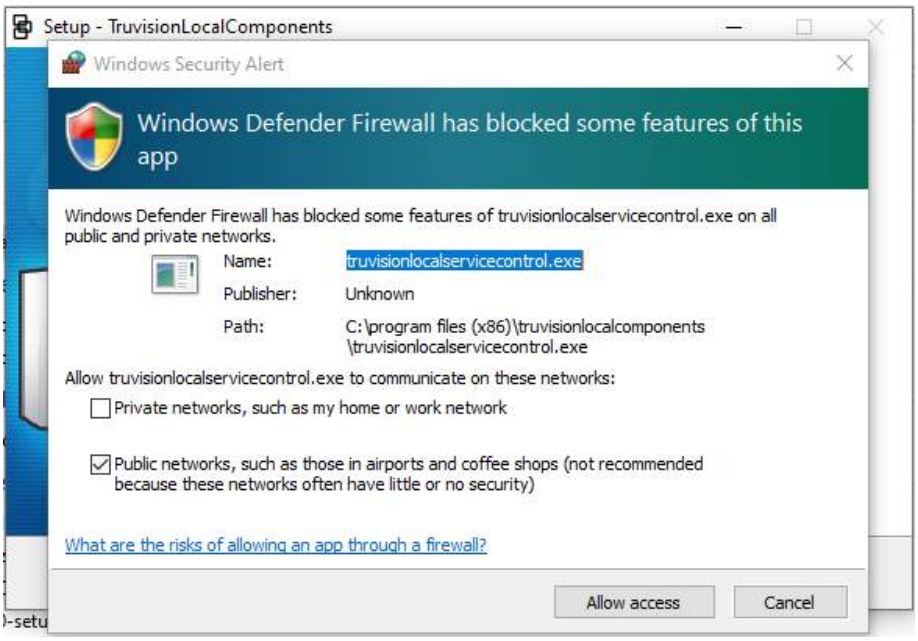
On the live view webpage of the recorder, click the “Download Plugin” icon on the top right corner to download the plugin installation file to your PC.

www.acornfiresecurity.com

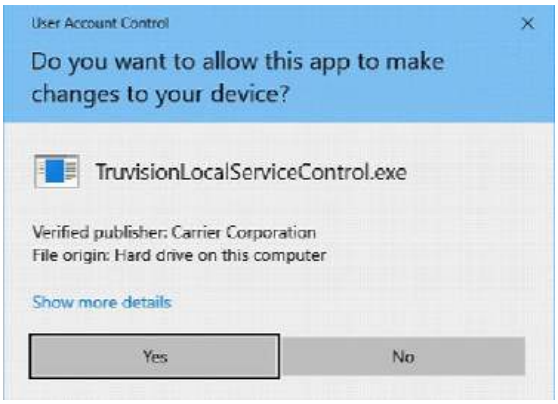
www.acornfiresecurity.com

Close the browser and install the downloaded plugin *TruVisionLocalComponents.exe* on your PC. Once it is installed, reopen the browser, and continue using it to watch live/playback video and configure the recorder.

During the plugin installation, Windows Defender may show a pop-up message. Click the “Allow access” button to accept it.



Note: This application starts automatically when opening Windows. Depending on your Windows configuration, you might see the pop-up message shown below after logging into Windows. Accept the message to enable the plugin for plugin-free browsers.



Plug-in free browser access

You can use the recorder without a plug-in for the browsers Google Chrome, Apple Safari, and Mozilla Firefox, and Microsoft Edge. However, there are limitations to the functions that can be accessed. See Table 1 on page 16.

www.acornfiresecurity.com

www.acornfiresecurity.com

Table 1: Browser plugin-free limitations

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	Not supported	
Configuration	Export device parameters		
	Import device parameters		
	Firmware upgrade		
	Draw area (Motion/VCA)		
	Export log		
	Local configuration		
	File path setting		

Access via the OSD

When you log in to the recorder, you see the OSD interface showing live view of one or more cameras. Many features of live view can be quickly accessed by placing the cursor on a live image and clicking the right button of the mouse. The mouse menu appears. For more information, see Chapter 14 “Live view in OSD mode” on page 180.

www.acornfiresecurity.com

www.acornfiresecurity.com

Startup wizard in OSD mode

The recorder has an express installation wizard when using OSD mode that lets you easily configure basic recorder settings when first used. The configuration of each camera and recorder can be customized as required.

By default, in OSD mode the startup wizard will start once the recorder has loaded. It will walk you through some of the more important settings of your recorder.

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

There is no startup wizard when using web mode. Once you log on to the recorder, you are immediately in live mode and must set up the recorder from the Configuration menu.

To use the Startup wizard in OSD mode:

1. Select the preferred language for the system and resolution from the drop-down list and then click **Apply**.
2. Log on to the recorder. If it is the first time using the device, the installation wizard automatically appears. By default, once set up the wizard no longer appears when logging on to the recorder.

   Note: To always launch the startup wizard when rebooting, enable **Wizard** in the **Configuration** > **System** > **General** > **Basic Settings** menu.
3. In each setup configuration page, enter the desired information and then click **Next** to move to the next page. The setup configuration pages are:

Wizard setup pages	Description
Time and date configuration	Select the desired time zone, date format, system time, and system date. If Daylight saving time (DST) is required, check Enable DST and enter the desired summer and winter months. **Note**: Recordings use the camera time and date.
Network configuration	Configure your network settings such as the IP address, subnet mask, and default gateway. Enter the preferred DNS server address as well as the alternate one to use.
HDD management	The hard drives are initialized at the factory. However, if you wish to clear all data, select the HDD, and click **Init** (Initialize) to initialize the HDD. You can also add and delete hard drives.
Camera Setup	The list shows thethe IP cameras that have been detected on the LAN and can be added to the recorder. **Note**: The number of cameras that can be added to the recorder depends on the camera model. You do not need to search for PoE cameras. They are automatically recognized when plugged in. Select one or more cameras from the list and click the **Add** button. The cameras will be added to the recorder. Every camera shall be activated before it is added to the recorder. The table shows the activation state for each camera. If the camera is not yet activated, select it and click **Activate**.

www.acornfiresecurity.com

www.acornfiresecurity.com

Wizard setup pages	Description
	You need to create the asmin password for the camera or select that the camera will use the IP camera activation password, that is stored in the recorder. If the selected camera(s) need to use H.265 encoding when they are added, you can enable that too. (this setting is only valid for IP cameras that support H.265). Click **Next** to move to the next page.
UltraSync	To add the recorder to UltraSync, you must first register the recorder in the UltraSync system. Select the **Register to UltraSync** to register. You can also register to UltraSync under **Configuration** > **Network** > **UltraSync** menu in web mode (see page 86 86).

4. Click **Finish** to exit the Wizard. The recorder is now ready to use. The live view window appears.

Change the recorder's language

You can set the language of the recorder when you log in via the web browser. Select the desired language from the drop-down list shown.

There are two ways to set the language when using the recorder OSD:

- It can be set from the Startup Wizard.
- It can also be set by selecting **System** > **General**.

www.acornfiresecurity.com

www.acornfiresecurity.com

Chapter 3
Browser configuration

When using Internet Explorer, there is a local browser configuration menu.

The browser-related functions that are in the local browser configuration menu of the web page, are not available in OSD mode nor when using the browsers Google Chrome, Mozilla Firefox, and Apple Safari when they are used without installing the plug-in (see “Google Chrome, Apple Safari, and Mozilla Firefox plug-in” on page 14). When this plug-in is used, the local browser configuration menu is also available for these browsers.

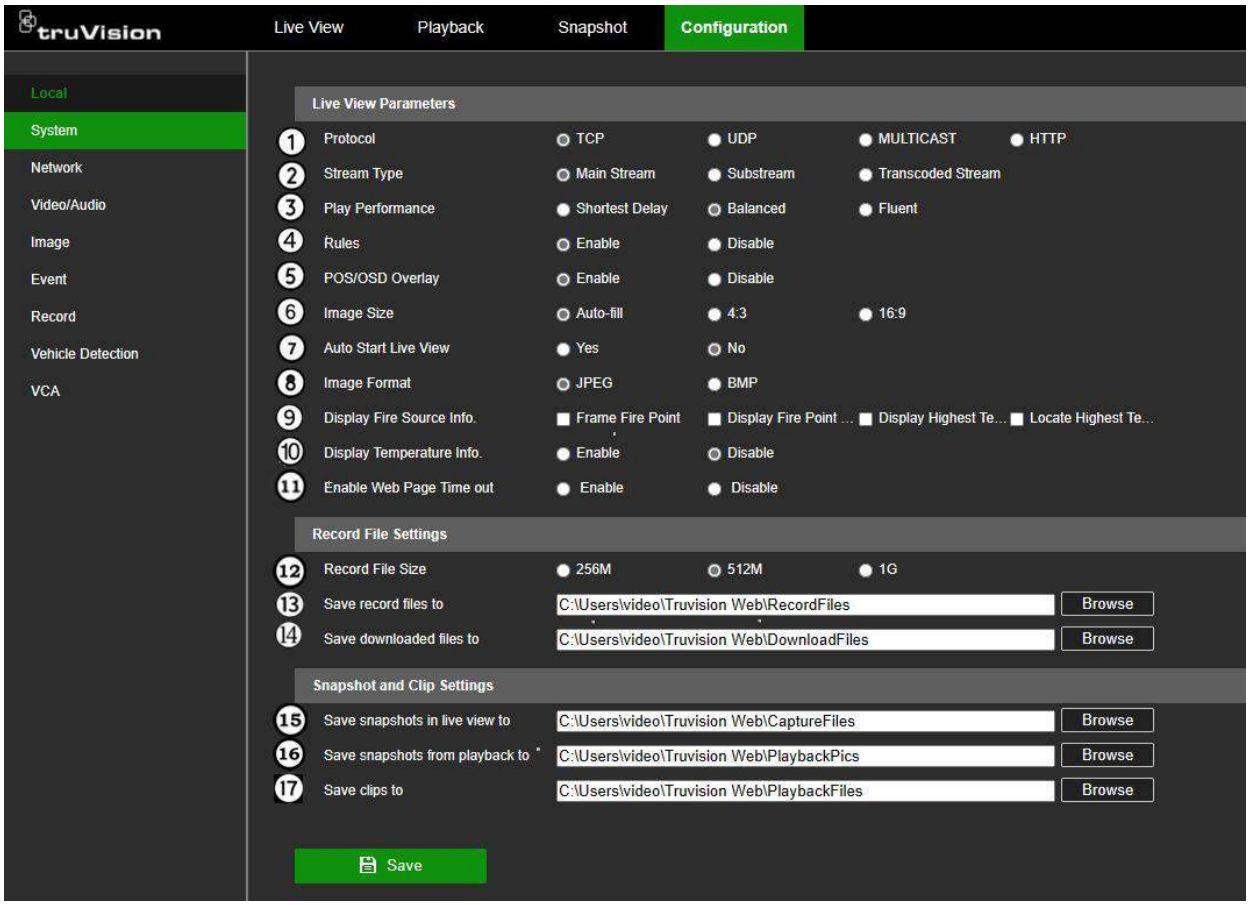
This local browser configuration menu lets you define communication and network parameters that are related to the web browser application, such as protocol type, maximum file size, stream type, and network transmission settings. You can also specify the directory locations for saving recorded and playback videos, captured imags, and downloaded files. The browser interface settings are saved on your PC, not on the recorder.

The other configuration menus (System, Network, Video/Audio, Image, Event, Record, Vehicle Detection and VCA) are for the recorder itself. They are also available in OSD mode.

www.acornfiresecurity.com

www.acornfiresecurity.com

Figure 5: Local configuration on the web browser (Internet Explorer, and Google Chrome/Mozilla Firefox, Microsoft Edge with additional plugin)



Options		Description
Live View Parameters		
1.	Protocol	Specifies the network protocol used. Options include TCP, UDP, MULTICAST, or HTTP. Default is TCP.
2.	Stream Type	Specifies the streaming method used. Options include Main Stream Substream or Transcoded Stream. Default is Main Stream. Use main stream for live viewing and recording with high resolutions and bandwidth. Use substream or Transcoded Stream when there is a bandwidth limitation, such as when using a mobile app.
3.	Play performance	Specifies the play performance of live view. Options include: Shortest delay, Balanced, or Fluent.
4.	Rules	Specifies if the gridlines/VCA lines are shown as an overlay on the video stream for events.
5.	POS/OSD overlay	Allows the display of text insertion information via the webpage. This option needs to be enabled when POS is used and has to be displayed on the webpage.
6.	Image Size	Specifies the maximum file size. Options include Autofill, 4:3, and 16:9.
7.	Auto Start Live View	Live view starts automatically when you log in. Options are Yes or No. Default is Yes.

www.acornfiresecurity.com

www.acornfiresecurity.com

Options		Description
8.	Image Format	Specifies the image format of snapshots, JPEG or BMP.
9.	Display Fire Source Info	**CAUTION**: Only use this function when the thermal camera supports fire detection. Not all TruVision thermal cameras support fire detection. 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. 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. You can select up to four options: Frame the fire point, Display point distance, Display the highest temperature, and locate highest temperature point. **IMPORTANT NOTICE**: This fire detection feature is not a substitute for a certified fire detection system.
10.	Display Temperature Info.	If TruVision thermal cameras support temperature detection, then temperature information is available. 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. It displays the temperature information in the frames that were set up in the thermal camera. **Note**: Behavior analysis is currently not supported by any TruVision cameras. **IMPORTANT NOTICE**: This fire detection feature is not a substitute for a certified fire detection system.
11.	Enable Web Page Time-out	The web page times out after five minutes if there is no mouse movement by the user. Options for time out are Enable and Disable. Default is Enabled. When disabled, the web page will not time out.
Record File Settings for manual recording of video on a PC or another network location		
12.	Record File Size	Specify the size of the recorded files. Options include 256M, 512M or 1G.
13.	Save Record Files To	Specifies the directory for saving recorded video in live view mode.
14.	Save Downloaded Files To	Specifies the directory for downloaded files.
Snapshot and Clip Settings		
15.	Save Snapshot In Live View To	Specifies the directory for saving snapshots in live view mode.
16.	Save Snapshots When In Playback To	Specifies the directory for saving snapshots in playback mode.
17.	Save Clips To	Specifies the directory for saving video clips in playback mode.

www.acornfiresecurity.com

www.acornfiresecurity.com

Chapter 4
System management

The System menu lets you specify the settings for viewing system information, time, RTSP/web authentication, restoring default parameters, updating firmware, searching system logs, restricting access, camera password management, camera management, user management, and live view default settings.

System settings

View the recorder information

You can view the device name and number, model, serial number, firmware version, encoding version, web version, plug-in version, number of channels, number of HDDs, number of alarm inputs, and number of alarm outputs. You can modify the device name and number.

To modify the recorder name and number in web mode:

1. Click **Configuration** > **System** > **System Settings** > **Basic Information**.
2. Enter the new device name and number. The other options cannot be changed.

Options	Description
Device Name	Define the recorder's name. Enter the new recorder name. Default is TVN 23.
Device No.	The device number to use for the recorder when linking the device to a network keyboard, etc. The value can be set between 1 and 255. The default value is 255.
Firmware Version	Shows the current firmware version of the recorder. If the recorder is connected to UltraSync and the service level is at least Core Video Plus, then it is possible to check if the current firmware version is also the most recent one. See page 219 for more information.

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

www.acornfiresecurity.com

www.acornfiresecurity.com

To modify the recorder name and number in OSD mode:

1. Click **System** > **General**.
2. Enter the new device name and device number.

Options	Description
Device Name	Define the recorder's name. Enter the new recorder name. Default is TVN 23.
Device No.	The device number to use for the recorder when linking the device to a network keyboard, etc. The value can be set between 1 and 255. The default value is 255.

2. Click **Apply** to save the changes.

Time settings

This browser menu lets you specify the recorder's time zone, network time protocol (NTP), and manual time synchronization. The start and end time of daylight-saving time (DST) in the year can also be set. DST is deactivated by default.

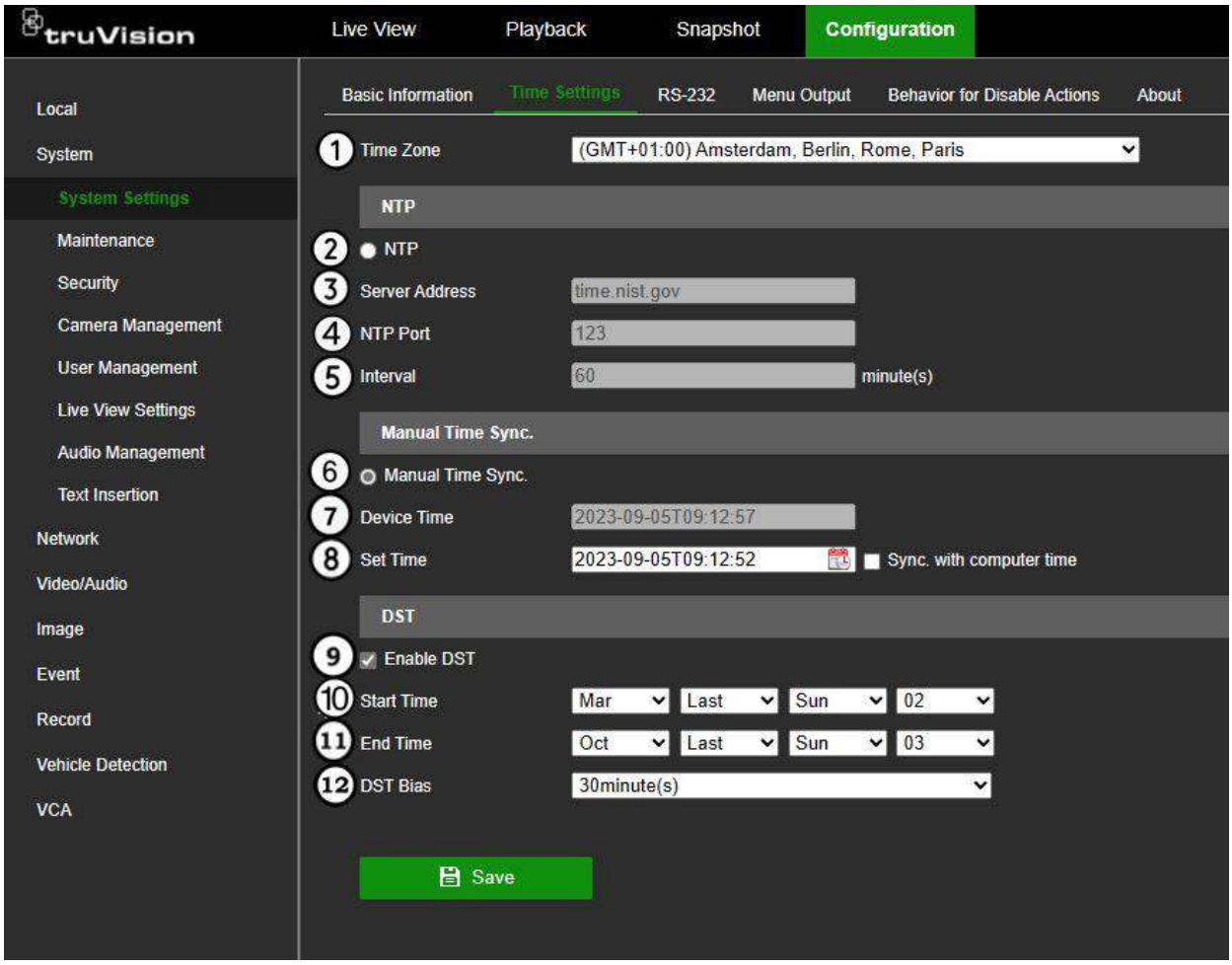
An NTP server can be configured on your recorder to keep the date and time current and accurate. You can also manually time synchronize the NTP server.

Note: If the device is connected to a public network, you should use an 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 set up in a more customized network, NTP software can be used to establish an NTP server used for time synchronization.

www.acornfiresecurity.com

www.acornfiresecurity.com

Figure 6: Time Settings menu in web mode



	Option	Description
1.	Time Zone	Select your time zone from the list.
	NTP	
2.	NTP	Select the check box to enable the feature. It is disabled by default.
3.	Server Address	IP address of the NTP server. Default is *time.nist.gov*.
4.	NTP Port	Port of the NTP server. Default is 123.
5.	Interval	Time in minutes to synchronize with the NTP server. The value can be between 1 and 10080 minutes. Default is 60 minutes.
	Manual Time Sync.	
6.	Manual Time Sync.	Select the check box to enable the feature. It is enabled by default.
7.	Device Time	The device time is automatically displayed.
8.	Set Time	Manually enter or select the date and time from the calendar. Check the **Sync. with computer time** to synchronize the device with that of the local computer.
	DST	
9.	Enable DST	Click the check box to enable or disable daylight savings time (DST). Default is *Disabled*.
10.	Start Time	Enter the start date and time for daylight savings.

www.acornfiresecurity.com

www.acornfiresecurity.com

	Option	Description
11.	End Time	Enter the end date and time for daylight savings.
12.	DST Bias	Set the amount of time to move DST forward from the standard time. Default is 60 minutes.

To modify the time and date settings in OSD mode:

1. Click **System** > **General**.
2. Select the date format.
3. Enter the new system time and date.
4. Click **Apply** to save the settings.

To modify daylight savings time in OSD mode:

1. Click **System** > **General**.
2. Enter the start and end times for DST.
3. Select the DST bias time. Default is 60 minutes.
4. Click **Apply** to save the settings.

VGA/HDMI resolution

You can select the resolution of the VGA and HDMI monitors.

To set the VGA/HDMI resolution in web mode:

1. Click **Configuration** > **System** > **System Settings**.
2. Click the tab **Menu Output**.
3. Select the desired resolution from the drop-down list for HDMI1/VGA1 and HDMI2/VGA2 (depending on recorder model):

1280*720/60 Hz (720P)	2560*1440/60 Hz (2K) (HDMI only)
1280*1024/60 Hz	3840*2160/30 Hz (4K) (HDMI only)
1600*1200/60 Hz	3840*2160/60 Hz (4K) (HDMI only)
1920*1080/60 Hz (1080P)	7680*4320/30 Hz (8K) (HDMI only)

www.acornfiresecurity.com

www.acornfiresecurity.com

4. Click **Save** to save the settings. The recorder automatically reboots.

To set the VGA/HDMI resolution in OSD mode:

1. Click **System** > **General**
2. Select the desired VGA/HDMI resolution for HDMI1/VGA1 and HDMI 2/VGA2 (depending on the recorder model. The same options as in web mode).
3. Click **Apply** to save the settings. The recorder automatically reboots.

Default live view monitor setup

You can set up the default layout of live view as displayed on the monitor and define the camera channel for each video tile.

To set up the default live view format in OSD mode:

1. Click **System** > **Live View** > **View**.

	Option	Description
1.	Channel list	Shows the list of available camera channels.
2.	Multiscreen options	Specifies the image scale in a video tile. Options are Full Screen, 1+1, 2x2, 1+5, 1+7, 3x3, 4x4. The number of channels available depends on the recorder model.
3.	Unassign all channels from the video tiles.	
4.	Assign all the channels to the video tiles.	
5.	Scroll between the different multiscreen pages. Cameras can be assigned to any video tile. Cameras can be assigned only once.	

www.acornfiresecurity.com

www.acornfiresecurity.com

6. Select the desired multiscreen format.
7. Assign a camera to a video tile.

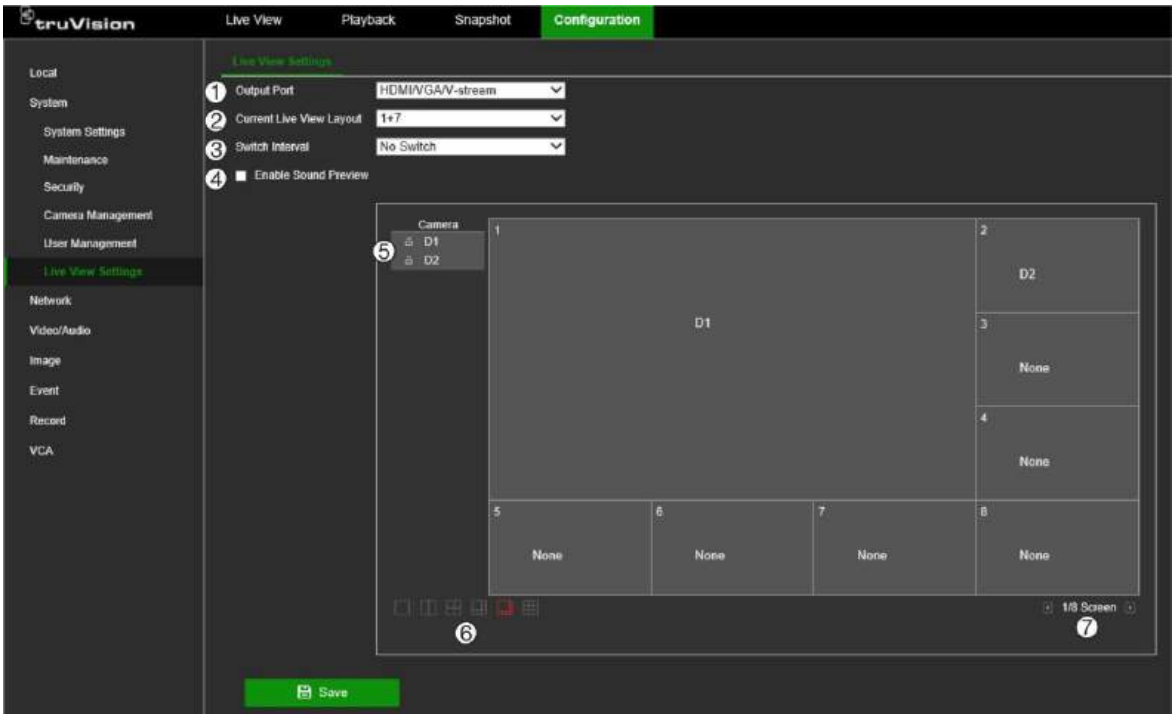
   You can assign each camera manually. Select a video tile and then double-click on the desired camera. To select the camera order for sequencing, select full-screen mode and allocate one camera per page.

   To remove a camera from a tile, click the X on the top right corner of the desired camera in a video tile.

   To assign all cameras automatically to the video tiles, click . The cameras are assigned in numerical order. Click to unassign the cameras.

To set up the default live view format in web mode:

1. Click **Configuration** > **System** > **Live View Settings**.



	Option	Description
1.	Output Port	Applies to OSD mode. CVBS/V-Stream, HDMI1/VGA1 or HDMI2/VGA2. (depending on recorder model)
2.	Current Live View Image	Shows the current multiview mode in use in OSD mode.
3.	Switch interval	This is the dwell time. It is the time a camera is displayed on screen before moving to the next camera. Sequencing can only be done in single-view display mode. The time options are No switch, 5s, 10s, 20s, 30s, 60s, 120s, or 300s.
4.	Enable Sound Preview	Applies to OSD mode only. Enable sound in live view for cameras that support sound.
5.	Camera list	Shows the list of available camera channels.
6.	Multiscreen options	Specifies the image scale in a video tile. Options are Full Screen, 1+1, 2x2, 1+5, 1+7, 3x3, 4x4. The number of channels available depends on the recorder model.

www.acornfiresecurity.com

www.acornfiresecurity.com

	Option	Description
7.	Multiscreen pages	Scroll between the different multiscreen pages. Cameras can be assigned to any video tile. Cameras can be assigned only once.

8. Select the desired multiscreen format.
9. Assign a camera to a video tile.

   You can assign each camera manually. Select a video tile and then double-click on the desired camera. To select the camera order for sequencing, select full-screen mode and allocate one camera per page.

   To remove a camera from a tile, click the X on the desired camera in a video tile.
10. Click **Save** to save the settings.

Behavior for 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. See “Disable Actions” on page 124. for more information.

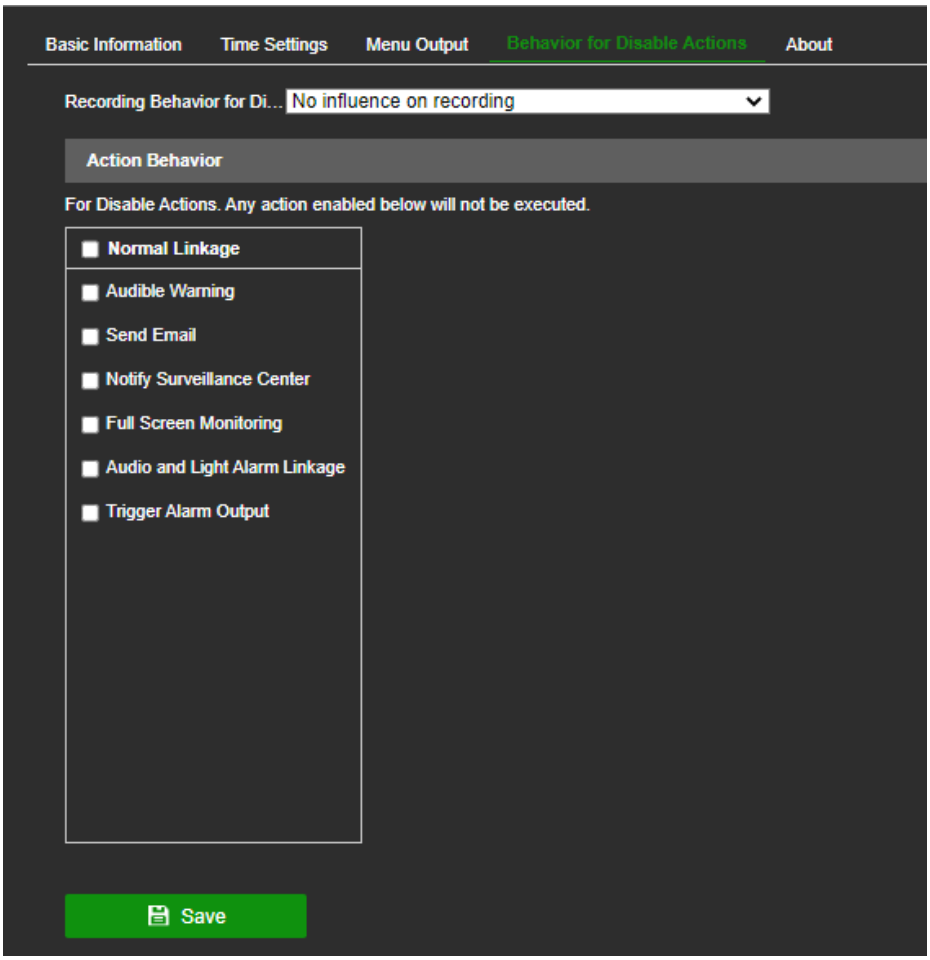
You can select how recordings are carried out for *Disable Actions*. Select one of the options:

- **No influence on recording**: *Disable Actions* will not influence the recordings. Recording of all cameras will continue as scheduled.
- **Disable all recordings**: *Disable Actions* will stop all recordings for all cameras, regardless of the schedule or recording type.
- **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.

You can also select what specific actions will not be executed for an event when Disable Actions is used.

www.acornfiresecurity.com

www.acornfiresecurity.com



For further information on Disable Actions, see “Disable Actions” on page 124.

The setup of the behavior for the event actions cannot be done in OSD mode.

To set the recording behavior for Disable Actions in web mode:

1. Click **Configuration** > **System > System Settings** > **Behavior for Disable Actions**.
2. Select the desired recording behavior from the drop-down list.
3. Click **Save** to save the settings. The recorder automatically reboots.

To set the behavior for the event actions for Disable Actions in web mode:

1. Click **Configuration** > **System > System Settings** > **Behavior for Disable Actions**.
2. Select the actions that will be disabled when the Disable Actions function is active.
3. Click **Save** to save the settings.

To set the recording behavior for Disable Actions in OSD mode:

1. Click **System** > **General**.
2. Under *Recording Behavior for Disable Actions* select the desired option from the drop-down list.

www.acornfiresecurity.com

www.acornfiresecurity.com

3. Click **Apply** to save the settings. The recorder automatically reboots.

Software licenses used

In web mode, click **Configuration** > **System** > **System Settings** > **About** to see the open-source licenses.

This function is not available using OSD mode.

Lock screen password

In OSD mode, you can configure the recorder so that a password is required to log in if the screen is locked. From the OSD menu toolbar, click **System** > **General**. Select **Enable Password**.

This function is not available using web mode.

Screen time out

In web mode, the webpage times out after five minutes if there is no mouse movement by the user.

However, in OSD mode you can change the period before which the screen times out or set up the system so that it never times out. From the OSD menu toolbar, click **System** > **General**. Under **Auto Logout** select the desired period before the system locks out.

Audio Management

It is possible to load AAC or MP3 audio files (max. 1MB) in the recorder that can be played when VCA events are triggered.

VCA events are smart events that some TruVision cameras support such as:

- Cross line detection
- Intrusion detection
- Region entry/exit detection
- Face capture via a TVGP-M01-0401-PTZ-G

To hear the audio, a speaker with amplifier will have to be connected to the audio output of the recorder.

The audio can also be heard via the speakers of connected HDMI monitor.

Via the recorder webpage, you can only setup the actions schedule for playing the audio files.

The OSD menu also allows you to select the audio file for each event.

www.acornfiresecurity.com

www.acornfiresecurity.com

To add custom audio files in the recorder:

Web:

1. Go to **Configuration > System > Audio Management.**
2. Click **Import**.
3. Browse to the location of the audio file, give the audio file a relevant description and import it. The audio file shall be an AAC or MP3 file and can have a max.file size of 1 MB.

OSD:

1. Go to **System > Audio Management**
2. Click **Import.**
3. Browse to the location of the audio file, give the audio file a relevant description and import it. The audio file shall be an AAC or MP3 file and can have a max.file size of 1 MB.

To set the audio files as actions:

Web:

1. Go to **Configuration > Event > Smart Event** and select one of the smart events for a camera that support the playback of the audio file.
2. Setup the event parameters and enable the event.
3. Go to **Actions** and select **Voice Prompt** as Normal Linkage.
4. By clicking on the “wheel” next to Voice Prompt you can setup a specific schedule when the audio will be played. Consider that this schedule must fall within the schedule for the event.

OSD:

1. Go to **Smart Analysis** and select one of the smart event groups from the list that support the playback of the audio files (face recognition, perimeter protection (for cross line and intrusion detection)).
2. Setup the event parameters and enable the event.
3. Go to **Linkage Action** and select Audio Alert as Normal Linkage.
4. By clicking on the “wheel” next to Audio Alert you can select the audio file that will be played and setup a specific schedule when the audio will be played. Please consider that this schedule must fall within the schedule for the event.

www.acornfiresecurity.com

www.acornfiresecurity.com

Maintenance

Reboot

Note: Only the administrator can reboot the recorder.

To reboot the recorder in web mode:

1. Click **Configuration** > **System** > **Maintenance** > **Upgrade & Maintenance** > **Reboot**.
2. A pop-up screen appears asking you to confirm your user name and password. Click **OK**.
3. The recorder reboots.

To reboot the recorder in OSD mode:

1. Click the Power button on the top right-hand corner of the screen.
2. Click the **Reboot** button in the *Power* pop-up window.
3. A pop-up screen appears asking you to confirm the admin name and password. Click **OK**.
4. The recorder reboots.

Upgrade system firmware

The firmware on the recorder can be updated using these methods:

- Via a USB device
- Via the recorder web page
- Via the recorder OSD
- Using TruVision Navigator. For further information, refer to the TruVision Navigator user manual.
- When the recorder is using UltraSync for the internet connection, it is possible to check if a new firmware is available. When it is available, it can be downloaded and installed.

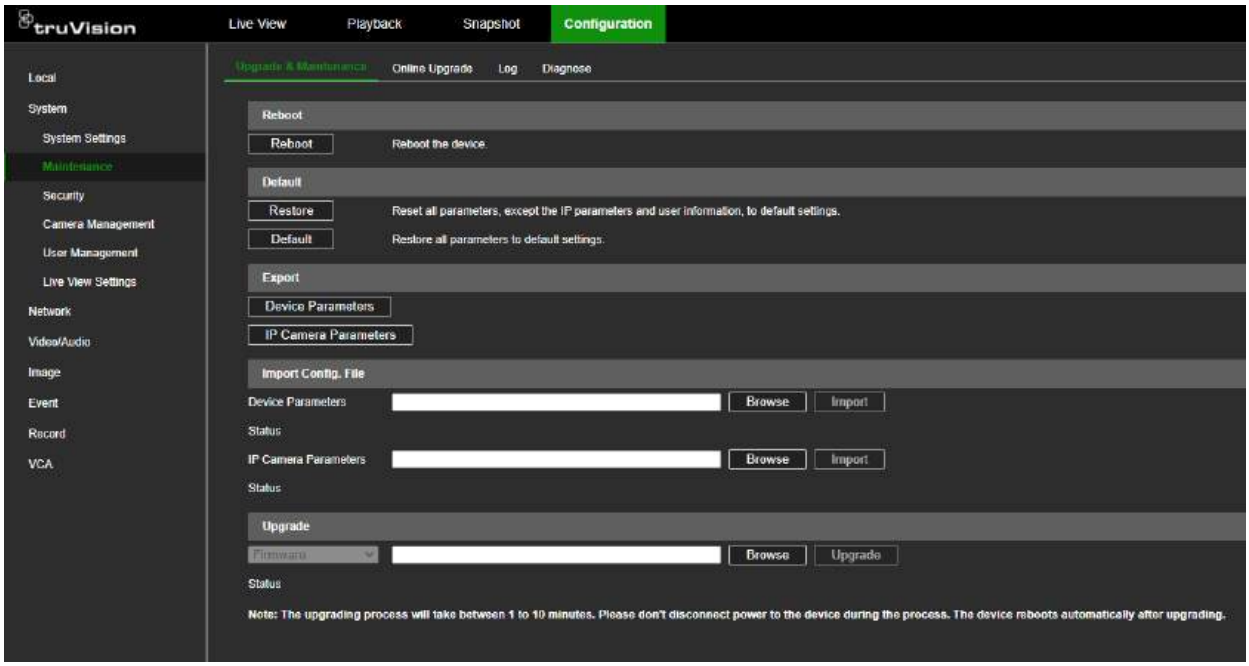
The firmware upgrade file is labeled *tvn12.dav*.

To update the system firmware in web mode:

1. Click **Configuration** > **System** > **Maintenance** > **Upgrade & Maintenance**.

www.acornfiresecurity.com

www.acornfiresecurity.com



2. Under the section “Upgrade”, click **Browse** and search for the latest firmware file. You can find the latest firmware on our website, www.firesecurityproducts.com, and search for “TVN 23 (S/P)”.
3. Click **Upgrade**.

To check if a new firmware is available via UltraSync in web mode:

Note: The firmware can only be upgraded online when the recorder is subscribed to the Core Video Plus service (or higher) for UltraSync. See Chapter 18 “UltraSync related functions” on page 216 for more information.

1. Click **Configuration** > **System** > **Maintenance** > **Online Upgrade**.
2. Click **Check Upgrade** to see if new firmware is available.
3. If a new version is detected on the UltraSync server, it will appear on screen.

   Click the **Upgrade** button to start the upgrade.

   A message appears saying that the device cannot be operated during the upgrade process. Press **OK** to start the upgrade.
4. When the upgrade is completed, the recorder will reboot automatically.
5. When the upgrade was done through a remote session the session will be ended.

To update the system firmware in OSD mode:

Via a USB device

1. Download the latest firmware to a USB device from our website at:

   www.firesecurityproducts.com and search for “TVN 23 (S/P)”

www.acornfiresecurity.com

www.acornfiresecurity.com

2. Connect the USB device to the recorder.
3. Click the Maintenance button from the top toolbar and select **Upgrade > Local Upgrade**
4. Select the USB stick from the dropdown menu and select the *tvn23.dav* file
5. Click the firmware upgrade button .
6. Click **Upgrade**.
7. When the upgrade process is completed, the recorder will reboot automatically.

Via the UltraSync cloud

Note: The online firmware upgrade is only possible when the recorder is subscribed to the Core Video Plus service (or higher) for UltraSync. See Chapter 18 “UltraSync related functions” on page 216 for more information.

1. Click the Maintenance button from the top toolbar and select **Upgrade > Cloud Upgrade**.
2. The current version is displayed. Click **Check Upgrade.** The recorder will check if a newer firmware can be found in the UltraSync cloud.
3. If a new version is detected on the UltraSync server, it will appear on screen.

   Click the **Upgrade** button to start the upgrade.

   A message appears saying that the device cannot be operated during the upgrade process. Press **OK** to start the upgrade.
4. When the upgrade is completed, the recorder will reboot automatically.

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.

To restore parameters to factory default settings in web mode:

1. Click **Configuration** > **System** > **Maintenance** > **Upgrade & Maintenance**.

   Note: Only the administrator can restore the default settings.
2. 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.

   — or —

   To restore all parameters, except network and user settings, to default factory settings:

www.acornfiresecurity.com

www.acornfiresecurity.com

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 and user settings to default.

3. Click **OK** to confirm.

To restore parameters to factory default settings in OSD mode:

1. Click the Maintenance button from the top toolbar.

   Note: Only the administrator can restore the default settings.

2. Click on **Default**.
3. Select the type of default restoration required:

   Restore Defaults: Restore all parameters, except the network (including IP address, subnet mask, gateway, MTU, NIC working mode, default route, server port, etc.) and user account parameters, to the factory default settings.

   Factory Defaults: Restore all parameters to the factory default settings.

   Restore to Inactive: Restore the recorder to the inactive status. Only the admin password will be restored.

4. Enter the admin password and click **Yes** to confirm the selection. The recorder will reboot automatically.

Import/export configuration files

You can export and import configuration settings from the recorder or IP cameras. This is useful when you are updating or replacing a recorder with IP cameras, or if you want to make a backup of the recorder and IP camera settings.

The exported recorder config file cannot be opened. However, the exported camera configuration file is a XLS file of all the cameras added to the recorder. This Excel file can be edited on a computer via Microsoft Excel.

If you are going to import this IP camera information to a new recorder, for example, change the recorder model name in the file to the new model's name, then be aware that the camera passwords are not displayed in the file. Go to "Display the camera passwords" on page 55 for information on how to see the camera passwords in the recorder. These can then be manually entered into the Excel file for each camera before importing the file into the new recorder.

Save the file on the PC as an Excel file. The file is then ready to be imported to a different TVN 23 (S/P) recorder.

Note: The recorder config file can only be exported and imported in web mode.

To export the recorder and camera configuration files in web mode:

1. Insert an external storage device into the recorder.
2. Click **Configuration** > **System** > **Maintenance** > **Upgrade & Maintenance**.

www.acornfiresecurity.com

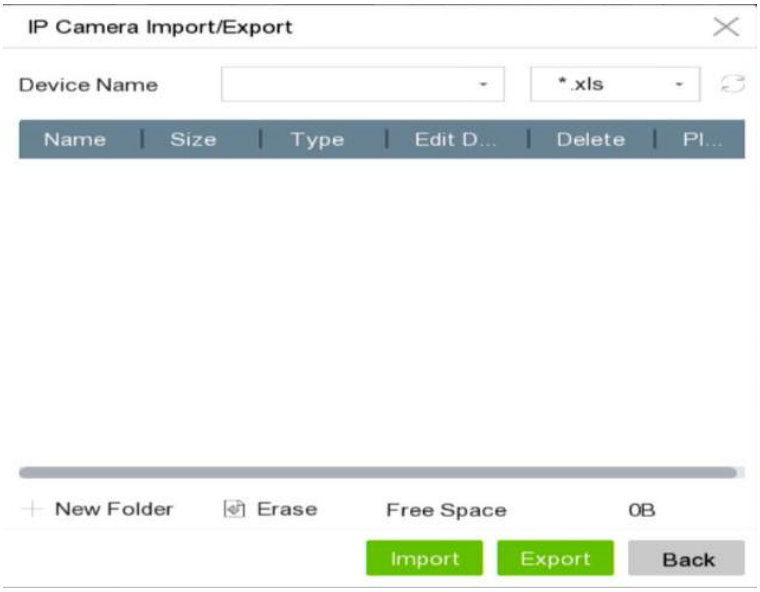
www.acornfiresecurity.com

3. Under *Export*, click **Device Parameters** to export the recorder's configuration settings into an external storage device. The recorder's configuration file cannot be opened.
4. Click **IP Camera Parameters** to export the camera configuration settings into an external storage device.
5. Make any changes required to the camera configuration file.

To export the camera configuration file in OSD mode:

1. Insert a backup device in the recorder.
2. Click **Camera** > **Camera** > **IP Camera** > **Import/Export**.

   The backup device name and path are displayed.



3. Select the configuration file and click **Export**. The file is saved to the backup device.

   Note: The passwords of the cameras are not exported. Their values in the exported file are empty.

To import the recorder and camera configuration files in web mode:

1. Insert an external storage device in the recorder that has your camera configuration XLS file.
2. Click **Configuration** > **System** > **Maintenance** > **Upgrade & Maintenance**.
3. To import a recorder's parameters, under the section "Import Config. File > Device Parameters" click **Browse** to locate the desired recorder configuration file on the external storage device. The file name is displayed beside the Browser button. Click **Import**.

www.acornfiresecurity.com

www.acornfiresecurity.com

4. To import the Excel file with the camera parameters, under the section “Import Config. File > IP Camera Parameters” click **Browse** to locate the desired camera configuration file on the USB stick or hard drive. The file name is displayed beside the Browser button. Click **Import**.

   If the camera passwords were included in the XLS file, the cameras are immediately connected to the recorder. If there are no camera passwords included in the file, you will need to add them manually to each camera (go to Camera Management > IP Camera > Modify.)

To import a camera configuration file in OSD mode:

1. Insert a backup device in the recorder.
2. Click **Camera** > **Camera** > **IP Camera** > **Import/Export**.
3. Select the desired configuration file and click **Import**.

   If the camera passwords were included in the XLS file, the cameras are immediately connected to the recorder. If there are no camera passwords included in the file, you will need to add them manually to each camera. Go to Camera > IP Camera, switch to the list view (press) and press Edit .

4. Enter the camera password in the Password field and press OK. Do this for every camera.

Search system logs in web mode

Many events of the recorder, such as operation, alarm, information, and notification are logged into the system logs. They can be viewed and exported at any time.

Up to 2000 log files can be viewed at once.

Log files can also be exported onto a USB device or hard drive. The exported file is named according to the time it was exported. For example: 20220919124841logBack.txt.

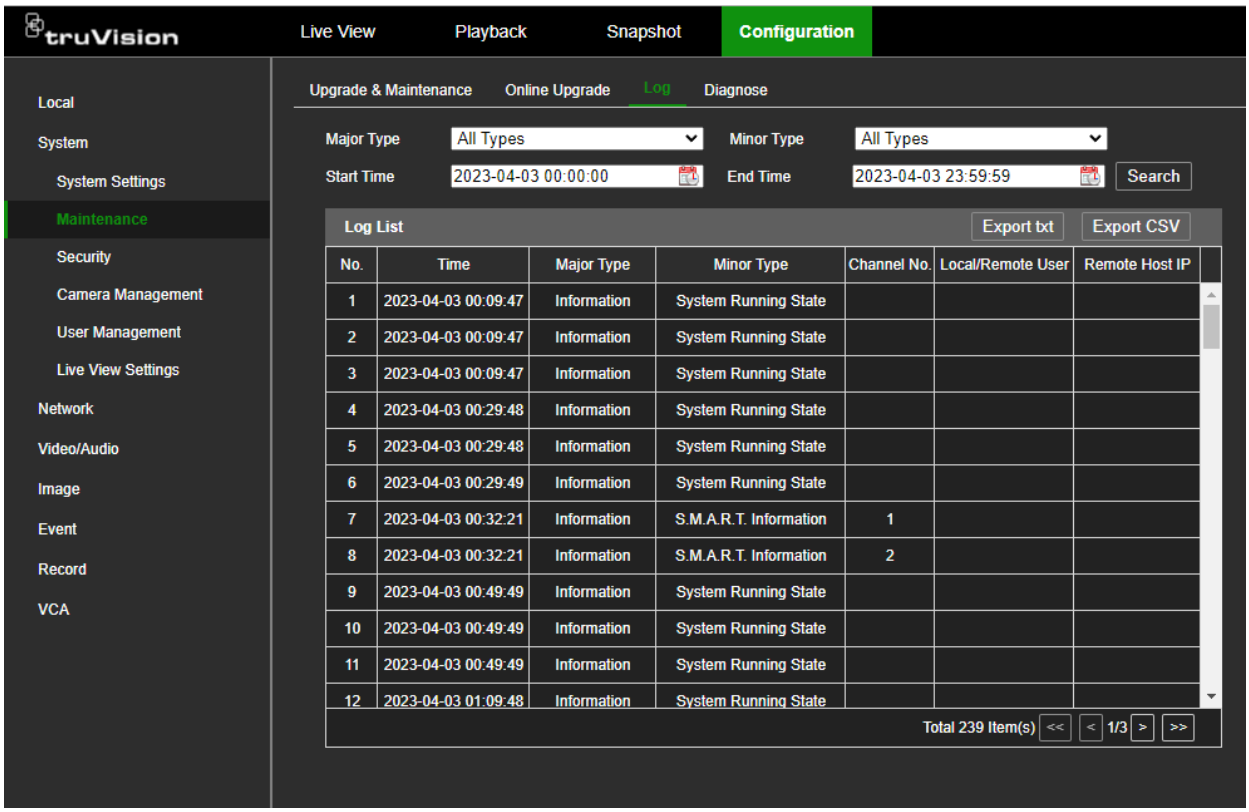
Note: Connect the backup device, such as a USB flash drive, to the recorder before commencing the log search.

To search for video from the system log in web mode:

1. Click **Configuration** > **System** > **Maintenance** > **Log**.
2. Select the search start and end date and times.
3. Select one of the **Major Type** and **Minor Type** options from the drop-down lists.
4. Click the **Search** button. A list of results appears.

www.acornfiresecurity.com

www.acornfiresecurity.com



For each log item, the log file shows the time, major type, minor type, channel number, local/remote user, remote host IP, and details.

5. Click **Export** to archive the log file to a USB flash device. The Export window appears. Select where you want to save the file. The default file type is *.txt. Click **Save** to export the selected file.

Search system logs in OSD mode

Many events of the recorder, such as operation, alarm, information, and notification are logged into the system logs. They can be viewed and exported at any time.

Up to 2000 log files can be viewed at once.

Log files can also be exported onto a USB device or hard drive. The exported file is named according to the time it was exported. For example: 20220919124841logBack.txt.

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

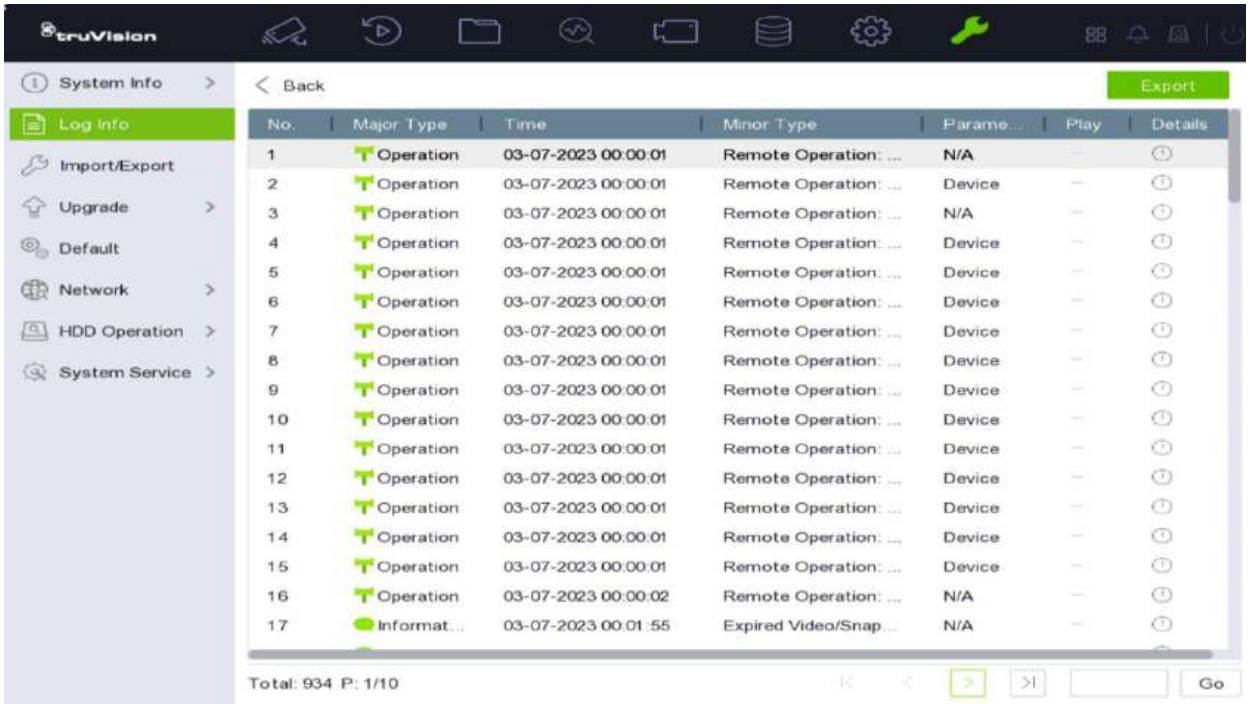
To search for video from the system log in OSD mode:

1. Click **Maintenance** > **Log Info**. The *Log Information* screen appears.
2. Select the search start and end date and time.
3. Select one of the **Major Type** and **Minor Type** options from the drop-down lists.
4. Click the **Search** button. A list of results appears.

www.acornfiresecurity.com

www.acornfiresecurity.com

For each log item, the log file shows the major type, time, minor type, channel number, local/remote user, remote host IP, and details.



5. Click **Export All** to archive the log file to an external storage device, such as a USB flash device. The Export window appears. Select where you want to save the file. The default file type is *.txt. Click **Save** to export the selected file.

Diagnose

This feature is only for Technical Support. The diagnose feature allows the technical support engineer to capture data from the recorder for troubleshooting.

You can save a file of a camera stream on a USB flash drive for later analysis.

The diagnostic functions are not available in OSD mode.

There are two diagnosis possibilities:

- Diagnose the recorder.
- Diagnose one or more camera streams.

To diagnose the recorder:

1. Get the special debug file from Technical Support.
2. Use an empty USB flash drive and install the debug file in the root directory.
3. Insert the USB flash drive into the recorder.
4. Click **Configuration** > **System** > **Maintenance** > **Diagnose**.
5. Select **USB Flash Drive Debugging** and click **Save**.
6. Reboot the recorder.

www.acornfiresecurity.com

www.acornfiresecurity.com

7. Once the recorder reboots, it will write diagnostic information to the USB flash drive.
8. Follow the instructions from Technical Support.
9. After the debugging session, go again to **Configuration** > **System** > **Maintenance** > **Diagnose**, deselect **USB Flash Drive Debugging,** and click **Save**.
10. Remove the USB flash drive and send the captured files to Technical Support.

To debug a camera stream:

1. Insert a USB flash drive into the recorder.
2. Click **Configuration** > **System** > **Maintenance** > **Diagnose**.
3. Under **Stream Debugging** > **Channel No**., select the desired camera.
4. Under **Stream Type**, select the stream type.
5. Click **Start Debugging**. The file is saved on the USB flash drive.

To export diagnostic information:

1. Click **Configuration** > **System** > **Maintenance** > **Diagnose**.
2. Under **Diagnose Information**, select **Enable Export Diagnostic Information**.
3. A dialog window will open, and you can save the file on the PC.
4. The exported file is for technical support purpose only and contains log information, system information and hardware information.

To capture network packages on a USB flash drive

This option allows you to capture network packages (in Wireshark format) between devices and the recorder.

1. Insert a USB flash drive in a USB port of the recorder.
2. Click **Configuration** > **System** > **Maintenance** > **Diagnose**.
3. Set the filter parameters:
   - IP address of the external device.
   - Network inferface of the recorder.
4. Click **Start Capture**.

Security

Authentication

The administrator can set the authentication to access RTSP and HTTP streams.

www.acornfiresecurity.com

www.acornfiresecurity.com

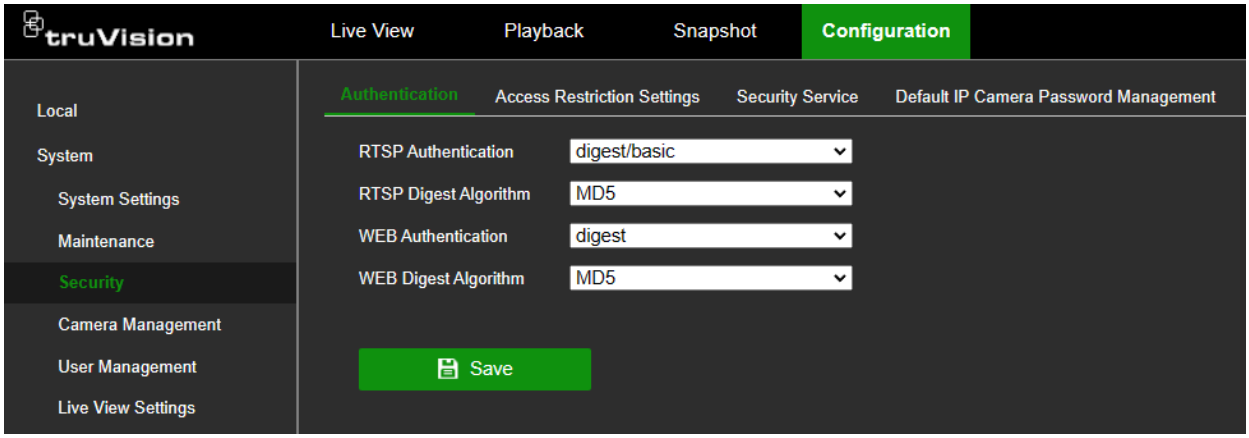
The RTSP authentication by default is set to “digest/basic”. The HTTP (Web) authentication is set by default to “digest”. The authentication type should be left at its default values unless otherwise instructed by the system administrator, as choosing the wrong value will negatively impact performance.

Note: RTSP and HTTP must first be enabled to be authenticated. Go to **Network** > **Advanced Settings** > **Network Service** (on the web page) to check their status. By default, they are enabled.

The ISAPI protocol can be enabled/disabled. ISAPI stands for “Internet Server Application Programming Interface”. This interface can enable external systems to interact with the recorder.

To set RTSP and HTTP (Web) authentication in web mode:

1. Click **Configuration** > **System** > **Security** > **Authentication**.



2. Select the desired authentication type, **Digest** or **Digest/Basic**. It is recommended to keep the values at default.
3. For Digest authentication:set the RTSP and HTTP (web) Digest Algorithm. The default value is MD5.
3. Click **Save** to save the settings.

To set RTSP and HTTP authentication in OSD mode:

1. Click **Maintenance > System Service >System Service**.

www.acornfiresecurity.com

www.acornfiresecurity.com

2. Select the **Enable** RTSP check box to enable the function. It is enabled by default.
3. Select the desired **RTSP authentication type**, **Digest** or **Digest/Basic**. It is recommended to keep the value at default.
4. Select the **Enable HTTP** check box to enable the function. It is enabled by default.
5. Select the desired **HTTP authentication type**, **Digest** or **Digest/Basic**. It is recommended to keep the value at default.
6. For Digest authentication:set the RTSP and HTTP (web) Digest Algorithm. The default value is MD5.
7. Click **Apply** to save the settings.

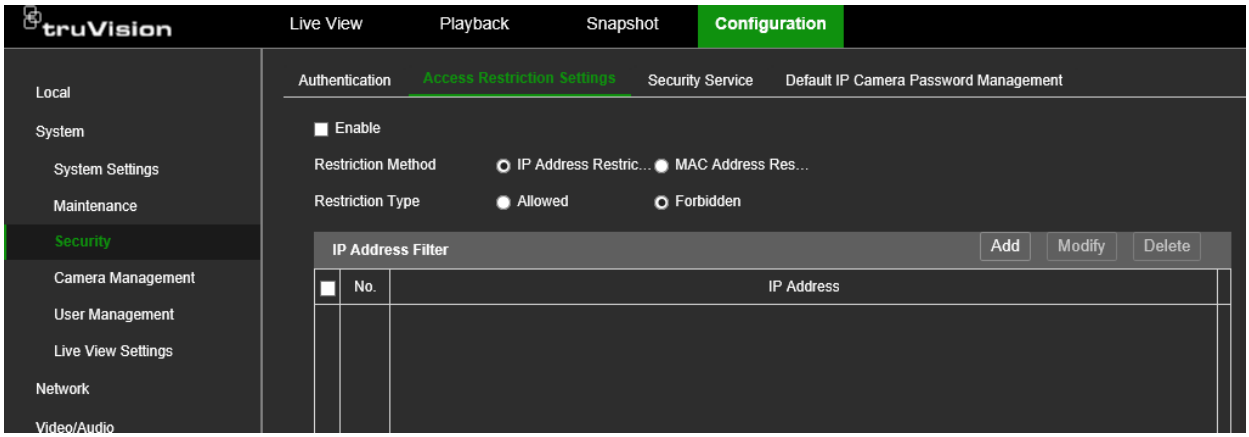
Restrict IP address access

Use this menu to restrict access to specified IP or MAC addresses to the recorder. This function can be used to control who can log on to your recorder.

This function is not available in OSD mode.

To enable/disable the IP address access restrictions in web mode:

1. Click **Configuration** > **System** > **Security** > **Access Restriction Settings**.



2. Select **Enable** to enable the function. It is disabled by default.
3. Select whether you want to restrict/allow an IP address or a MAC address. Then under **Restriction Type**, select **Allowed** or **Forbidden**.
4. Click **Add** to save the setting and enter the IP address or MAC address.

   Addresses in the list can be modified and deleted.
5. Click **Save** to save the setting.

SSH network protocol

SSH or Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network.

This function is for technical support only and is not available using OSD mode.

www.acornfiresecurity.com

www.acornfiresecurity.com

To enable/disable the SSH protocol in web mode:

1. Click **Configuration** > **System** > **Security** > **Security Service**.
2. Select **Enable SSH** if required. It is disabled by default.
3. Click **Save** to save the setting.

Picture URL Digest Authentication (web only)

When using HTTP protocol to download the pictures which are uploaded by SDK, picture URL digest authentication controls whether the picture download process requires digest authentication or not. You can configure picture URL digest authentication via web browser.

To enable/disable picture URL Digest Authentication:

1. Click **Configuration** > **System** > **Security** > **Security Service**.
2. Select **Enable Picture URL Digest Authentication** if needed.
3. Click **Save** to save the setting.

Serial Port Authentication Service (web only)

The serial port can be used to capture device information for technical support reasons. The serial port authentication service provides the authentication for the serial port usage.

To enable/disable serial port authentication service:

1. Click **Configuration** > **System** > **Security** > **Security Service**.
2. Select **Enable Serial Port Authentication Service** if needed.
3. Click **Save** to save the setting.

You will notice that disabling this service will show an extra entry field for the Service Close Time.

Service Close Time

When you disable the authentication, you need to specify how many days that the serial port will be closed.

For example, if Service Close Time is set as 3, the serial port authentication service will be closed for 3 days. And after 3 days, serial port authentication service will be enabled.

Text insertionText insertion lets you insert or display text from a point-of-sale (POS) automated teller machine (ATM) or other systems on the video display of the recorder.

www.acornfiresecurity.com

www.acornfiresecurity.com

The text is saved and time-stamped together with the video. You can then search the text for specific video clips. The text can be enabled or disabled during live view and playback.

You can apply text insertion for half of the channels that a recorder model supports.

Setting up text insertion

To set up text insertion via the OSD

1. Click **System > Text Insertion.**
2. Select a text insertion channel by clicking on a video tile.
3. Click **Edit**.
4. **Enable** text insertion.
5. Select the text insertion protocol from the dropdown list.

   The available protocols are: Universal, EPSON and Probridge.

   - **Universal:**

     Click **Advanced** to expand more settings when selecting the universal protocol. You can set the start line identifier, line break tag, and end line tag for the POS overlay characters, and the case-sensitive property of the characters. You can also optionally check the filtering identifier and the XML protocol.

   - **EPSON:**

     The EPSON protocol is used with the NPCII (*) over IP or serial connection.

     (*) For the NPCII: this text insertion converter is offered by the German company SHL Systems and that is compatible with this recorder. SHL Systems can offer customized firmware to adapt the NPCII to specific needs.

   - **Probridge:**

     The Probridge protocol works with the old Kalatel text insertion modules.

6. Select the **Connection Mode** and click **Parameters** to configure the parameters for each connection mode.

   - **TCP Connection**

     When using TCP connection, the port must be set from 1 to 65535, and the port for each POS machine must be unique.

     Set the **Allowed Remote IP Address** of the device sending the POS message.

   - **UDP Connection**

www.acornfiresecurity.com

www.acornfiresecurity.com

When using UDP connection, the port must be set from 1 to 65535, and the port for each POS machine must be unique.

Set the Allowed Remote IP Address of the device sending the POS message.

- **USB-to-RS-232**

  Configure the USB-to-RS-232 convertor port parameters, including the port serial number, baud rate, data bit, stop bit, parity, and flow control.

- **RS-232 Connection**

  Connect the device and the POS machine via RS-232. The RS-232 settings can be configured via **System > Serial > RS-232** . The Usage must be set to **Transparent Channel**.

- **Multicast Connnection**

  When connecting the device and the POS machine via Multicast protocol, set the multicast address and port.

- **Sniff Connection**

  Connect the device and the POS machine via Sniff. Configure the source address and destination address settings.

To setup text insertion via the webpage:

1. Click **Configuration > System > Text Insertion**.
2. Enable **Text Insertion**.
3. Select the channel from the dropdown list.
4. Select the text insertion protoctol and set up the parameters.

To configure the text insertion overlay (OSD only):

1. Click **System > Text Insertion.**
2. Select a text insertion channel by clicking on a video tile.
3. Click **Edit**.
4. In Channel Linkage and Display, select a camera in the dropdown list that will be assigned to this text insertion chaannel.
5. Set the following parameters:
   a. Character Encoding format
   b. Overlay Mode: to show the characters scrolling over the image or to display them per page.
   c. Font size and color.
   d. Display time (sec.) of the characters. The value needs to be between 5 and 3600 sec.

www.acornfiresecurity.com

www.acornfiresecurity.com

   e. Timeout of POS event: The value needs to be between 5 and 3600 sec. When the device ha snot received the POS message within the defined time, the transaction ends.

6. In **Privacy Settings**, set the POS privacy information to not display on the image, e.g., the card number, user name, etc. The defined privacy information will be displayed using ***on the image instead.
7. Check **Overlay POS in Live View**. When this feature is enabled, the POS information is overlaid on the Live View image.
8. Click **Apply** to activate the settings.

To setup the arming schedule and the actions:

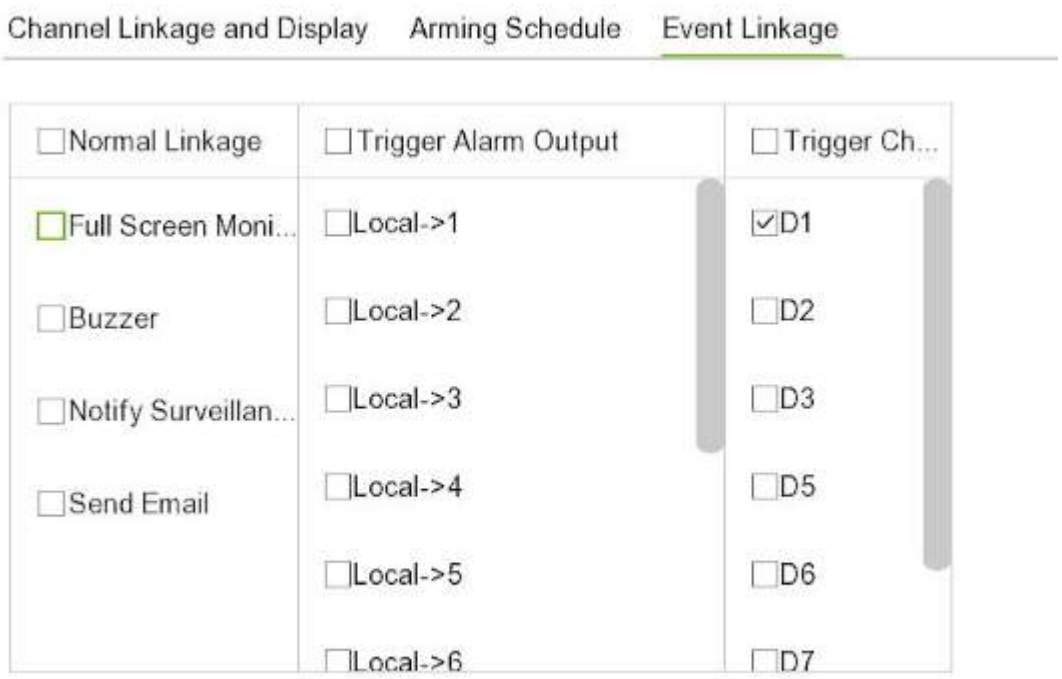
A text insertion event can trigger the recording of camera's, trigger the full screen monitoring etc.

1. **To setup the arming schedule and the actions (via the OSD):**Click **System > Text Insertion**
2. Select a text insertion channel by clicking on a video tile.
3. Click **Edit**.
4. Setup the **Arming Schedule** for the actions**.**
5. Setup action in **Event Linkage.** You can setup normal linkage actons: full screen monitoring, sound the recorder buzzer, notify the surveillance cneter (= send the events to TruVision Navigator) and/or send an email.

   One or more alarm output(s) can be triggered or the event can trigger the recording for one or more cameras.
6. Click **Apply** to activate the settings.

www.acornfiresecurity.com

www.acornfiresecurity.com



To setup the arming schedule and the actions (webpage):

1. Click **Configuration > System > Text Insertion**
2. Select the channel from the dropdown list.
3. Setup the schedule in the **Arming Schedule** tab and define the actions in the **Actions** tab.

www.acornfiresecurity.com

www.acornfiresecurity.com

Chapter 5
Camera management

Camera Management allows you to add and remove IP cameras as well as modify their settings. The recorder supports most TruVision IP cameras and encoders and is compliant with ONVIF profile S cameras. See Table 2 below for the list of cameras supported by the recorder.

Note: Ensure that any ONVIF camera has been tested together with the recorder before installation.

Table 2: TruVision cameras, encoders, and decoders supported by TVN 23 (S/P)

Camera Series	Features
S1 IP Cameras (TVx-11xx)	Support for live view and continuous/event recording, as well as search and playback.
S2 IP Cameras (TVx-12xx)	Support for live view and continuous/event recording, as well as search and playback.
S3 IP Cameras (TVx-53xx)	Support for live view and continuous/event recording, as well as search and playback.
S4 IP Cameras (TVx-54xx)	Support for live view and continuous/event recording, as well as search and playback.
S5 IP Cameras (TVx-55xx)	Supported.
S6 IP Cameras (TVx-56xx)	Supported.
M Series IP Cameras (TVGP-M01 fixed cameras)	Supported. Able to set target type (people/vehicle) and search for these events in the recorder.
Full color cameras (TVFC-M01-040x-BUL-G, TVFC-M01-040x-DOM-G, TVFC-M01-040x-TUR-G, TVFC-M01-0401-WED-G)	Supported. Able to set target type (people/vehicle) and search for these events in the recorder.
S7 IP Cameras (TVx-57xx)	Supported (FW upgrade S7 camera needed to hide non-supported person/vehicle option in TVN 23 (S/P) camera configuration menu).
P Series IP cameras (TVGP-P01 fixed cameras)	Supported.

www.acornfiresecurity.com

www.acornfiresecurity.com

Camera Series	Features
Stainless Steel Dome Camera (TVD-5801)	Support for live view and continuous/event recording, as well as search and playback.
Stainless Steel PTZ Camera (TVP-5201)	Support for live view and continuous/event recording, as well as search and playback.
FishEye - 360* Cameras (TVF-110x)	Support for live view and continuous/event recording, as well as search and playback.
FishEye – 360° Cameras (TVF-520x)	Supported up to 6MP.
360° cameras TVPA-S01-060x-360-G, TVPA-S01-120x-360-G	Supported up to 6MP
Compact IP PTZ Cameras (TVP- 5101/5102/5103)	Supported.
Full-size IP PTZ Cameras (TVP-5104/5105)	Supported.
Legacy IP PTZ Cameras (TVP-110x)	Support for live view and PTZ control, continuous/event recording, as well as search and playback.
IP PTZ Camera (TVP-1122)	Supported.
Panoramic Camera (180 TVW-3130)	Support for live view and continuous/event recording as well as search and playback.
Multi-imager Camera (TVS-5101)	Supported.
Thermal IP Camera (TVB-5701)	Support for streaming/recording and thermal events.
ANPR cameras (TVB-5412/5413)	Only streaming/recording. No ANPR events.
Encoders (TVE-110/410/810/1610)	Supported, H.264 only.
Encoders (TVE-120/420/820/1620)	Supported, H.264 and H.265.
Decoders TVE-DEC11/12	Supported.
S Series Thermal IP camera (TVTH-S01)	Supported. Able to set target type (people/vehicle) and search for these events in the recorder.
M Series IP PTZ Cameras (TVGP-M01-xxxx-PTZ-G)	Supported. Able to set target type (people/vehicle) and search for these events in the recorder. Support for face capturing.
M Series IP PTZ Cameras (TVGP-P01-xxxx-PTZ-G)	Supported. Able to set target type (people/vehicle) and search for these events in the recorder. Support for face capturing.

The TVN 23 (S/P) contains protocols from third-party camera manufacturers that allow you to add cameras from these manufacturers to the recorder.

The cameras cannot be discovered via the discovery feature of the recorders. These cameras need to be added manually. See Figure 7 on page 50 when using web mode and Figure 8 on page 51 when using OSD mode for more details.

www.acornfiresecurity.com

www.acornfiresecurity.com

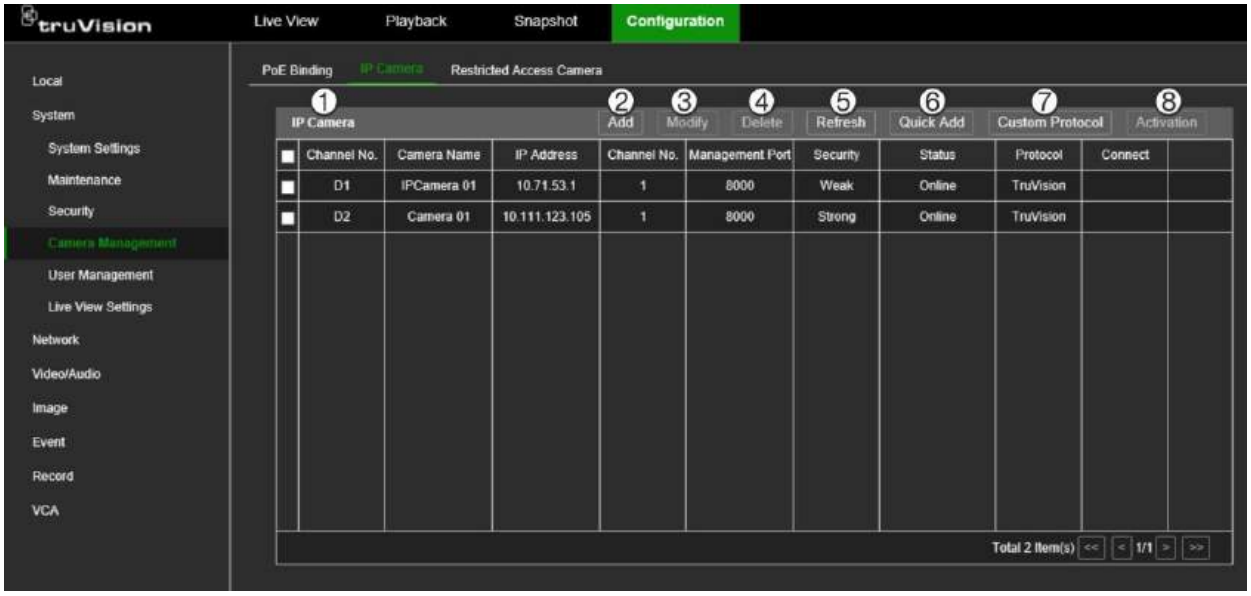
The following brands are supported: Acti, Arecont, Axis, Bosch, Brickom, Canon, Hunt, Panasonic, Pelco, Samsung, Sanyo, Sony, Vivotek, and Zavio.

Carrier cannot provide a list of supported cameras. It is the responsibility of the installer to test a third-party camera before installing it.

Manage IP cameras in web mode

Click **Configuration** > **System** > **Camera Management** > **IP Camera** to get to the web page for managing cameras.

Figure 7: Managing IP cameras in web mode



Feature	Description
1. IP camera list	This shows the list of IP cameras added to the recorder. The camera information shown is Camera Number, Camera Name, Channel Number, IP Address, Management Port, Security, Status, Protocol, and Connect. The “Connect” column is the list of bridge PoE/IP addresses that can be clicked to go to the selected camera web page. It only appears on this page if the “Bridge PoE/IP” function” under *Network* > *Advanced Settings* > *Other* is enabled. See “Open the camera web page from within the recorder web page” on page 85 for more information.
2. Add	Manually add a camera to the recorder by entering its IP address and other required information.
3. Modify	Select a camera from the list to change its IP Camera Address, Protocol, Management Port, Channel No., and Transfer protocol. You also need to enter the name and password of the selected camera. The camera by default is time synchronized with the recorder. For more information on managing camera passwords, see “Manage camera passwords” on page 55.
4. Delete	Delete the selected IP camera from the list.
5. Refresh	Reload webpage.

www.acornfiresecurity.com

www.acornfiresecurity.com

Feature	Description
6. Quick Add	Add an IP camera from the network. **Note**: The camera password must be recognized by the recorder. It should be either the same as the recorder password or the same as the default IP camera password. Change the camera password in **Modify**.
7. Custom Protocol	You can see the protocol in use under the “Protocol” column. Use the “Custom Protocol” feature to connect an IP camera that does not use a standard protocol, such as TruVision. Many IP cameras can stream video using the RTSP protocol. The recorder allows you to define an RTSP custom protocol per camera type and to add cameras to the recorder via RTSP. Select one of the customized protocols listed and give it a name. Select the main stream or substream and the protocol type, transfer protocol, port, RTSP, and the stream path. **Note**: When adding cameras via RTSP, only video streaming is available. No other functionality will be supported by the recorder.
8. Activation	Enter the selected IP camera’s password so that it is activated by the recorder. By enabling the “Use Default IP Camera Password” the recorder will use the default camera password that applies to all cameras activated by the recorder. See “Manage camera passwords” on page 55 for more information.

Note: More functionality is available using OSD mode.

Manage IP cameras in OSD mode

Click **Camera** > **Camera** > **IP Camera** to get to the OSD page for managing camera.

Figure 8: Managing IP cameras in OSD mode

www.acornfiresecurity.com

www.acornfiresecurity.com

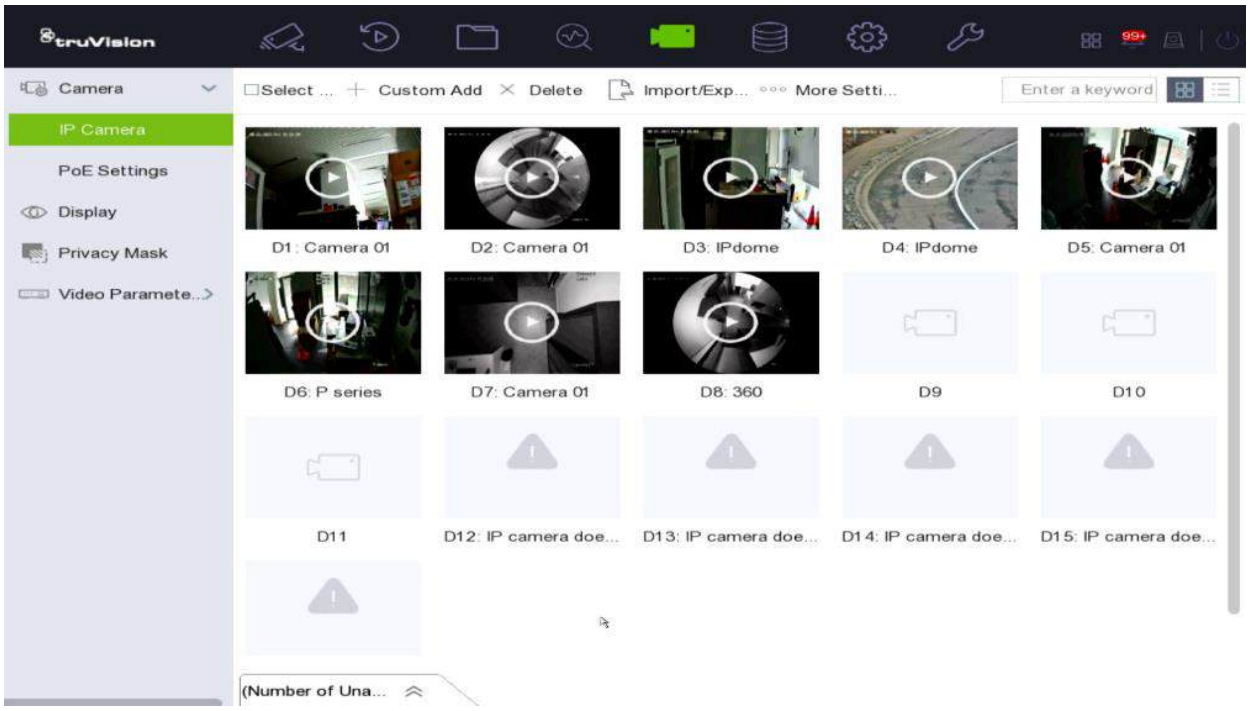
Feature	Description
Added Device List	
1. Camera List	This is the list of IP cameras added to the recorder. The maximum number of cameras permitted will depend on the recorder model. The camera information shown is Number, Delete, Status, Security, IP address, Edit, Upgrade, Camera Name, Protocol, Device Model, Management Port, Serial Number, Firmware Version, Advanced Settings.
2. +Custom Add	Manually add a camera listed under the *Online Device List* to the recorder by entering its IP address and other required network information. You can enable the **Camera Activation Password** from here. For more information on managing camera passwords, see “Manage camera passwords” on page 55. You can also enable the IP camera time sync, to sync the time of the camera with the recorder time. There is a possibility to use the default management port for the selected camera and to view the security certificate of the selected camera.
3. Delete	Delete the selected camera from the *Added Device List*.
4. Import/Export	To import or export the IP camera parameters from the recorder. See page 36 for more information.
5. …. More	Several more functions are available: **H.265 Auto Switch Configuration**: When you enable this option, the recorder will automatically switch to the H.265 stream when the IP camera is initially added (if the IP camera supports H.265 video format). Default is enabled. **Upgrade**: Upgrade the firmware of the selected cameras. The cameras will automatically reboot after the upgrade is complete. **Protocol**: Displays the protocol in use. However, instead of using a standard protocol, such as TruVision, you can set up an RTSP custom protocol per camera type and add cameras to the recorder via RTSP. Select a custom protocol to create and then complete the protocol information requested. You can set up a custom protocol for main and substream. Click **OK**. Once the custom protocol is set up, you can link the protocol to a camera. When adding a new custom camera, this RTSP custom protocol can be selected as the camera’s protocol. **Channel Default Password Management:** See page 56
Online Device List	
6. Online Device List	This is the list of devices found on the LAN and not linked to this recorder. The devices, however, could be linked to another recorder. Devices with an orange triangle as their status indicate that these cameras are already added to another recorder. You can enable/disable this function via the web or OSD. Via the web: Go to **Configuration** > **Network** > **Advanced Settings** > **Other** and select **Enable IP Camera Link Detection**. Via the OSD: Go to **Maintenance** > **System Service** and enable/disable **Enable IP Camera Occupation Detection**
7. +Add	Add an IP camera from the LAN to the recorder. If there are already the maximum number of permitted cameras connected to the recorder, a message will appear saying that this camera cannot be added.

www.acornfiresecurity.com

www.acornfiresecurity.com

Feature	Description
	For PoE models: when all PoE ports are enabled, you cannot add cameras from the LAN network. Go to **PoE Binding** to disable PoE ports first before you can add cameras from the LAN network (see “Use the LAN network” on page 58 for more information). **Note**: The camera password must be recognized by the recorder. It should be either the same as the recorder password or the same as the default IP camera password. Change the camera password in **Modify**.
8. Activate	Activate the selected cameras before adding them to the recorder.
9. Refresh	Refresh the status of the cameras in the list.

Besides the list view for the cameras (as shown in the above screenshot), It is also possible to show a visual overview of the connected cameras.To switch to the visual view click on the icon in the top right corner of the screen:



To switch to the list view of the connected cameras, click on the other icon:

The visual view shows a small video tile for every connected camera.

You can hover over the video tile with the mouse to view more information about the camera:

www.acornfiresecurity.com

www.acornfiresecurity.com

You can also upgrade, delete or edit the camera (see icons in the green bar).

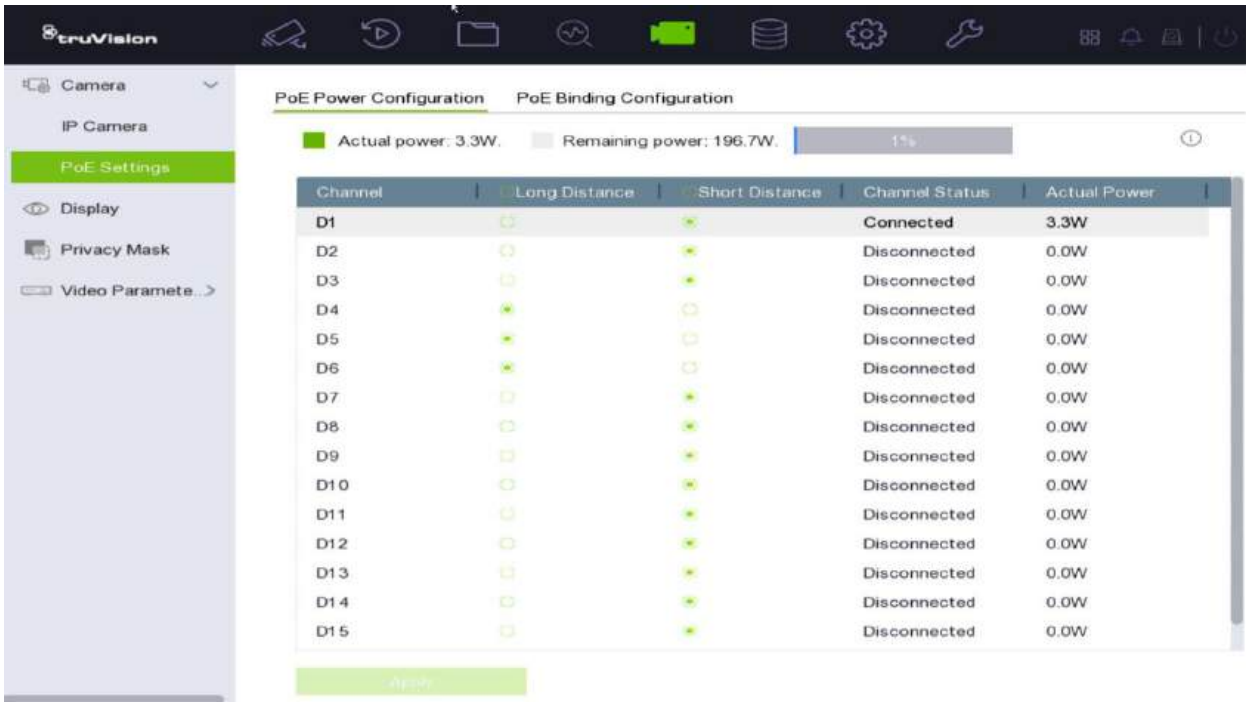
Pressing the play icon will start live view of the camera in a pop-up screen.

PoE settings

Only S models of the recorder have PoE ports for camera connections. The number of PoE channels available depends on the recorder model.

The PoE Channel menu in web mode and the PoE Settings menu in OSD mode is only available for cameras with PoE ports.

Figure 9: PoE Power Configuration menu in OSD mode



In the example shown above, there is only one camera connected to PoE port 1 (D1).

There can be other cameras connected through the LAN network to the recorder.

In OSD mode you can also see the power consumption and can select the cable length used for the PoE connection. “Long distance” is for cables between 100 and 300 m, and “Short distance” is for cables less than 100 m. Short distance is selected by default. Changing the cable length selected can change the power consumption.

Note: For distances between 100 and 250 m use a CAT5e or CAT6 network cable. For distances above 250 m use a CAT6 network cable.

- The PoE ports are enabled with the short-distance mode by default.
- The bandwidth of the IP camera connected to the PoE a via long network cable (100 to 300 m) cannot exceed 6 Mbps.
- The allowed maximum long network cable may be less than 300 meters depending on the IP camera models and cable materials.

www.acornfiresecurity.com

www.acornfiresecurity.com

Manage camera passwords

You can change the camera password to be the same as that of the recorder. However, you can keep the original camera passwords when connecting the cameras to the recorder by using the “Camera Activation Password” or the “Default IP Camera Password” in the recorder.

Display the camera passwords

When in OSD mode, you can display the passwords of all the cameras connected to the recorder. This function is not available in web mode.

To display the camera passwords in OSD mode:

1. Click **Camera > Camera > IP Camera**.
2. Select List View in the right-top corner and click the checkbox **Show Password**.

Enter the recorder admin password. The passwords of all the cameras connected to the recorder appear in the column *Camera Password*.

Change a camera’s password

You can directly change a camera’s password from the recorder when in OSD mode. This function is only available for cameras that have been added via the LAN network.

To change a camera’s password in OSD mode:

1. Click > **Camera** > **Camera > IP Camera**.
2. In the table with cameras added to the recorder, use the horizontal scroll bar to go the end of the table at the right.
3. Select **Advanced Settings** for the desired camera.
4. In the pop-up screen, select the **Password** tab.
5. Enter the current and new camera password. Confirm the new password and then click **Apply**.

Camera activation password

You can set up a camera-specific password in the recorder that allows a selected camera to be accessed by the recorder even when the password of the camera itself is different from that of the recorder.

To set up a camera activation password for a camera in web mode:

1. Click **Configuration** > **System** > **Camera Management** > **IP Camera**.

www.acornfiresecurity.com

www.acornfiresecurity.com

2. Select the desired camera and then click the **Activation** button.
3. In the pop-up screen, enter the activation password and re-enter it to confirm it. Click **OK**.

   Note: If you enable the “Use Default IP Camera Password” check box, the activation password text boxes are disabled for the selected camera.

To set up a camera activation password for a camera in OSD mode:

1. Click **Camera** > **Camera** > **IP Camera > More Settings** and select **Channel Default Password Management** from the drop-down list.
2. Enter the activation password and click **OK**. To modify an existing password, select the checkbox **Change Password**.
3. To associate this activation password with a specific camera, select a camera from the “Device Added List” and click **Edit**. Select the **Use Camera Activation Password** check box and click **OK**.

Default IP camera password

You can set up a single default camera-specific password in the recorder that allows all the cameras connected to the recorder to have a different camera password from that of the recorder and yet still be recognized by the recorder.

When “Sync IP Password” is enabled and you then add a camera to the recorder that is on the online device list, the recorder will check that the camera’s password is the same as the one entered in the recorder (the Default IP Camera Password). If they are identical, the camera is added and comes online. If the two passwords are not identical, you will need to enter the correct password manually.

If adding cameras to the recorder that have a different password than the camera password in the recorder, select the **Sync. IPC Password** function and click **Save**.

To set up the default password for all cameras when activating an IP camera:

1. When initially activating the recorder, you can enter the default IP camera password, if desired. This applies to both web and OSD modes.

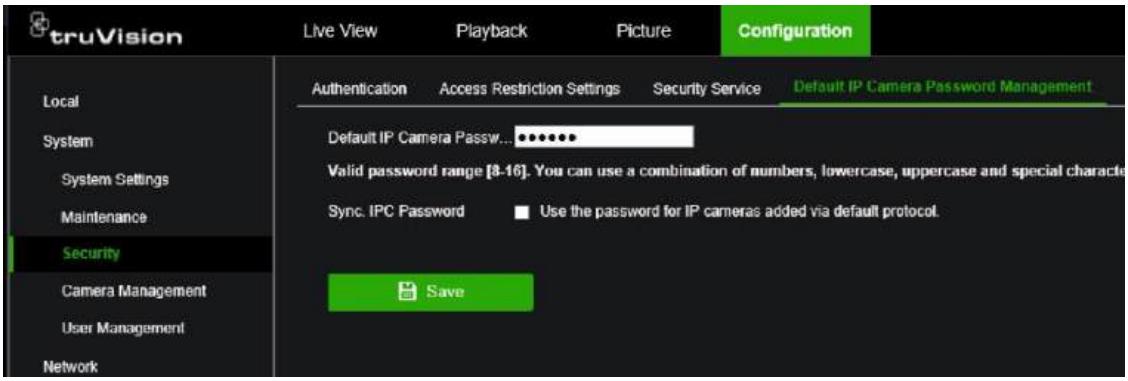
   Note: This is the only time that the default IP camera password can be set in OSD mode.

To set up a default password for all cameras in web mode:

1. Click **Configuration** > **System** > **Security** > **Default IP Camera Password Management**.

www.acornfiresecurity.com

www.acornfiresecurity.com



2. Under **Default IP Camera Password**, enter the new password. It will apply to all cameras activated and added to the recorder.
3. Enable **Sync IPC Password** for the recorder to check the camera's password against the default IP camera password in the recorder.
4. Click **Save** to save the setting.

Add an IP camera

This section describes how to add IP cameras to the recorder.

The process depends on the recorder type (with/without PoE ports), camera status (activated/inactivated), and method used for adding the cameras (via the OSD menu or via the webpage).

Use the recorder's PoE ports (for S models only)

Note: When adding cameras to the recorder that have a different password than the camera password in the recorder, select the *Sync.IPC Password* function and press Save. See "Default IP camera password" on page 56 for more information on using the "Sync IP password" function.

To add an IP camera via the PoE ports:

- **Camera is not yet activated:**

1. Set up the camera password in the recorder in web mode (see "Manage camera passwords" on page 55).
2. Connect the IP camera to one of the free PoE ports at the back of the recorder.
3. The recorder assigns an IP address (192.168.254.x) to the camera and will automatically activate the camera using the password set up in the recorder. This process will take a couple of minutes.
4. The camera automatically connects to the recorder. This process will take a couple of minutes. The recorder starts recording video as soon as the camera has been successfully added.

www.acornfiresecurity.com

www.acornfiresecurity.com

- **Camera is already activated, has a LAN IP address, and has the same password as the recorder:**

1. Connect the IP camera to one of the free PoE ports at the back of the recorder.
2. The recorder assigns an IP address (192.168.254.x) to the camera and will come online. This process will take a couple of minutes.
3. The camera automatically connects to the recorder. The recorder starts recording video as soon as the camera has been successfully added.

Note: If adding cameras to the recorder that have a different password than the camera password in the recorder, select the **Sync. IPC Password** function and click **Save**.

Use the LAN network

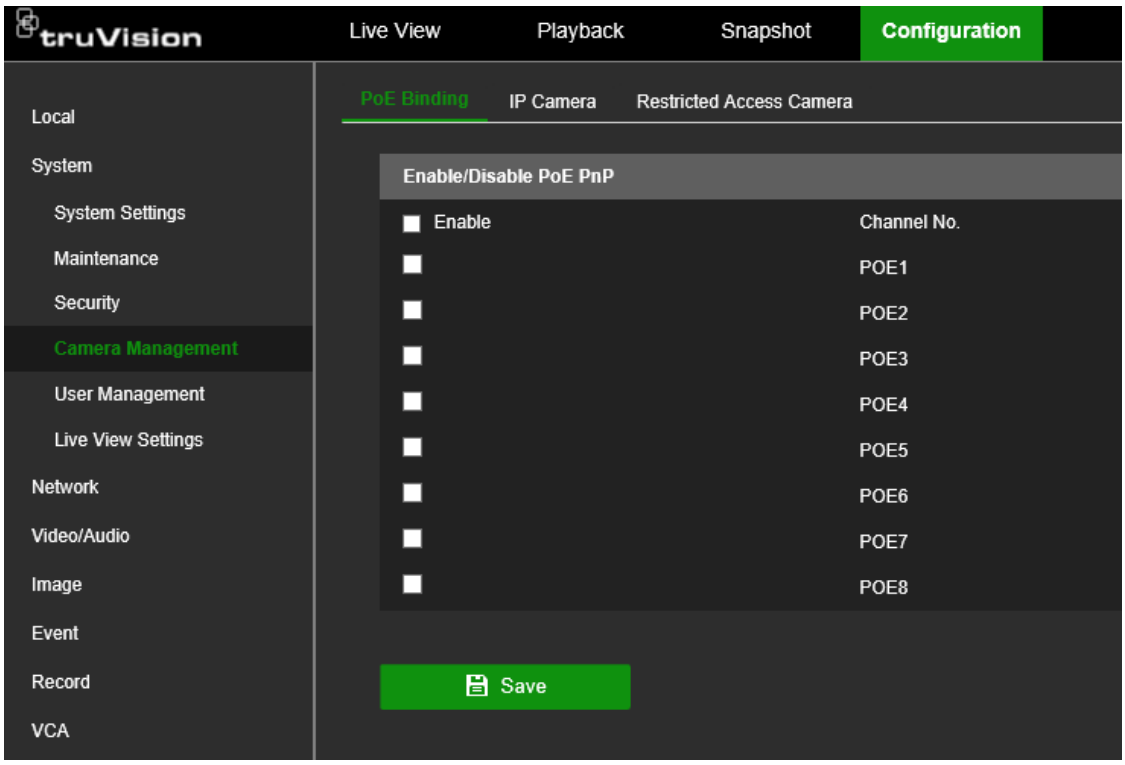
This method can be used for all recorder models.

For recorders with PoE ports make sure that one or more of the PoE ports on the recorder are disabled so that cameras that are on the LAN can be added to the recorder. You can do this via the OSD or the webpage.

To see which cameras are connected to a PoE port in web mode:

1. To see which cameras are connected to a PoE port, click **Configuration** > **System** > **Camera Management** > **PoE Binding**.

   The list of cameras appears showing which are connected to a PoE port.



www.acornfiresecurity.com

www.acornfiresecurity.com

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

To see which cameras are connected to a PoE port in OSD mode:

1. To see which cameras are connected to a PoE port, click **Camera** >**Camera** > **PoE Settings** > **PoE Binding Configuration**. Make changes if needed by selecting the desired channel numbers.
2. Click **Apply** to save any changes.

- **Camera is not yet activated:**

Note: A camera that is not activated has the default IP address 192.168.1.70.

The camera can only be activated successfully in web mode as described below if the recorder's IP address is within the same network segment as the default IP address of the camera.

When the recorder has an IP address in another network range, you must activate the IP camera first via the TruVision Device Manager or follow the process in OSD mode.

To add an IP camera on the LAN in web mode:

1. Click **Configuration** > **System** > **Camera Management** > **IP Camera**.
2. Click **Quick Add** to find the cameras on the LAN. Select the desired camera and click **OK**.
3. Select the desired camera from the list and click **Activation**. You will be asked to enter a camera password, or you can select to use the default IP camera password that you added in the recorder and click **OK** (see "Manage camera passwords" on page 55).
4. The camera is activated and comes online. This process will take a couple of minutes. Click **Refresh** to refresh the webpage and see the camera status change from offline to online.
5. Add another camera by following steps 2 to 4.

To add an IP camera on the LAN in OSD mode:

1. Click **Camera** > **Camera** > **IP Camera**.
2. Check the table at the bottom of the screen to to display the list of cameras in the LAN.
3. Select the camera that you want to add and click **Activate**.
4. The recorder asks you to enter a new password or you can select to use the camera password that is stored in the recorder. The camera is activated.
5. You can now add it with the default IP address (192.168.1.70) to the recorder.
6. The camera can then be added to the recorder via the **+Add** button.
7. The camera will get a DHCP address from the network and will be added to the recorder.

www.acornfiresecurity.com

www.acornfiresecurity.com

- **Camera is already activated:**

To add an IP camera on the LAN network in web mode:

1. Make sure that the cameras are on the same network segment as the recorder. If needed, use the TruVision Device Manager to change the network settings of the cameras.
2. Click **Configuration** > **System** > **Camera Management** > **IP Camera**.
3. Click **Quick Add** to find the cameras on the LAN. Select the desired camera(s) and click **OK**.
4. Click **Refresh** to refresh the webpage. The camera(s) will come online when the camera password is identical to the camera password that is defined in the recorder.

Note: If adding cameras to the recorder that have a different password than the camera password in the recorder, select the **Sync. IPC Password** function and click **Save**.

To add an IP camera on the LAN in OSD mode:

1. Make sure that the cameras are on the same network segment as the recorder. If needed, use the TruVision Device Manager to change the network settings of the cameras.
2. Click **Camera** > **Camera** > **IP Camera**.
3. Check the table at the bottom of the screen to display the list of cameras in the LAN.
4. Select the camera(s) that you want to add and click **+Add** to add the camera(s) to the recorder.

Note: If adding cameras to the recorder that have a different password than the camera password in the recorder, select the **Sync. IPC Password** function and click **Save**.

Change camera settings

If the camera's settings (such as the IP address, protocol, management port, channel number, camera user name, camera's admin password, and transfer protocol) are changed after activating the camera in the recorder, you will then need to manually update them in the recorder. If this is not done, the recorder will no longer be able to connect with the camera.

To change camera settings in web mode:

1. Click **Configuration** > **System** > **Camera Management** > **IP Camera.**
2. Select the camera whose setting you want to change and click **Modify**. The *IP Camera* pop-up screen appears.
3. Make the desired changes and click **OK** to save them.

www.acornfiresecurity.com

www.acornfiresecurity.com

To change camera settings in OSD mode:

1. Click **Camera** > **Camera** > **IP Camera**.
2. Use the list view and select the camera whose setting you want to change and click **Edit** . The *Edit IP Camera* pop-up screen appears. Change the desired settings.

   If you want to use the camera activation password, select the check box.
3. To change the camera password, click **Advanced settings** (at the far-right column of the camera table). In the pop-up screen, click the “Password” tab. Enter the current and new passwords and confirm. Click **Apply** to save.

   Note: The Advanced Settings function is only available for cameras that have been added via the LAN network.
4. Make the desired changes to the camera settings and then click **OK**.
5. If you want the camera time to synchronize with the other cameras connected to the recorder, click **Edit** for a selected camera and select the **Enable IP Camera Time Sync function**. Click **OK**.

Verify certificate

A camera security certificate can be used to setup a secure communication between camera and recorder.

It is possible to verify this certificate.

In web mode:

1. Click **Configuration > System > Camera Management > IP Camera**. Select camera and click **Modify**.
2. Enable the certificate verification.
3. Click **OK** to close the window.

In OSD:

1. Click **Camera > Camera > IP Camera** and use the table view.
2. Click **Edit** for the desired camera.
3. Clcik the checkbox for Verify Certificate.
4. Click **OK** to close the window.

The certificate is a form of identification for the camera that provides more secure camera authentication. It requires to import the network camera certificate to the device first when you use this function. To import the camera certificate in the recorder, see below. Import Network Camera Certificate.

You can import a network camera certificate into the recorder.

To import the network camera certificate (web):

1. Log in to the camera webpage.

www.acornfiresecurity.com

www.acornfiresecurity.com

2. Go to **Configuration > Network > Advanced Settings > HTTPS** to export its certificate.
3. Click **Export Certificate** to save the certificate.
4. Log in to the TVN 23 (S/P) webpage.
5. Go to **Configuration > System > Security > Trusted Root Certificate Authorfities.**
6. Click **Import** to import the network camera certificate.
7. Click **Save**.

Restrict viewing cameras on a VGA/HDMI monitor

You can restrict the display of cameras on the local monitor. This might be needed if you want to avoid all cameras appearing on the local monitor.

To set up the restriction in web mode:

1. Click **Configuration** > **System** > **Camera Management** > **Restricted Access Camera**.
2. Enable the channels that you do not want to show on the VGA/HDMI monitor.
3. Click **Save**.
4. The restriction will be applied after the user logs out of the OSD menu.

To set up the restriction in OSD mode:

1. Click **Sytem > User** > **Restricted Access Camera**.
2. Enable the channels that you do not want to show on the VGA/HDMI monitor.
3. Click **Save**.
4. The restriction will be applied after the user logs out of the OSD menu.

www.acornfiresecurity.com

www.acornfiresecurity.com

Chapter 6
User management

You can manage users in both web and OSD modes.

The system administrator (admin user) can create, modify, or delete users and operators and allocate different permissions to them.

The admin user can also create a special operator who has permission to create, modify, or delete users. This user must be named “MasterOperator” (written as one word with capital “M” and “O”). There can only be one MasterOperator. The MasterOperator can only manage other users via the webpage.

Manage users

You can have a maximum of 32 users (the administrator as well as operators and users). The User window shows the list of users for the recorder, their names, and user level (Administrator, Operator, or User).

Important: When you connect the TVN 23 (S/P) to UltraSync, the system automatically creates a user called “UltraSync”. This user cannot be modified or deleted.

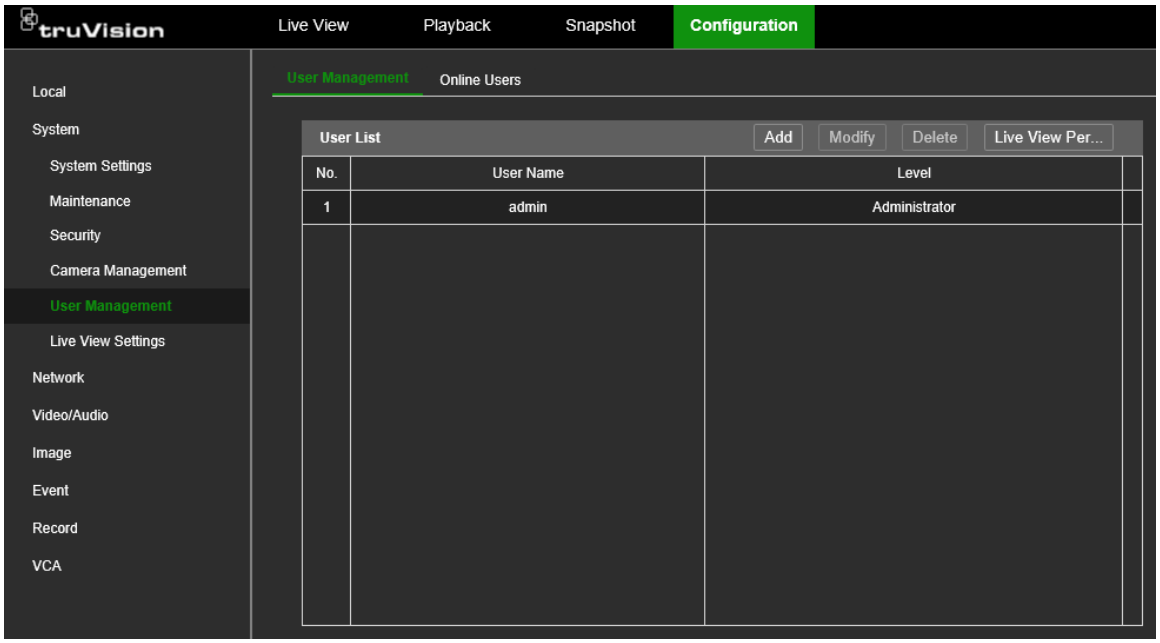
Add or delete users

To add a new user (web):

1. Click **Configuration** > **System** > **User Management** > **User Management**.

www.acornfiresecurity.com

www.acornfiresecurity.com



2. Click **Add** to enter the *Add User* window.
3. Select the new user's access level: Operator or User. Default is User.
4. Enter the password of the admin user or the MasterOperator user (depending on the user that logged in).
5. Enter the new user's name and password. Both the username and password can have up to 16 alphanumeric characters. Confirm the user's password.

   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.
   - 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.
6. If required, modify the user's access permissions. See "Modify a user's access permissions" on page 67 for the list of options.
7. Click the **OK** button to save the settings and return to the previous window.

To add a new user (OSD):

1. Go to **System > User**.

www.acornfiresecurity.com

www.acornfiresecurity.com

2. Click **+ Add.**
3. Enter the admin user credentials and click **Next.**
4. Enter the new username and the password. See point 5 above for the password rules.
5. Confirm the new password.
6. Select the user level for the new user from the dropdown menu: Guest or Operator. And if needed, add the User's MAC address when address filtering is used.
7. Click **OK.**

To create a MasterOperator user who can manage non-admin users:

Web:

1. Click **Configuration** > **System** > **User Management** > **User Management**.
2. Click **Add** to enter the *Add User* window.
3. Select **Operator** as the new user's access level.
4. Enter the administrator's password.
5. Enter the name **MasterOperator** as the new user's name and create a password. Confirm the user's password.

This MasterOperator user can now manage users (but cannot manage the admin user account).

OSD:

1. Go to **System > User.**
2. Click **+ Add.**
3. Enter the admin user credentials and click **Next.**
4. Enter MasterOperator as new username and enter a password. See the password rules on page 55Confirm the new password.
5. Set the user level for MaasterOperator to **Operator**. And if needed, add the User's MAC address when address filtering is used.
6. Click **OK.**

This MasterOperator user can now manage users (but cannot manage the admin user account) via the webpage.

No special user permissions are needed to allow this special user to manage other users.

www.acornfiresecurity.com

www.acornfiresecurity.com

To modify a user's information:

Web:

1. Login to the recorder via the admin account or MasterOperator account.
2. Click **Configuration** > **System** > **User Management** > **User Management**.
3. From the user list, select the user to be modified.
4. Click **Modify** to enter the *Modify User* window.
5. Enter the password of the admin user or MasterOperator user (depending on the user that logged in).
6. Change the desired information on the user, such as the password, level, or name.
7. Click **OK** to save the settings and return to the previous window.

OSD:

1. Login to the recorder via the admin account.
2. Go to **System** > **User**.
3. From the user list, select the user to be modified.
4. Click **Modify** to edit the user.
5. Click again **Modify** in the pop-up screen**,** next to the Password field to modify the user's password, user level or MAC address.
6. Click **OK** to save the settings.

To delete a user:

Web:

1. Login to the recorder via the admin account or MasterOperator account.
2. Click **Configuration** > **System** > **User Management** > **User Management**.
3. From the user list, select the user to be deleted.
4. Click **Delete** and enter the-password of the admin user or MasterOperator user (depending on the user that logged in)
5. Click the **OK** button to save the settings and return to the previous window.

OSD:

1. Login to the recorder via the admin account.
2. Go to **System** > **User.**
3. From the user list, select the user to be deleted.
4. Click **Delete** and enter the-password of the admin user. Click **Next** and click **Yes** to confirm that the selected user can be deleted.

www.acornfiresecurity.com

www.acornfiresecurity.com

Modify a user's access permissions

Only an administrator or MasterOperator (via the webpage only) can allocate access permission to operators and users. The access permissions can be customized for each operator and user's needs. By default, the administrator has access to all access permissions, and these cannot be changed. See Table 3 for more information.

Table 3: Description of default access permissions by user type

User type	Default access permissions
Administrator	Can access all permissions. Permissions cannot be changed.
Operator	Local playback, local log search, local manual operation, local PTZ control, local video search, remote log search/interrogate working status, remote bi-directional audio, remote live view, remote manual record, remote PTZ control, and remote playback/download. By default, with this permission the user is not allowed to configure the recorder.
User	Local playback, local log search, remote log search/interrogate working status, remote live view, and remote playback/download. By default, with this permission the user is not allowed to configure the recorder.

Local configuration settings

By default, only the local log search, local playback, remote log search/interrogate working status, and remote live view settings are enabled for users.

- **Local: Upgrade/Format:** Locally upgrade the firmware or format the HDD.
- **Local: Shutdown/Reboot:** Shut down or reboot the recorder.
- **Local: Parameters Settings:** Configure parameters and import the configuration from the recorder.
- **Local: Log Search:** Search and view logs of the recorder.
- **Local: Camera Management:** Locally add, delete, and edit IP cameras.
- **Local: Playback:** Locally play recorded files that are on the recorder.
- **Local: Manual Operation:** Locally start/stop manual recording on any of the channels, snapshots, and video clips
- **Local: PTZ Control:** Locally control PTZ dome cameras.
- **Local: Video Export:** Locally back up recorded files from any of the channels.

Remote configuration settings

- **Remote: Parameters Settings:** Remotely configure parameters and import configuration.
- **Remote: Log Search/Interrogate Working Status:** Remotely view logs that are saved on the recorder.
- **Remote: Upgrade/Format:** Remotely upgrade the firmware and format the HDD.

www.acornfiresecurity.com

www.acornfiresecurity.com

- **Remote: Bi-directional audio:** Use bi-directional audio between the remote client and the recorder
- **Remote: Shutdown/Reboot:** Remotely shut down or reboot the recorder.
- **Remote: Notify Surveillance Center/Trigger Alarm Output**
- **Remote: Video Output Control:** For future use.
- **Remote: Serial Port Control**: Remotely configure RS-232 and RS-485 ports.
- **Remote: Camera Management:** Remotely enable and disable channels.
- **Remote: Live View:** Remotely select and view live video over the network.
- **Remote: Manual Record**: Remotely start/stop manual recording on any of the channels.
- **Remote: PTZ Control:** Remotely control PTZ dome cameras.
- **Remote: Playback/Download:** Remotely play and download recorded files that are on the recorder.

To customize a user's access privileges:

Web:

1. Login to the webpage as admin or MasterOperator user.2. Click **Configuration** > **System** > **User Management** > **User Management**.
3. Select a user and click **Modify**. The Modify User window appears.
4. Enter the admin or MasterOperator password (depending on the user that logged in)**.**
5. Select the desired access privilege settings for the user**.**
6. Click the **OK** button to save the settings and return to the previous window.

OSD:

1. Login to the OSD with the admin account.
2. Go to **System > User.** The user list will be shown.
3. Cllick on the icon in the **Permission** column for the user for which you want to customize the permssions.
4. Select the desired access privilege settings for the user.
5. Click **OK** to save the settings.

See which users are online

When in web mode, you can easily see which users are online using the recorder.

To see who is online:

1. Click **Configuration** > **System** > **User Management** > **Online Users**.

www.acornfiresecurity.com

www.acornfiresecurity.com

The *User List* window appears, listing all users currently online.

Double Verification permission for non-admin users

After double verification is enabled in the recorder, a non-admin user must be verified by an authorized user to get the permission for certain features. Only the admin user has the authorization to setup double verification.

The double verification user can any user with Operator or User level.

The double verification can be used for:

- Local Playback
- Remote Playback/Download
- Local Video Export

To setup double verification users:

Via the webage:

1. Click **Configuration > System > Security > Double Verification Configuration.**
2. Enable the feature by clicking the checkbox.
3. Add a user that will be used as the double verification user. The users that are created here are different users than the users created via User Management. Here you can only create users that will need to be used to enter their user credentials when the double verification is used.
4. Select the appropriate permissions for which this user needs to enter his credentials when an operator/guest wants to use them (local playback, local video export, remote playback/download).

   Maximum 8 users can be created here.

Via the OSD:

1. Click **Maintenance > System Service > Double Verification**
2. Enable the feature by clicking the checkbox.
3. Add a user that will be used as the double verification user. The users that are created here are different users than the users created via User Management. Here you can only create users that will need to be used to enter their user credentials when the double verification is used.

www.acornfiresecurity.com

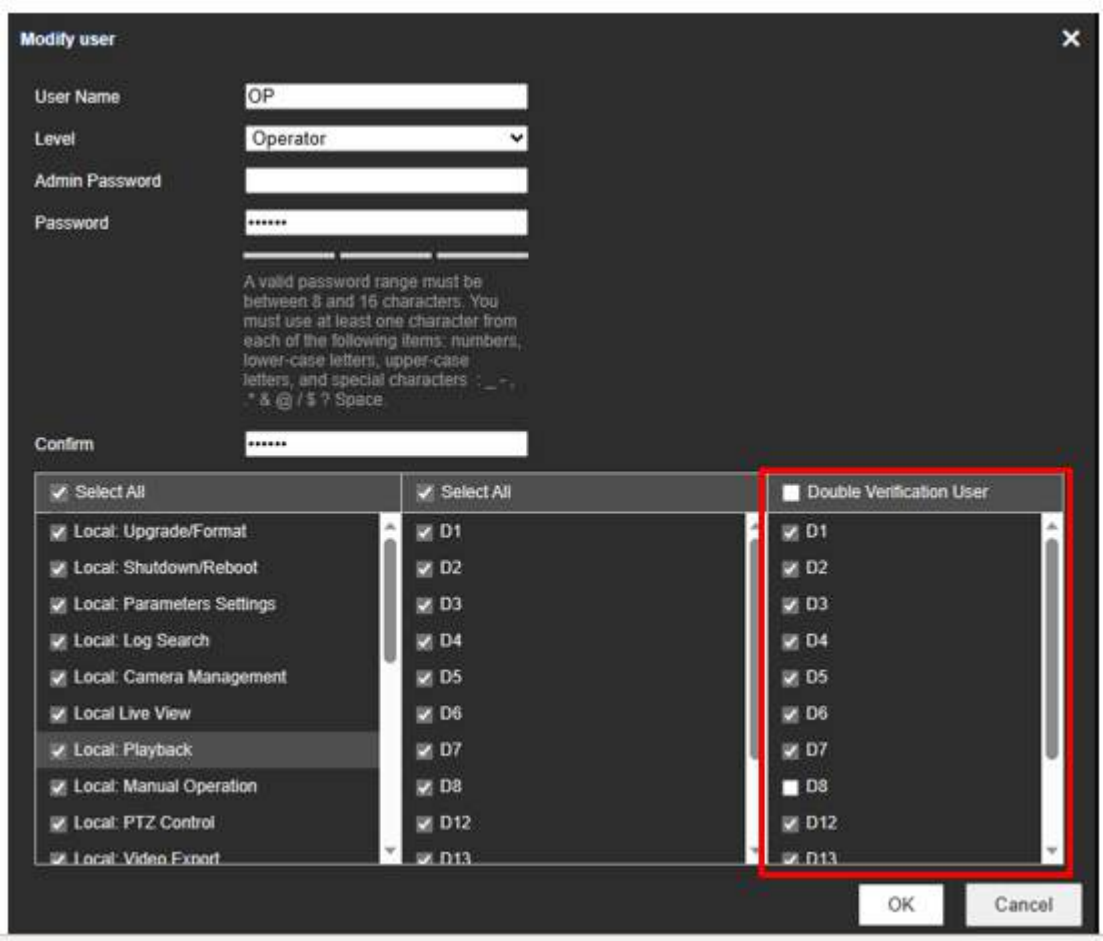
www.acornfiresecurity.com

4. Select the appropriate permissions for which this user needs to enter his credentials when an operator/guest wants to use them (local playback, local video export, remote playback/download)
5. Click **Apply** to save the settings.

When the double verification users are created, you have to set the double verification requirement for any normal user that needs to use this.

Web:

1. Go to **Configuration > System > User management**
2. Select an **Operator** or **User** and click **Modify**
3. Depending on the requirements, click on Local Playback, Local Video Export and/or Remote:Playback/Download
4. You will see that there is a column called **Double Verification User**.
5. Select the channel(s) for which you want that double verification will be used.



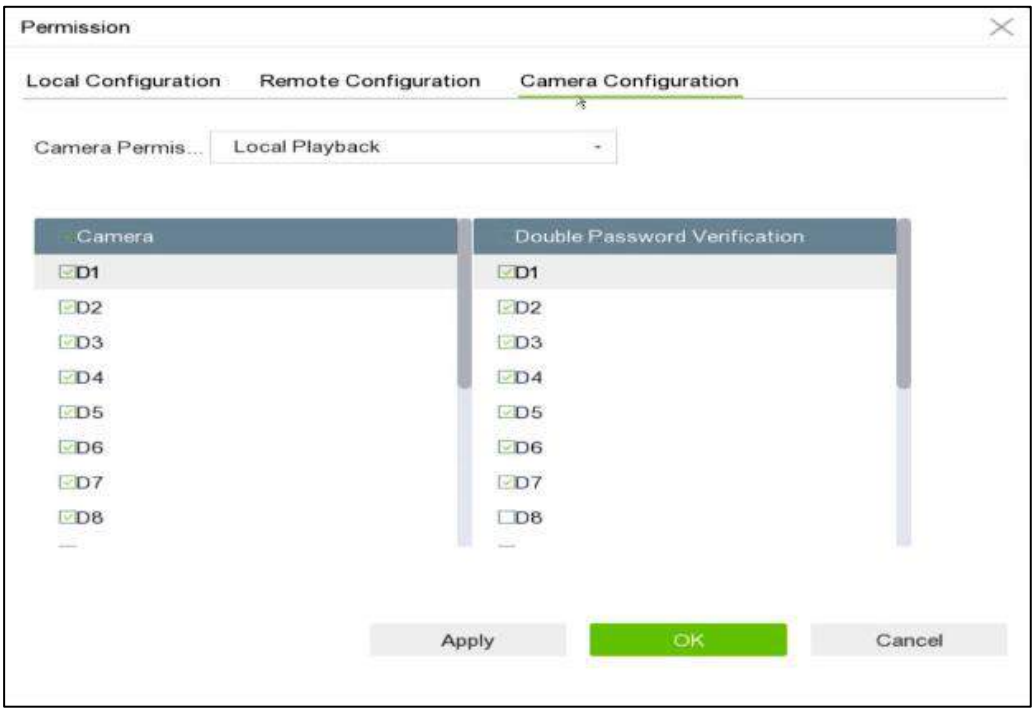
6. **Save** the settings.

www.acornfiresecurity.com

www.acornfiresecurity.com

OSD:

1. Click **System > User** and click on **Permission** for an Operator/User user.
2. Enter the admin password to continue.
3. Click on the tab **Camera Configuration** and as required, select Local Playback, Local video Export or Remote Playback/Export from the dropdown list.
4. You can then select the camera for which you want that double verification will be used.



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

When the normal user then wants to do one of the functions (local playback, local export and/or remote playback/export), there will be **a pop-up screen** when the double verification user will have to enter his/her password.

www.acornfiresecurity.com

www.acornfiresecurity.com

Chapter 7
Network settings

The Network menu allows you to manage all network-related aspects of the recorder including general network settings, DDNS, PPPoE, port settings, NTP synchronization, email setup, UPnP settings, FTP server setup, and IP address filter.

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

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

TCP/IP 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 (web and OSD modes):

1. In web mode:

   Click **Configuration** > **Network** > **Basic Settings** > **TCP/IP**.

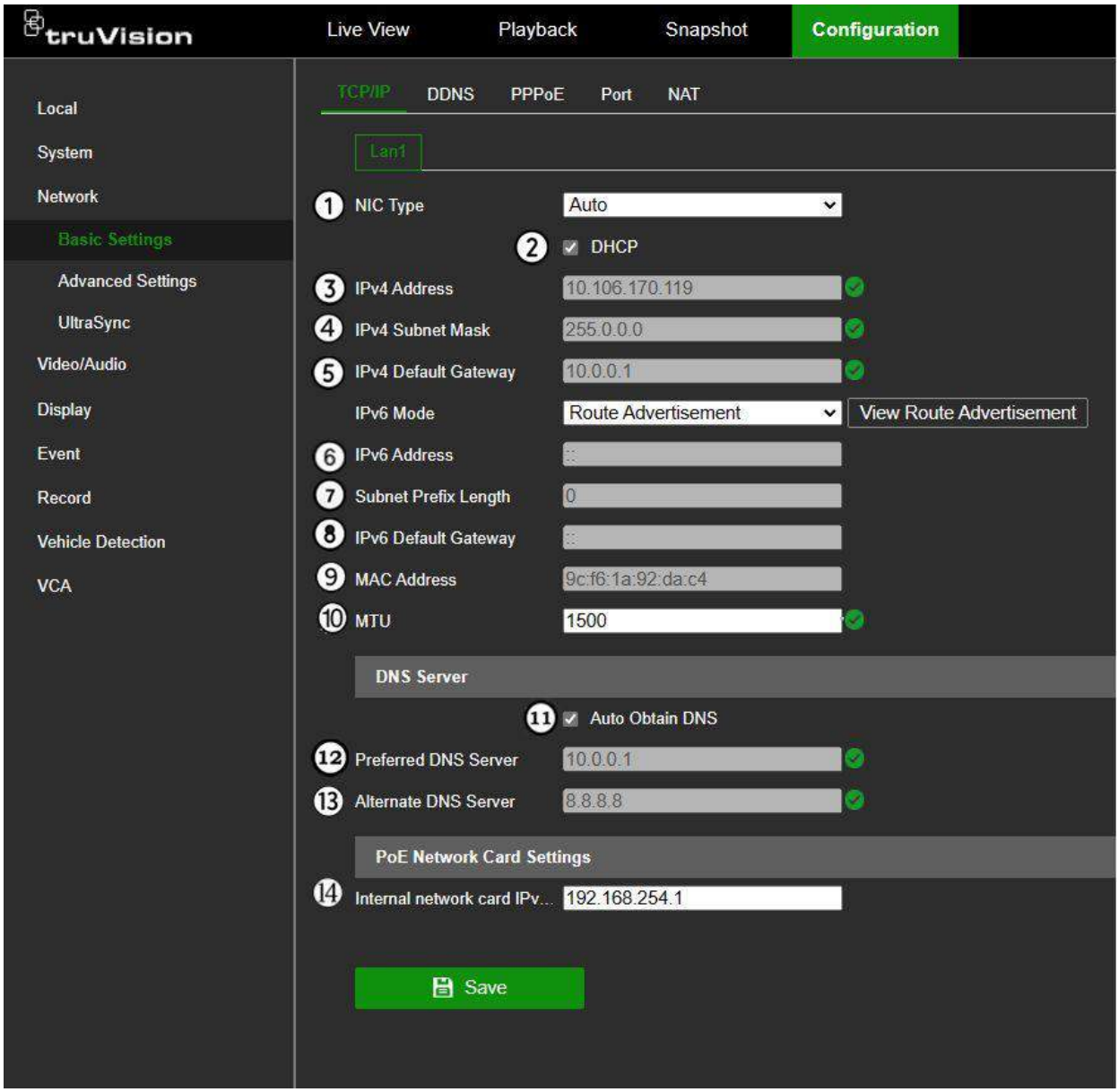
   — or —

   In OSD mode:

   Click **System** > **Network** > **TCP/IP** > **TCP/IP**.
2. Enter the required settings: (web mode shown)

www.acornfiresecurity.com

www.acornfiresecurity.com



Option	Description
1. 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.
2. DHCP	DHCP (Dynamic Host Configuration Protocol) is a protocol for assigning an IP address dynamically to a device each time it connects to a network. Select this check box if you have a DHCP server running and want your recorder to automatically obtain an IP address and other network settings from that server. The DHCP server is typically available in your router. Default value is Disable. In OSD mode, it is called “DHCP (IPv4)”.
3. IPv4 Address	Enter the IPv4 address of the recorder. The default IP address is 192.168.1.82. In OSD mode, it is called” IP Address”.

www.acornfiresecurity.com

www.acornfiresecurity.com

Option		Description
4.	IPv4 Subnet Mask	Enter the subnet mask for your network so the recorder will be recognized within the network. Default value is 255.255.255.0. In OSD mode, it is called “Subnet Mask”.
5.	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.
6.	IPv6 Address	Enter the IPv6 address of the recorder.
7.	Subnet Prefix Length	This displays the number of bits in the subnet address.
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, and it cannot be changed.
10.	MTU	Enter a value between 500 and 9676. Default is 1480.
11.	Auto Obtain DNS	This function is automatically enabled when DHCP is enabled. When enabled, the preferred and alternate DNS servers are automatically obtained. In OSD mode, it is called “Enable Obtain DNS Server Address Automatically”
12.	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.
13.	Alternate DNS Server	Enter the alternate domain name server to use with the recorder.
14.	Internal network card IPv4 Address	Enter the internal NIC IPv4 address. This is the IP address of the recorder's internal network managing only the PoE port cameras. This is not the LAN IP address. Default value is 192.168.254.1.

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

DDNS settings

DDNS servers allow you to connect to your recorder using a dynamic address. This dynamic address needs to be registered with a DNS service. The DDNS setup menu allows you to enable or disable DDNS and 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

www.acornfiresecurity.com

www.acornfiresecurity.com

need to change it to another value. See Appendix B “Port forwarding info” on page 233 for more information.

There are three ways to set up a DDNS account:

- **ezDDNS**: A free-of-charge service included with your recorder and fully managed within the recorder interface. It is exclusive to TruVision products.
- **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.

Caution: If you use the services of DynDNS or No-IP, your account user name, and password for these services will be sent to them in clear text format when you set up your connection in the recorder.

Note: You cannot have two recorders with the same hostname.

To set up DDNS in web and OSD modes:

1. In web mode:

   Click **Configuration** > **Network** > **Basic Settings** > **DDNS**.

   — or —

   In OSD mode:

   Click **System** >**Network** > **TCP/IP** > **DDNS**.

2. Select the **Enable DDNS** check box to enable this feature. It is enabled by default. Option is called “Enable” in OSD mode.
3. Under **DDNS Type**, select one of the DDNS types listed:

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

   The maximum length for the hostname field is 64 characters. This limit does not include tvr-ddns.net. An example of a hostname 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 website. 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

www.acornfiresecurity.com

www.acornfiresecurity.com

Password: mypassword

— or —

NO-IP: Enter server address (for example, dynupdate.no-ip.com). In the hostname field, enter the host obtained from the NO-IP website. Then enter the user name and password that are registered with the No-IP network.

4. Click **Save** in web mode or **Apply** in OSD mode 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 in web mode:

1. Click **Configuration** > **Network** > **Basic Settings** > **PPPoE**.
2. Select the **Enable PPPoE** check box.
3. Enter your user name and password and confirm the password.

   Note: The user name and password should be assigned by your ISP.
4. Click **Save**. It is recommended to reboot the recorder.

To configure PPPoE settings in OSD mode:

1. Click **System** > **Network** > **TCP/IP** > **PPPoE.**
2. Select the **Enable PPPoE** check box.
3. Enter your user name and password and confirm the password.

   Note: The user name and password should be assigned by your ISP.
4. Click **Save**. It is recommended to reboot the recorder.

Port settings

Network protocols and plug-in applications

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.

www.acornfiresecurity.com

www.acornfiresecurity.com

See “Alarm host setup” on page 84 for information on setting up an alarm host with ports.

To configure port settings in web mode:

1. Click **Configuration** > **Network** > **Basic Settings** > **Port**.
2. Enter the port values:

   HTTP port: This is used to connect via a browser. Default value is 80.

   RTSP (Real Time Streaming Protocol) port: This is a video streaming protocol. Default value is 554.

   HTTPS port: 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. The HTTPS setting is only available in web mode. See “HTTPS ” on page 81 for information server certificates.

   Server port: Use the server port for remote client software access. The port range is between 1024 and 65535. Default value is 8000.

   Enhanced SDK Service port: this port is used when the enhanced SDK service is used. The port range is between 1024 and 65535. The default value is 8443.

   WebSocket port: This is used to live view on non-IE browsers. Default value is 7681. This port setting is only available in web mode.
3. Click **Save** to save the settings.

To configure the port settings in OSD mode:

Note: The HTTPS, Enhanced Service Port and WebSocket ports can only be set up via the browser.

1. Click **System** > **Network** > **Advanced** > **More Settings**.
2. Enter the port values:

   Alarm Host IP/Alarm Host Port: see page 84

   Server port: Use the server port for remote client software access. The port range is between 1024 and 65535. Default value is 8000.

   HTTP protocol: is used to connect via the IE browser. Default value is 80.

   Multicast IP: see page 85

   RTSP (Real Time Streaming Protocol) port: This is a video streaming protocol. Default value is 554.

   Enhanced SDK Service Port: this port is used when the enhanced SDK service is used. The port range is between 1024 and 65535. The default value is 8443.
3. Click **Save** to save the settings.

www.acornfiresecurity.com

www.acornfiresecurity.com

NAT (UPnP) settings

The recorder supports UPnP (Universal Plug and Play). This feature lets the recorder automatically configure its 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.

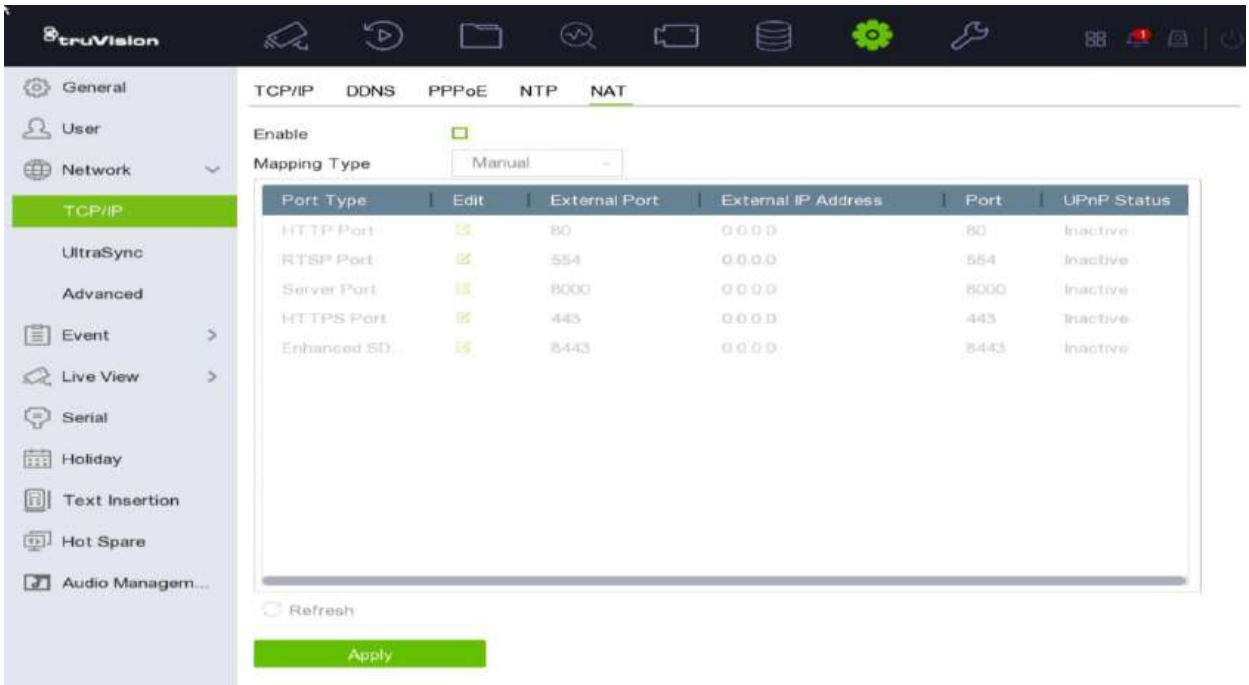
Manual mapped type: Enter the desired external port settings and IP addresses required to connect to the desired router.

To enable UPnP in OSD mode:

1. Connect the recorder to a router.

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

2. Click **System**> **Network** > **TCP/IP** > **NAT**.



3. Select the **Enable** check box.

4. From **Mapping Type**, select Auto or Manual.

   If Manual is selected, enter the external ports and IP addresses required. Click the Edit icon to change the values.

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

To enable UPnP in web mode:

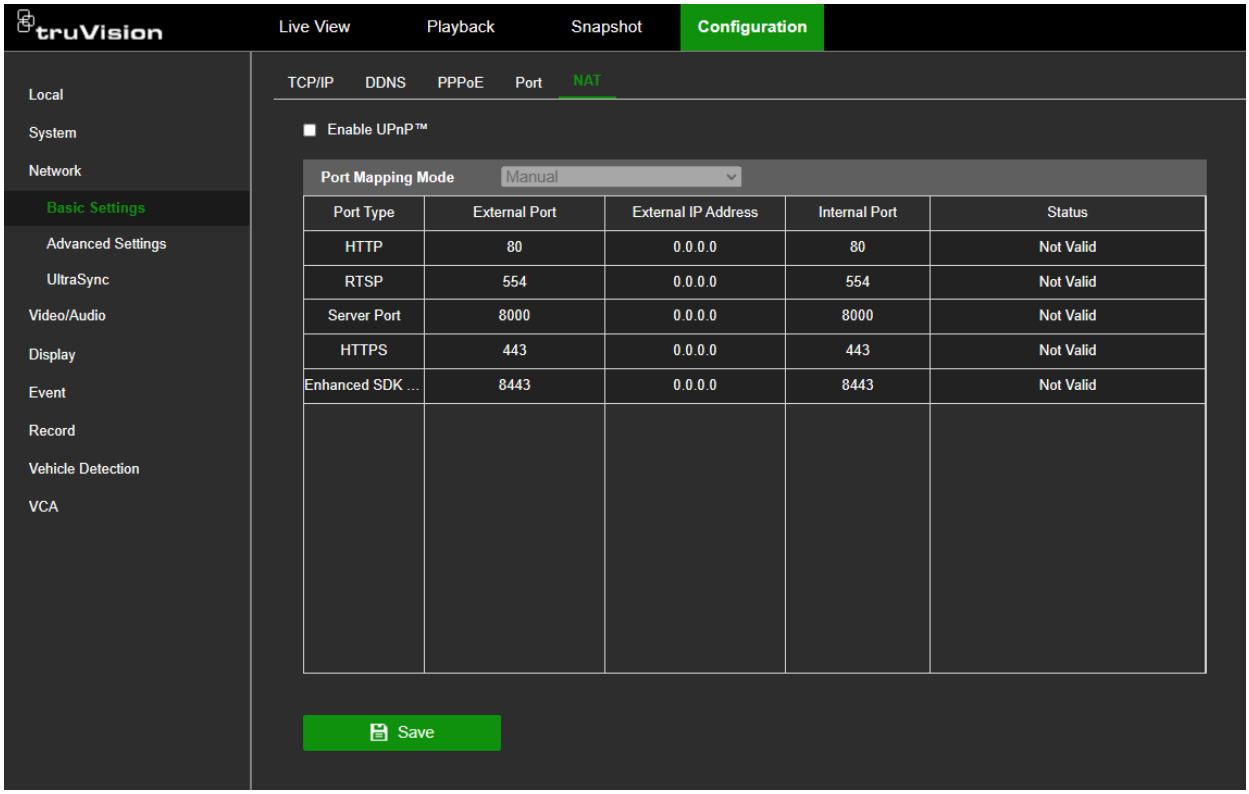
1. Connect the recorder to a router.

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

www.acornfiresecurity.com

www.acornfiresecurity.com

2. Click **Configuration** > **Network** > **General** > **NAT**.



3. Select the **Enable UPnP** check box.
4. From **Port Mapping Mode**, select Auto or Manual.

   If Manual is selected, enter the external ports and IP addresses required, by overwriting the current values in the table.
5. Click **Save** to save the settings.

Email settings

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

Notes:

- Ensure that the DNS address has been set up correctly beforehand.
- The TVN 23 (S/P) uses TLS 1.2 for email communication.

To configure email settings via the web:

1. Click **Configuration** > **Network** > **Advanced Settings** > **Email**.
2. Enter the required settings.

Option	Description
Sender	Enter the name of the sender of the email.

www.acornfiresecurity.com

www.acornfiresecurity.com

Option	Description
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 SSL/TLS if it is required by the SMTP server. This feature is optional.
Attahed Image	Select the check box if you want to send an email with attached alarm images.
Interval	Select the interval time between the snapshots that are sent in a single email. The default interval is 2 seconds. The interval range represents the time range between the alarm/event snapshots being sent. For example, if you set the interval range at two seconds, the second alarm/event snapshot will be sent two seconds after the first alarm image.
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 the name of the receiver of the email.
Receiver's Address	Enter the email address of the receiver.

3. Click **Test** to the test email settings.

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

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

To configure email settings via the OSD:

1. Click **System** > **Network** > **Advanced** > **Email**.
2. Enter the required settings.

Option	Description
SMTP Server	Enter the SMTP server's IP address.
SMTP Port	Enter the SMTP port. The default TCP/IP port for SMTP is 25.
SSL/TLS	Select the check box to enable SSL/TLS if it is required by the SMTP server. This feature is optional.
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.
Sender	Enter the name of the sender of the email.
Sender's Address	Enter the sender's email address.
Select Receivers	Select an email recipient. Up to three receivers can be selected.

www.acornfiresecurity.com

www.acornfiresecurity.com

Option	Description
Receiver	Enter the name of the receiver of the email.
Receiver's Address	Enter the email address of the receiver.
Attached Image	Select the check box if you want to send an email with attached alarm images.
Interval	Select the interval time between the snapshots that are sent in a single email. The default interval is 2 seconds. The interval range represents the time range between the alarm/event snapshots being sent. For example, if you set the interval range at two seconds, the second alarm/event snapshot will be sent two seconds after the first alarm image.

If needed, setup an alternative SMTP server as well.

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

Network Service (web only)

HTTP

The Hypertext Transfer Protocol (HTTP) is the protocol used for various communications to and from the recorder. Disabling this feature effectively locks down all HTTP communications, making it inaccessible remotely over the network.

The HTTP setting is always enabled and cannot be disabled.

HTTPS

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.

An HTTPS connection needs to use a certificate to ensure network security. By default, there is already a self-signed certificate installed in the recorder.

To enable HTTPS:

1. Click **Configuration > Network > Advanced Settings > Network Service.**
2. Select **Enable HTTPS.**
3. Click **Save** to save the settings.

The HTTPS setting is enabled by default for the TVN 23 (S/P).

www.acornfiresecurity.com

www.acornfiresecurity.com

Enhanced SDK Service

When the recorder interacts with software via the SDK, it is possible to do this via a secured/enhanced connection. TruVision Navigator 9.2 (and newer versions) also supports this secured/enhanced connection.

By enabling the Enhanced SDK service (in combination with enabling the stream over a TLS connection) the connection with the SDK is secured.

To set up the Enhanced SDK Service and streaming over TLS via the web:

1. Click **Configuration** > **Network** > **Advanced Settings** > **Network Service.**
2. Select **Enable Enhanced SDK Service.**
3. Select **Enable Stream Over TLS**.
4. Click **Save** to save the settings.

Note: Before changing these parameters, make sure that the video management software supports Enhanced SDK service.

To set up the Enhanced SDK Service port via the OSD:

1. Click **System** > **Network** > **Advanced** > **More Settings.**
2. Enter the port for the Enhanced SDK Service. The port range is between 1024 and 65535.The default port is 8443.
3. Click **Apply** to save the settings.

The set up of the streaming via TLS is only possible via the webpage.

RTSP

RTSP can be used to stream video from the recorder in another software.

The RTSP streaming can be enabled or disabled. It is by default enabled.

To set up the RTSP streaming (web mode):

1. Click **Configuration** > **Network** > **Advanced Settings** > **Network Service**.
2. Enable or disable RTSP.
3. Click **Save** to save the settings.

To setup the RTSP streaming (via OSD):

1. Click **Maintenance** > **System Service.**
2. Select **Enable RTSP**.
3. Click **Apply** to save the settings.

www.acornfiresecurity.com

www.acornfiresecurity.com

802.1x

802.1X is a standard for port-based access control. It provides an authentication mechanism for 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 (web mode only):

1. Click **Configuration** > **Network** > **Advanced 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 communications channel is protected.

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

Option	Description
Protocol	Select EAP-PEAP
EAPOL version	Versions 1 and 2 are 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.

www.acornfiresecurity.com

www.acornfiresecurity.com

-Or-

If EAP-TLS is selected:

EAP-TLS (EAP Transport Layer Security) was subsequently defined by IETF RFC 5216. The protocol was created as an open standard leveraging the TLS (Transport Layer Security) protocol and it primarily consists of the original EAP authentication protocol.

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

Option	Description
Protocol	Select EAP-TLS.
EAPOL version	Versions 1 and 2 are supported. Defines the format of the exchange.
User Name	This is a valid user name for the authentication server (usually a RADIUS server).
Password	This is a valid password for the username specified in the previous field.
CA Certificate	This should be obtained from the network administrator, as network policies may differ.
User Certificate	This should be obtained from the network administrator, as network policies may differ.
Privacy Key	This should also be requested from the network administrator.

Click **Save** to save the settings.

Other network 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 in web mode:

1. Click **Configuration** > **Network** > **Advanced Settings** > **Other**.
2. Enter the **Alarm Host IP** and the **Alarm Host Port** values.

   The alarm host IP is the IP of the remote PC where the TruVision Navigator software is installed. The alarm host port value must be the same as the software's alarm monitor port. The default alarm host port value is 5001.
3. Click **Save** to save the settings.

www.acornfiresecurity.com

www.acornfiresecurity.com

To set up an alarm host in OSD mode:

1. Click **System** > **Network** > **Advanced** > **More Settings**.
2. Enter the **Alarm Host IP** and the **Alarm Host Port** values.

   The alarm host IP is the IP of the remote PC where the Network Video Surveillance software is installed. The alarm host port value must be the same as the software's alarm monitor port. The default alarm host port value is 5001.

3. Click Apply to save the settings.Multicast IP address

The network devices must support multicast and be enabled. The recommended multicast address is between 239.252.0.0 and 239.255.255.255.

To enable multicast in web mode:

1. Click **Configuration** > **Network** > **Advanced Settings** > **Other**.
2. Enter the multicast address.
3. Click **Save** to save the settings.

To enable multicast in OSD mode:

1. Click **System** > **Network** > **Advanced** > **More Settings**.
2. Enter the multicast IP address.
3. Click **Apply** to save the settings.

Video Download bandwidth (web only)

It is possible to define the download bandwidth that is foreseen for downloading video.

To setup the video download bandwidth:

1. Click **Configuration > Network > Advanced Settings > Other.**
2. Enter the desired download bandwidth.
3. Click **Save** to save the settings.

Open the camera web page from within the recorder web page

This function can only be done in web mode.

www.acornfiresecurity.com

www.acornfiresecurity.com

To open a camera webpage from within the recorder's webpage:

1. Click **Configuration** > **Network** > **Advanced Settings** > **Other**.
2. To allow the recorder to connect to cameras via a browser, select **Enable Bridge PoE/IP**.
3. Click **Save** to save the settings.

Detect if a camera is already connected to another device

You can set up the recorder to allow it to detect whether a camera is already connected to another device. This function can only be done in web mode.

When this feature is enabled, you can see if a camera is already added to another device from the OSD menu (Online Device List). See “Manage IP cameras in OSD mode” on page 51.

To detect if a camera is connected to another device:

1. Click **Configuration** > **Network** > **Advanced Settings** > **Other**.
2. To allow the recorder to detect whether an IP camera is already connected to another device, select **Enable Camera Link Detection**.
3. Click **Save** to save the settings.

Integration protocol

ISAPI

To enable/disable ISAPI authentication in web mode:

1. Click **Configuration** > **Network** > **Advanced Settings** > **Integration Protocol**.
2. Select the **Enable ISAPI** check box to enable the function. It is enabled by default.
3. Click **Save** to save the setting.

To enable/disable ISAPI authentication in OSD mode:

1. Click **System** > **System Service**.
2. Select the **Enable ISAPI** check box to enable the function. It is enabled by default.
3. Click **Save** to save the setting.

Connect the recorder to UltraSync

The recorder lets you stream video to applications that support UltraSync.

An UltraSync connection enables a remote connection to the recorder without using port forwarding in a router.

www.acornfiresecurity.com

www.acornfiresecurity.com

Configuration steps

Pre-requisites

- A network cable with RJ-45 connector that contains an Internet connection.

The recorder will first need to be added to the LAN network.

TCP/IP 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 (web and OSD modes):

1. In web mode:

   Click **Configuration** > **Network** > **Basic Settings** > **TCP/IP**.

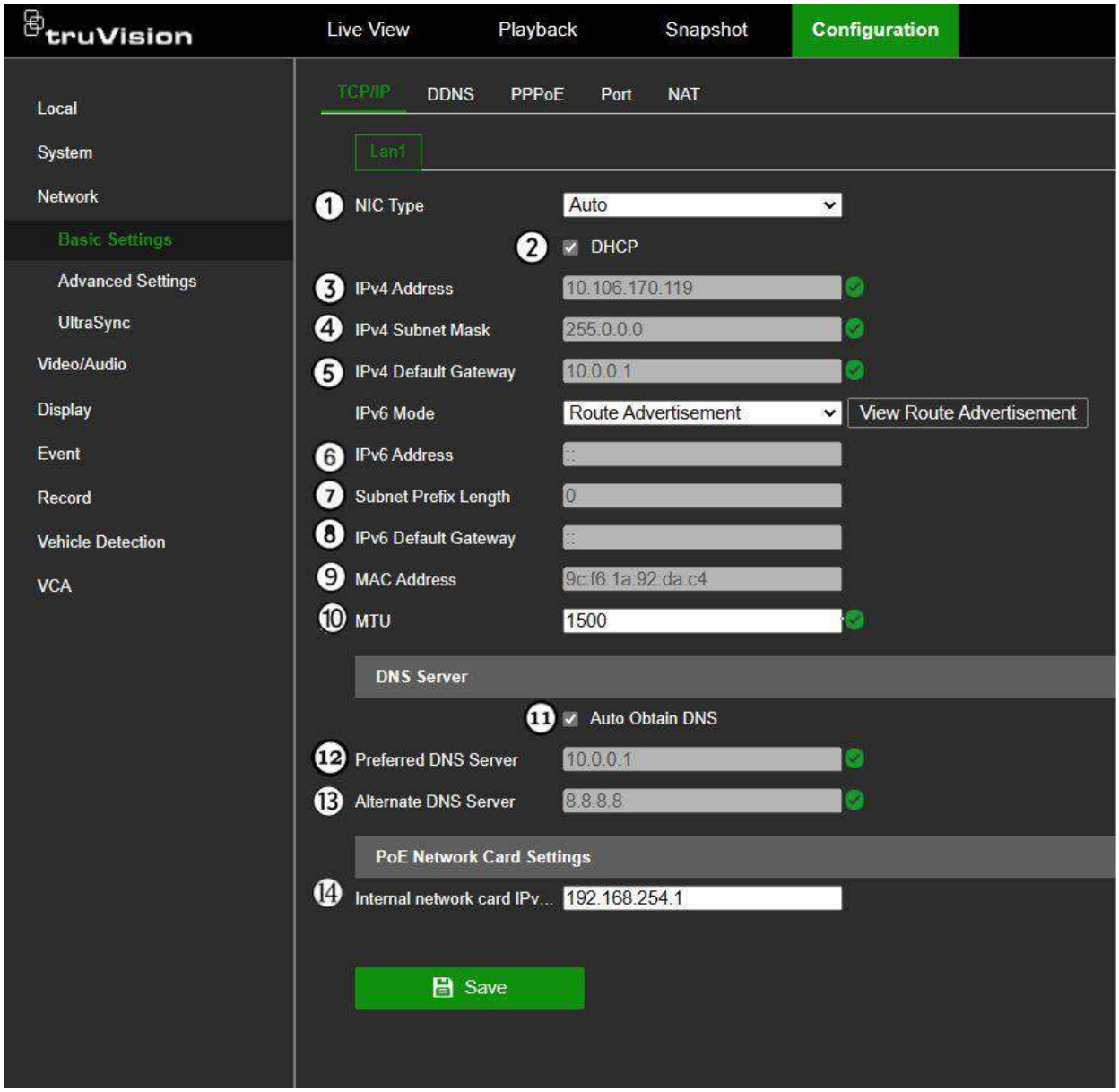
   — or —

   In OSD mode:

   Click **System > Network** > **TCP/IP**.
2. Enter the required settings: (web mode shown)

www.acornfiresecurity.com

www.acornfiresecurity.com



Option	Description
1. 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.
2. DHCP	DHCP (Dynamic Host Configuration Protocol) is a protocol for assigning an IP address dynamically to a device each time it connects to a network. Select this check box if you have a DHCP server running and want your recorder to automatically obtain an IP address and other network settings from that server. The DHCP server is typically available in your router. Default value is Disable. In OSD mode, it is called “DHCP (IPv4)”.
3. IPv4 Address	Enter the IPv4 address of the recorder. The default IP address is 192.168.1.82. In OSD mode, it is called” IP Address”.

www.acornfiresecurity.com

www.acornfiresecurity.com

Option		Description
4.	IPv4 Subnet Mask	Enter the subnet mask for your network so the recorder will be recognized within the network. Default value is 255.255.255.0. In OSD mode, it is called “Subnet Mask”.
5.	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. In OSD mode, it is called “Default Gateway”.
6.	IPv6 Address	Enter the IPv6 address of the recorder. This setting is not available in OSD mode.
7.	Subnet Prefix Length	This displays the number of bits in the subnet address. This setting is not available in OSD mode.
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, and it cannot be changed.
10.	MTU	Enter a value between 500 and 9676. Default is 1480.
11.	Auto DNS	This function is automatically enabled when DHCP is enabled. When enabled, the preferred and alternate DNS servers are automatically obtained. In OSD mode, it is called “Auto Obtain DNS”. **Note**: Please make sure you use a public DNS server. If you have doubts, please use 8.8.8.8 (= primary DNS server for Google DNS).
12.	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. **Note**: Please make sure you use a public DNS server. If you have doubts, please use 8.8.8.8 (= primary DNS server for Google DNS).
13.	Alternate DNS Server	Enter the alternate domain name server to use with the recorder.
14.	Internal IPv4 Address	Enter the internal NIC IPv4 address. This is the IP address of the recorder's internal network managing only the PoE port cameras. This is not the LAN IP address. Default value is 192.168.254.1.

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

Time and NTP settings

It is important to correctly set up the time zone for the recorder and to use a NTP server. Go to “Time settings” on page 23 for further information.

www.acornfiresecurity.com

www.acornfiresecurity.com

Connect the recorder to UltraSync

The recorder lets you stream video to applications that support UltraSync.

An UltraSync connection enables a remote connection to the recorder without using port forwarding in a router.

To connect the recorder to UltraSync in web mode:

Note: This setup must be done by an installer. It cannot be done by an end-user.

1. Click **Configuration** > **Network** > **UltraSync**.

2. Select **Enable** to enable this function for the recorder. Click **Apply**.

   After clicking Apply, it will take a couple of minutes before the recorder will be connected to UltraSync. A QR code will be shown when the recorder is connected.

3. The installer needs to scan the QR code with his mobile phone.

   The *Recorder Registration Process* screen then appears:

1. Enter a valid UltraSync portal username.
2. Enter the password for the username.
3. This field automatically displays the SID number of the recorder.
4. Enter a unique site name for the recorder.
5. This field shows the service level for this recorder. Select the required service level for the recorder.
6. Press **Register** to pair the recorder to the UltraSync account.

www.acornfiresecurity.com

www.acornfiresecurity.com

Note: If you do not have an UltraSync account, please contact your Aritech account manager or distributor.

The end-user can only view video from the UltraSync-connected recorder in the mobile application when the recorder is paired to an installer account.

See the *Operator Guide* for information on adding the recorder to the mobile application, TVRMobile.

To connect the recorder to UltraSync in OSD mode:

Note: This setup must be done by an installer. It cannot be done by an end-user.

1. Click **System** > **Network** > **UltraSync**.
2. Enable for **Register to UltraSync**.
3. The Connection Status will show when the recorder is connected to UltraSync.
4. As soon as the recorder is connected to UltraSync, a QR code will be shown on the same screen.
5. The installer needs to scan this QR code with his mobile phone.

IMPORTANT:

The installer will need to pair this recorder on UltraSync via this QR code. The recorder cannot stream video over UltraSync without this pairing.

This QR code is only for the installer.

The *Recorder Registration Process* screen then appears:

www.acornfiresecurity.com

www.acornfiresecurity.com

1. Enter a valid UltraSync portal username.
2. Enter the password for the username.
3. This field automatically displays the SID number of the recorder.
4. Enter a unique site name for the recorder.
5. This field shows the service level for this recorder. Select the required service level for the recorder.
6. Press **Register** to pair the recorder to the UltraSync account.

Note: If you do not have an UltraSync account, please contact your Aritech account manager.

The end-user can only view video from the UltraSync-connected recorder in the mobile application when the recorder is paired to an installer account.

See the *Operator Guide* for information on adding the recorder to the mobile application, TVRMobile.

Add the recorder to TVRMobile

TVRMobile is the name of the mobile application for iOS and Android devices that allows you to see live and playback video of TruVision recorders as well as control the recorders on a mobile device.

Download the application from Google Play Store (Android) or Apple App Store (iOS). The application is supported on Android version 9 and higher and iOS version 14 and higher.

To add the recorder to TVRMobile:

1. Open the TVRMobile app.
2. Go to **Devices**. Tap ⊕ and then tap **Manual Add**.
3. Enter the recorder's name to be linked. The name can have up to 16 alphanumeric characters. Default name is Device01.
4. Under **Register Mode**, select either ezDDNS, IP/Domain, or UltraSync.

ezDDNS	When the device is registered in the ezDDNS server, you need to type in the registered ezDDNS server address and the device domain name.
IP/Domain	Manually access the device using a fixed IP address or a domain server. You need to edit the IP address or domain address.

www.acornfiresecurity.com

www.acornfiresecurity.com

UltraSync	Add the device that is registered to UltraSync. On the recorder, click the QR code icon in the toolbar (OSD menu) or on web live view page. The QR code of the SID/SCI code appears in a pop-up window. Scan the QR code by pressing the scan icon on the mobile app. Both the SID and SCI fields in the app will be populated with the SID/SCI of the recorder.

5. Enter the user name and password.

   Note: The number of cameras under the device can be obtained after the device has been successfully added.

6. Tap to confirm the settings. The device is added to the device list.
7. Tap to exit and return to the previous page.

The recorder's *Operator Guide* also describes to the end-user how to add the recorder to TVRMobile.

For further information on using TVRMobile, please refer to its user manual.

www.acornfiresecurity.com

www.acornfiresecurity.com

Chapter 8
Video and audio configuration

Audio

Select whether to hear audio from cameras in both live and playback modes. However, to be able to hear audio in playback, you must enable the audio output setting. Audio is disabled by default.

Setting up audio in OSD mode enables audio for the monitor output. If using an HDMI monitor, the audio is outputted directly from the HDMI monitor (if available). If using a VGA monitor, audio is heard from the audio output on the back panel when Audio is enabled.

To set up audio in OSD mode:

1. In OSD mode, from the menu toolbar, click **System** > **Live View.**
2. Enable **Audio Output**. It is disabled by default. Adjust the volume to the desired level.
3. Click **Apply** to save the settings.

To set up audio in web mode:

1. In web mode, from the menu toolbar, click **Configuration** > **System** > **Live View Settings**.
2. Select **Enable Sound Preview**. It is disabled by default.

   Note: The sound level can only be adjusted from the OSD mode.
3. Click **Save** to save the settings.

www.acornfiresecurity.com

www.acornfiresecurity.com

Dual VCA

Enabling the Dual-VCA function will send the VCA event information (e.g., intrusion detection, line crossing detection, face detection, etc.) to the connected back-end device for further analysis. Not all camera models support this function.

Note: This function is not available via OSD mode.

To set up Dual VCA in web mode:

1. In web mode, from the menu toolbar, click **Configuration** > **Video/Audio** > **Display Info. On Stream**.
2. Select the **Enable Dual-VCA** check box for the desired camera(s)
3. Click **Save** to save the settings.

V-Stream encoding

If the available bandwidth is limited, you can remotely view several channels in real-time with one stream over the web browser or VMS (Video Management System), such as TruVision Navigator, using the V-stream encoding option ("V" stands for "virtual"). When enabled, you can see the output from the cameras on a remote client monitor in one stream.

To set up V-Stream encoding in web mode:

1. Click **Configuration** > **Video/Audio** > **V-Stream**.
2. Select the **Enable V-Stream Encoding** check box to enable the feature.
3. Select the **Max. Bitrate** from the drop-down list.
4. Select the **Frame Rate** from the drop-down list.
5. Click **Save** to save the settings.

To set up V-Stream encoding in OSD mode:

1. Click **System** > **Live View** > **V-Stream**.
2. Select the **Enable V-Stream Encoding** check box to enable the feature.
3. Select the **Max. Bitrate** from the drop-down list.
4. Select the **Frame Rate** from the drop-down list.
5. Click **Apply** to save the settings.

www.acornfiresecurity.com

www.acornfiresecurity.com

Chapter 9
Image settings

The chapter describes how to adjust a camera's image settings, add information to be displayed on-screen, and set up privacy masks. You can also set up a day /night function when using OSD mode.

Display settings

You may need to adjust the brightness, contrast, and saturation values depending on the location background to get the best image quality. More functions are available using OSD mode, which allows you to also rotate the image and use mirror mode as well as set the day/night switch, digital noise reduction (DNR), and wide dynamic range (WDR).

To adjust display settings in web mode:

1. Click **Configuration** > **Image** > **Display Settings**.
2. Under **Camera**, select the desired camera.
3. Under **Image Settings**, 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. Under **Exposure Settings**, adjust the iris mode and exposure time.
5. Under **Backlight Settings**, adjust the BLC area and WDR setting.

To adjust display settings in OSD mode:

1. Click **Camera** > **Display**.
2. Under **Camera**, select the desired camera.
3. Under **Camera Name**, you can change the camera name, if desired.
4. Under **OSD settings**, you can select to display the camera name, to display the date and set the date format and select what display mode will be used.

www.acornfiresecurity.com

www.acornfiresecurity.com

As Display Mode, you can select how you want the camera information displayed. Select one of the options from the drop-down list.

- Transparent & Flashing
- Transparent & Not Flashing
- Non-transparent & Flashing
- Non-transparent & Not Flashing (default)

5. Under **Image Settings**, adjust the brightness, contrast, and saturation values by dragging each scroll bar.

Select how you want the camera to rotate the image. There are two rotation functions:

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

6. Under **Exposure**, you can set the exposure time for the camera.
7. Under Day/Night, you can set the behavior for day and night. See page 99.
8. Under **Backlight**, select the WDR option: Off, On, or Auto. Default is Auto.

When enabled, wide dynamic range (WDR) provides clear images when there is high contrast between light and dark areas in the field of view of the camera. Both bright and dark areas can be displayed in the frame.

9. Under **Image Enhancement**, select the DNR type: Close, Normal Mode, or Expert Mode. Default is Normal Mode. Digital noise reduction (DNR) reduces noise, especially in low light conditions, to improve image performance.

When *Normal Mode* is selected, set the level of noise reduction. Higher value has a stronger noise reduction. Default is 50.

When *Expert Mode* is selected, select the desired Time DNR Level and Space DNR Level. Default is 50.

10. Click **Apply** to save the settings.

www.acornfiresecurity.com

www.acornfiresecurity.com

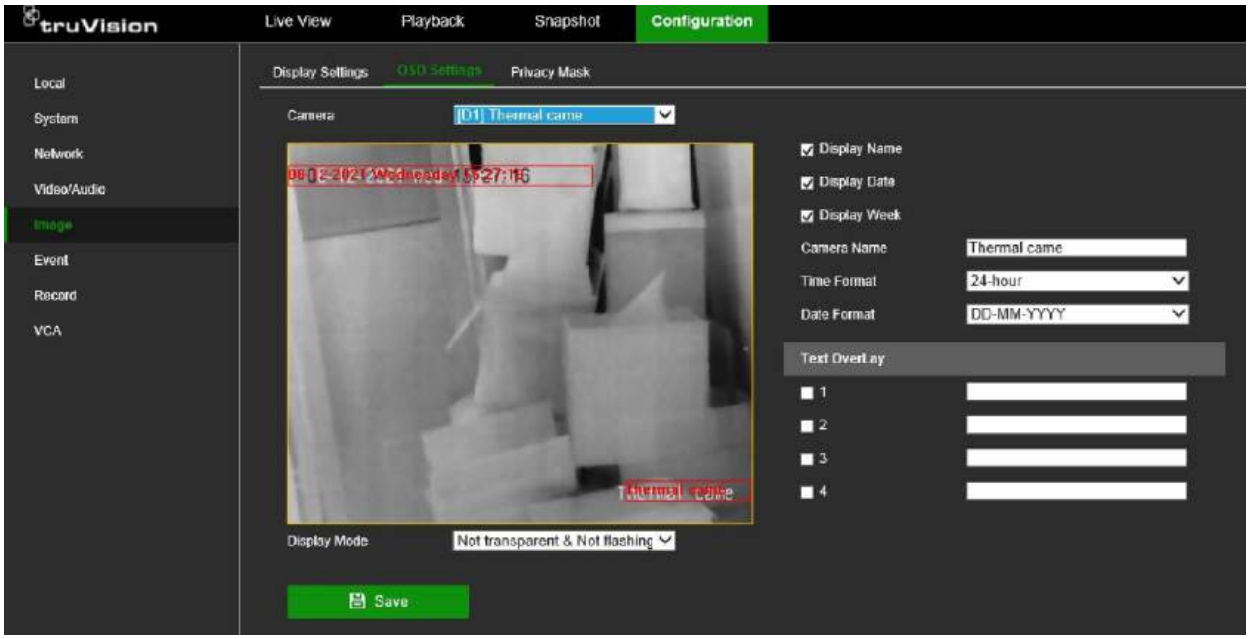
Camera OSD in web mode

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

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

To configure the OSD settings in web mode:

1. Click **Configuration** > **Image** > **OSD Settings**.



2. Under **Camera**, select the desired camera.
3. Select the **Display Name**, **Display Date**, and **Display Week** checkboxes to display the camera name, date, and week.
4. Select a date format and a time format.
5. Define the text to be added on-screen to display extra information, such as contact information. This text is embedded in the video and cannot be removed. Up to four lines of text can be added.

   Note: The text overlay function is not available in OSD mode.
6. Click **Save** to save the settings.

Day/night switch

This function is only available in OSD mode.

You can define whether the camera is in day or night mode. The day (color) option could be used, for example, if the camera is located indoors where light levels are always good.

www.acornfiresecurity.com

www.acornfiresecurity.com

To configure the day/night switch in OSD mode:

1. Click **Camera** > **Display** > **Day/Night Switch**.
2. Under **Camera**, select the desired camera.
3. Under **Day/Night Switch**, select one of the options:

   Day: Camera is always in day mode.

   Night: Camera is always in night mode.

   Auto: The camera automatically detects which mode to use. Select the sensitivity of the switch between day and night. Default is 4.

   Auto-Switch: The camera switches between day and night modes according to the configured period. Enter the start and end times.

   Triggered by Alarm Input: The camera switches to day or night mode after an alarm is triggered. Default is Day.
4. Click **Apply** to save the settings.

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 can be viewed in live view and recorded mode. It appears as a black area on the video image.

The number of privacy masks is determined by the number supported by the camera.

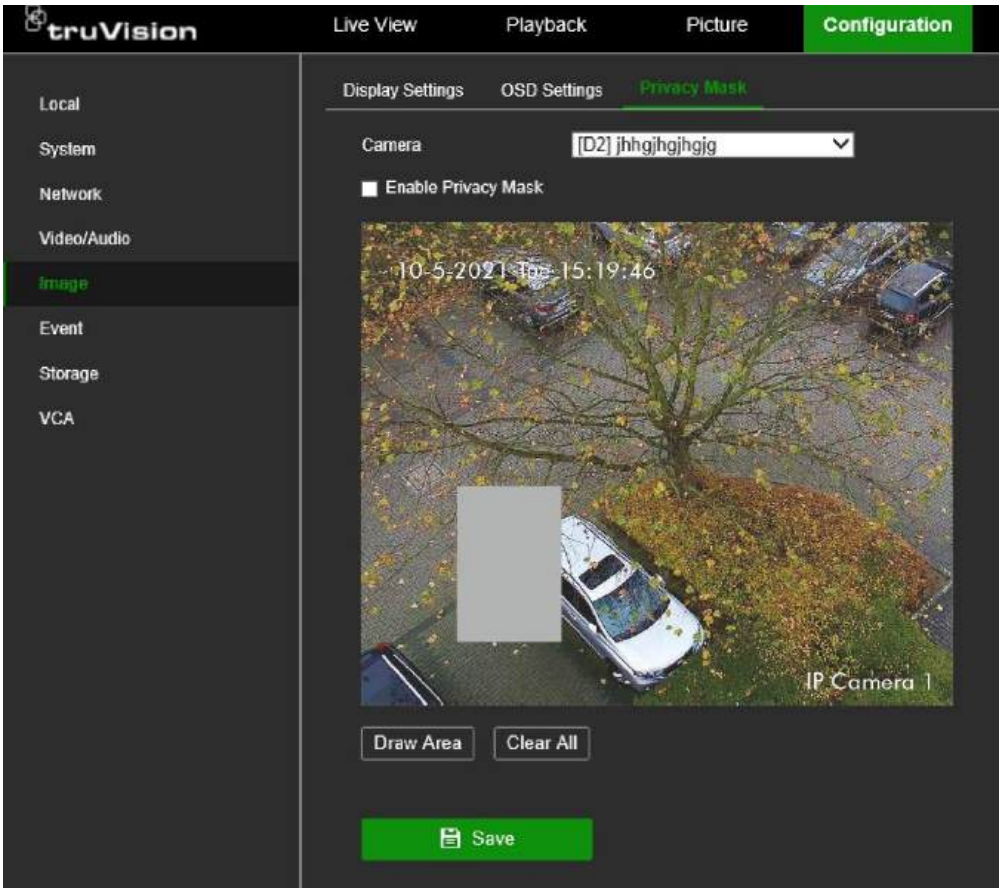
To setup a privacy mask in web mode:

1. Click **Configuration** > **Image** > **Privacy Mask**.
2. Select the camera for which to set up privacy masking.
3. Select the **Enable Privacy Mask** check box to enable the function.
4. Set up the mask area.

   Click **Draw Area**. Using the mouse, click and drag a privacy-mask box in the camera view window over the desired area. You can set up to four areas for privacy masking. To delete the masks, click **Clear All**.

www.acornfiresecurity.com

www.acornfiresecurity.com



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

To setup a privacy mask in OSD mode:

1. Click **Camera** > **Privacy Mask**.
2. Select the camera for which to set up privacy masking.
3. Select the **Enable** check box to enable the function.
4. Set up the mask area.

   Using the mouse, click and drag a privacy-mask box in the camera view window over the desired area. You can set up to four areas for privacy masking. Each area has a different colored frame. To delete the masks, click **Clear**.
5. Click **Apply** to save the settings.

www.acornfiresecurity.com

Chapter 10
Event setup

This chapter describes how to configure for the detection of alarms and events such as motion detection, video loss, camera tampering, and VCA events. There is also information on the different types of alarms and connected responses. Intrusion integration is also explained.

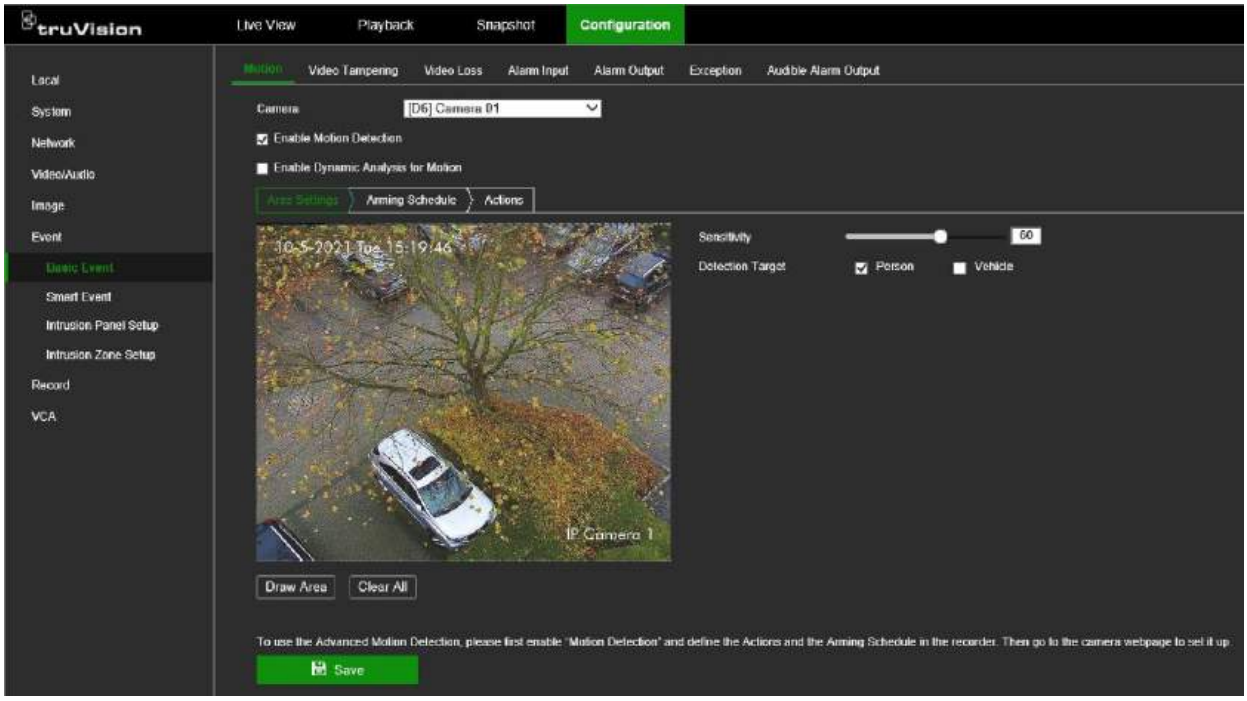
Motion detection

The motion detection function is used to detect motion in a selected area. You can 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.

Note: Not all cameras support this function.

To set up motion detection in web mode:

1. Click **Configuration** > **Event** > **Basic Event** > **Motion**.



www.acornfiresecurity.com

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**. This allows you to see on-screen motion being detected while setting up the feature. Areas, where motion is detected, are shown as solid red squares in the motion grid.
5. Click the **Area Settings** tab to create specific areas on-screen to be sensitive to motion. Click **Draw Area** and drag the mouse cursor over the window to select the areas sensitive to motion detection. Click **Stop Drawing**. Repeat this Draw Area-Stop Drawing action for each motion-sensitive area.

Set the sensitivity level. Drag the Sensitivity scroll bar to the desired sensitivity level.

6. If the camera supports people/vehicle detection, set the Detection Target as **Person** and/or **Vehicle**. Alarms that are not triggered by people and/or vehicles are ignored.

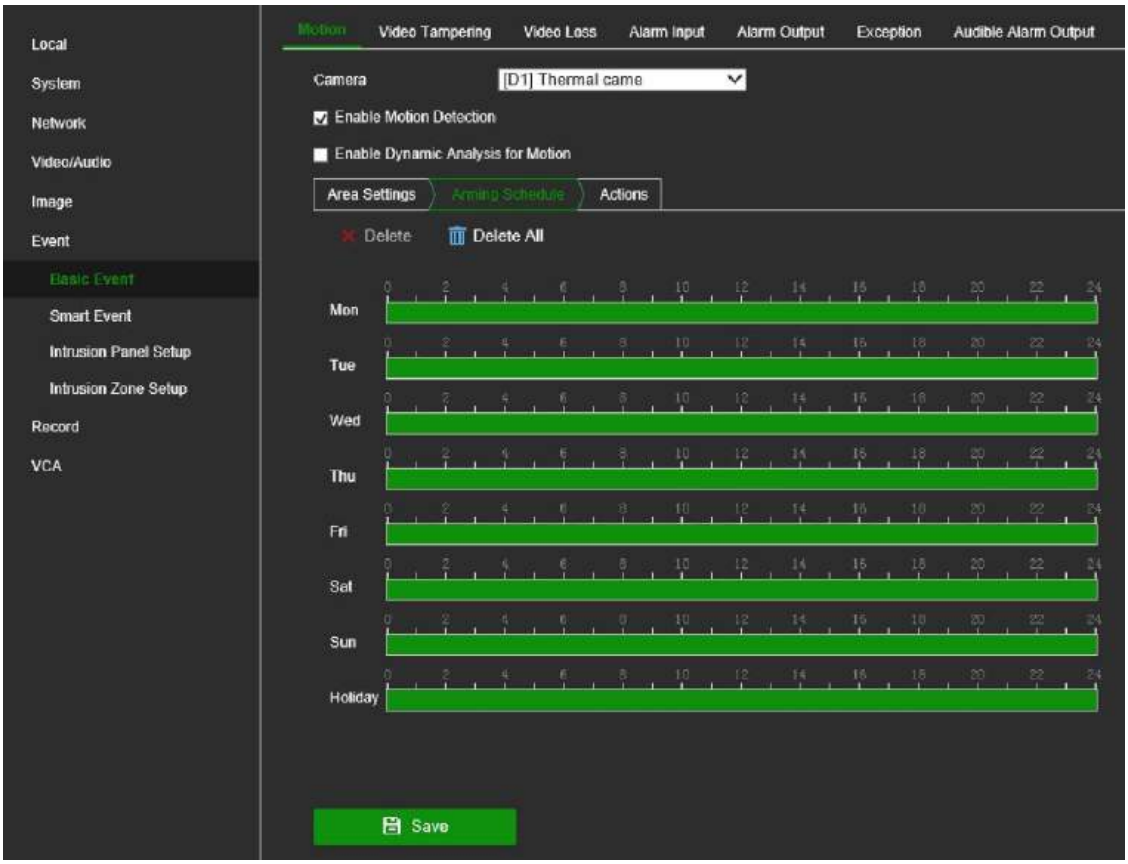
   Note: Not all cameras support this function. See the list of supported cameras on page 488.

7. Click the **Arming Schedule** tab to select the daily arming schedules for motion detection.

   Click the desired day of the week and a pop-up screen appears where you can enter the start and end times when motion detection can trigger the given actions. You can schedule eight periods in a day. Default is 24 hours.

www.acornfiresecurity.com

www.acornfiresecurity.com



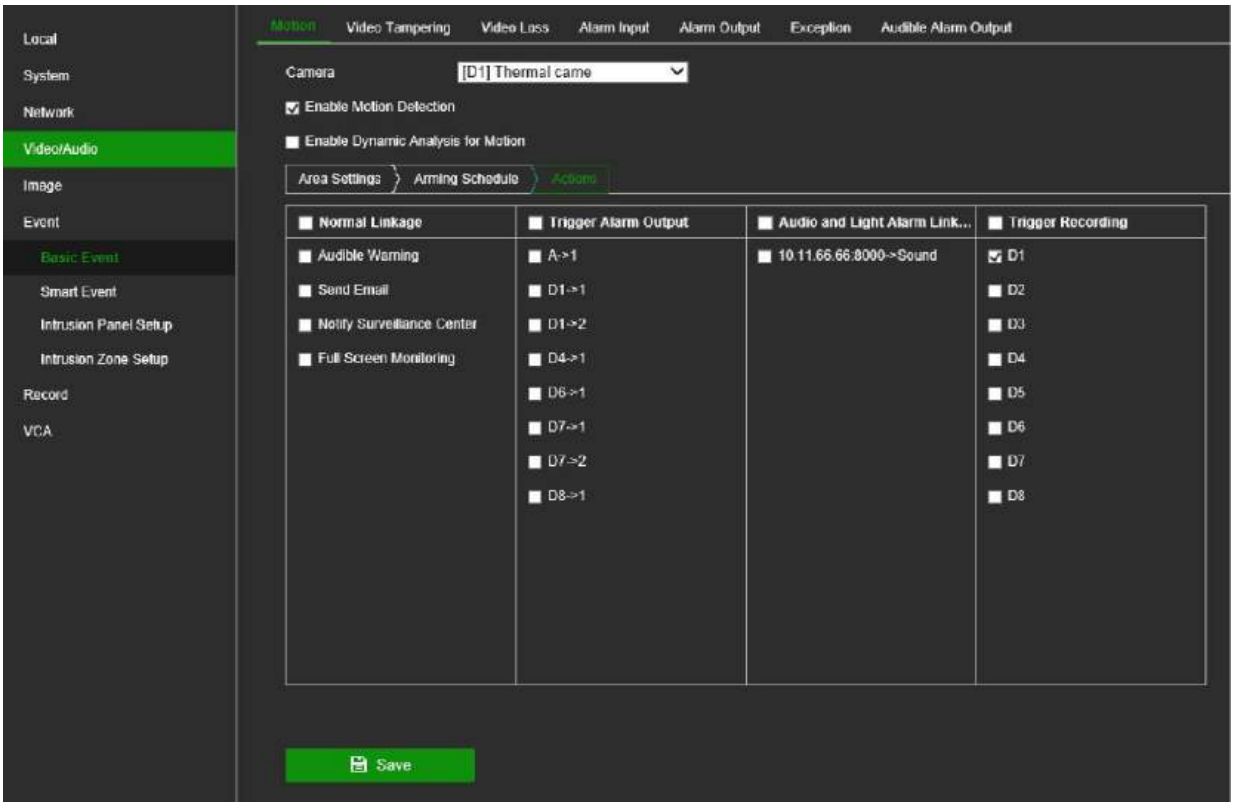
Note that when motion detection is enabled, motion events will always trigger event recording, regardless of the recording schedule (see page 145 for more information on recording schedules).

8. Link the corresponding action to motion detection.

   Click the **Actions** tab to define the method by which you want the recorder to notify you of the alarm: Full-screen Monitoring, Audible Warning (recorder's buzzer), Notify the Surveillance Center, Send Email, Trigger Alarm Output, as well as Audio and Light Alarm Linkage (only for supported cameras) and trigger the recording for one or more cameras.

www.acornfiresecurity.com

www.acornfiresecurity.com

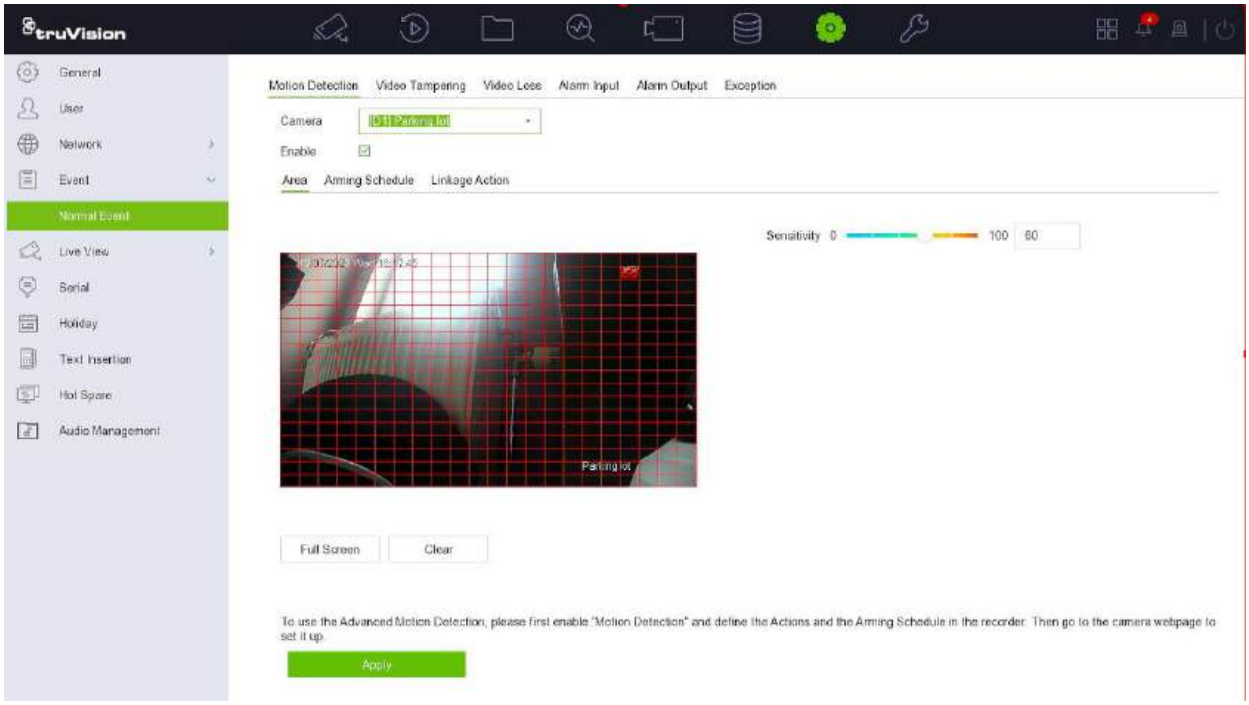


The list of action options available depends on the camera.

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

To set up motion detection in OSD mode:

1. Click **System** > **Event** > **Normal Event** > **Motion Detection**.



2. Select the camera to detect motion. Each camera must be set up individually.

www.acornfiresecurity.com

www.acornfiresecurity.com

3. Select **Enable** to enable motion detection. If this is not enabled, motion will not be recorded.

   Note: **Enable Dynamic Analysis for Motion** is only available in web mode.

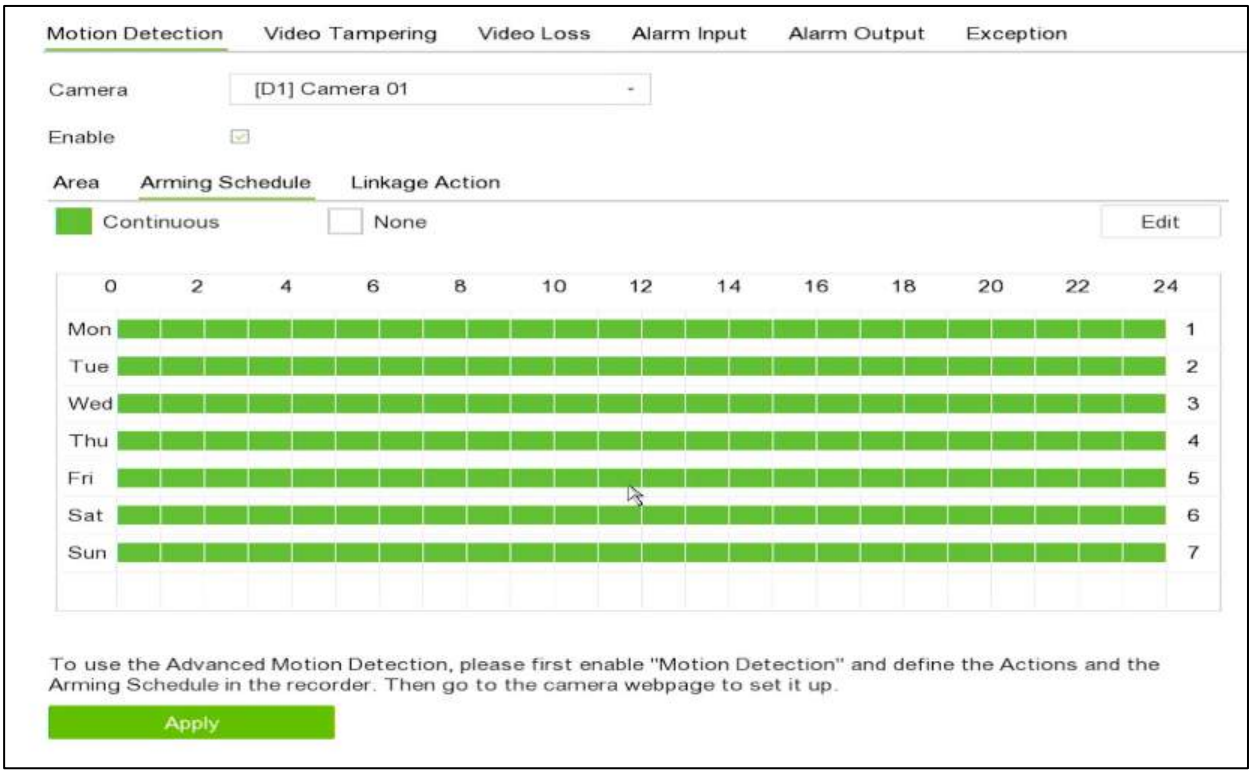
4. Click the **Area** tab to create specific areas on-screen to be sensitive to motion. Click **Draw Area** and drag the mouse cursor over the window to select the areas sensitive to motion detection.

   Set the sensitivity level. Drag the Sensitivity scroll bar to the desired sensitivity level.

5. If the camera supports people/vehicle detection, set the Detection Target as **Person** and/or **Vehicle**. Alarms that are not triggered by people or vehicles are ignored.

6. Click the **Arming Schedule** tab to select the daily arming schedules for motion detection.

   Click **Edit** to edit the schedule. A pop-up screen appears where you can enter the start and end times when motion detection can trigger the given actions for every day. You can schedule eight periods in a day. Default is 24 hours.



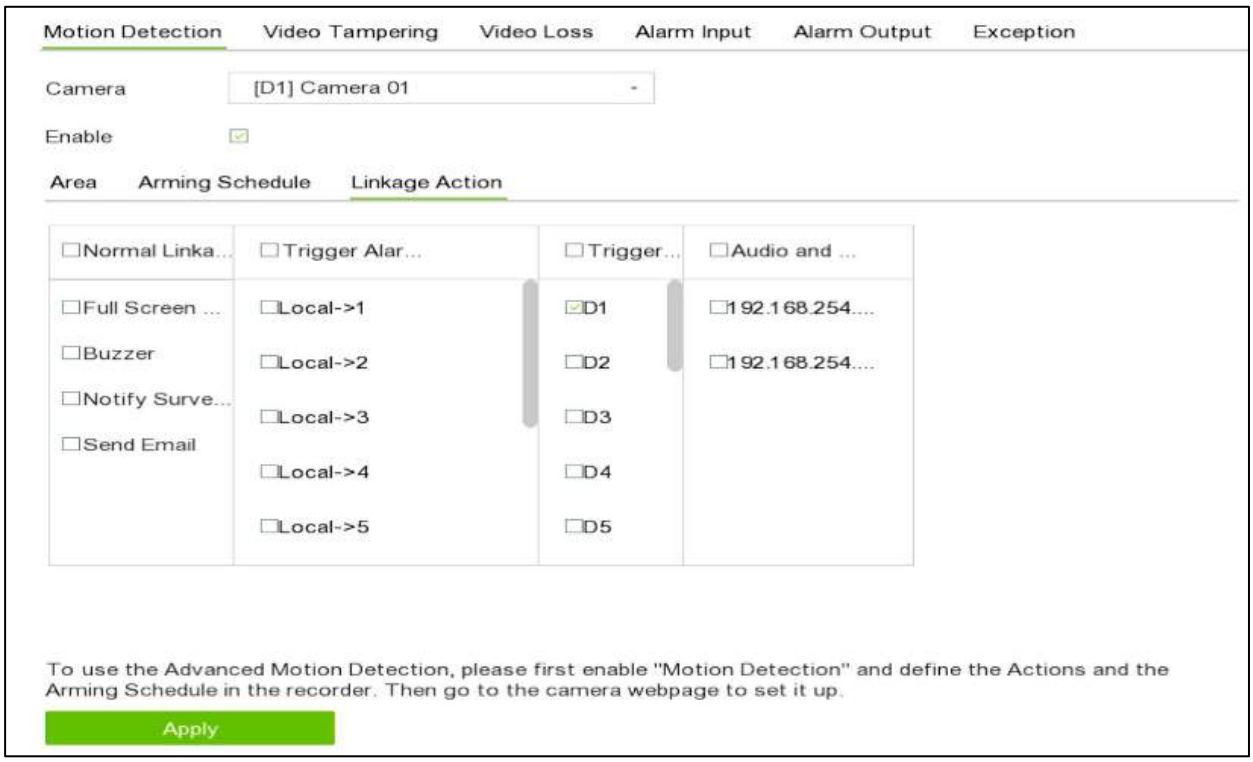
   Note that when motion detection is enabled, motion events will always trigger event recording, regardless of the recording schedule (see page 145 for more information on recording schedules).

7. Link the corresponding action to motion detection.

   Click the **Actions** tab to define the method by which you want the recorder to notify you of the alarm: Full-screen Monitoring, Enable Alarm Audio, Notify the Surveillance Center, Send Email, and Trigger Alarm Output, as well as Audio and Light Alarm Linkage (only for supported cameras).

www.acornfiresecurity.com

www.acornfiresecurity.com



The list of action options available depends on the camera.

8. Click **Apply** to save the 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 recorders, 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.

Camera tamper

You can set up 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 select a specific area of the camera screen to detect tampering.

This function is not supported by all camera models.

www.acornfiresecurity.com

www.acornfiresecurity.com

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

To set up video tampering detection in web mode:

1. Click **Configuration** > **Event** > **Basic Event** > **Video Tampering.**
2. Select a camera to configure for video tampering detection.
3. Select the **Enable Video Tampering** check box to enable the function.
4. Create a specific area on-screen that is sensitive to detect tampering.

   Click the **Area** tab and click **Draw Area**. Drag the mouse cursor across the screen to select the area sensitive to tamper. Only one area can be drawn. Click **Clear All** to delete the area.

   Select the tamper detection sensitivity level by clicking the sensitivity scroll bar.
5. Select the recording schedules to detect tampering.

   Click the **Arming Schedule** tab and then click the day to set up a period during which alarms can be recorded. In the pop-up box that appears, enter the start and end times. You can schedule up to eight periods in a day. Default is 24 hours for a day.

   Note: The periods defined during a day cannot overlap.
6. Select the response method to an external alarm.

   Click the **Actions** tab and select the method by which you want the recorder to notify you of the alarm.

   Normal Linkage: This applies to the recorder. It is the alarm notifications that the recorder can send. The options are Audible Warning, Send Email, Notify Surveillance Center, and Full Screen Monitoring. More than one option can be selected.

   Note: “Audible warning” is called “Buzzer” in OSD mode.

   Trigger Alarm Output: This applies to the cameras connected to the recorder. A message is sent to the selected camera to trigger an alarm contact. The options are A-> x (this is the relay output of the recorder, x = relay number output of the recorder), and D->1 for the output of the IP camera, connected to the recorder. More than one option can be selected.
7. Click **Save** to save the settings.

To set up video tampering detection in OSD mode:

1. Click **System** >**Event** > **Normal Event** > **Video Tampering**.
2. Select a camera to configure for video tampering detection.
3. Select the **Enable** check box to enable the function.
4. Create a specific area on-screen that is sensitive to detect tampering.

www.acornfiresecurity.com

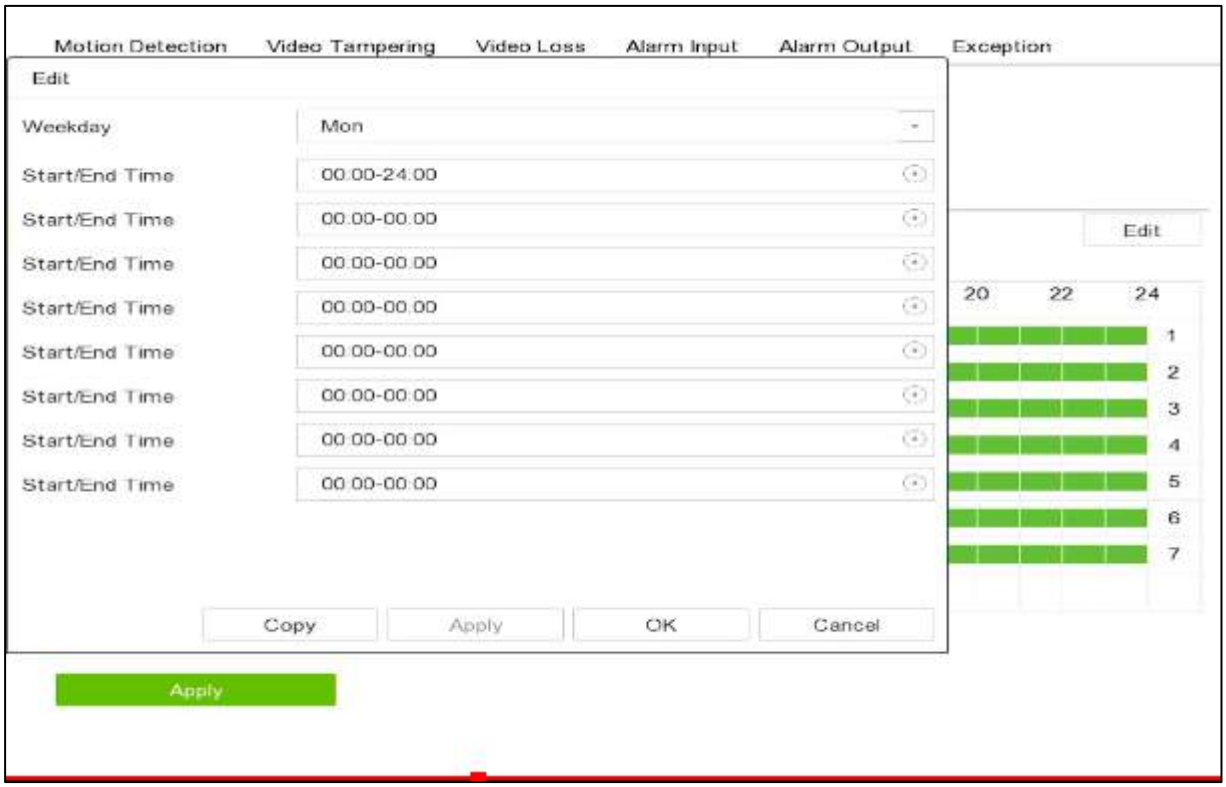
www.acornfiresecurity.com

Click the **Area** tab and then drag the mouse cursor across the screen to select the area sensitive to tamper. Only one area can be drawn. Click **Clear** to delete the area.

Select the tamper detection sensitivity level by clicking the sensitivity scroll bar.

5. Select the recording schedules to detect tampering.

   Click the **Arming Schedule** tab and click **Edit** to enter the start and end times for each period required in a day. You can schedule up to eight periods in a day. Default is 24 hours.



When in the schedule pop-up screen (see above), click **Copy to** to copy the schedule from one day to another.

Note: The periods defined during a day cannot overlap.

6. Select the response method to an external alarm.

   Click the **Linkage Action** tab and select the method by which you want the recorder to notify you of the alarm.

   Normal Linkage: This applies to the recorder. It is the alarm notifications that the recorder can send. The options are Full Screen Monitoring, Buzzer, Notify Surveillance Center, and Send Email. More than one option can be selected.

   Alarm Output Linkage: This applies to the cameras connected to the recorder. A message is sent to the selected camera to trigger an alarm contact. The options are Local -> 1 (this is the relay output of the recorder), and the IP addresses of cameras that have an output contact and are connected to the recorder.

www.acornfiresecurity.com

www.acornfiresecurity.com

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

Video loss detection

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 set up video loss detection in web mode:

1. Click **Configuration** > **Event** > **Basic Event** > **Video Loss**.
2. Select a camera to configure for video loss detection.
3. Select the **Enable Video Loss Detection** check box to enable the function.
4. Set the arming schedule for detecting video loss.

   Click the **Arming Schedule** tab and then click the day to set up a period during which alarms can be recorded. In the pop-up box that appears, enter the start and end times. You can schedule up to eight periods in a day. Default is 24 hours for a day.

   Note: The periods defined during a day cannot overlap.
5. Select the alarm response method.

   Click the **Actions** tab and select the method by which you want the recorder to notify you of the alarm.

   Normal Linkage: This applies to the recorder. It is the alarm notifications that the recorder can send. The options are Audible Warning, Send Email, Notify Surveillance Center, and Full Screen Monitoring. More than one option can be selected.

   Note: “Audible warning” is called “Buzzer” in OSD mode.

   Trigger Alarm Output: This applies to the cameras connected to the recorder. A message is sent to the selected camera to trigger an alarm contact. The options are A -> x (this is the relay output of the recorder; x = relay number output of the recorder), and D->1 for the output of the IP camera), and Dx→1 for the output of the IP camera , connected to the recorder. More than one option can be selected.
6. Click **Save** to save the settings.

To set up video loss detection in OSD mode:

1. Click **Configuration** > **Event** > **Basic Event** > **Video Loss**.
2. Select a camera to configure for video loss detection.
3. Select the **Enable** check box to enable the function.
4. Set the arming schedule for detecting video loss.

   Click the **Arming Schedule** tab and then click Edit to modify the start/end times during which alarms can be recorded. In the pop-up box that appears, enter the

www.acornfiresecurity.com

www.acornfiresecurity.com

start and end times. You can schedule up to eight periods in a day. Default is 24 hours for a day.

Note: The periods defined during a day cannot overlap.

5. Select the alarm response method.

   Click the **Linkage Action** tab and select the method by which you want the recorder to notify you of the alarm.

   Normal Linkage: This applies to the recorder. It is the alarm notifications that the recorder can send. The options are Buzzer, Send Email, Notify Surveillance Center, and Full Screen Monitoring. More than one option can be selected.

   Alarm Output Linkage: This applies to the cameras connected to the recorder. A message is sent to the selected camera to trigger an alarm contact. The options are: Local -> 1 (this is the relay output of the recorder), and the channel numbers of the cameras that have an output contact and are connected to the recorder. More than one option can be selected.

6. Click **Apply** to save the settings.

Set up alarm inputs

The recorder can be configured to record when an alarm is triggered by an external alarm device (for example, a PIR detector, dry contacts…). They are the physical inputs on the cameras and recorder.

To set up external alarms in web mode:

1. Click **Configuration** > **Event** > **Basic Event** > **Alarm Input**.
2. Select the desired alarm input number of the recorder or camera, alarm type (NO (normally open) or NC (normally closed)). Default is NO. You can also enter a name for the alarm.

   The camera IP address is automatically entered depending on the alarm input number selected.

3. If you set *Settings* to **Not used**, the alarm input will be disabled. If you set Settings to **Input**, the selected linkage method(s) of the alarm input will be disabled. For information on *Disable Actions*, see “Disable Actions” on page 124.
4. Set the arming schedule for detecting external alarms.

   Click the **Arming Schedule** tab and then click the day to set up a period during which triggered alarms can be recorded. In the pop-up box that appears, enter the start and end times. You can schedule up to eight periods in a day. Default is 24 hours for a day.

   Note: The periods defined during a day cannot overlap.

5. Select the alarm response method.

www.acornfiresecurity.com

www.acornfiresecurity.com

Click the **Actions** tab and select the method by which you want the recorder to notify you of the alarm.

Normal Linkage: This applies to the recorder. It is the alarm notifications that the recorder can send. The options are Audible Warning, Send Email, Notify Surveillance Center, and Full Screen Monitoring. More than one option can be selected.

Note: “Audible warning” is called “Buzzer” in OSD mode.

Trigger Alarm Output: This applies to the cameras connected to the recorder. A message is sent to the selected camera to trigger an alarm contact. The options are: Local -> 1 (this is the relay output of the recorder), and the channel numbers of the cameras that have an output contact and are connected to the recorder. More than one option can be selected.

Trigger Recording: This applies to the cameras connected to the recorder. A message is sent to the selected camera to trigger recording. More than one camera can be selected.

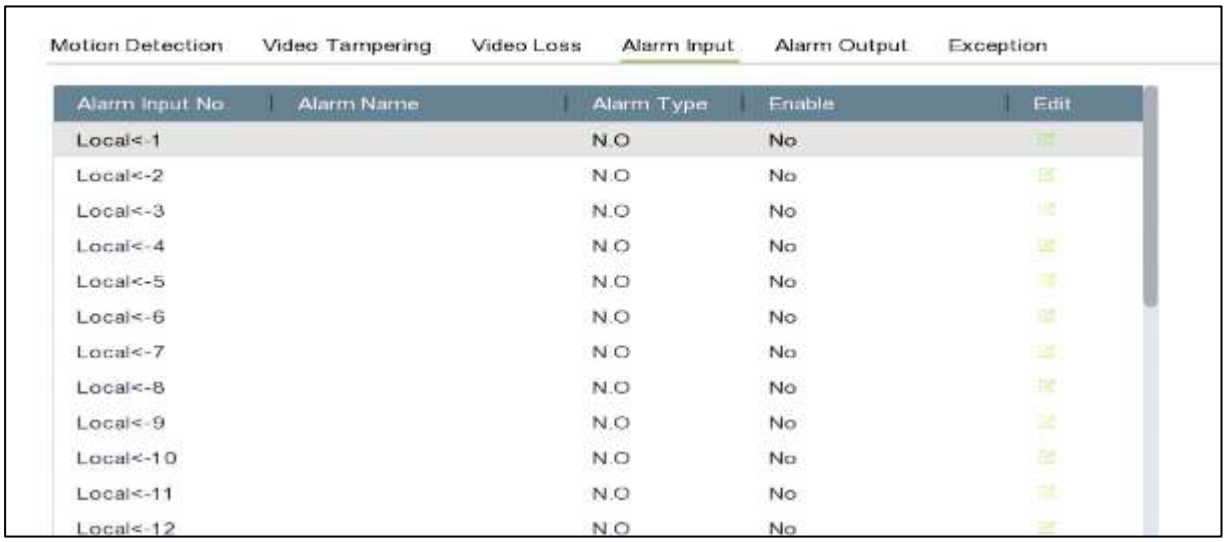
PTZ Linking: This is the PTZ camera function required in response to an external alarm. Select the PTZ camera under **PTZ Linkage**. Enter the preset, preset tour, or shadow tour that is triggered when the alarm is detected.

6. If you want to copy a camera’s settings to another camera, click **Copy to**. In the pop-up window that appears, select the camera to which to copy the settings. Click **OK**.
7. Click **Save** to save settings.

To set up external alarms in OSD mode:

1. Click **System >Event** > **Normal Event** > **Alarm Input**.

   The window displays the status of the alarm inputs is shown for the recorder and cameras.



www.acornfiresecurity.com

www.acornfiresecurity.com

2. To change the settings for any recorder or camera alarm input, click **Edit** for the desired recorder/camera. Change the alarm type (NO (normally open) or NC (normally closed)). Default is NO. You can also enter a name for the alarm.
3. If you set *Settings* to **Not used**, the alarm input will be disabled. If you set Settings to **Input**, the selected linkage method(s) of the alarm input will be disabled. For information on *Disable Actions*, see “Disable Actions” on page 124.
4. Set the arming schedule for detecting external alarms.

   This function is only available in web mode.
5. Select the alarm response method.

   This function is only available in web mode.
6. Click **Apply** to save the settings.

Combined Alarm (OSD only)

With the Combined Alarm feature, you can combine the alarm input with an event.

The combined alarm will be triggered when there is an event triggering for both an alarm input and an event.

The events that can be used: motion detection, video tampering, and other smart events such as cross line detection, intrusion detection etc.

Make sure you have setup the camera event and the alarm input as needed.

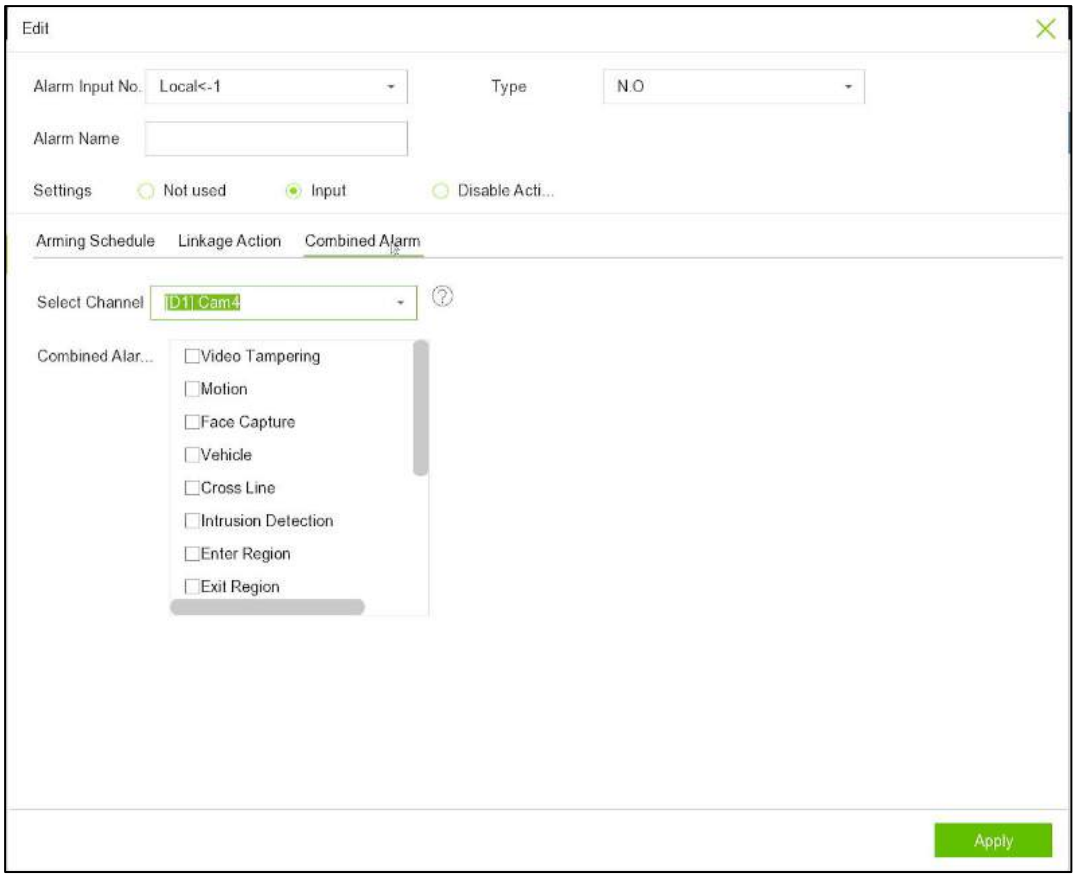
To set up the Combined Alarm:

1. Click **System > Event > Normal Event > Alarm Input**
2. Select an alarm input from the list and click edit .
3. Select **Settings** as **Input**.
4. Clcik Combined Alarm.
5. Select the desired camera channel from the dropdown list.
6. Select the **Combined Alarm Event**.
7. Click **Apply**.

Note: the combined alarm arming schedule and linkage actions are the same as the selected event(s).

www.acornfiresecurity.com

www.acornfiresecurity.com



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.

The alarm status of a recorder or camera is disabled by default. It can be triggered by an event such as motion detection when its status will then change from OFF to ON. However, there are up to two ways to manually trigger the alarm output of a device. The alarm can be manually triggered from the Configuration > Event menu (web) or System > Event > Normal Event > Alarm Output > Edit as well as from live view when in web mode only.

If, for example, you want to enable an output, go to live view in web mode, and the bottom right corner of the screen click the *Alarm Output* icon and enable the desired recorder/camera. The alarm status under Event > Basic Event > Alarm Output then changes to ON. When you want to disable the output, return to *Alarm Output* in live view and deselect the option. The alarm status changes back to OFF.

www.acornfiresecurity.com

www.acornfiresecurity.com

To set up an alarm output in web mode:

1. Click **Configuration** > **Event** > **Basic Event** > **Alarm Output**.
2. Select the desired alarm output number of the recorder or camera. You can also enter a name for the alarm. The camera IP address is automatically entered depending on the alarm input number selected.
3. Under *Delay*, select a timeout option between 5 seconds and 10 minutes or select “Manual”.

   The delay setting (or dwell time) lets you define how long an alarm signal remains active after the alarm has ended. If you select **Manual**, the alarm status remains unchanged until it is manually changed.
4. To manually change the alarm status of the selected recorder or camera:

   Live view: At the bottom right corner of the screen, click the *Alarm Output* icon and enable the desired recorder/camera. The alarm status of the selected device changes from OFF to ON.

   — or —

   Configuration > Event > Basic Event > Alarm Output: Click the **Manual Alarm** button. The alarm status of the selected device changes from OFF to ON. The button is renamed *Clear Alarm*. Click **Clear Alarm** to disable the alarm status.
5. Set the arming schedule for the alarm outputs.

   Click the **Arming Schedule** tab and then click the day to set up a period during which triggered alarms can be recorded. In the pop-up box that appears, enter the start and end times. You can schedule up to eight periods in a day. Default is 24 hours for a day. Click **Delete All** to delete all saved schedules or **Delete** to delete the schedule for the selected day.

   Note: The periods defined during a day cannot overlap.
6. If you want to copy a camera’s settings to another camera, click **Copy to**. In the pop-up window that appears, select the camera to which to copy the settings. Click **OK**.
7. Click **Save** to save the settings.

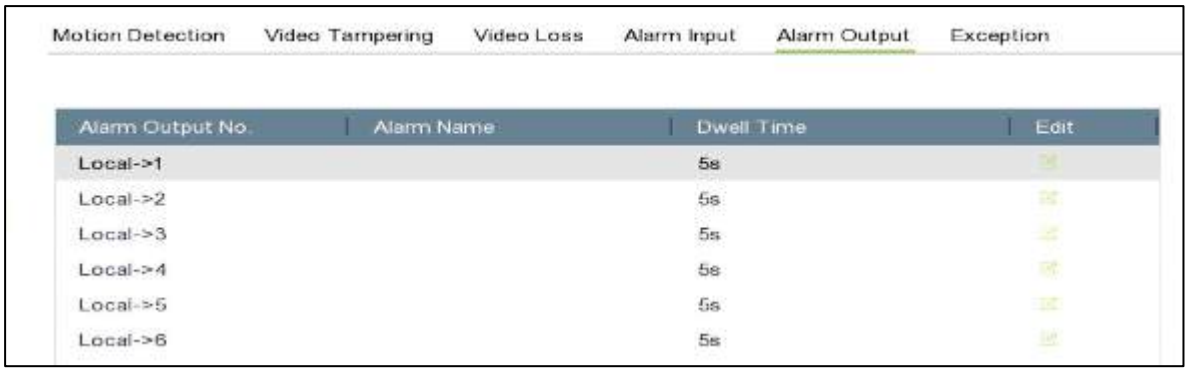
To set up an alarm output in OSD mode:

1. Click **System** > **Event** > **Normal Event** > **Alarm Output**.

   The status of the alarm outputs is shown for the recorder and cameras.

www.acornfiresecurity.com

www.acornfiresecurity.com



2. To change the settings for any recorder or camera alarm output, click **Edit** for the desired recorder/camera. You can also enter a name for the alarm.
3. Under *Duration*, select a timeout option between 5 and 600 seconds or select “Manually Clear”.

   The dwell time lets you define how long an alarm signal remains active after the alarm has ended. If you select **Manually Clear**, the alarm status remains unchanged until it is manually changed.
4. To manually change the alarm status of the selected recorder or camera, click the **Trigger** button at the bottom of the screen. The alarm status of the selected device changes from *Close* to *Enable*. The button is renamed Clear. Click **Clear** to disable the alarm status.
5. Set the arming schedule for the alarm outputs.

   Click the **Arming Schedule** tab and then click the day to set up a period during which triggered alarms can be recorded. In the pop-up box that appears, enter the start and end times. You can schedule up to eight periods in a day. Default is 24 hours for a day. Click **Clear All** to delete all saved schedules or **Clear** to delete the schedule for the selected day.

   Note: The periods defined during a day cannot overlap.
6. If you want to copy a camera’s settings to another camera, click **Copy to**. In the pop-up window that appears, select the camera to which to copy the settings. Click **OK**.
7. Click **Apply** to save the settings.

Manually trigger an alarm output

You can manually trigger the outputs of the recorder.

To trigger or clear alarm outputs manually in web mode:

1. Click **Configuration** > **Event** > **Basic Event** > **Alarm Output**.
2. Select the desired alarm output and click the **Manual Alarm** button to trigger or stop an alarm output. Click **Clear Alarm** to clear an alarm output.
3. Click **Save**. The alarm is silenced.

www.acornfiresecurity.com

www.acornfiresecurity.com

To trigger or clear alarm outputs manually in OSD mode:

1. Click **System**> **Event** > **Normal Event** > **Alarm Output**.
2. Click the **Edit** button for the desired alarm output of a recorder/camera. The arming schedule window opens.
3. Click the **Trigger** button to trigger an alarm output. Click **Clear** to clear an alarm output.
4. Click **Apply**. The alarm is silenced.

Exception notification

You can select the alarm and event exception types to be included in the alarm center that lists the detected alarm and event notifications. Click the alarm center icon in the top right of the screen (OSD) to get the list of exception types that have been triggered.

The different types of exception types:

- **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.
- **IP Conflict**: Conflict in IP address setting.
- **Illegal Login:** Wrong user ID or password used.
- **Vidoe Signal Loss:** no video signal on a camera.
- **Record/Capture Exception:** 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 Conflicted:** Conflict in the IP address setting for an IP camera.
- **Hot Spare Exception:** an issue with hot spare function.
- **PoE Power Overload:** PoE power overload detected. Note that this is only shown in OSD mode.
- **Resolution or Bitrate of Substream not supported.**
- **HDD Overheat Exception:** the HDD temperature is too high.
- **HDD Low temperature Excepton:** the HDD temperature is too low.
- **HDD Bad Sector Exception:** the HDD has bad sectors.
- **HDD Shock Exception:** the HDD has detected a shock and might be damaged
- **HDD Severe Failure Exception:** the HDD is faulty.
- **No Stream Exception:** When the camera is connected but not streaming video data.
- **Log Disk Exception:** Not applicable**.**

www.acornfiresecurity.com

www.acornfiresecurity.com

To set up event notifications in web mode:

1. Click **Configuration** > **Event** > **Basic Event** > **Exception**.
2. Select an event notification and how the recorder should respond to it.

   Under **Exception Type**, select the desired alarm or event to be notified.
3. Select the alarm response method.

   Select the method by which you want the recorder to notify you of the alarm.

   Normal Linkage: This applies to the recorder. It is the alarm notifications that the recorder can send. The options are: Audible Warning, Send Email, and Notify Surveillance Center. More than one option can be selected.

   Note: “Audible warning” is called “Buzzer” in OSD mode.

   Trigger Alarm Output: This applies to the cameras connected to the recorder. A message is sent to the selected camera to trigger an alarm contact. The options are: A -> x (this is the relay output of the recorder; x = relay number output of the recorder), and D->1 for the output of the IP camera), and Dx→1 for the output of the IP camera, connected to the recorder. More than one option can be selected.
4. Click **Save** to save the settings.

To set up event notifications in OSD mode:

1. Click **System** > **Event** > **Normal Event** > **Exception**.
2. Select the **Enable Event Hint** check box to enable the function.
3. Select **Event Hint Configuration**, to select the events that will be shown in the Alarm and Exception list and how the recorder should respond to it.

   Under **Exception Type**, select the desired recorder alarm or event o be notified.
4. Select the alarm response method.

   Select the method by which you want the recorder to notify you of the recorder alarm.

   Normal Linkage: This applies to the recorder. It is the alarm notifications that the recorder can send. The options are Buzzer, Send Email, and Notify Surveillance Center. More than one option can be selected.

   Trigger Alarm Output: This applies to the cameras connected to the recorder. A message is sent to the selected camera to trigger an alarm contact. The options are: Local -> 1 (this is the relay output of the recorder), and the IP addresses of the cameras that have an output contact and are connected to the recorder. More than one option can be selected.
5. Click **Apply** to save the settings.

www.acornfiresecurity.com

www.acornfiresecurity.com

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
- 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.

The *Intrusion Panel Setup* and *Intrusion Zone Setup* functions are only available in web mode.

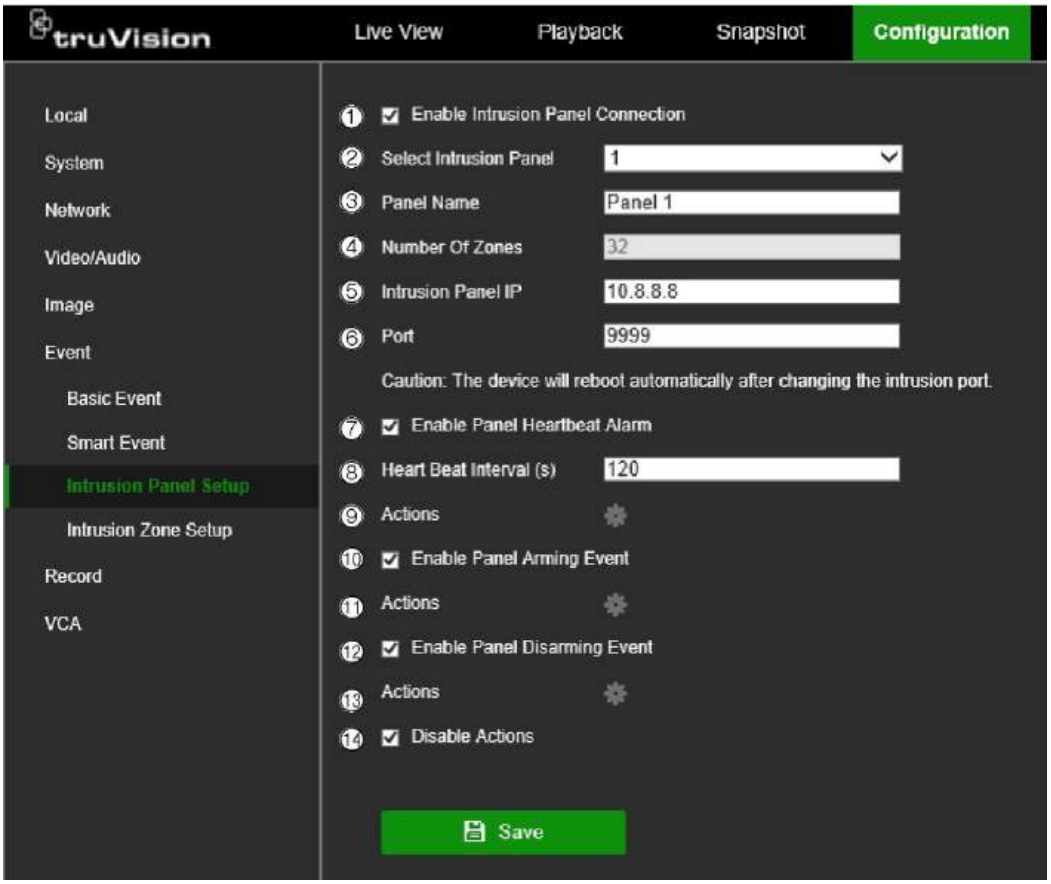
This function is **only available in web mode**.

www.acornfiresecurity.com

www.acornfiresecurity.com

To set up an alarm panel in the recorder in web mode:

1. Click **Configuration** > **Event** > **Intrusion Panel Setup**.
2. In the *Intrusion Panel Setup* window, enter the required settings.



Option		Description
Set up the intrusion panel connection parameters:		
1.	Enable Intrusion Panel Connection	Select this check box to enable the intrusion panel connection.
2.	Select Intrusion Panel	Select which panel you want to set up. Up to three panels can be set up.
3.	Panel Name	Enter a name for the panel.
4.	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.
5.	Intrusion Panel IP	Enter the panel’s IP address. The IP address must be in the same LAN as the recorder.
6.	Port	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.
Set up the heartbeat alarm parameters:		
7.	Enable Panel Heartbeat Alarm	Select this check box to enable the panel heartbeat alarm. The heartbeat alarm will then be reported to the recorder.

www.acornfiresecurity.com

www.acornfiresecurity.com

8.	Heartbeat Interval(s)	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.
9.	Actions	Click the **Actions** button to set up the actions linked to the panel heartbeat alarm. Go to step 3.
Set up the panel arming event parameters:		
10.	Enable Panel Arming Event	Select this check box to enable the panel arming event. When the panel is armed, it will be reported to the recorder.
11.	Actions	Click the **Actions** button to set up the actions linked to the panel arming event. Go to step 3.
Set up the panel disarming alarm parameters:		
12.	Enable Panel Disarming Alarm	Select this check box to enable the panel disarming event. When the panel is disarmed, it will be reported to the recorder.
13.	Actions	Click the **Actions** button to set up the actions linked to the panel disarming alarm. Go to step 3.
14.	Disable Actions	Select this check box to enable the execution of event/alarm actions and to influence the recording behavior. Default is Disabled. See “Disable Actions” on page 124 for further information.

3. To define the actions for the heartbeat, panel arm and panel disarm alarms that are reported by the intrusion panel, enable the desired functions, and click the **Actions** tab for each to set up the arming schedule and alarm response actions.

www.acornfiresecurity.com

www.acornfiresecurity.com

Arming Schedule:	Define the alarm schedule for the actions over a week and for holidays. You can schedule one period in a day. Default is 24 hours.
Actions:	**Normal Linkage**: This applies to the recorder. It is the alarm notifications that the recorder can send. The options are Audible Warning, Send Email, Notify Surveillance Center, and Full-screen Monitoring.
	Trigger Alarm Output: This applies to the cameras connected to the recorder. A message is sent to the selected camera to trigger an alarm contact. The options are the channels numbers of the cameras that have an output contact and are connected to the recorder. More than one option can be selected.
	Trigger Recording: This applies to the cameras connected to the recorder. A message is sent to the selected camera to start recording. More than one camera can be selected.
	PTZ Linking: Select the PTZ camera as well as the preset, preset tour, or shadow tour that is triggered when the alarm/event is detected. **Note**: The preset tour and a shadow tour have a time limitation when using them as an action here.

Click **OK** to return to the main window.

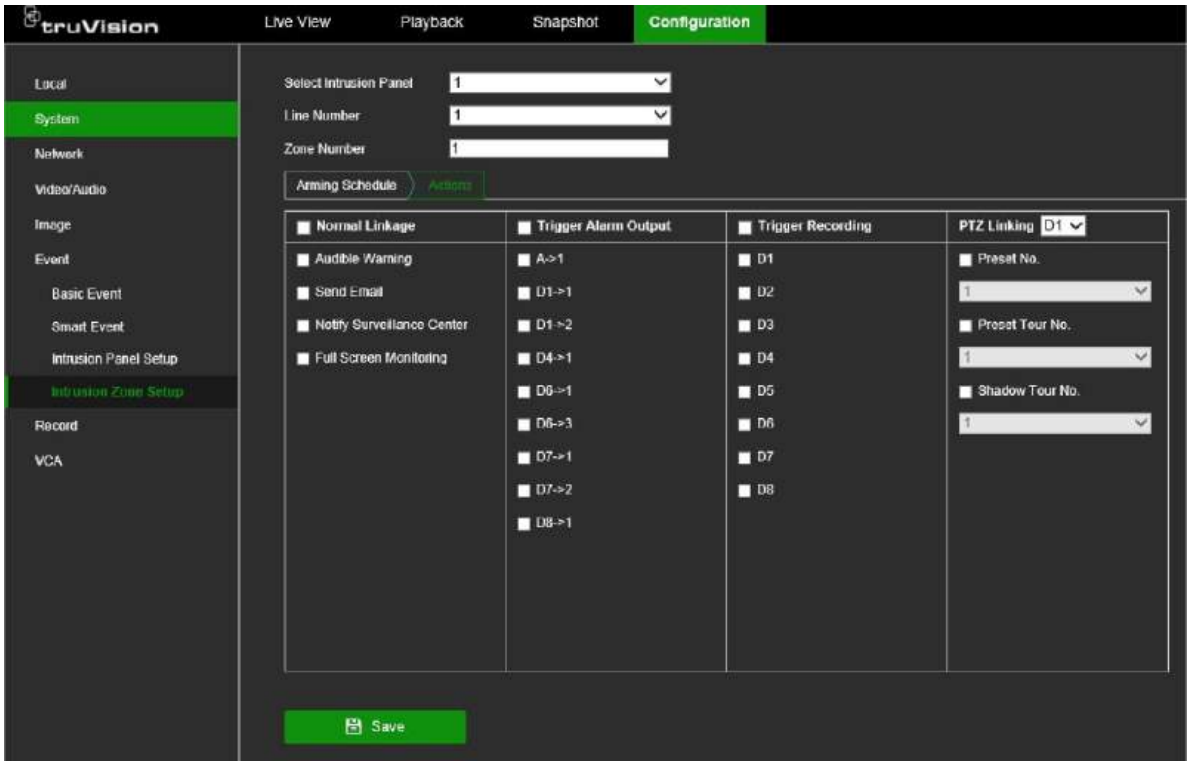
4. Click **Save** to save the intrusion panel setup parameters.

To set up the zones in an alarm panel in web mode:

1. Click **Alarm & Event Setup** > **Intrusion Zone Setup**.
2. Under **Select Intrusion Panel**, select intrusion panel 1, 2, or 3.
3. Under **Line Number**, select the desired line number. The line number can be any valid number of the panel, which does not need to match the zone ID.
4. Select the desired ID of a zone. The maximum is 32. The number does not have to match the line number.
5. Click the *Arming Schedule* tab to set the arming schedule for the selected zone number. Click the day to set up a period during which triggered alarms can be recorded. In the pop-up box that appears, enter the start and end times. You can schedule one period in a day. Default is 24 hours for a day.
6. Click the *Actions* tab to set the alarm response method. Select the method by which you want the recorder to notify you of the alarm.

www.acornfiresecurity.com

www.acornfiresecurity.com



Normal Linkage: This applies to the recorder. It is the alarm notifications that the recorder can send. The options are: Audible Warning, Send Email, and Notify Surveillance Center. More than one option can be selected.

Trigger Alarm Output: This applies to the cameras connected to the recorder. A message is sent to the selected camera to trigger an alarm contact. The options are the channels numbers of the cameras that have an output contact and are connected to the recorder. More than one option can be selected.

Trigger Recording: This applies to the cameras connected to the recorder. A message is sent to the selected camera to start recording. More than one camera can be selected.

PTZ Linking: Select the PTZ camera as well as the preset, preset tour, or shadow tour that is triggered when the alarm/event is detected.

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

Transparent Transmission Configuration (Web only)

Some TruVision IP cameras contain extra events than the events that can be seen in the normal events or mart events.

Transparent transmission makes some of these extra events configurable, and the event alarms from these cameras can be directly transmitted.

www.acornfiresecurity.com

www.acornfiresecurity.com

The list will only display events that the connected cameras support. You can custom the event description as your desire, by clicking in the field of the event description and updating the text. Transparent transmission is configurable via web browser only.

You can setup an arming schedule and the actions for extra events via the Smart Events menu.

Example: a TruVision P Series IP camera has some extra events, related to it's VCA configuration.

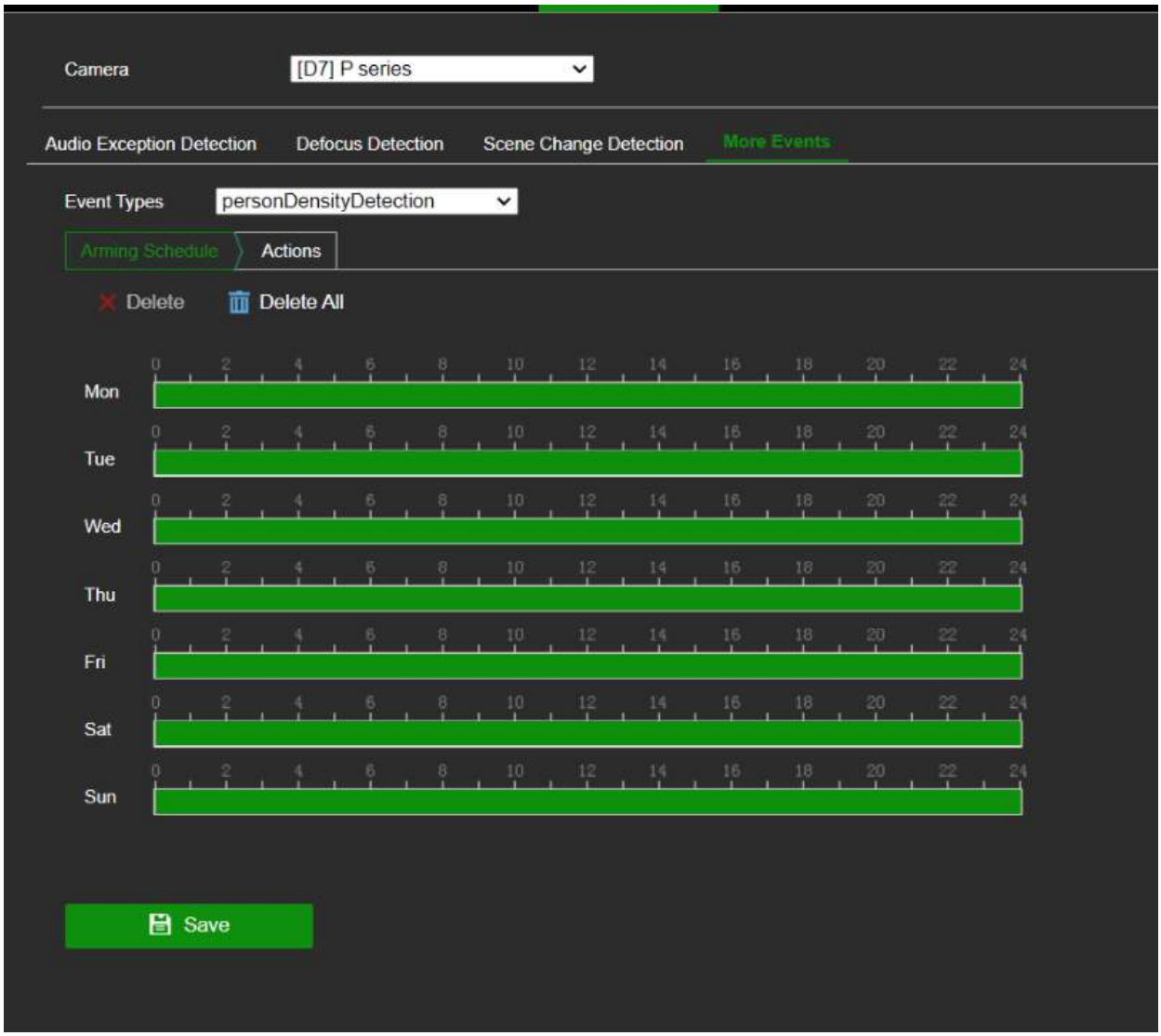
To use the Transparent Transmssion Configuration:

1. Setup the required VCA configuration and events in the camera webpage.
2. Login to the webpage of the TVN 23 (S/P) recorder.
3. Go to **Configuration > Event > More Events**.

   The table will show the extra evenst that can be reported from the camera to the recorder.
4. Go to **Configuration > Event > Smart Event**.
5. From the dropdown list select the camera that creates this extra event.

www.acornfiresecurity.com

www.acornfiresecurity.com



6. Select the extra event as Event Type from the dropdown menu.
7. You can now assign an arming schedule and actions for this event.
8. Click **Save** to save the settings.

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 from receiving unnecessary notifications (push notifications, emails, events in TruVision Navigator) or triggering actions (alarm output, PTZ preset, ...). See page 28 for details on how to disable the actions.

www.acornfiresecurity.com

www.acornfiresecurity.com

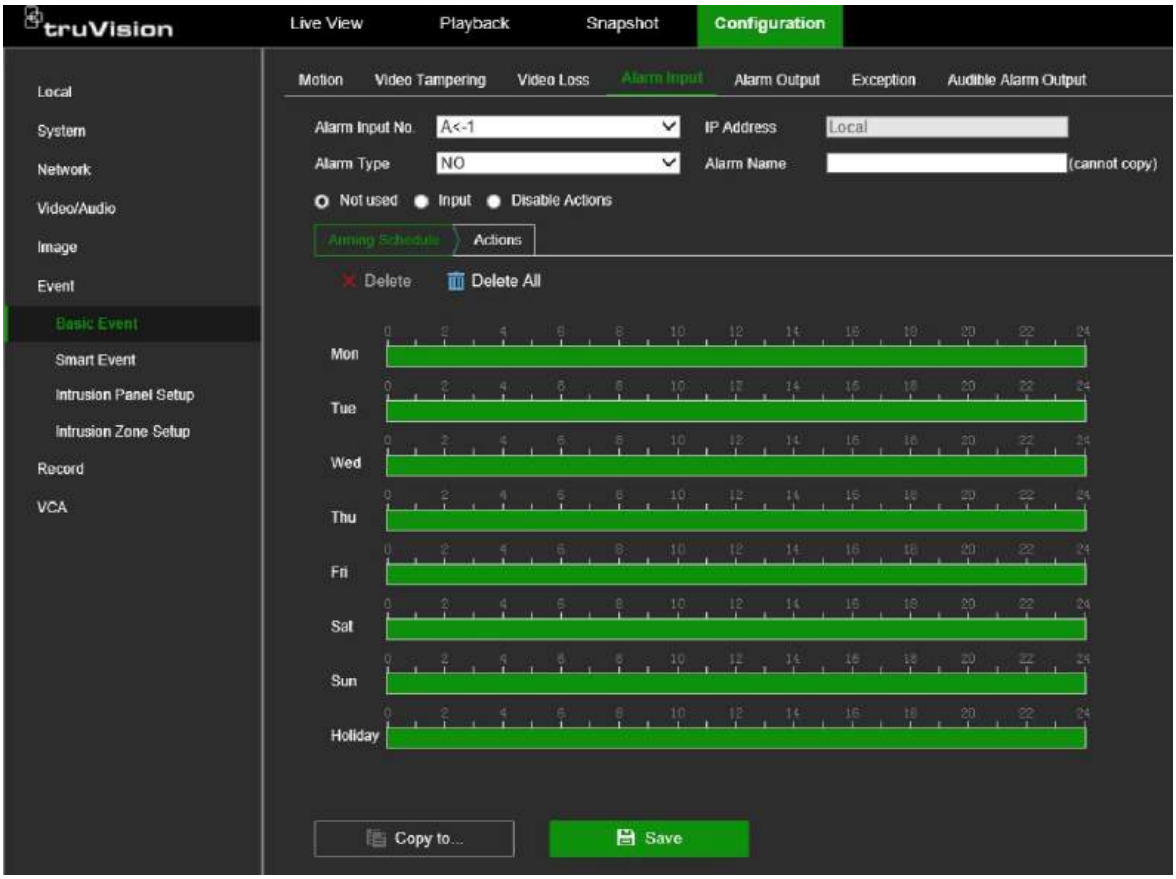
When the panel is armed again, the recorder will resume its scheduled operation and execute the configured actions and recordings.

The *Disable Actions* function can be used via Alarm Input 1 or the OH integration.

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

To set up Disable Actions via alarm input 1 in web mode:

1. Click **Configuration** > **Event** > **Basic Event** > **Alarm Input**.



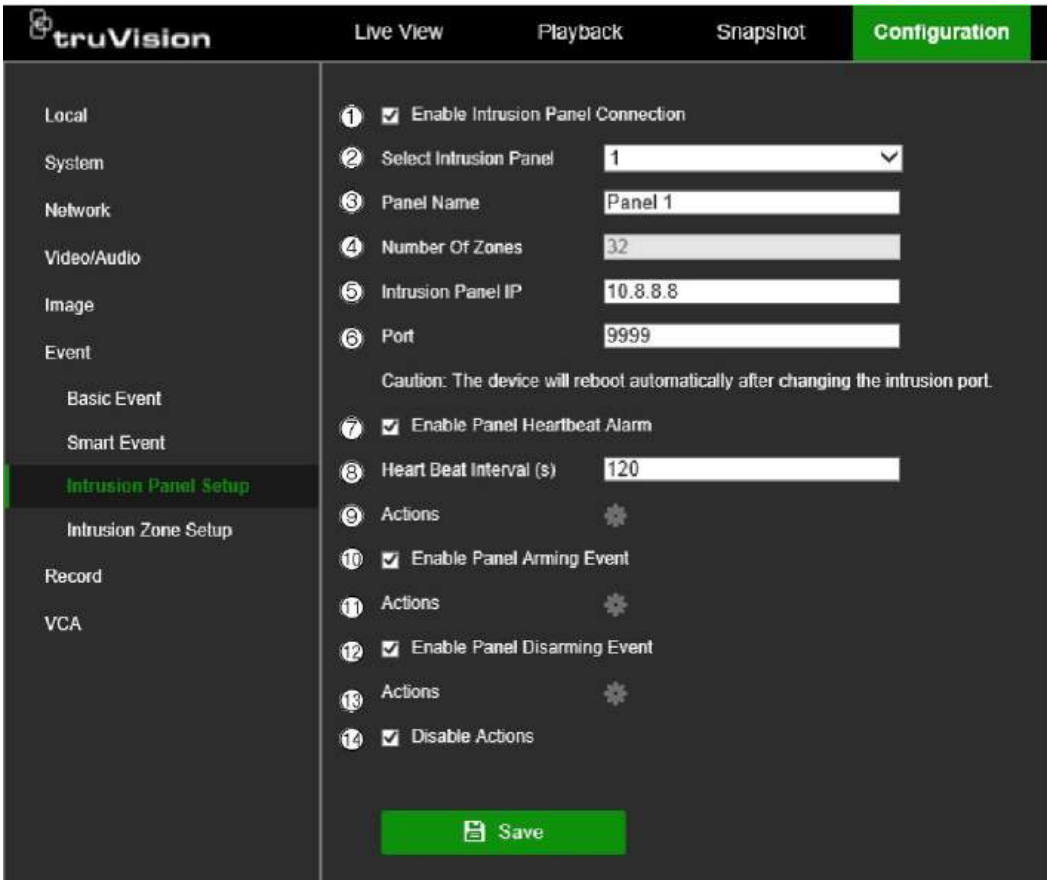
2. Select **Disable Actions** for alarm input 1. The Disable Actions function is only available for alarm input 1.
3. Make sure the alarm panel has a relay contact to connect it to the recorder. Connect one wire to alarm input 1 and connect the other wire to one of the Ground ('G') connections.
4. Select 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) in web mode:

1. Click **Configuration** > **Event** > **Intrusion Panel Setup**.

www.acornfiresecurity.com

www.acornfiresecurity.com



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 118 for further information.

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

   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 in web mode:

1. Click **Configuration** > **System** > **System Settings**.
2. Click the tab **Recording Behavior for Disable Actions**.
3. Select one of the options from the drop-down list. The options are:

   No influence on recording: Disable Actions will not influence the recordings. Recording of all cameras will continue as scheduled.

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

   Disable event/alarm recordings: Disable Actions will stop the scheduled recordings for events (motion, VCA) and alarms (alarm inputs, intrusion panel

www.acornfiresecurity.com

www.acornfiresecurity.com

alarms). Cameras that are scheduled for continuous recording will not stop the recording.

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

To set up Disable Actions via alarm input 1 in OSD mode:

1. Click **System**> **Event** > **Normal Event** > **Alarm Input**.
2. Under Operation, click the **Edit** button for the desired alarm input of a recorder/camera.
3. Select **Disable Actions** for the recorder alarm input 1. The Disable Actions function is only available for the recorder alarm input 1.
4. 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.
5. Select the alarm input type, NO (normally open) or NC (normally closed). Default is NO.
6. When the alarm input is triggered, the actions for motion detection and VCA event will be disabled.
7. Click **Apply** to save the changes.

Smart event

The configuration of each individual smart event that is available in a camera can be configured via the recorder. It is possible sometimes to fine tune the configuration in the camera webpage.

There are several types of smart events to select from. The type of smart events listed depends on what the camera supports. When a smart event is detected, a series of linkage methods can be triggered. See Table 4 below.

Note: Smart events use event recording settings.

Table 4: Smart types

Smart event types	Description
Face Detection	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 a narrow corridor.
Audio Exception Detection	Audio exception detection detects the loss of sound as well as the sudden increase or decrease of sound that is above a selected threshold.

www.acornfiresecurity.com

www.acornfiresecurity.com

Smart event types	Description
Cross Line Detection	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. Unidirectional is crossing the line from left to right or from right to left. Bidirectional is crossing the line from both directions. This event can be used to detect people or vehicles when this function is supported by TruVision cameras.
Intrusion Detection	You can set up an area in the surveillance scene to detect when an intrusion occurs. If someone enters the area, a set of alarm actions can be triggered. This event can be used to detect people or vehicles when this function is supported by TruVision cameras.
Vehicle Detection	Vehicle detection can be used with TruVision ANPR cameras and TruVision P Series IP PTZ cameras. Besides the capturing of the license plates, the function can also detect the vehicle brand, vehicle type and vehicle color. **Note:** The accuracy for vehicle brand and color is limited!!
Defocus Detection	The camera can detect image blur caused by defocusing the lens, triggering a series of alarm actions. 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 the current image.
Scene Change	You can configure the camera to trigger an alarm when the camera detects a change in the scene caused by a physical repositioning of the camera.
Enter Region Detection	This function detects people, vehicles, or other objects that enter a designated region from outside the designated region.
Exit Region Detection	Region exiting detection function detects people, vehicles or other objects that exit from a designated region, and certain actions can be configured to occur when the alarm is triggered.
Object Left Behind Detection	Unattended baggage detection function detects the objects left in the designated region such as baggage, a purse, dangerous materials, etc.
Object Removed Detection	Object removal detection function detects objects removed from a designated region, such as exhibits on display.
Fire Detection	This event type detects a fire source. Its schedule and actions are set up in the recorder. It is only available via the web browser. **IMPORTANT NOTICE**: This fire detection feature is not a substitute for a certified fire detection system.
Temperature Difference Alarm	This event option is currently not supported by the thermal camera. This event type triggers an alarm when the temperature difference between two regions exceeds the defined temperature threshold value. Its schedule and actions are set up in the recorder. It is only available via the web browser.
Temperature Alarm	This event type triggers an alarm when the temperature exceeds the defined temperature threshold value. Its schedule and actions are set up in the recorder. It is only available via the web browser.

www.acornfiresecurity.com

www.acornfiresecurity.com

To set up Smart Event actions OSD mode:

1. Click **Smart Analysis** > **Smart Event Settings**
2. Select a smart event type: facial recognition (for face detection), perimeter protection (for cross line and intrusion detection), vehicle detection or other events (such as object left behind, object removed and sudden scene changes).

   The events that can be selected depend on the used camera models.

3. Select the desired camera to set up a smart event.

   If supported, open the Area Settings tab and setup the desired detection area for the selected event.

4. Select the schedules for the smart event and the linked actions.

   Click the **Arming Schedule** tab and select the day of the week and the periods during the day when the event can be triggered. You can schedule up to eight time periods in a day. Default is 24 hours.

   Note: The periods defined cannot overlap.

5. Select the response method by which you want the recorder to notify you of the Smart event.

   Click the **Linkage Action** tab and select the desired options. More than one option can be selected.

   Normal Linkage: This applies to the recorder. It is the alarm notifications that the recorder can send. The options are: Buzzer, Full Screen Monitoring, Notify Surveillance Center and Send Email. More than one option can be selected.

   Trigger Alarm Output: The recorder alarm outputs are shown as Local → x (x = the number of the recorder relay output). The event can also trigger an output of a connected IP camera. In that case the IP address is shown followed by “-1”. More than one option can be selected.

   Trigger Channel: This applies to the cameras connected to the recorder. A message is sent to the selected camera to start recording. More than one camera can be selected.

   PTZ Linkage: Select the PTZ camera as well as the preset, preset tour, or shadow tour that is triggered when the alarm/event is detected.

   Audio and Light Alarm Linkage: Only for supported cameras. This action lets you hear a pre-recorded audio message and see a flashing white LED.

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

To set up Smart Event actions in web mode:

1. Click **Configuration > Event > Smart Event**
2. Select the desired camera to set up the smart event.

   The Smart types available are displayed as tabs. The list depends on what is supported by the camera.

www.acornfiresecurity.com

www.acornfiresecurity.com

3. If supported, open the **Area Settings** tab and setup the desired detection area for the selected event.
4. Click the **Arming Schedule** tab and select the day of the week and the periods during the day when the event can be triggered. You can schedule up to eight time periods in a day. Default is 24 hours.

   Note: The periods defined cannot overlap.
5. Select the response method by which you want the recorder to notify you of the Smart event.
6. Click the **Actions tab** and select the desired options. More than one option can be selected.

   Normal Linkage: This applies to the recorder. It is the alarm notifications that the recorder can send. The options are: Audible Warning, Send Email, Notify Surveillance Center, and Full Screen Monitoring. More than one option can be selected.

   Trigger Alarm Output: The recorder alarm outputs are showna s Local → x (x = the number of the recorder relay output). The event can also trigger an output of a connected IP camera. In that case a D is shown followed by “-1”. More than one option can be selected.

   Audio and Light Alarm Linkage: Only for supported cameras. This action lets you hear a pre-recorded audio message and see a flashing white LED.

   Trigger Recording: This applies to the cameras connected to the recorder. A message is sent to the selected camera to start recording. More than one camera can be selected.

   PTZ Linkage: Select the PTZ camera as well as the preset, preset tour, or shadow tour that is triggered when the alarm/event is detected.
7. Click **Save** to save the changes.

Smart report (OSD only)

The smart report features gies the possibility to create people counting report or heat map report.

People counting

People counting calculates the number of people entering or leaving a certain configured area and creates daily/weekly/monthly/annual reports for analysis.

Note: the function must be supported by the connected IP camera and the corresponding parameters must be set.

www.acornfiresecurity.com

www.acornfiresecurity.com

To see the report:

1. Go to **File Management > Smart Report > People Counting**.
2. Select a people counting camera.
3. Select the report type.
4. Set Date to analyze.
5. **Optional:** Click Export to export the report in Microsoft Excel format.

Heat map

A heat map is a graphical representation of data. The heat map function is used to analyze how many people visited and stayed in a specific area.

Note: the function must be supported by the connected IP camera and the corresponding parameters must be set.

To see the heat map.

1. Go to **File Management > Smart Report > Heat Map**.
2. Select a camera.
3. Select the report type.
4. Set Date to analyze.
5. Click **Counting**.
6. You will see the vidoe image with a colroed overlay.

   A red color block (255, 0, 0) indicates the most trafficked area, and blue color block (0, 0, 255) indicates the less-popular area.
7. **Optional**: Click **Export** to export the statistics report in Microsoft Excel format.

The vehicle detection function lets you configure the ANPR (license plate) detection for TruVision IP ANPR cameras.

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.

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.

Vehicle Detection Configuration

Use this function to define the area on the screen where the license plate shall be captured.

www.acornfiresecurity.com

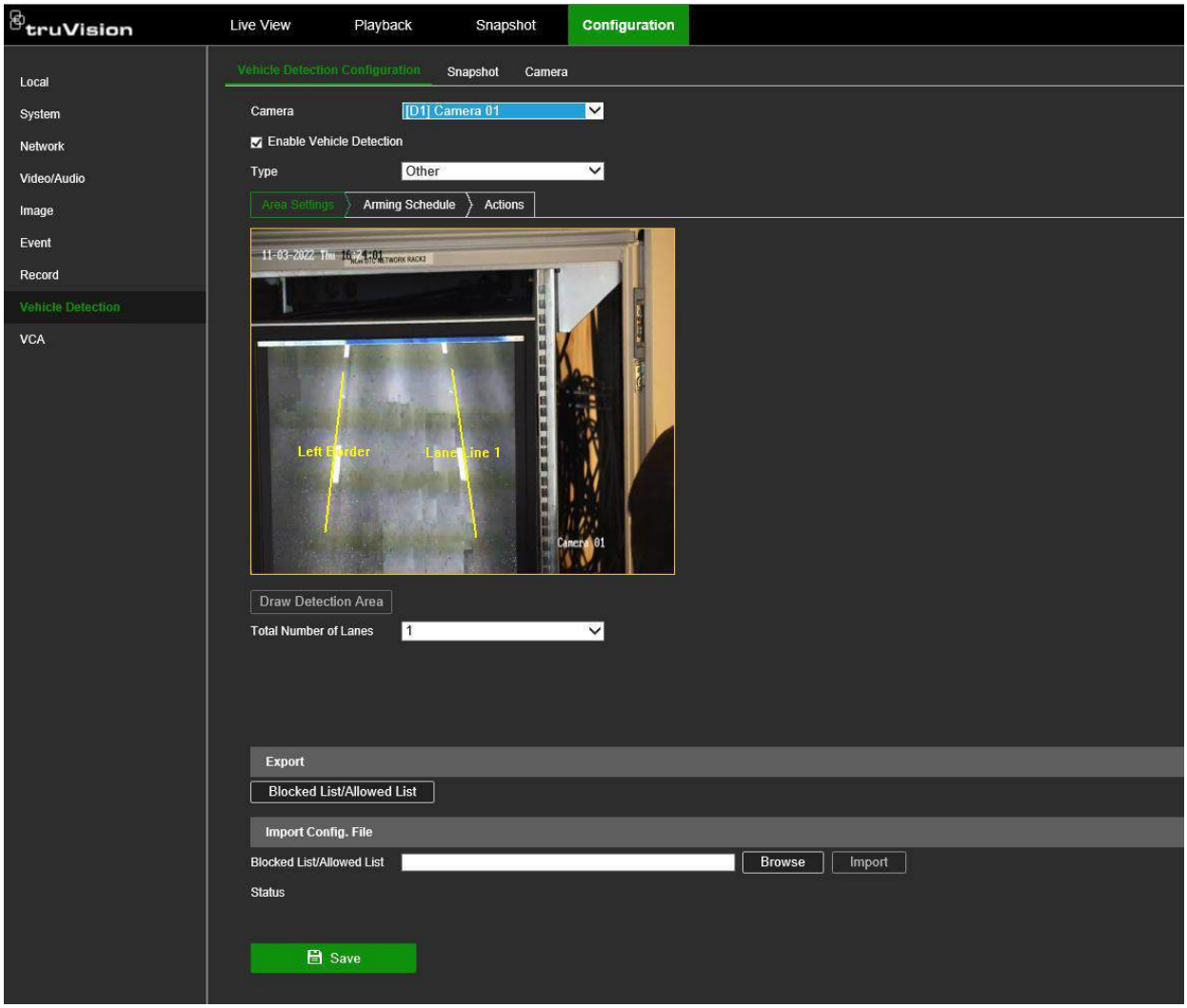
www.acornfiresecurity.com

To set up the detection area in web mode:

1. Click **Configuration > Vehicle Detection > Vehicle Detection Configuration**.
2. Select the desired ANPR camera from the camera drop-down list.
3. Select the **Enable Vehicle Detection** checkbox to enable license plate capture.
4. Select the Area Setup tab to set up the detection area.

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

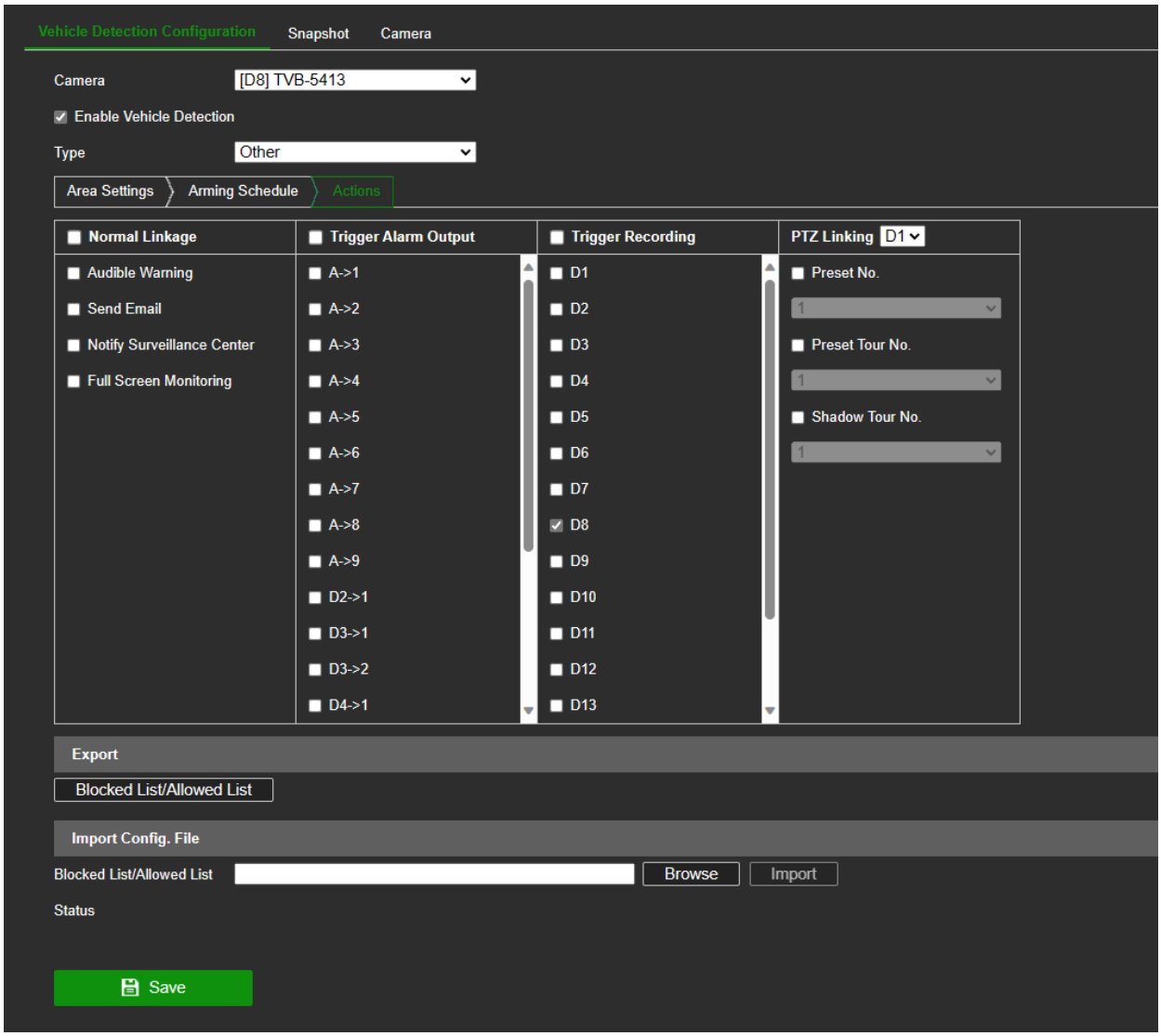
   Click the **Draw Detection Area** button to set up the lanes. Select the desired detection area on the image. Using the mouse, click and drag the yellow lane line to set the area.



5. Select the *Arming Schedule* tab to set up the arming schedule and linking action for the Allowed list, Blocked list, and Other list.

www.acornfiresecurity.com

www.acornfiresecurity.com



Under **Type**, select the license plates group: Allowed List, Blocked 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. To delete periods, click **Delete** or **Delete All**.

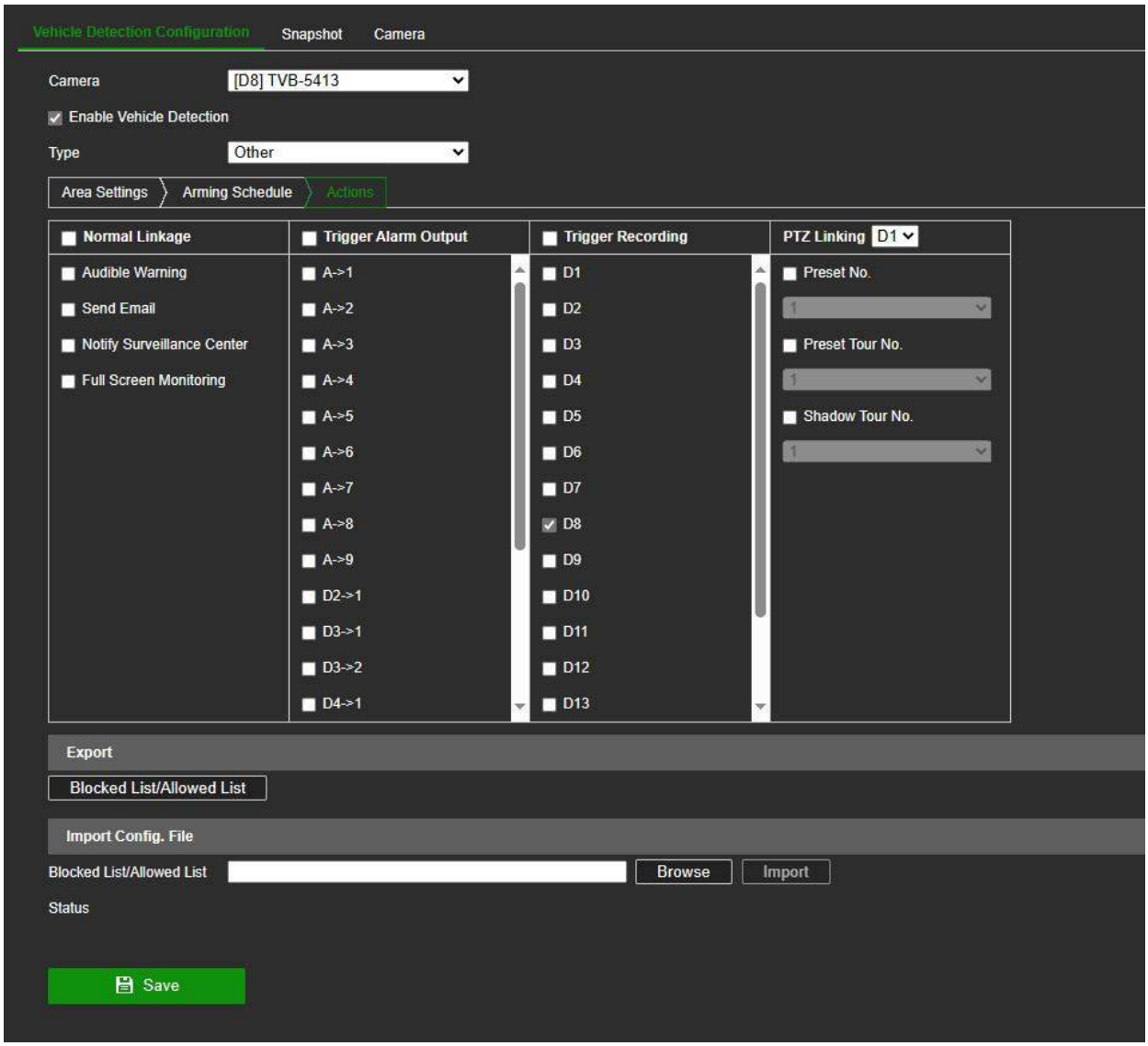
Note: The periods defined for a day cannot overlap.

6. To set up the linkage method when an event occurs:

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

www.acornfiresecurity.com

www.acornfiresecurity.com



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

Normal Linkage	Select the alarm linking method. Select the method by which you want the recorder to notify you of the alarm: Audible Warning, Send Email, Notify Surveillance Center, or Full-Screen Monitoring
Trigger Alarm Output	Select the alarm outputs to be triggered. Set the external alarm outputs to be triggered when an event occurs.
Trigger Recording	Set the channels to be recorded when an event occurs.
PTZ Linking	Select the PTZ linking to be triggered. Select the PTZ camera for linking and select the preset, preset tour, and/or shadow tour to be triggered when the alarm is detected. Enable the preset, preset tour, and/or shadow tour.

7. Click **Save** to save changes

www.acornfiresecurity.com

www.acornfiresecurity.com

To set up the detection area in OSD mode:

1. Click **Smart Analysis > Smart Event Settings > Vehicle Detection**
2. Select the desired ANPR camera from the camera drop-down list.
3. Enable **Vehicle Detection**.
4. **Optional:** Check **Save VCA Picture** to save the captured vehicle detection pictures.
5. Configure rules, including Area Settings, Snapshot, Overlay Content, and Blocklist and Allowlist.

   Area Settings

   Up to 4 lanes are selectable.

   Blocklist and Allowlist

   You can export the file first to see its format and edit it and import it to the device.
6. Click **Apply** to save the settings.
7. Set the Linkage Action and Arming Schedule.

Blocked and Allowed lists

You can store a list of blocked and allowed entries on the recorder to match against when automatically analyzing the captured numbered plates. By default, a list of a maximum of 2,048 license plates can be loaded into the recorder. See Table 5 below for the description of the list types.

Table 5: Description of Blocked list, Allowed list, and Other

Blocked list	These are license plates marked in the list as restricted vehicles.
Allowed list	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 blocked/allowed license plates, you can export the template to create one. It can then be imported back into the recorder. It is one single list in which you mark your license plate as allowed or blocked list. 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, there should be no spaces between the letters and numbers. For example, if the actual license number plate is “2-KDL-81”, in the list it should be written as “2KDL81”. See Figure 10 below. When entering 0 in column C, the license plate will be marked as blocked listed. Entering 1 in column C marks the license plate as an allowed list.

www.acornfiresecurity.com

www.acornfiresecurity.com

Figure 10: Example of blocked/allowed list template

	A	B	C	D
1	No	Plate Num	Group(0 Blocklist, 1 Allowlist)	
2	0	2KDL81	0	
3	1	1ABC003	1	
4	2	MG5387	1	
5	3	ELMN321	0	
6	4	RT123H	0	
7	5	E03SXT	1	
8	6	2BFV096	1	
9				

To import blocked and allowed lists from a PC to the recorder:

1. From the menu toolbar, click **Configuration** > **Vehicle Detection** > **Area Settings**. Under *Import Config file*, 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 blocked/allowed list file to upload to the recorder; either use the existing name (Default) or give it a new name (Custom).

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

To export blocked and allowed lists from the recorder to the PC:

1. From the menu toolbar, click **Configuration** > **Vehicle Detection** > **Area Settings**. Under Export, click **Blocked/Allowed list** and enter where you want to export the file.

IMPORTANT NOTE: The file needs to be edited or created with Office 2010, Office 2013, or Office 2016Pro and saved as Excel 97-2003.

Snapshots

Select the ANPR camera from the camera list to set up the snapshot parameters.

You can define the snapshot quality (in %) or the snapshot size.

- Snapshot quality: It is recommended to set the snapshot quality to less than 50% to avoid the snapshot size will be greater than 1024 kB (this is the maximum size for a snapshot in the TVN 243 (S/P)). When the quality setting is greater than 50%, the size of the snapshot size will be greater than 1024 kB so snapshots will not be stored by the recorder. The size of a snapshot is defined by the content.

  Recommended setting for snapshot quality: less than 50%

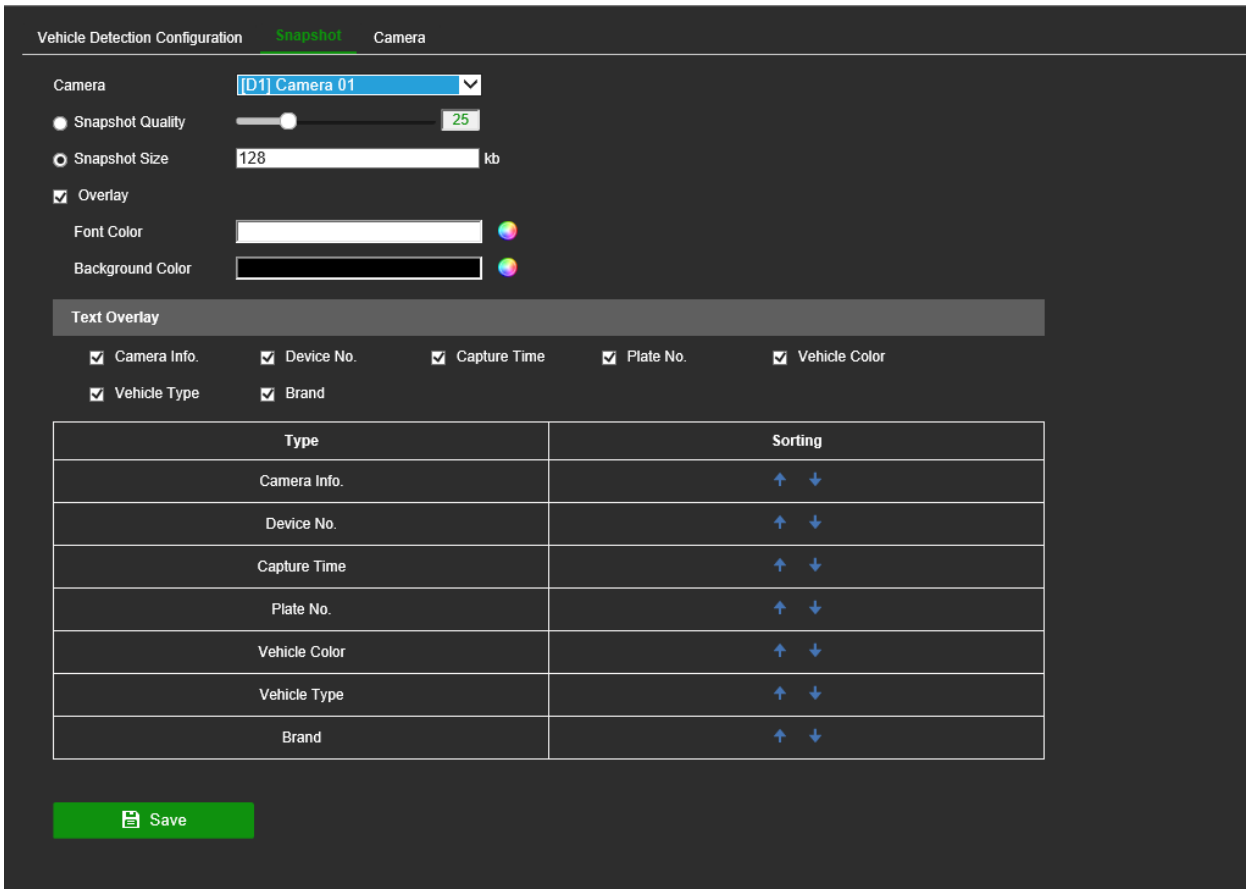
- Snapshot size: Enter the snapshot size between 64 kB and 512 kB. This value is only a reference value. This means that even if the size is set to 512 kB, the actual snapshot can still be higher (and even be around 1024 kB, the maximum size for a snapshot in the TVN 23 (S/P)).

  Recommended setting for snapshot-size: 512 kB

www.acornfiresecurity.com

www.acornfiresecurity.com

The text overlay appears at the bottom of the license plate snapshots. You can configure fields such as *Device No.*, *Camera Info,* and more to be displayed in the snapshot overlay.



To set up vehicle detection snapshots and text overlay:

1. From the menu toolbar, click **Configuration** > **Vehicle Detection** > **Snapshot**.
2. Select the desired ANPR camera from the camera drop-down list.
3. Drag the bar to select the desired image quality.

   - Or -

   Enter the desired snapshot size (in kB).
4. Select the **Overlay** check box to enable the function.
5. Select the color of the font and background.
6. Select the desired text overlay options to display at the bottom of the stored snapshots: Camera Info, Device No., Capture Time, Plate No., Vehicle Color, Vehicle Type, and Vehicle Brand. The fields can be sorted using the blue up/down arrows in column **Sorting**.
7. Click **Save** to save changes.

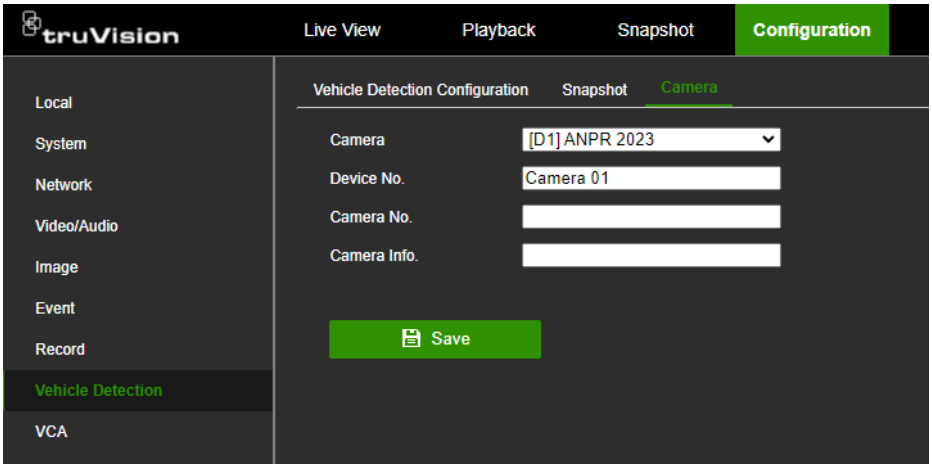
www.acornfiresecurity.com

www.acornfiresecurity.com

Camera information

Use this menu to select additional information to be included only in ANPR camera snapshots.

Enter information in these fields to appear in the text overlay of snapshots for ANPR cameras. See the menu **Vehicle** > **Snapshot** on page 136 to set up the text overlay.



Behavior analysis (web only)

The behavior analysis function lets you configure the cameras to detect specific behavior events. For each event type, you can define several parameters such as the event rules, arming schedule, the alarm response method, the shield region and how to display the VCA event.

This function is only available in web mode.

Behavior analysis is currently only supported by the new TruVision thermal cameras (TVTH-S01 cameras).

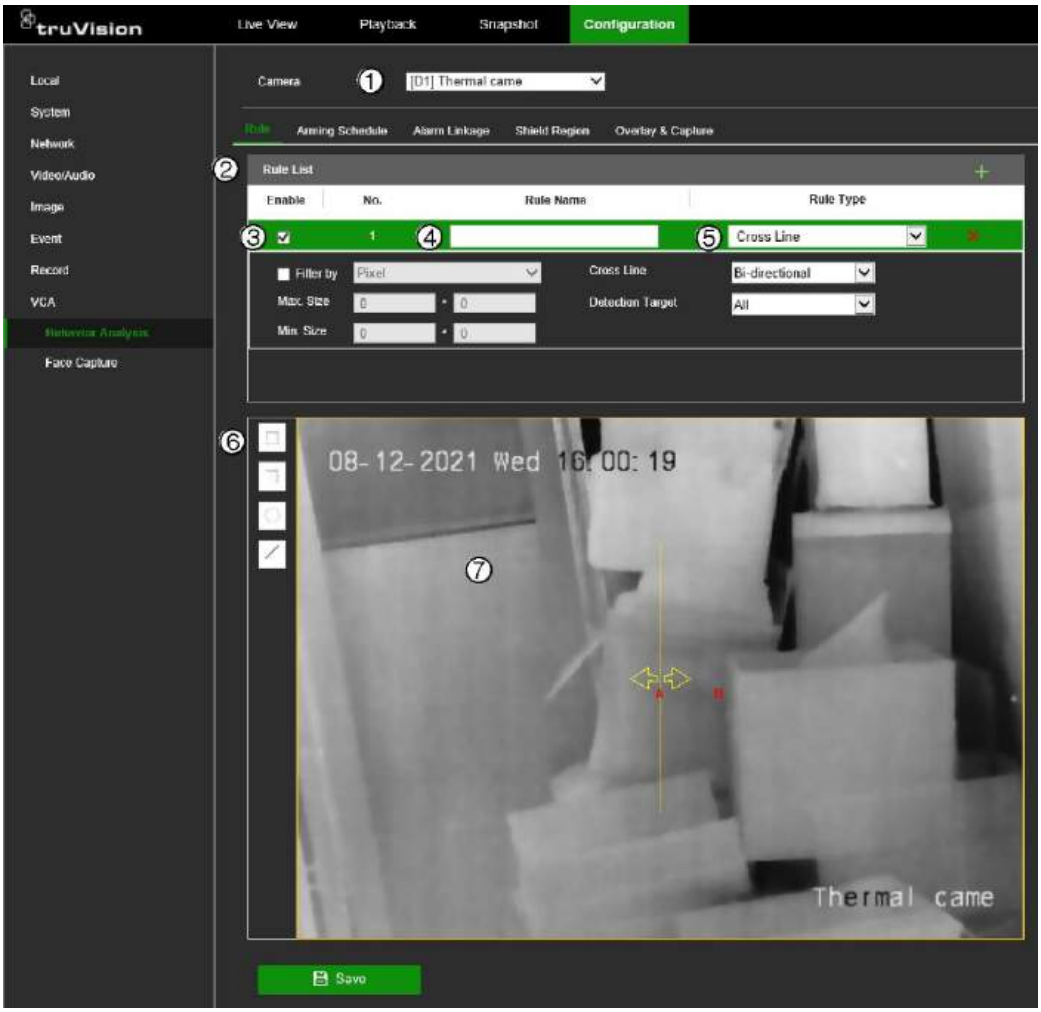
Behavior analysis rules for thermal cameras

Use the **VCA** > **Behavior Analysis** > **Rule** menu to set up the rule parameters for behavior analysis. See Figure 11 below.

www.acornfiresecurity.com

www.acornfiresecurity.com

Figure 11: Description of the rule menu (Cross line behavior type shown)

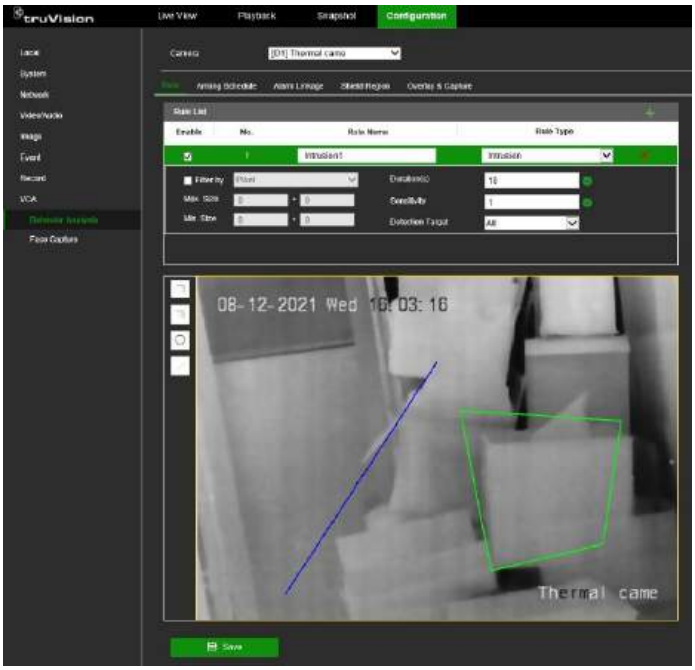


Item	Description
1. Camera	Select the desired camera. The camera must support the behavior analysis function.
2. Rule list	You can create up to eight rules for a camera. Click ➕ to add a new rule. Click ✕ to delete a rule.
3. Enable a rule	Select the check box ☑ of a rule to enable it.
4. Name of the behavior type	Enter the name of the rule.
5. Behavior type	Select one of the four behavior types for the rule from the drop-down menu: Cross Line, Intrusion, Region Entrance, or Region Exiting. Depending on the behavior type selected, the list of parameters that can be modified is displayed.
6. Draw the detection area in the viewer.	
⁄	**Cross line**: An alarm is triggered when a person and/or vehicle crosses the line. Click this button to draw the detection line and then click **Save**. The yellow arrow on the line shows the entry direction. Change the detection direction, if needed, by selecting one of the options from the *Cross Line* parameter drop-down list.

www.acornfiresecurity.com

www.acornfiresecurity.com

Item	Description
	Intrusion: An alarm is triggered when a person and/or vehicle stays in the detection area beyond the set time (blue area). Click this button to draw the intrusion detection area. **Region entrance:** An alarm will be triggered when a person and/or vehicle enters the detection area. Click this button to draw the intrusion detection area. **Region exiting:** An alarm will be triggered when a person and/or vehicle leaves the detection area. Click this button to draw the intrusion detection area. **Note**: You can only have one behavior type per rule.
	Maximum and minimum detection sizes: When you have selected intrusion, region entrance, or region exiting as the behavior type, you can define the maximum and minimum sizes of the object to be detected. Click each icon and draw the minimum and maximum size of the area that can be detected. Only objects that fall within these limits will be detected.
7. Viewer	The behavior type detection areas of all rules created are displayed here. The Intrusion/Region Entrance/Region Exiting polygon area of the selected rule is green. A Cross Line is yellow. The detection area polygons/lines of unselected rules are blue. See the figure below. The green selected detection area shown is for an intrusion rule. The behavior type polygon/line of the selected rule can be modified. You can also draw a new area in the viewer and the old behavior type is deleted when the change is saved.



You need to set up how the behavior analysis as well as the arming schedule and linking methods for the alarm actions.

To set up the behavior rules:

1. Click **Configuration** > **VCA** > **Behavior Analysis** > **Rule**.

www.acornfiresecurity.com

www.acornfiresecurity.com

2. Select the desired camera.
3. Click ➕ to add a new rule. Click ✕ to delete a rule. Existing rules can also be changed.
4. Enter the name of the new rule or change the name of an existing rule.
5. Select the desired behavior type from the drop-down list. Change the parameters shown below, if required.
6. Draw the detection area in the viewer. See Figure 11 on page 139 for more information. Click **Save** to save changes.
7. Set up the arming schedule:
   a) Click the *Arming Schedule* tab. If there is more than one rule, select the desired rule. The arming schedule of each rule must be set up separately.
   b) Click the day you want to schedule. The Time pop-box appears. Enter the desired start and end times to detect motion and click **Save**.
   c) If you want to copy a day's schedule, move the mouse cursor to the end of the day where a green icon appears. A pop-dialog box appears. Select the desired days to which to copy the schedule and click **OK** to save the changes.
   d) Repeat steps a to c for each rule.
8. Set up the linking method to the behavior event alarm:

   Click the *Alarm Linkage* tab. select one or more response methods for the system when a motion detection alarm is triggered. More than one option can be selected.

   Normal Linkage: This applies to the recorder. It is the alarm notifications that the recorder can send. The options are: Audible Warning, Send Email, and Notify Surveillance Center. More than one option can be selected.

   Trigger Alarm Output: This applies to the cameras connected to the recorder. A message is sent to the selected camera to trigger an alarm contact. A message is sent to the selected camera to trigger an alarm contact. The options are A -> 1 (this is the relay output of the recorder), and the channel numbers of the cameras that have an output contact and are connected to the recorder. More than one option can be selected.

   Trigger Recording: This applies to the cameras connected to the recorder. A message is sent to the selected camera to start recording. More than one camera can be selected.
9. Click **Save** to save changes.

Shield regions for thermal cameras

You can mask small areas on the camera image so that they cannot be counted. Live view does not display the various counting/detection boxes on screen. If, for example, a camera is mounted on a high ceiling and views a few entrances, but you only want the behavioral analysis carried out on one of the entrances, you can draw a shield area

www.acornfiresecurity.com

www.acornfiresecurity.com

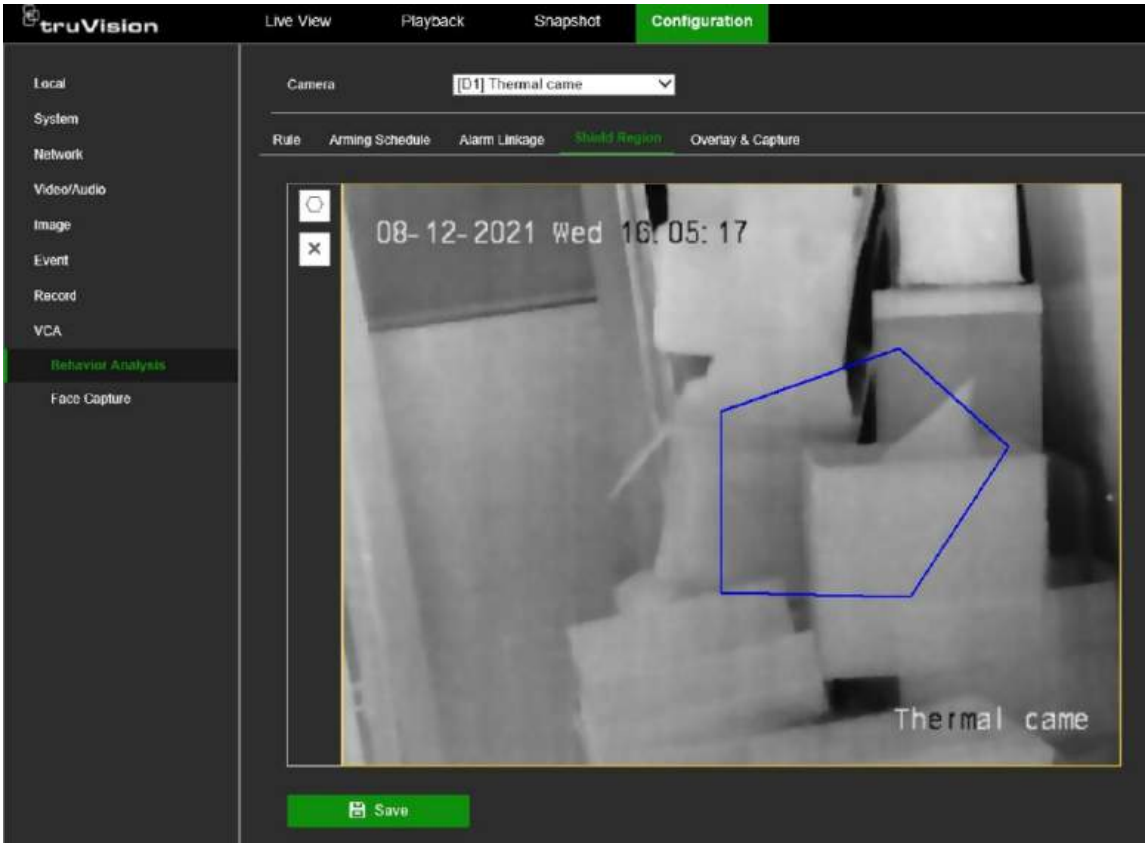
over the other entrances on screen to prevent them being included in the analysis. You can draw up to four shield regions.

This function is only available in web mode.

To set up shield regions:

1. Set up the behavioral analysis rules (see “Behavior analysis rules for thermal cameras” on page 138 for instructions).
2. Click **Configuration** > **VCA** > **Behavior Analysis** > **Shield Region**.

   All the rule areas set up are visible on screen in blue.



3. Click ⬡ and draw a polygon shield region on the desired area in the image. Click ✕ to delete all the shield regions.
4. Click **Save** to save changes.

Overlay and capture

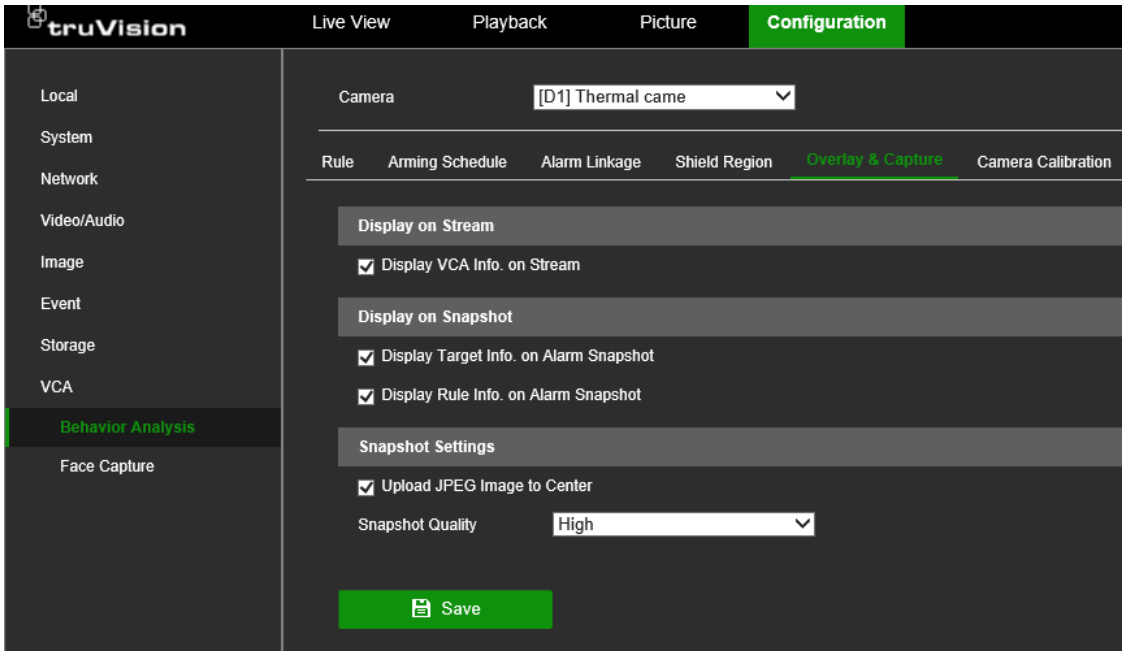
Use this menu to select how you want information displayed on the image as well as the snapshot settings for thermal cameras. You can also set the flow overlay settings.

In web mode, click **Configuration** > **VCA** > **Behavior Analysis** > **Overlay & Capture** and select the desired options. Click **Save** to save changes.

www.acornfiresecurity.com

www.acornfiresecurity.com

Figure 12: VCA Overlay & Capture window



	Item	Description
1.	Display VCA Info on Stream	Select **Display VCA Info on Stream** to display a green frame on the detected target in live and playback modes.
2.	Display on Snapshot	Select overlay target information and rule information on the alarm snapshot.
3.	Snapshot Settings	Select to upload a JPEG snapshot of the alarm event to the notification center. You can also select the quality of the snapshot to upload (high, medium, or low).

Face capture

The Face Capture function is only supported by the latest TruVision PTZ cameras (TVGP-M01 and TVGP-P01 cameras) and the TruVision P Series IP cameras.

This function is only available in web mode.

The Face Capture settings in the TVN 23 (S/P) are limited to setting up the rule and defining the recorder actions. For more detailed settings for this feature, please see the configuration manual of the PTZ camera.

To set up the basic settings for face capture in web mode:

1. Go to **Configuration** > **VCA** > **Face Capture**.
2. Select the PTZ camera that supports the face capture option in the camera drop-down list.
3. Click the **Face Capture** tab.
4. Under **Arming Schedule**, define the desired arming schedule for the actions.

www.acornfiresecurity.com

www.acornfiresecurity.com

5. Click the **Actions** tab to define which recorder actions need to be executed when a face is captured by the camera.

   Normal Linkage: This is a group selection. The options are Audible Warning, Send Email, Notify Surveillance Center, and Full Screen Monitoring. More than one option can be selected.

   Trigger Alarm Output: This applies to the cameras connected to the recorder. A message is sent to the selected camera to trigger an alarm contact. The options are Local -> 1 (this is the relay output of the recorder), and the IP addresses of cameras that have an output contact and are connected to the recorder. More than one option can be selected.

   Trigger Recording: This applies to the cameras connected to the recorder. A message is sent to the selected camera to trigger recording. More than one camera can be selected.

   PTZ Linking: This is the PTZ camera function required in response to an external alarm. Select the PTZ camera under PTZ Linking. Enter the preset, preset tour, or shadow tour that is triggered when the alarm is detected.

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

www.acornfiresecurity.com

www.acornfiresecurity.com

Chapter 11
Recording

This chapter describes how to schedule video recording, set up the camera recording settings, and set up holiday recording schedules.

Recording schedule for video recording

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 recording schedule.

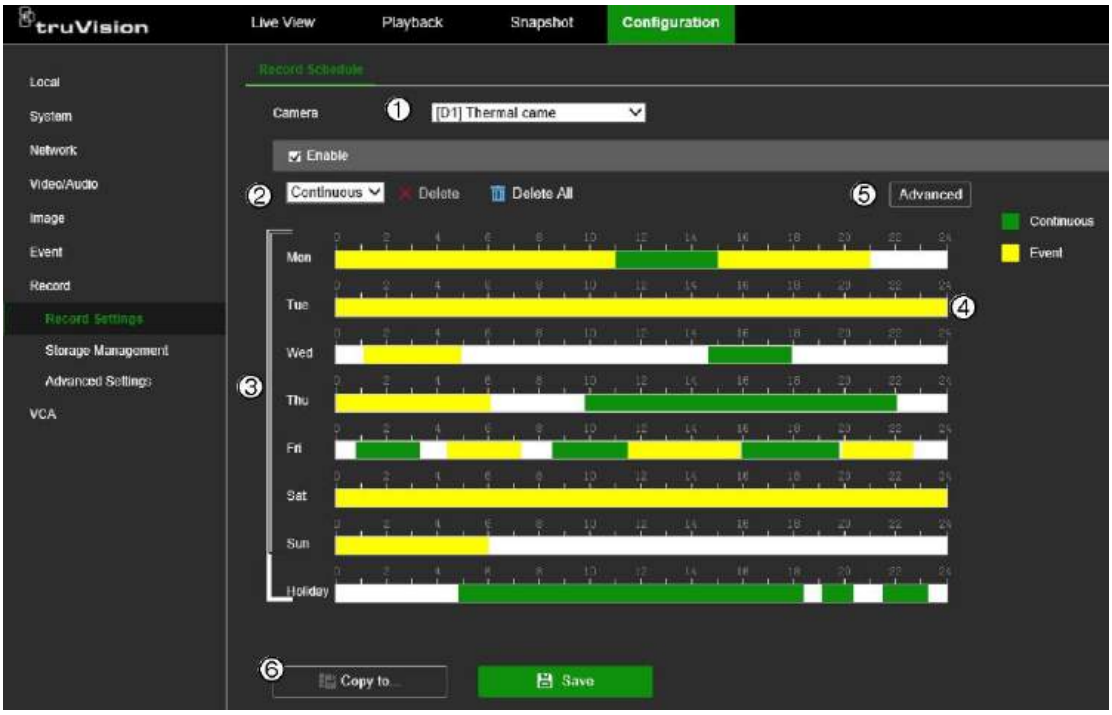
The schedules are visually presented on a map for easy reference. See Figure 13 on page 146 for a description of the recording schedule window.

Note: If a camera is set up for continuous recording, it will still switch to event recording if events are triggered.

www.acornfiresecurity.com

www.acornfiresecurity.com

Figure 13: Description of the recording schedule window in web mode



1. **IP camera**. Select a camera.
2. **Recording type**. There are two types of recording to select, which are color-coded:
   - Event (Yellow): Records all events (basic and smart, alarms, and VCA events).
   - Continuous (Green): Records continuous recording. By default, continuous recording is scheduled for 24 hours.
3. **Schedule map**. There are eight days to select: Sunday (Sun), Monday (Mon), Tuesday (Tue), Wednesday (Wed), Thursday (Thu), Friday (Fri), and Saturday (Sat), and Holiday (if enabled).
4. **Timeline**. There is a 24-hour timeline for each day. Up to eight recording periods can be scheduled during the 24-hour period.
5. **Advanced button.** Click to set extra recording settings such as recording audio, enabling EFR, pre- and post-recording times, stream type, and the number of days to keep videos/snapshots.
6. **Copy button.** Click to copy schedules between cameras.

To set up a recording schedule for video recording in web mode:

1. Click **Configuration** > **Record** > **Record Settings** > **Record Schedule**.
2. Select the camera.
3. Select the **Enable** check box to enable recording.
4. Set the recording schedule for the camera.

   To change a schedule, click the scheduled recording in the timeline for the desired day. In the pop-up box that appears, select whether you want to record continuous or event recording and enter the start and end times. Click **Save**.

Recording type	Description
Continuous	This is continuous recording.
Event	Video will be recorded when any event (basic event, smart event, and alarm input trigger) is triggered. Besides configuring the recording schedule, you must configure the settings for the respective events. See Chapter 10 “Event setup” on page 101.

www.acornfiresecurity.com

www.acornfiresecurity.com

To add another recording period to the timeline, in an area of the time with no scheduling drag the mouse to the desired end time. You can then click on this scheduled period and in the pop-up dialog box fine-tune the start and end times.

You can schedule up to eight periods in a day. Default is 24 hours for a day.

5. Click the **Advanced** button.

   Select the stream type to set the pre- and post-recording times as well as the stream type. These values apply to all recording schedules.

   Pre-record time: The pre-record time is set to start recording before the scheduled time or event. For example, if an alarm triggers a recording at 10:00, and the pre-record time is set to 5 seconds, the camera starts to record at 9:59:55. The pre-record time can be configured as No Pre-record or 5 s.

   Note: The five-second pre-event recording time cannot always be reached. It depends on the resolution, the bit rate setting, and the quality setting for the camera. The use of high-resolution cameras (>4MP), high bit rate settings, and high-quality settings may result is a shortened pre-event recording time.

   Post-record time: The post-record time is set to stop recording after the scheduled time or the event. For example, if an alarm-triggered recording ends at 11:00, and the post-record time is set to 5 seconds, the camera records until 11:00:05. The post-record time can be configured as 5 s, 10 s, 30 s, 1 min, 2 min, 5 min, or 10 min.

   Stream type: You can select to record main stream, substream, or Dual Stream.

   To record audio, select the **Record Audio** check box. Only applicable to cameras that support audio.

   To enable Edge Failover Recording (EFR), select the **Enable EFR** check box. Edge Failover Recording means that an SD card is used in the camera. When this feature is enabled, the camera will automatically detect a disconnection from the recorder and will record on the SD card (continuous recording). When the connection with the recorder is restored, the data will be automatically written from the SD card to the hard drive of the recorder.

   If you want that saved videos and snapshots to be automatically deleted after a certain number of days, enter the number of days in the **Keep Videos/Snapshots for … days(s)** field box. The default value is 30 days.

6. Set the recording types and periods for the other days of the week.

   If you want to copy a camera's schedule to other days, click at the end of the time bar of the desired day to copy the schedule. The *Copy to* pop-up window appears. Select the desired days to which to copy the schedule and click **OK** to save the changes.

7. Set the recording parameters for the other cameras.

   If you want to copy a camera's schedule to other cameras, click **Copy to,** and in the pop-up dialog box, select the cameras and then click **OK**.

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

www.acornfiresecurity.com

www.acornfiresecurity.com

To set up a recording schedule for video recording in OSD mode:

1. Click **Storage** > **Schedule** > **Record.**
2. Select the camera to set up the recording.
3. Select the **Enable Schedule** check box to enable recording.
4. Set the recording schedule for the camera.

   Click **Edit** and in the pop-up menu select the day of the week and the type of recording required.

Recording type	Description
Continuous	This is continuous recording.
Event	Video will be recorded when any event or alarm is triggered. Besides configuring the recording schedule, you must configure the settings for the events/alarms. See Chapter 10 “Event setup” on page 101.

   Enter the start and ends times for each period during the day. Up to eight periods can be entered per day. Periods cannot overlap. Set the required periods for each day. You can also copy the settings to one or more other days. Click **Copy** and select the day(s) and click **OK**.

   If you want to copy a camera’s schedule to other cameras, click **Copy to,** and in the pop-up dialog box, select the cameras.

   Click **OK** when completed.

5. Click the **Advanced** button.

   Set the pre- and post-recording times as well as the stream type. These values apply to all recording schedules for the camera.

   Pre-record time: The pre-record time is set to start recording before the scheduled time or event. For example, if an alarm triggers a recording at 10:00, and the pre-record time is set to 5 seconds, the camera starts to record at 9:59:55. The pre-record time can be configured as No Pre-record or 5 s.

   Note: The five-second pre-event recording time cannot always be reached. It depends on the resolution, the bit rate setting, and the quality setting for the camera. The use of high-resolution cameras (>4MP), high bit rate settings, and high-quality settings may result in a shortened pre-event recording time.

   Post-record time: The post-record time is set to stop recording after the scheduled time or the event. For example, if an alarm-triggered recording ends at 11:00, and the post-record time is set to 5 seconds, the camera records until 11:00:05. The post-record time can be configured as 30 s, 60 s, 120 s, 300 s, or 600 s.

   Stream type: You can select to record main stream, substream, or dual stream.

   To record audio, select the **Record Audio** check box.

   If you want that saved videos and snapshots to be automatically deleted after a certain number of days, enter the number of days in the **Video/Snapshot Expiry Time (day)** field box. The default value is 30 days.

www.acornfiresecurity.com

www.acornfiresecurity.com

Note: It is not possible to select **Enable EFR** in OSD mode.

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

Recording schedule for snapshot capturing

It is possible to define a specific recording schedule for storing snapshots in the recorder.

Snapshots can be recorded with a defined interval time or (extra) snapshots can be stored after a camera event was triggered.

About the snapshot creation:

The source for the creation of event snapshots depends on the type of event.

- A snapshot for motion detection can only be generated by the recorder. This will be done by setting up this recording schedule for snapshots.
- A snapshot for a smart event (VCA) can be generated by the camera if the “Save VCA Snapshot” feature is enabled for the event. If needed, extra snapshots can be saved by setting up a recording schedule for snapshots.

The recording schedule that you can define for snapshots can be for continuous capturing or for event capturing.

When continuous capturing is selected, the recorder will store snapshots for the selected camera based on the capture parameters for Continuous (OSD)/Time Sync (webpage).

When event capturing is selected, the recorder will store (extra) snapshots for the selected camera based on the capture parameters for Event (OSD)/Event Triggered (webpage).

You can also define a post capture time for event captured snapshots. This the time that snapshots are captured after the event trigger ended.

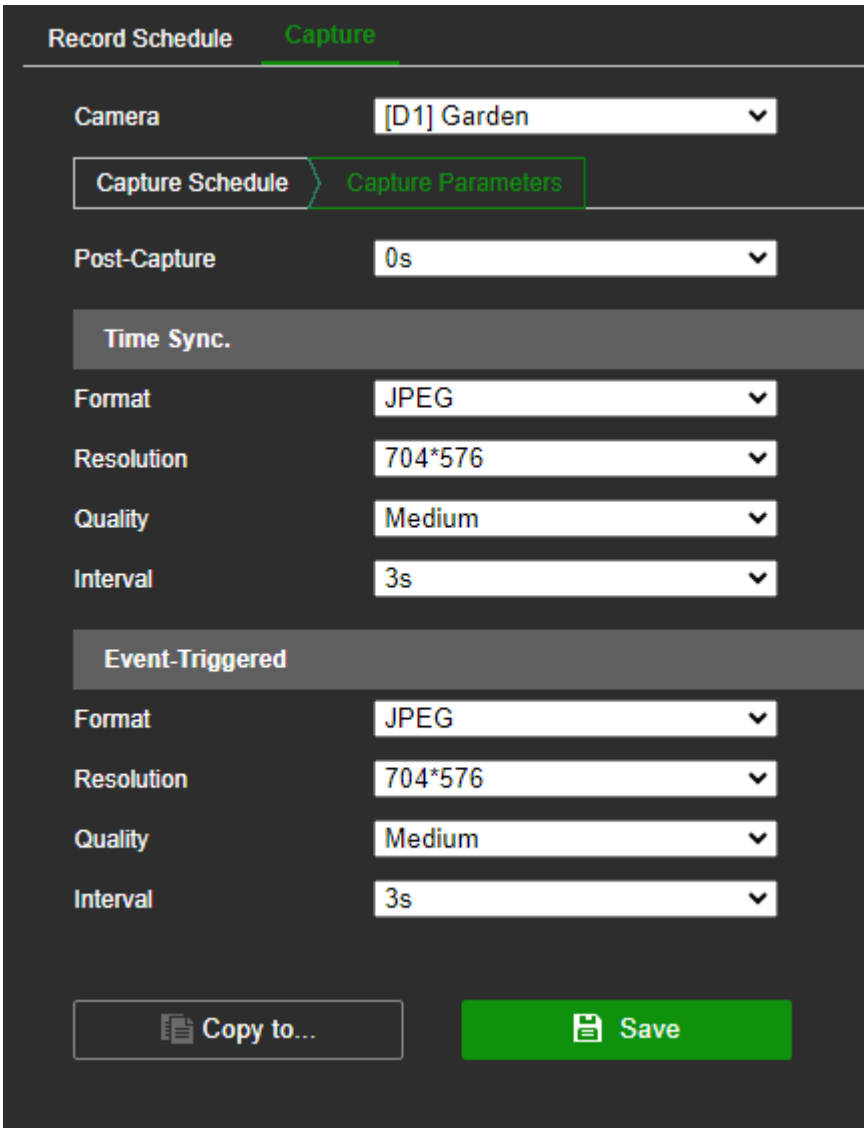
During this post capture time, the recorder will store as many snapshots as defined by the interval time.

To setup the snapshot storage via webpage

1. Go to **Configuration > Record > Record Settings > Capture**.
2. Selected the required camera from the dropdown list.
3. Open the tab **Capture Parameters.**

www.acornfiresecurity.com

www.acornfiresecurity.com



On this page, you can set the image parameters for the event triggered snapshots and or the time lapse (Time Sync) snapshots.

The post-capture time defines the time that snapshots are recorded after the event stopped.

Example:

Set Post-Capture to 30 seconds and interval to 3s. The recorder will store the snapshots every 3s for 30 seconds after the event.

The recorder will also store snapshots during the event with the selected interval.

4. In the Capture Schedule tab, you can define the schedule when the snapshots are recorded. Set the schedule to Event for capturing event triggered snapshots. Set the schedule to Continuous for the time lapse snapshots.
5. Click **Save** to save the settings.

www.acornfiresecurity.com

www.acornfiresecurity.com

To setup the capture parameters and schedule in the OSD:

1. Click **Storage > Schedule > Capture.**
2. Select the required camera from the dropdown list.
3. Click **Advanced** to see the details for the capture parameters and set them up accordingly.

   Note: The Post-Capture time is called ‘Capture Delay Time’ in the OSD.
4. Click **OK** to save the settings.
5. Click **Enable Schedule** and **Edit** to define the capture schedule per day.
6. Click **Apply** to save the settings.

The capture parameters and schedule settings are the same in the webpage and the OSD.

Search for snapshots

The search for snapshots is possible via the webpage and the OSD.

To search for stored snapshots via the OSD

In the OSD, you can search for snapshots by events, or you can search for snapshots captured by appearance.

Search by Events

1. Go to **File Management > Snapshot > Search by Event** for searching snapshots captured for events.
2. Select the required start/end date/time and the required camera channel.
3. As **Capture Type** select an event type that is used by the camera. (You see also event types in the list that are not supported by TruVision cameras.)
4. Click **Start Search** and the results will be shown.

Limitation: The snapshots stored for motion detection by the NVR, cannot be searched with event type set to ‘Motion’. They can only be shown when the event type is set to ‘All ’.

Search by Appearance

1. Go to **File Management > Snapshot by Appearance** for searching snapshot that were captured manually during live view or playback view (via OSD) or that were captured based on the configured schedule.
2. Select the required start/end date/time and the required camera channel.

www.acornfiresecurity.com

www.acornfiresecurity.com

3. As **Capture Type** select Scheduled Capture or Manual Capture.
4. Click **Start Search** and the results will be shown.

To search for stored snapshots via the webpage

1. Go to **Snapshot.**
2. Select the required camera from the dropdown list.
3. As File Type, the following options are possible.
    - **Continuous Schedule**: for the snapshots that were stored when the recording schedule for snapshot is setup for Continuous storage.
    - **Manual/Capture:** for manual captured snapshots via the OSD during live view.
    - **Event Schedule:** for the snapshots that were stored when the recording schedule for snapshot is setup for Event storage.
    - **Playback Capture:** for manual captured snapshots via the OSD during playback.
    - **Fire Source Detection:** used with thermal cameras.
    - **Temperature Measurement Alarm:** used with thermal cameras.
    - **Temperature Difference Alarm:** used with thermal cameras.
    - **Vehicle Detection:** for cameras that capture license plates when ‘Save VCA snapshot’ is enabled in the Vehicle Detection setup.
    - **All Types:** to search all snapshots.
4. Enter the required start/end date and time (and for vehicle detection a filter on country can be setup).
5. Click **Search** to show the recorded snapshots.

Limitation: The snapshots stored for motion detection by the NVR, cannot be searched with event type set to ‘Motion’. They can only be shown when the event type is set to ‘All Types’.

www.acornfiresecurity.com

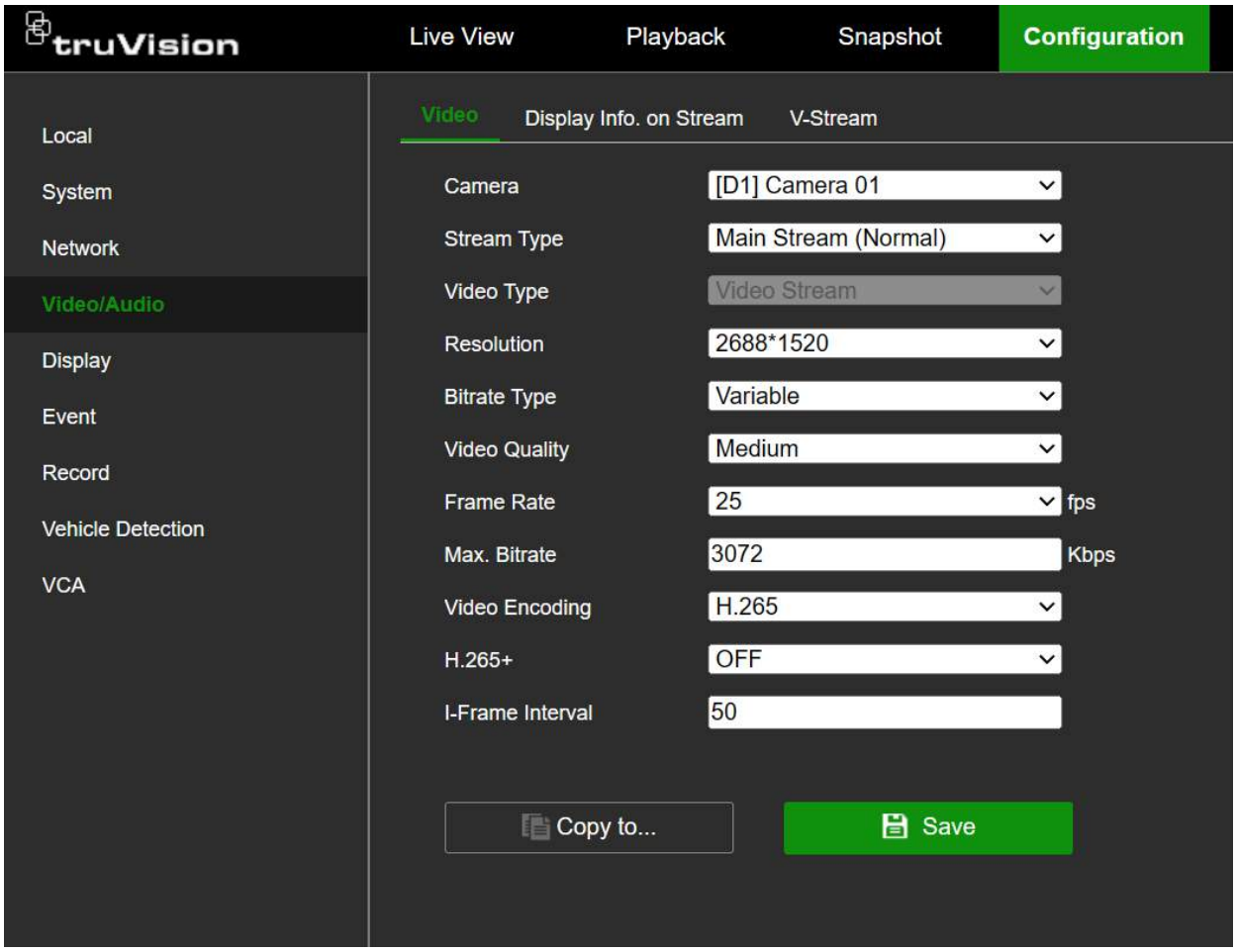
www.acornfiresecurity.com

Camera encoding settings

You can define the encoding settings for each camera.

To configure camera encoding settings in web mode:

1. Click **Configuration** > **Video/Audio** > **Video**.



2. Select the camera you want to configure.
3. Configure the following encoding settings (options available depend on the camera model):
   - **Stream Type**: Select the type of stream to record, Main Stream (Normal), Main Stream (Event), or Substream.
   - **Video Type**: Select whether to encode Video or Video & Audio. Default is Video.

     Note: The volume level of the audio is set in OSD mode.
   - **Resolution:** Select the resolution of the recording. The available resolutions depend on the camera model.
   - **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.

www.acornfiresecurity.com

www.acornfiresecurity.com

- **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. The options listed depend on the camera model.
- **Max. Bitrate (kbps)**: Enter the maximum bitrate value.
- **Video Encoding**: Select the desired video encoding standard. Depending on the camera model, you can select H264, H265, H.264+ orH265+ (via the Enable H.264+ or H.265+ switch).

  The available video encoding parameters depend on the camera model.
- **I-Frame interval:** the I-Frame or complete frame is a reference frame. An I-Frame contains all the information that of an image, captured by a camera.

  The value for the I-Frame interval is the interval in number of frames between two I-Frame captures.

  The lower the I-Frame interval, the higher the bit rate/bandwidth usage will be.

  Set the I-Frame interval to a low number (10-25) when the camera is used in a very busy environment.

  Set the I-Frame interval to a high number (75-100) when the camera is used in a quiet environment with little activity.

  The default value is 50 and is normally good for various situations.

  The I-Frame interval cannot be setup when a smart codec is used (H.264+ or H.265+).

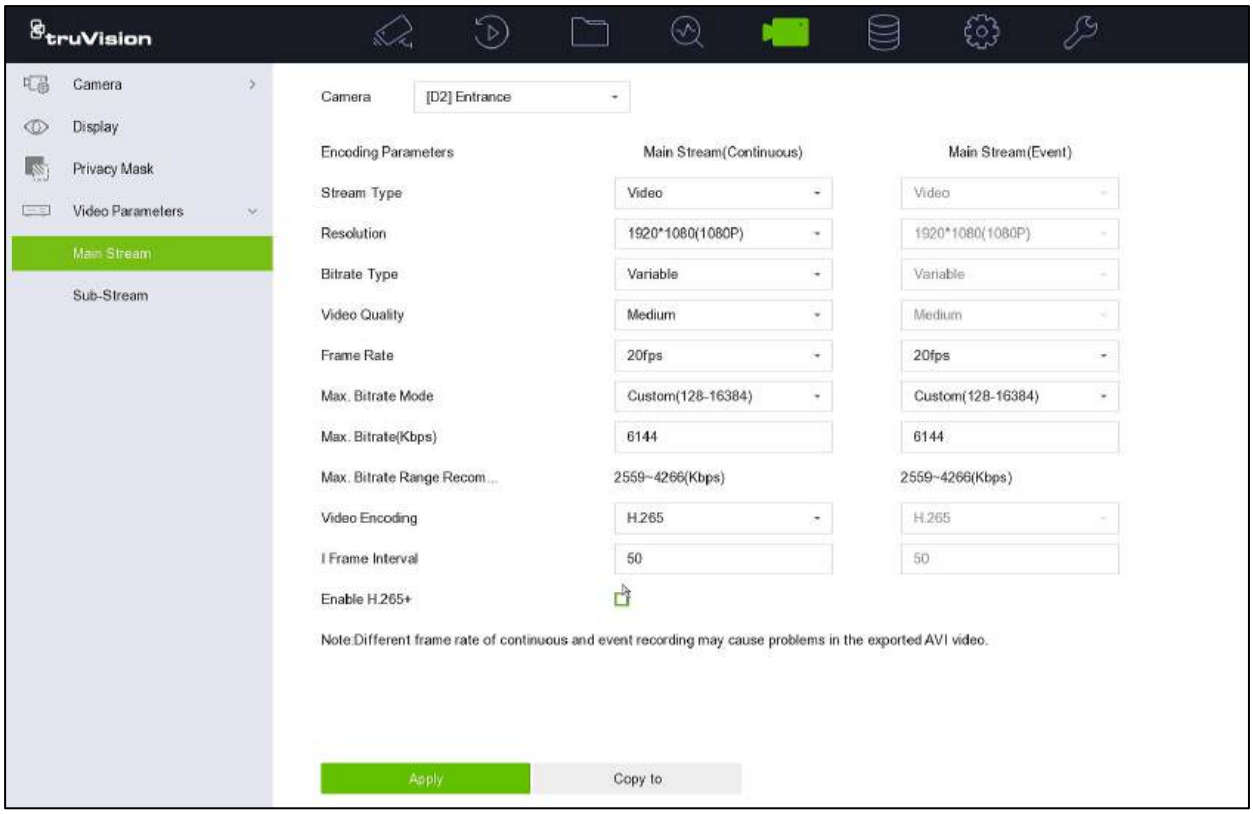
4. Click **Save** to save the settings.

To configure camera encoding settings in OSD mode:

1. Click **Camera** > **Video Parameters**

www.acornfiresecurity.com

www.acornfiresecurity.com



2. Select the camera you want to configure.
3. Select the stream type. Click the Main Stream or Substream tab.
4. Configure the following encoding settings (options available depend on the camera model). If main stream has been selected, you can select the parameters for both continuous and event recording.
   - **Stream Type**: Select the type of stream to record, either Video or Video & Audio. Default is Video.
   - **Resolution:** Select the recording resolution. The options listed depend on the camera model.
   - **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)**: Enter the maximum bitrate value.
   - **Video Encoding**: Select the desired video encoding standard. Depending on the camera model, you can select H264 or H265.

www.acornfiresecurity.com

www.acornfiresecurity.com

For H.264 or H.265, you can select **Enable H.264+ or H.265+**.

The support support of H.264+ and H.265+ depends on the TruVision camera.

- **I-Frame interval:** The value for the I-Frame interval is the interval in number of frames between two I-Frame captures. The default value is 50.

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

Holiday recording schedules

It is possible to create separate recording schedules for holiday periods. Once one or more holidays are created, a separate entry for a holiday will be included in the recording schedule. See Figure 13 on page 146 for further information.

Note: This function is not available in OSD mode.

To set up a holiday recording schedule in web mode:

1. Click **Configuration** > **Record** > **Advanced Settings** > **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.
4. Select whether the holiday period will be categorized by date, week, or month, and then enter the start and end dates. Click **OK**.
5. Click **OK** to return to the Edit window.
6. Repeat steps 2 to 5 for other holiday periods.
7. Click **Save** to save the settings.

www.acornfiresecurity.com

www.acornfiresecurity.com

Chapter 12
Storage management

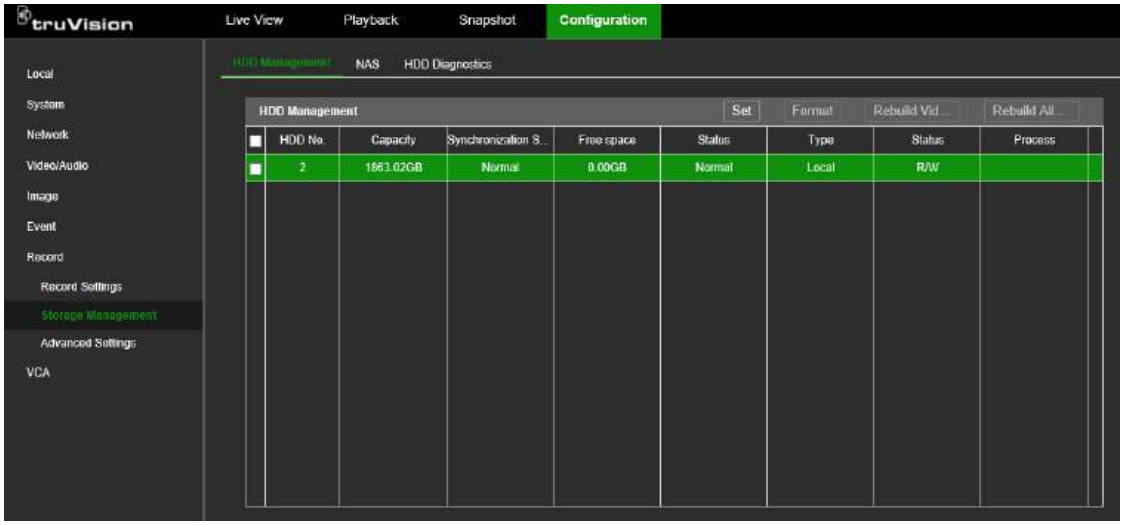
This chapter describes the management of hard drives and network storage systems as well as storing data.

Storage status information

You can check the status of any of the installed HDDs on the recorder at any time. The maximum number of HDDs that can be installed depends on the recorder model.

To check the storage status in web mode:

1. Click **Configuration** > **Record** > **Storage Management** > **HDD Management**.



2. Note the status of the HDDs and NAS listed under the Status column.

   If the status is listed as *Normal* or *Sleeping*, the HDD/NAS is in working order. If it says *Inactive*, the HDD needs to be activated. Refer to “Activate a new HDD” on page 158 for more information.

To check the storage status in OSD mode:

1. Click **Storage** > **Storage Device**.

www.acornfiresecurity.com

www.acornfiresecurity.com

2. Note the status of the HDDs/NAS listed under the Status column.

   If the status is listed as *R/W*, the HDD/NAS is in working order. If it says *Inactive*, the HDD/NAS needs to be activated. Refer to “Activate a new HDD” below for more information.

Activate a new HDD

The recorder automatically detects when a new HDD has been added. The newly added HDD is not activated or recognized. The status column will show, “Not active”. Before the new HDD can be initialized, it needs to be activated.

This function is not available in OSD mode.

To activate a new HDD in web mode:

1. Click **Configuration** > **Record** > **Storage Management** > **HDD Management**.
2. Click the **Set** button to set up the criteria of the HDD to activate it.

Initialize an HDD

The built-in HDD does not need to be initialized before it can be used. You can also re-initialize the HDD. However, all data on the HDD will be destroyed.

To initialize an HDD in web mode:

1. Click **Configuration** > **Record** > **Storage Management**.

2 Select the hard drive to be initialized.

3. Click the **Format** button to begin initialization.

   After the HDD has been initialized, the status of the HDD changes to Normal.

To initialize an HDD in OSD mode:

1. Click **Storage** > **Storage Device**
2. Select the storage system to initialize.
3. Click the **Init** button to begin initialization.
4. Enter the admin password. Initialization then proceeds.

   After the storage system has been initialized, the status of the HDD changes to Normal.

Add a network storage system

You can use a network storage system (NAS) or storage area network (SAN) to remotely store recorder recordings. You can add up to eight storage systems.

www.acornfiresecurity.com

www.acornfiresecurity.com

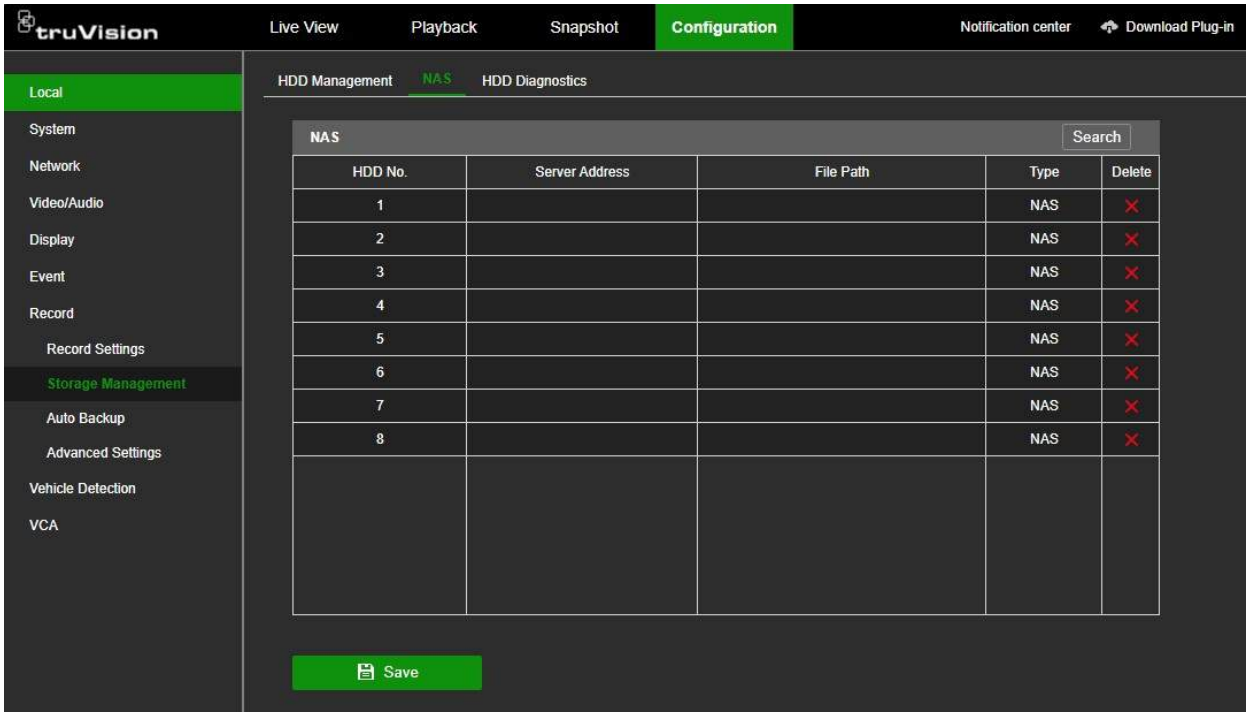
The recommended brands of storage systems to use are:

- Seagate BlackArmor NAS 220
- Iomega StorCenter ix2-dl
- NETGEAR ReadyNAS Pro 2
- QNAP TS-219 II Turbo NAS

You can add up to eight network disks to the recorder.

To set up a network storage system in web mode:

1. From the menu toolbar, click **Configuration** > **Record** > **Storage Management** > **NAS**.



2. There are two ways to enter the information on the NAS to be added.

   a) Search online.

   Click the **Search** button. Select the type of remote system to add, NAS or IP-SAN. Under *Server Address*, enter the IP address of the desired remote storage system. When the remote storage is located, it is listed in the table. Click **OK**. The newly added NAS/IP-SAN

   — or —

   b) Manually enter the NAS information.

   Under the *Server Address* column, manually enter the IP address in the *Server Address* column. Under the *File Path* column, manually enter the file path name for where on the remote storage system you want to store the files. Under the *Type* column, select NAS or IP-SAN.

   Note: If using the NAS storage systems Seagate BlackArmor NAS 220 or Iomega StorCenter ix2-dl, you must add the prefix “/nfs” to the NAS path.

www.acornfiresecurity.com

www.acornfiresecurity.com

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

To set up a network storage system in OSD mode:

1. Click **Storage > Storage Device**.
2. Click the **+Add** button.
3. Select the number of the storage system to use.
4. Under **Type**, select the type of storage system to be used: NAS or IP-SAN. Default is NAS.
5. Under **NAS IP**, enter the IP address of the storage system.
6. Under **NAS Directory**, search for the file path name to define where on the remote storage system you want to store the files.

   Note: If using the NAS storage systems Seagate BlackArmor NAS 220 or Iomega StorCenter ix2-dl, you must add the prefix “/nfs” to the NAS path.
7. Click **OK** to save the changes and return to the Storage window.

S.M.A.R.T. settings

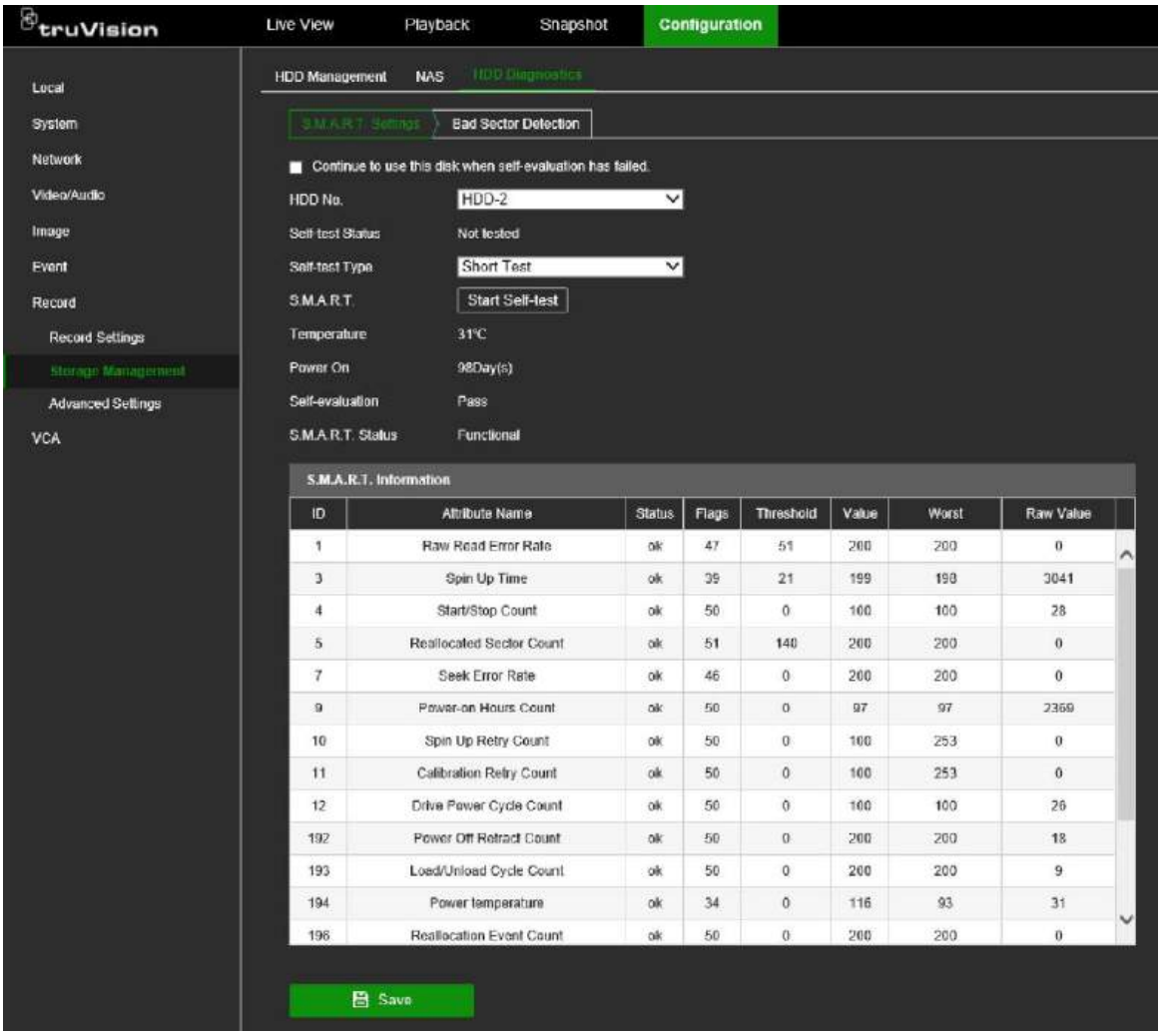
S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) reports on a variety of indicators of hard drive reliability while protecting video stored on the hard drive.

To view the S.M.A.R.T. information of an HDD in web mode:

1. Click **Configuration** > **Record** > **Storage Management** > **HDD Diagnostics** > **S.M.A.R.T. Settings**.
2. If you want to continue to use an HDD when the S.M.A.R.T. test has failed, select the check box **Continue to use when this disk when self-evaluation has failed**.
3. Select the HDD whose data you want to see. A detailed listing of S.M.A.R.T. information is displayed.

www.acornfiresecurity.com

www.acornfiresecurity.com



4. If you want to test the HDD selected, select the type of self-test from the drop-down list and then click the **Start Self-test** button.
5. Click **Save** to save the changes.

To view the S.M.A.R.T. information of an HDD in OSD mode:

1. Click **Maintenance** > **HDD Operation** > **S.M.A.R.T**

   The content is the same as in web mode.

Bad sector detection

You can improve the performance of your HDDs by ensuring that they have no bad sectors. Bad sectors can slow down an HDD when reading or writing data, for example.

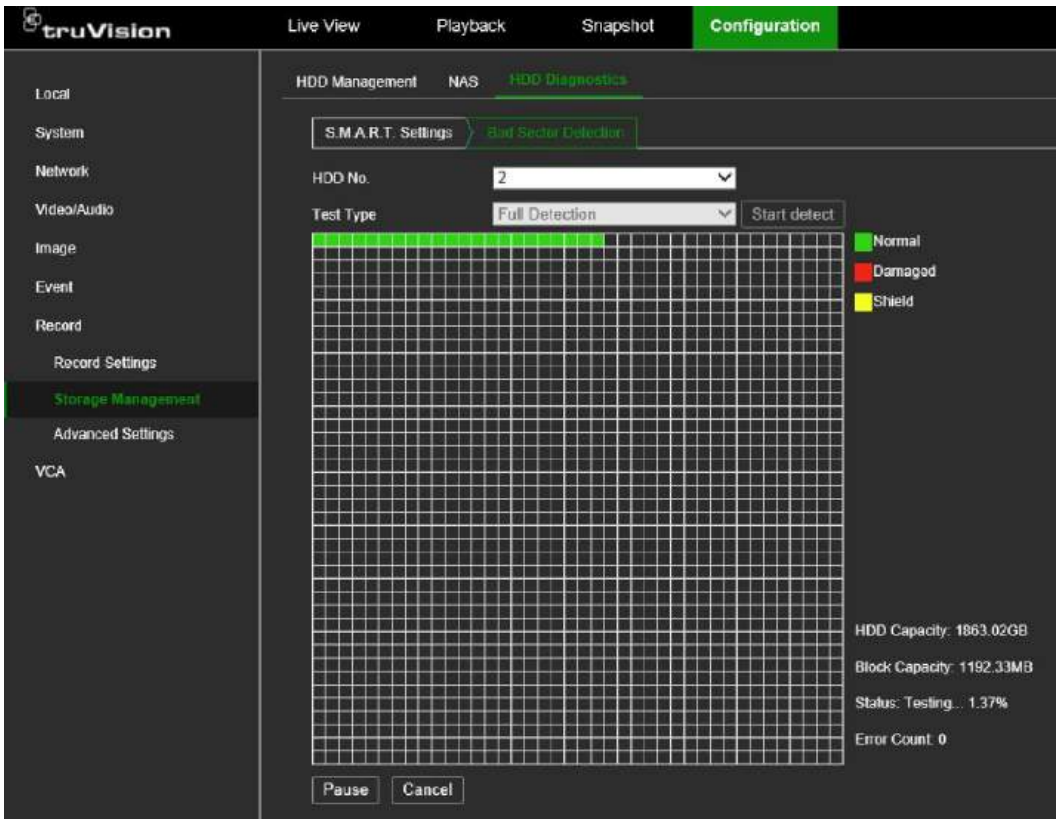
To detect HDD bad sectors in web mode:

1. Click **Configuration** > **Record** > **Storage Management** > **HDD Diagnostics** > **Bad Sector Detection**.
2. Select the HDD you want to test.

www.acornfiresecurity.com

www.acornfiresecurity.com

3. Select whether you want to do a key area detection or a full detection and click **Start Detect**.
4. The system checks the HDD. The color-coded result is displayed on screen.



5. If required, click **Pause** to pause the test or **Cancel** to cancel it.
6. Click **Save** to save the changes.

To detect HDD bad sectors in OSD mode:

1. Click **Maintenance > HDD Operation > Bad Sector Detection**

   The content is the same as in web mode.

HDD sleep mode

You can set the HDD to enter standby mode or sleep mode, after a period of inactivity. Sleep mode decreases the power consumption of an HDD.

To enable HDD sleep mode in web mode:

1. Click **Configuration** > **Record** > **Advanced Settings** > **Other**.
2. Select the **Enable HDD Sleeping** check box to enable sleep mode. Default is Enable.
3. Click **Save** to save the settings.

www.acornfiresecurity.com

www.acornfiresecurity.com

To enable HDD sleep mode in OSD mode:

1. Click **Storage** > **Advanced**.
2. Select Enable **HDD Sleeping** check box to enable sleep mode. Default is Enable.
3. Click **Apply** to save the settings.

Overwrite an 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 HDD to overwrite in web mode:

1. Click **Configuration** > **Record** > **Advanced Settings** > **Other**.
2. Select **Enable Overwriting** check box to enable overwrite mode. Default is Enable.
3. Click **Save** to save the settings.

To enable HDD overwrite in OSD mode:

1. Click **Storage** > **Advanced**.
2. Select the **Overwrite** check box to enable sleep mode. Default is Enable.
3. Click **Apply** to save the settings.

Record file duration (web only)

The feature makes it easier to export files. If the standard files of 1 GB need to be exported, it takes more time to do so than if the files are time-based and consequently smaller.

Important: This feature has nothing to do with the individual setting per camera for the storage duration (which is the number of days that the files are kept on the hard drive).

When this feature is disabled, the recorder stores video files up to a maximum size of 1 GB.

When this feature is enabled, the recorder will split the video files into files of a specified duration. The duration can be set between 10 minutes and 300 minutes (5 hours).

To enable Record File Duration in web mode

1. Click **Configuration** > **Record** > **Advanced Settings** > **Other**.
2. In the **Record File Duration field**, enter the time in minutes.

www.acornfiresecurity.com

www.acornfiresecurity.com

Storage mode

To ensure efficient use of the storage space available on HDDs, you can control an individual camera's storage capacity using HDD quota management.

Note: This function is not available in web mode.

To set the HDD quota for a camera in OSD mode:

1. Click **Storage > Storage Mode**.
2. Under the Mode option, select **Quota**.
3. Select a camera whose storage capacity you want to change and enter the values in GB for the maximum record and snapshot capacities. The available quota space available is displayed on screen.
4. If you want to copy these values to other cameras, click **Copy** and select each camera individually. Click **OK**.
5. Click **Apply** 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 specific HDD group. You could, for example, save the recordings from a couple of high-priority cameras to one HDD, and save the recordings from all the other cameras to another HDD.

If needed, extra HDDs can be purchased. It is strongly advised to use only hard drives that are designed for video surveillance applications, such as Western Digital Purple hard drives.

You can buy the spare HDD kits from Carrier Fire & Security. For the prices, please contact your Carrier account manager.

When more than one HDD is used, you can set up HDD groups in the recorder or use the HDD redundancy option (see page 165).

Note: This function is not available in web mode.

To set up an HDD group in OSD mode:

1. Click **Storage** > **Storage Mode**.
2. Under **Mode**, select **Group**.
3. Click **Apply**. The recorder will reboot.
4. Click **Storage > Storage Device**. All hard drives are added to group 1.
5. Select a hard drive and click **Edit.**
6. Select a group number for the HDD and click **OK**. You will be asked if it is OK to regroup the cameras for the HDD if the group number is changed. Click **Yes** to continue.

www.acornfiresecurity.com

www.acornfiresecurity.com

7. Click **Storage > Storage Mode** and select the group number that was assigned to a HDD in point 6.
8. Add cameras to the group and click **Apply**. You can assign a camera only to 1 group.

Redundancy in group mode

You can set one or more hard drives as redundant drives. The redundant hard drive(s) will record the cameras simultaneously.

Be aware that using the redundancy option reduces the storage capacity of the recorder.

There must be more than one hard drive installed in the recorder before setting up this function.

To set up redundancy in the recorder in OSD mode:

1. Click **Storage** > **Storage Mode**.
2. Under **Mode**, select **Group**.
3. From the menu toolbar, click **Storage** > **Storage Device**.
4. Select the HDD to use for redundant recording and click **Edit** in the *Edit* column. Select **Redundancy** and click **OK**.
5. From the menu toolbar, click **Storage** > **Schedule** > **Record Schedule Schedule** > **Advanced**. Select **Redundant Record** for the desired camera and click **OK**.

   This option must be manually set for each camera.
6. Click **Apply** to save the settings.

To set up redundancy in the recorder in web mode:

1. In OSD mode, set the storage mode first as **Group**. You cannot set the storage mode in web mode.
2. From the web mode menu toolbar, click **Configuration** > **Record** > **Storage Management** > **HDD Management**.
3. Select the HDD to be used for redundant recording. In the Status column, click the status item of the HDD, and from the drop-down list select **Redundancy** and click **Set**.
4. From the menu toolbar, click **Configuration** > **Record Settings** > **Advanced**. Select **Redundant Record** for the desired camera and click **OK**.

   This option must be manually set for each camera.
5. Click **Save** to save the settings.

www.acornfiresecurity.com

www.acornfiresecurity.com

Repair HDD database

There are two ways to repair an HDD:

- **Rebuild Video (web mode only)**: This function will only rebuild and refresh the data library related to video. The rebuild speed is relatively fast. When video cannot be queried by the data library, use this route to quickly view the video.
- **Rebuild All Data (web mode) / Repair Database (OSD mode)**: This function will rebuild all databases on the HDD (video, snapshots, alarms, events). Existing data will not be affected but search and playback functions will not be available during the rebuild. The first 30% of the progress is rebuilding the video database. It is recommended to rebuild all databases.

Note: Do not shutdown the recorder during rebuilding.

To repair databases on an HDD in web mode:

1. Click **Configuration** > **Record** > **Storage Management**.
2. Select the desired HDD and then click **Rebuild Video** or **Rebuild All Data**.
3. Click **OK**. The rebuilding starts.

To repair databases on an HDD in OSD mode:

1. Click **Storage** > **Storage Device**
2. Select the desired HDD and then click **Repair Database**.
3. Click **Yes**. The rebuilding starts.

Manage eSATA (OSD only)

When there is an external eSATA device connected to the recorder, you can configure the usage and manage the eSATA device.

To setup up the eSATA usage:

1. Go to **Storage > Advanced.**
2. As **Usage**, select **Export** or **Record/Capture**.
    - Export:for back-up purposes.
    - Record/Capture: as storage expansion.

Auto backup

An eSATA device can be used for the auto backup function.

www.acornfiresecurity.com

www.acornfiresecurity.com

See “Manage eSATA (OSD only)“ on page166 to set up the eSATA device for backup.

You can create an automatic backup plan so that the recorder will backup the recordings of 24 hours ahead of the backup start time to the eSATA device.

To create the back-up plan:

1. Go to **Configuration > Record > Auto Backup** (web) or **Storage > Auto Backup** (OSD).
2. Enable Auto Backup.
3. Select the cameras to backup.
4. Select the required Backup stream Type: main stream, sub stream or Dual stream (= main & sub stream).
5. Select the Overwrite setting; disable (= HDD is full, backup will stop) or Enable (= HDD is full, oldest files are deleted and overwritten).
6. Click **Apply**.

Dynamically Adjust Recording writing buffer (OSD only)

The recording writing buffer of the recorder can be dynamically adjusted when the bit rate exceeds the limit.

To enable the feature:

1. Go to **Storage > Advanced.**
2. Enable the Dynamically Adjust Recording Writing Buffer to avoid video loss when the bit rate is higher than 4 Mbps. The default setting is Disabled.

Note: The function will result in higher memory use. Restart the recorder after you enable/disable the function.

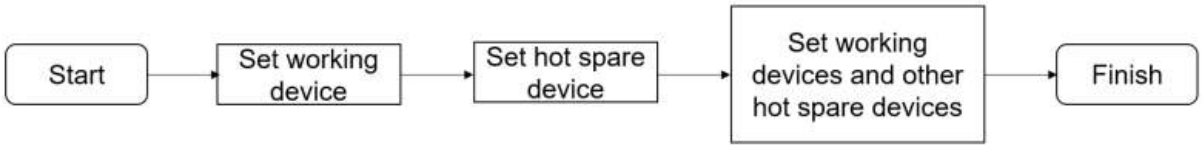
Hot spare device backup (OSD only)

Video recorders can form an N+M hot spare system. The system consists of several working video recorders and at least one hot spare video recorder. When a working video recorder fails, the hot spare video recorder would switch into operation, which increases the reliability of the system.

www.acornfiresecurity.com

www.acornfiresecurity.com

A bidirectional connection shown in the figure below is required to be built between hot spare video recorder(s) and working video recorders.



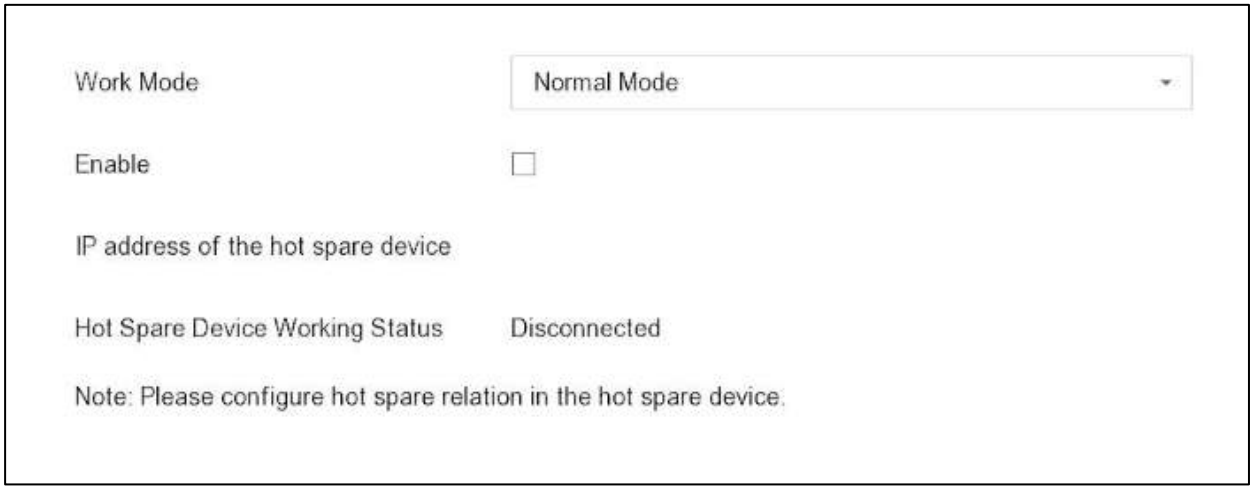
Note:

- Up to 32 working devices and 32 hot pare devices ae allowed.
- It is recommended to use all devices in a same model for compatibility.

To setup the working device:

1. Go to **System > Hot Spare**.
2. Set **Work mode** to **Normal Mode**. (= default)
3. Click **Apply** to save the settings.

Repeat the above steps for other devices.



To setup the Hot Spare device:

A hot spare device will take over working device tasks when working device fails.

1. Go to **System > Hot Spare**
2. Set **Work mode** to **Hot Spare Mode**.
3. Click **Apply** to save the settings.
4. Click Yes in the pop-up screen. The recorder will restart automatically.

www.acornfiresecurity.com

www.acornfiresecurity.com

Note:

- The camera connection will be disabled when the recorder works in hot spare mode.
- It is highly recommended to restore the device defaults after switching the work mode of hot spare devices to normal mode to ensure the normal operation afterwards.

To manage the hot spare system:

Note:

- Up to 32 working devices and 32 hot spare devices are allowed in the hot spare system.
- Only one hot spare device can add working devices and other hot spare devices. You can find the hot spare device IP address from working devices.

1. Go to **System > Hot Spare** on the hot spare device.
2. Click **Add** in **Working Device Settings** to add working devices to the hot spare system. After refreshing the interface, you can view the working status of working devices from the hot spare device interface. Also, the working status and IP address of the hot spare device can be viewed from the working device interface.

Working Status	Description
Monitoring	Working devices are working properly.
No need for backup	The working device goes offline and has never been monitored before.
Backing up	The working device has been monitored before but goes offline. A hot spare device will take over the working device, and record the videos of network cameras connected to the working device. The video backup function can be enabled for one working device at a time.
Waiting for synchronization	The working device comes back online, and waits for the a hot spare device to sync videos.
Synchronizing	The hot spare device is restoring videos back into the working device. The synchronization function can be enabled for one working device at a time.
Synchronization finished	Videos are restored back to the working device. The work device is recovered.

4. Click **Add** in **Hot Spare Device Settings** to add hot spare devices to the hot spare system.
5. **Optional**: Click **Delete** to delete the working devices or hot spare devices as required.

www.acornfiresecurity.com

www.acornfiresecurity.com

Disk Array (P models only and with 4TB/disk or larger)

A disk array is a data storage virtualization technology that combines multiple physical disk drives into a single logical unit. Also known as a "RAID", an array stores data over multiple HDDs to provide enough redundancy so that data can be recovered if one disk fails. Data is distributed across the drives in one of several ways called "RAID levels", based the redundancy and performance required.

Only the TVN 23P models support RAID.

Create a Disk Array

The video recorder supports **software-based disk arrays**. Enable the RAID function as required and ensure **each HDD capacity is not less than 4 TB**.

There are two ways for creating an array: one-touch configuration and manual configuration.

One-Touch Creation

One-touch configuration creates the disk array. By default, the array type created by one-touch configuration is RAID 5.

Before You Start

Install at least 3 HDDs with a minimum capacity of 4TB. Make sure to use hard drives of the same model and capacity for this RAID function.

To setup a disk array via One-Touch Configurationn (via OSD):

1. Go to **Storage > Advanced**
2. Click **Enable RAID**.
3. Click **Apply** and reboot the device to have settings take effect.
4. After the reboot, go to **Storage** > **RAID** > **Physical Disk.**
5. Click **One-touch Config**.
6. Edit Array Name and click **OK** to start configuring. The default RAID configuration via One-Touch Configuration is RAID 5.

Note: If you install 4 or more HDDs, a hot spare disk for array rebuilding will be created.

7. **Optional:** The video recorder will automatically initialize the created array. Go to **Storage > RAID > Array** to view the information of the created array.

www.acornfiresecurity.com

www.acornfiresecurity.com

To setup a disk array via One-Touch Creation (via web):

1. Go to **Configuration > Record > Advanced Settings > Other**.
2. Click **Enable RAID**.
3. Click **Save** and reboot the device to have settings take effect.
4. After the reboot, go to **Configuration > Record > Array Configuration**.> **Physical disk.**
5. Click **One-touch Configuration**.
6. Enter the array name and click **OK** to start configuring. The default RAID configuration via One-Touch Configuration is **RAID 5**.
7. **Optional**: The video recorder will automatically initialize the created array. Go to **Configuration > Record > Arrray Configruation > Array** to view the information of the created array.

Manual creation of RAID array

It is also possible to create the RAID array manually and to select the desired RAID level.

Each RAID level requires a minimum number of hard drives.

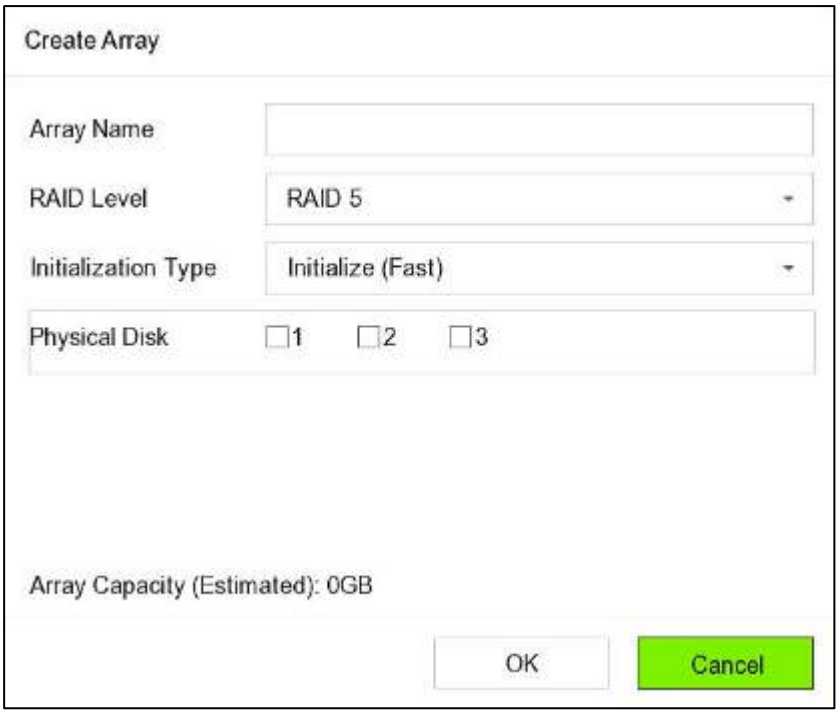
RAID level	Minimum number of hard drives.
RAID 0	At least 2 hard drives
RAID 1	At least 2 hard drives
RAID 5	At least 3 hardd rives
RAID 6	At least 4 hard drives
RAID 10	The number of HDD must be an even range from 4 to 8.

To create the disk array manually (OSD):

1. Go to **Storage** > **Advanced**.
2. Click **Enable RAID**.
3. Click **Apply** and reboot the device to have settings take effect.
4. After the reboot, go to **Storage** > **RAID** > **Physical Disk.**
5. Click **Create**.

www.acornfiresecurity.com

www.acornfiresecurity.com



6. Enter Array Name.
7. Select RAID Level as required.
8. Select the physical disks that will form the array.
9. Click **OK**.
10. **Optional:** The video recorder will automatically initialize the created array. Go to **Storage > RAID > Array** to view the information of the created array.

No.	Name	Capacity	Physical Disk	Hot S...	Status	Level	Rebuild	Delete	Task
1	ARRAY	11176G	1 2 3		Functional	RAID 5			None

To create the disk array manually (Web):

1. Go to **Configuration > Record > Advanced Settings**.
2. Click **Enable RAID**.
3. Click **Save** and reboot the device to have settings take effect.
4. After the reboot, go to **Configuration > Record > Array Configuration > Physical Disk**.
5. Click **Create Array**.
6. Give a name for the disk array, select the RAID type, according to the number of available hard drives, select the hard drives for the array and select the initialization method.
7. Click **OK**.to start the array creation.

www.acornfiresecurity.com

www.acornfiresecurity.com

8. **Optional:** Click **Configuration > Record > Array Configuuration > Array** to view the information of the created array.

Rebuild a disk array

The array status includes Functional, Degraded, and Offline. To ensure the high security and reliability of the data stored in an array, take immediate and proper maintenance of the arrays according to its status.

- **Functional**

  No disk loss in the array.

- **Offline**

  The number of lost disks has exceeded the limit.

- **Degraded**

  If any hard drive fails in the array, the array degrades. Restore it to Functional status by rebuilding the array.

Configure a Hot Spare Disk

The hot spare disk is required for the automatic rebuilding of the disk array.

To configure a Hot Spare Disk (OSD):

1. Go to **Storage > RAID > Physical Disk**.
2. Click of an available hard drive to set it as hot spare disk.

To configure a Hot Spare Disk (Web):

1. Go to **Configuration > Record > Array Configuration > Physical disk**.
2. Click in the Hot Spare column for the hard drive that you want to use as hot spare disk.

Automatically rebuild an array

The video recorder can automatically rebuild degraded arrays with the hot spare disks.

Create one or more hot spare disks. See above.

When the array is degraded, one of the hot spare disks will be used for the automatic rebuilding.

Manually rebuild an array:

www.acornfiresecurity.com

www.acornfiresecurity.com

If no hot spare disks are configured, rebuild a degraded array manually.

To rebuild an array manually (OSD):

1. Go to **Storage > RAID > Array**.
2. Click for the degraded array.
3. Select the available physical disk.
4. Click **OK.**
5. Click **OK** on the pop- up message box "Do not unplug the physical disk when it is under rebuilding."

To rebuild an array manually (Web):

1. Go to **Configuration > Record > Array Configuration >Array**.
2. Click the icon in the Rebuild column to start rebuilding the degraded array.

HDD clone (OSD only)

The HDD clone function can be used to clone the content of an HDD to an eSATA HDD.

Before you start, make sure to connect an eSATA hard drive to the recorder.

To clone the content of HDD to eSATA (OSD only):

1. Click **Maintenance > HDD Operation > HDD Clone**
2. Select an HDD to clone. The capacity of the selected HDD must match the capacity of the eSATA HDD.
3. Click **Clone**.
4. Click **Yes** in the pop-up message to create the clone.

HDD health detection (OSD only)

The TVN 23 (S/P) recorders are using Western Digital Purple hard drives. Western Digital has introduced a health status reporting that reports the detailed status to the recorder. This health status can be seen in the local menu (OSD) of the recorder.

To see the health status for the hard drive(s):

1. Go to **Maintenance > HDD Operation > Health Detection.**
2. The page shows the health status for the hard drives:

www.acornfiresecurity.com

www.acornfiresecurity.com

3. Click on the hard drive to see more details.

Example:

No.	Alarm Name	Status	Current Value	Advice
1	Lifetime Power On Reset Alert	HDD is healthy.	5.00	
2	Power On Hours Alert	HDD is healthy.	75.00	
3	Head Load Lifetime Count Alert	HDD is healthy.	15.00	
4	Current Temperature Alert	HDD is healthy.	26.00	
5	Total Lifetime Workload Alert	HDD is healthy.	0.00	
6	Total Workload Rate Alert	HDD is healthy.	2.00	
7	Power On Reset Rate Alert	HDD is healthy.	0.00	
8	Head Load Rate Alert	HDD is healthy.	0.00	
9	Soft Reset Alert	HDD is healthy.	0.00	
10	Hard Reset Alert	HDD is healthy.	0.00	
11	Mechanical Failure Alert	HDD is healthy.	0.00	
12	Interface CRC Alert	HDD is healthy.	0.00	
13	Uncorrectable Errors Alert	HDD is healthy.	0.00	
14	Read Recovery Alert	HDD is healthy.	0.00	
15	Reallocated Sector Count Alert	HDD is healthy.	0.00	
16	Asynchronous Signal Recovery Alert	HDD is healthy.	0.00	
17	Low Temperature Alert	HDD is healthy.	0.00	
18	High Temperature Alert	HDD is healthy.	0.00	

www.acornfiresecurity.com

www.acornfiresecurity.com

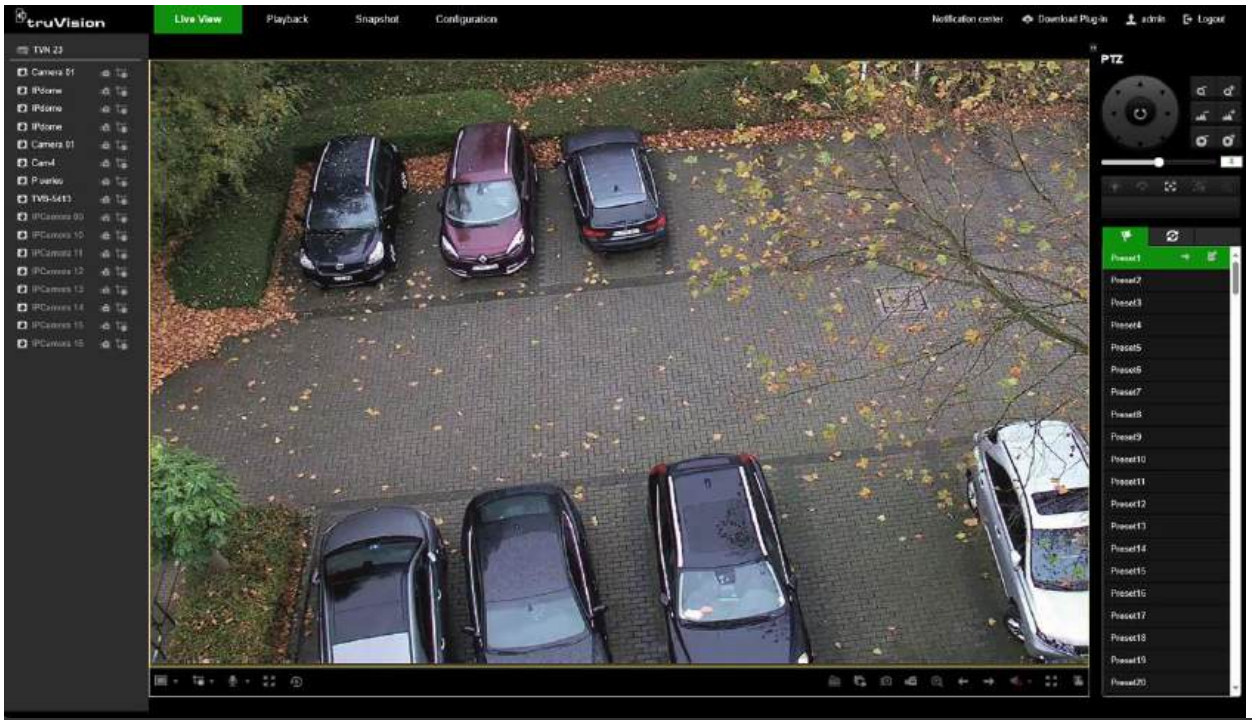
Chapter 13
Live view in web mode

Live view mode is the normal operating mode of the recorder where you watch live images from the cameras. The recorder automatically enters live view mode once powered up. On the monitor you can see whether a recording is in progress and, if set up to do so, the current date and time, as well as the camera name.

This chapter describes how to use live view in web mode.

Description of live view

Figure 14: Live view in web mode



	Description
1.	Camera panel. Click the camera to display in the selected video tile.
2.	Live view viewer.

www.acornfiresecurity.com

www.acornfiresecurity.com

	Description
3.	Notification Center. Click to see the list of all events.
4.	Click to hide or display the PTZ control panel.
5.	PTZ control panel.
6.	Live view toolbar:
	Multiview type: Switch between the different multiview options from the drop-down list.
	Stream type: Switch between main stream (1), substream (2)and transcoded stream (3)
	Bi-directional audio: Turn the microphone on/off.
	Full screen: Only video tiles appear on-screen. Press ESC to return to the screen with the menus and viewer.
	Transcoding: 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.
	QR code: This is a QR code that contains the SCI code for the recorder when it is registered to UltraSync. The SCI code needs to be entered when the recorder is added to TVRMobile. Instead of entering this SCI code manually, the QR code can be scanned to add the SCI code automatically in the SCI field of the mobile app. For further information on adding the recorder to TVRMobile, see “Add the recorder to TVRMobile” on page 92.
	Live views: Stop/start all live views.
	Capture: Capture a snapshot of a video image. See Figure 5 on page 20 for the location where the snapshots are to be saved.
	Recording: Stop/start recording live view and save the files on the PC (not the recorder).
	Digital zoom: Stop/start digital zoom to zoom in/out of the selected camera image.
	/ **Previous page / Next page**: View the previous and next camera respectively. If viewing in multiview format, the live view moves to the next group of cameras for the selected number of video tiles.
	Audio: Adjust the audio level.
	Alarm output: Select an alarm output to switch it ON or OFF.

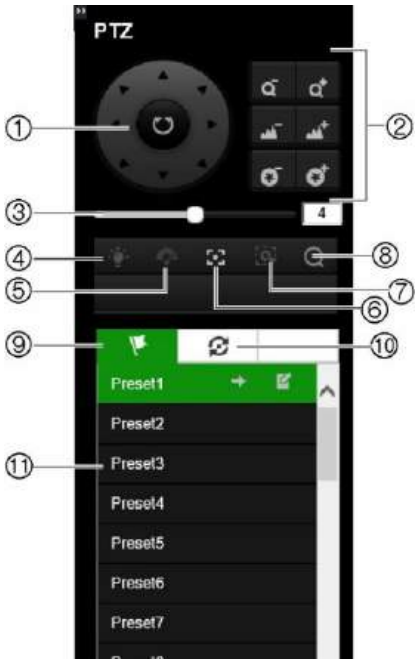
PTZ control

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

www.acornfiresecurity.com

www.acornfiresecurity.com

Figure 15: PTZ control panel description (web)



1. Directional pad/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 zoom, focus, and iris.
3. Adjust the speed of the PTZ dome camera.
4. Turn on or off the camera light (if available on the camera).
5. Start or stop the camera wiper (if available on the camera).
6. Auxiliary focus: Automatically focus the camera lens for the sharpest picture.
7. Start manual tracking.
8. Start 3D zoom.
9. Preset tab. Click to get the list of the presets available.
10. Preset Tour path tab. Click to get the list of the preset tours available.
11. Start the selected preset/preset tour (depending on the function selected).

Preset and preset tours

When in live view you can quickly call up the list of existing presets, and preset tours by using the mouse or keypad. See Figure 15 above for a description of the PTZ control panel.

Note: The PTZ dome camera used must be able to support a preset command.

Presets have previously defined locations of a PTZ dome camera. It allows you to quickly move the PTZ dome camera to a desired position.

Preset Tours are defined series of presets. You can program up to a maximum of four.

Note: Shadow tours are only available in OSD mode.

If the display was in multiview format, it changes to a single-screen format for the selected camera.

Presets

To set up a preset:

1. In live view, click the desired video tile.
2. In the PTZ control panel, select the **Preset** tab and then select the desired preset to use from the list.
3. Using the directional buttons, position the camera in the desired direction. Adjust the focus and zoom as required.
4. Click to set the preset. The preset is saved.

www.acornfiresecurity.com

www.acornfiresecurity.com

To call up a preset:

1. In live view, select the desired video tile.
2. In the PTZ control panel, select the **Preset** tab and click the desired preset from the list.
3. Click to call the preset. The camera immediately jumps to the preset position.

Preset tours

To set up a preset tour:

1. In live view, select the desired video tile.
2. In the PTZ control panel, select the **Preset Tour Path** tab and then select the desired preset tour path to use from the list.
3. Click to start a preset tour path. The Step window appears.

4. Click to add a preset to the preset tour path. Enter the preset number, the speed at which the camera moves from this preset to the next, and the duration in seconds that the camera will stay at this preset.

   The minimum speed setting is 1 and the maximum speed setting is 40.

   The minimum duration is 15 seconds. The maximum duration is 120 seconds.

5. Repeat step 4 for each preset you want to add to the preset tour.

   To change the order of the presets, click the up or down blue arrows. To delete a preset, select it in the list and click .

   Note: A preset tour should have at least two presets.

6. Click **OK** to save the settings and return to the main preset tour path window.

To call up a preset tour:

1. In live view, the desired video tile.
2. In the PTZ control panel, select the Preset Tour Path tab and then select the desired preset tour path to use from the list.
3. Click to start the preset tour path. The camera immediately carries out the preset tour movement. Click the to stop the tour.

   To delete a preset tour path, click .

www.acornfiresecurity.com

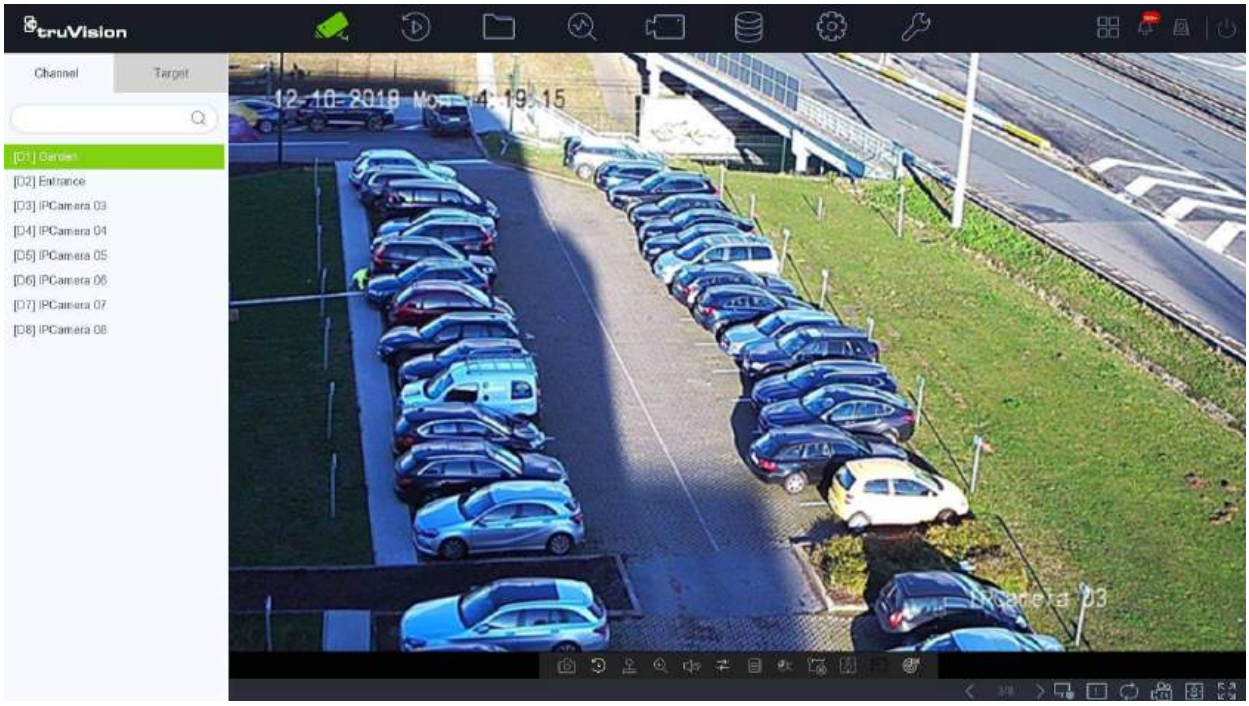
www.acornfiresecurity.com

Chapter 14
Live view in OSD mode

Live view mode is the normal operating mode of the unit where you watch live images from the cameras. The recorder automatically enters live view mode once powered up. On the monitor you can see whether a recording is in progress and, if set up to do so, the current date and time, as well as the camera name.

This chapter describes how to use live view in OSD mode.

Figure 16: Live view in OSD mode



Status information

When in OSD mode, information on the system and camera status is displayed as icons on the main and auxiliary monitors. The camera status icons are shown for each camera. Each icon represents information on a specific item. These icons include:

www.acornfiresecurity.com

www.acornfiresecurity.com

Table 6: Description of the on-screen status icons

Icon	Description
	Indicates an alarm or event.
	Indicates that a camera channel is being recorded.

The recorder can display more than one icon at the same time.

These status icons do not appear in web mode.

Live view control toolbar

The OSD live view toolbar lets you quickly access regularly used commands. Position the cursor over a video tile to see the control toolbar (see Figure 17 below).

It is not possible to take snapshots in OSD mode.

Figure 17: OSD live view control toolbar

Icon	Description
	Snapshot: Take a snapshot and store it on the HDD of the recorder.
	Instant playback: Playback the recorded video from the last five minutes. If no recording is found, then there was no recording made in the last five minutes. Select the desired camera and click the icon to start playback.
	PTZ Control: Enter PTZ control mode. See “PTZ control” on page 177 for more information.
	Digital Zoom: Enter digital zoom. See ”Digital Zoom” on page 187 for more information.
	Audio on/off: Enable/Disable audio output. The stream type must be set to Video/Audio. See “Audio” on page 94 for further information.
	Live View Strategy: helps to get the best live view experience depending on the network quality. Possible selections are: Real time, Balanced, Fluency
	Stream information: Shows information of the camera stream (frame rate, actual bitrate, resolution, encoding type,stream type)
	360° camera dewarping: 360° camera dewarping options for TVF and TVPA TruVision 360° cameras
	Switch between main and sub stream
	Display VCA info: allows to show or hide the VCA line information

www.acornfiresecurity.com

www.acornfiresecurity.com

Icon	Description
	Text insertion: allows to enable/disable the text overaly from a POS device, captured by the text insertion feature.
	3D- positioning (for PTZ cameras): Enable/disable 3D positioning for PTZ cameras

Live view mouse menu

Many features of live view can be quickly accessed by placing the cursor on a live image and clicking the right button of the mouse to get the mouse menu (see Figure 18 below).

Figure 18: The OSD mouse menu

	Name	Description
1.	Menu	When the video tiles are shown without the menu, press to include the menu in the display.
2.	Single Screen	Switch to a single-screen view for the selected camera from the drop-down list.
3.	Window Division	Switch between the different multiview options from the drop-down list. See “Single and multiview display modes” on page 184 for information on selecting multiview formats.
4.	Previous Screen	Displays the previous page of multiscreen video tiles.
5.	Next Screen	Displays the next page of multiscreen video tiles.
6.	Start Auto-Swtch	Turn on sequence mode. The window automatically sequences between cameras. To set up the sequence dwell time, go to Configuration > System > Live View Settings > Switch Interval (web) or System > Live View > General > Dwell time (OSD) and select a sequence dwell time value.
7.	Playback	Enter the Playback window.

www.acornfiresecurity.com

www.acornfiresecurity.com

	Name	Description
8.	PTZ Control	Open the PTZ control panel in live view.

When doing a right-click in a video tile, you see the following menu:

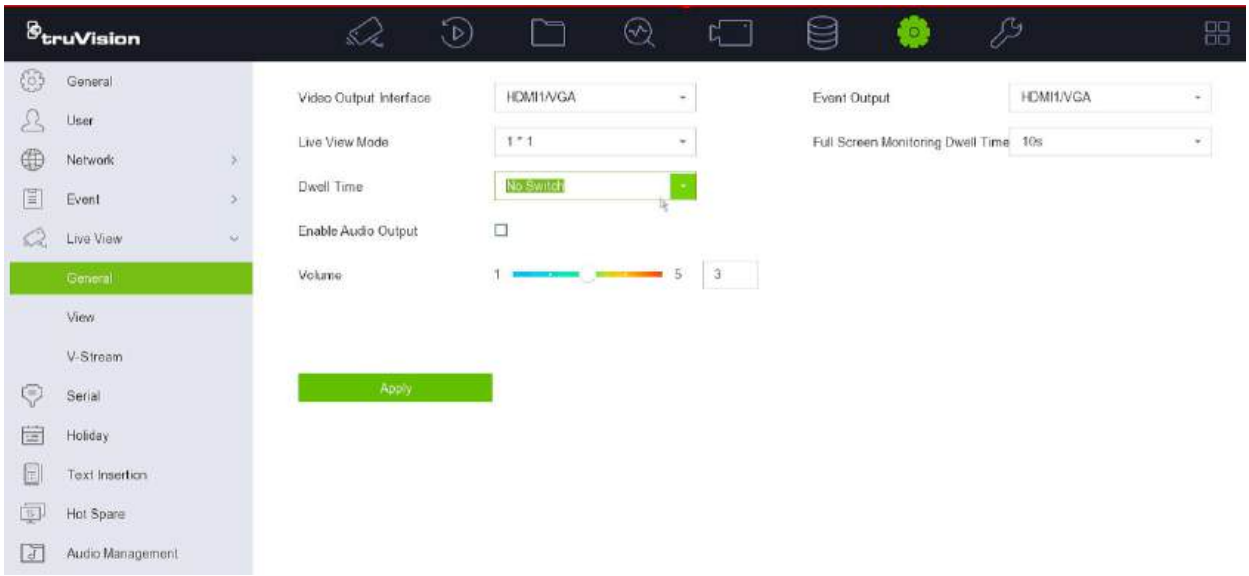
The only option that is different is the **Full Screen** option. It allows to see the vidoe tiles without the menus.

Live view general setup menu

You can easily set up several live view functions such as the default multiscreen layout, the sequence dwell time, the alarm pop-up output and delay as well as enable audio and its volume.

From the OSD mode menu toolbar, click **System** > **Live View** > **General**.

Figure 19: General settings for live view in OSD mode



www.acornfiresecurity.com

www.acornfiresecurity.com

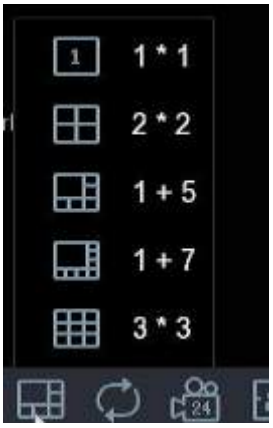
	Name	Description
1.	Video Output Interface	Select the video output: HDMI1/VGA, HDMI2, Aux CVBS-V-Stream
2.	Live View Mode	Select the default multiscreen layout. See “Default live view monitor setup” on page 26 for information on assigning channels to video tiles.
3.	Dwell Tile	Define delay between two consecutive channels during sequencing.
4.	Event Output	HDMI1/VGA, HDMI2, Aux CVBS/V-Stream
5.	Full Screen Monitoring Dwell Time	Define the time that a camera in alarm will be shown in full screen. The minimum is 1 s, and the maximum is 10 s.Default is 10s.
6.	Enable Audio Output	Enable Audio to hear audio via the HDMI monitor or, for VGA, the audio output on the back panel of the recorder
7.	Volume	Adjust the audio level.

Single and multiview display modes

The recorder has single and multiview formats. The number of multiview display modes available depends on the recorder model.

There are four ways to select the multiview format:

- Place the mouse cursor on the desired video tile and right-click the mouse. In the OSD mouse menu that appears, select the desired multiview option (see Figure 18 on page 182).
- In the bottom-right of live mode, click the multiview icon and select the desired option.



- Double-click a selected video tile to switch between multiview and single-view format. The multiview format used is shown at the bottom-right of the screen.
- Go to **System** > **Live View** > **General** and select the desired live view mode format.

www.acornfiresecurity.com

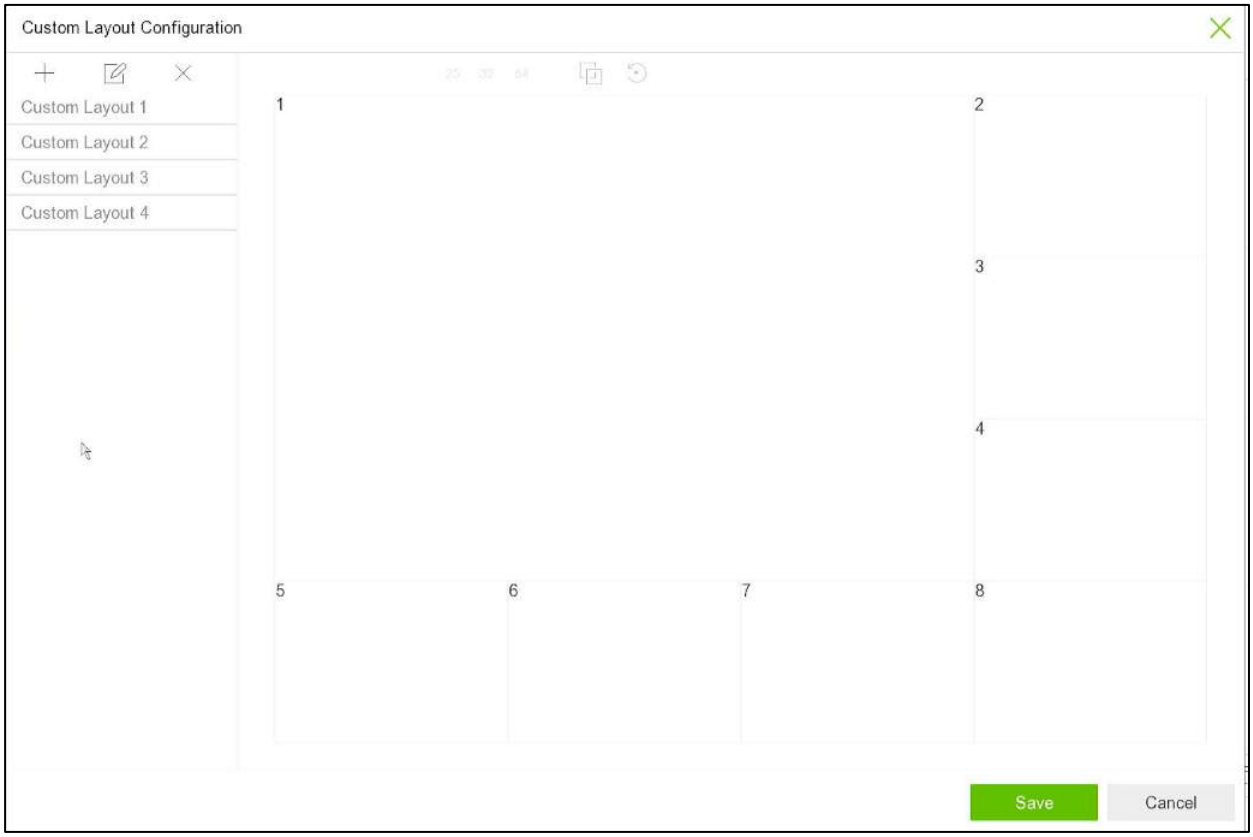
www.acornfiresecurity.com

Custom layout configuration and usage (OSD)

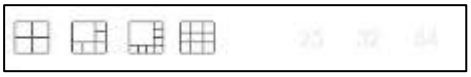
The custom layout configuration feature allows to create custom layout patterns that can be selected in OSD live view. That can be useful when some cameras are used in hallway mode or when the standard layouts are not applicable for the application.

To create a custom layout:

1. Click **System > Live View > View**.
2. Click **Set Custom Layout**
3. A pop-up window will open:



4. Click **+** to create a new custom layout; Maximum 4 custom layouts can be created.
5. Give the layout a meaningful name and click **OK**.
6. Select a window division mode from the toolbar



7. Select multiple tiles and click to joint the tiles to 1 tile. The selected tiles must be in a rectangular area.

www.acornfiresecurity.com

www.acornfiresecurity.com

8. Click **Save** to save the settings and the saves layout will appear in the list.
9. To modify the layout, click . To delete a layout, click .

To assign camera to a custom layout:

1. Click **System > Live View > View**.
2. Select the custom layout from the dropdown list in the bottom toolbar.
3. Assign cameras to the video tiles.
4. Click **Apply** to save the settings.

To use the custom layout in live view:

1. Go the live view screen.
2. Click the multiview icon and select the desired custom layout.

Sequencing feature

The sequencing feature allows that a camera is displayed briefly in full screen, before advancing to the next camera in the sequence list or when a multicamera layout is used (for example 2x2), the sequencing will happen between the different cameras in the multicamera layout.

See “Default live view monitor setup” on page 26 for more information on assigning cameras to video tiles.

The default sequence displays each camera in numerical order. In OSD mode, go to **System** > **Live View** > **View** to define the sequence order.

There are two ways to start sequencing in live view:

www.acornfiresecurity.com

www.acornfiresecurity.com

- Select the camera where you want to start sequencing. Right-click the mouse and select **Start Sequence** to start the sequencing. Right-click again and select **Stop Sequence** to stop sequencing.
- In the bottom-right of live mode, click the sequencing icon to start sequencing. It becomes green when enabled. Click again to disable sequencing.

To set up camera sequencing from web mode, go to **Configuration** > **System** > **Live View Settings**.

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. Left-click the mouse on the desired camera. The live view toolbar appears.
2. Click the digital zoom icon. The camera image is magnified four times. Use the scroll wheel on the mouse to zoom in or out.
3. To exit digital zoom, right-click the mouse.

Target display details in live view

The live view screen of the TVN 23 (S/P) can show details of the captured events as they happen.

This view provides instant event details for operators.

The details can be shown for:

- Smart detection : this is only for temperature measurement events from TruVision thermal cameras.
- Vehicle detection (license plates)
- Face detection
- People detection: not supported with actual TruVision cameras

It is possible to select multiple event types.

There is a possibility to define for what cameras the events will be shown.

The details will be shown as events happen.

www.acornfiresecurity.com

www.acornfiresecurity.com

When you leave the live page, and come back, the table with events will be cleared as well. When the screen is full events, the oldest events will move to the historical events.

To see the target details:

1. Make sure you add cameras to the recorder than can create the events.
2. Open the live view page on the OSD.
3. Select **Target**, select the necessary event types.
4. Trigger events on the camera(s) and see how the target list is filled with snapshots.
5. You can click on a snapshot to see the recorded video for the event.

PTZ control

When in live view you can quickly call up the list of existing presets, preset tours, and shadow tours by using the mouse or keypad. You can also control the movement of the PTZ camera.

Mouse	Left-click the mouse on the desired camera image. The live view toolbar appears. Click the PTZ control icon to enter PTZ mode. The PTZ control panel appears.
Keypad	Press the Enter ↵ button on the keypad.

If the display was in multiview format, it changes to a single-screen format for the selected camera. See Figure 20 below for a description of the PTZ control panel.

Note: The PTZ dome camera used must be able to support a preset command.

Figure 20: PTZ control panel

www.acornfiresecurity.com

www.acornfiresecurity.com

Shortcut

	Name	Description
1.	Directional pan/auto-scan buttons	Controls the movements and directions of the PTZ. The center button is used to start auto-pan by the PTZ dome camera.
2.	PTZ movement	Adjusts the speed of PTZ movement.
3.	Zoom, focus, and iris	Adjust the zoom in and out.

www.acornfiresecurity.com

www.acornfiresecurity.com

	Name	Description	
			Adjust the focus in and out.
			Adjust the iris in and out.
4.	Select PTZ command	Displays the desired function from the scroll bar: **Aux Function**: Gives access to extra camera functions (depending on the camera model) **Preset Tour**: This is a defined series of presets. **Shadow Tour**: Allows you to record a manual movement of a PTZ and to follow the same tour later. **Preset**: Presets are previously defined locations of a PTZ dome camera. It allows you to quickly move the PTZ dome camera to a desired position.	

Presets

To call up a preset:

1. In live view, select the desired video tile. Select the PTZ control icon in the control toolbar, or right-click the mouse and select **PTZ Control**. The PTZ control panel appears.

2. Click at the bottom of the screen, select a preset number and press Call, to call the preset.

Or click to show the thumbnails of the stored presets. Press the thumbnail of tehd esried preset to call it.

To set up a preset:

1. In live view, select the desired video tile. Select the PTZ control icon in the control toolbar, or right-click the mouse and select **PTZ Control**. The PTZ control panel appears.

2. Using the directional buttons, position the camera in the desired direction. Adjust the focus and zoom as required.

3. Click select a preset number, overwite ‘Preset’ with a meaningful name and press **Apply** to save the preset.

www.acornfiresecurity.com

www.acornfiresecurity.com

Preset tours

To call up a preset tour:

1. In live view, select the desired video tile. Select the PTZ control icon in the control toolbar, or right-click the mouse and select **PTZ Control**. The PTZ control panel appears.
2. Click the **Preset Tour** tab and double-click the **Call** button of the desired preset tour from the list. The camera immediately carries out the preset tour movement. Click the **Stop** button to stop the tour.

To set up a preset tour:

1. In live view, select the desired video tile. Select the PTZ control icon in the control toolbar, or right-click the mouse and select **PTZ Control**. The PTZ control panel appears.
2. Click the **Preset Tour** tab.
3. Click the desired preset tour from the preset tour list.
4. Press Set to add a preset tour. Enter the preset number, the speed at which the camera moves from this preset to the next, and the duration the camera will stay at this preset. Click **OK**. The preset is added to the preset tour list.
5. Repeat step 4 for each preset you want to add to the preset tour.
6. When you have finished entering presets to the preset tour, click **Apply**.

Shadow tours

Note: Shadow tours are only available in OSD mode.

To call up a shadow tour:

1. In live view, select the desired video tile. Select the PTZ control icon in the control toolbar, or right-click the mouse and select **PTZ Control**. The PTZ control panel appears.
2. Click the **Shadow Tour** tab and click the **Call** button of the desired shadow tour from the list. The camera immediately carries out the shadow tour movement.

To set up a shadow tour:

1. In live view, select the desired video tile. Select the PTZ control icon in the control toolbar, or right-click the mouse and select **PTZ Control**. The PTZ control panel appears.
2. Click the **Shadow Tour** tab.
3. Select the desired shadow tour from the shadow tour list.
4. Click the **Record** button and then use the directional PTZ buttons to move the camera to the desired locations. Adjust the focus and zoom as required. Click the **Stop** button to stop the shadow tour recording.

www.acornfiresecurity.com

www.acornfiresecurity.com

360° camera dewarping

The TVN 23 (S/P) recorder supports 360° camera dewarping in live and playback via the OSD.

This allows you to only add the 360° view of the TruVision 360° IP cameras and then do a dewarping to see another view.

To do 360° dewarping:

1. In live view or playback view, click in the video tile. You will see the audio and vidoe control bar. Press the 360° camera dewarping icon .
2. A menu will be shown with the different dewarping possibilities:

	Mode	Description
	180° panorama	Shows the fisheye view as two 180° panorama views.
	360° panorama	Shows the fisheye view as one 360° panorama view.
	PTZ Expansion	Shows the fisheye view and a part that is zoomed in.The part can be chosen by clicking with the mouse in the fiseheye view.
	Fisheye + 3 PTZ	Shows the fisheye view with 3 PTZ tiles. Click and hold the left mouse button and move the cursor in a PTZ view to change the view.
	Cylinder	Shows the camera view in a cylinder. Click and hold the left mouse button and move the cursor to rotate the cylinder.
	Hemisphere	Shows the camera view in a hemisphere. Click and hold the left mouse button and move the cursor the change the view.
	4 PTZ	Shows the camera view in 4 PTZ tiles. Click and hold the left mouse button in each PTZ tile, to change the PTZ view.

www.acornfiresecurity.com

www.acornfiresecurity.com

Chapter 15
Playback in web mode

This chapter explains playback when using web mode. However, more playback functions are available in OSD mode.

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

- 24-hour playback of one day's recorded video. You can also create video clips.
- Search video by different themes such as main stream or substream as well as by time (see Chapter 17 "Search recordings" on page 208 for further information)

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 "Modify a user's access permissions" on page 67 for more information).

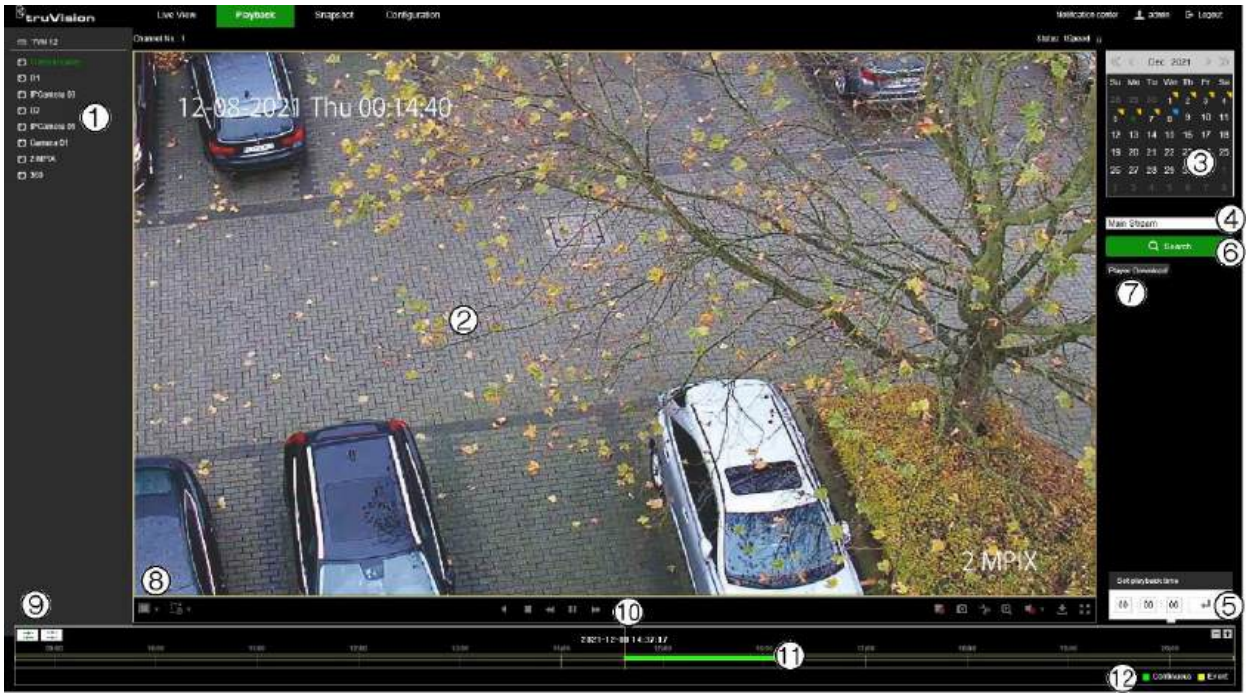
Description of the web playback window

To search and play back recorded video, click **Playback** in the menu bar to display the Playback window.

www.acornfiresecurity.com

www.acornfiresecurity.com

Figure 21: 24-hour playback window (web mode)



	Description
1.	**Camera panel**. Select the camera(s) for playback.
2.	Playback viewer.
3.	**Calendar panel**. *Green date number*: Selected day of playback. *Date number with a blue triangle in the top right corner*: Continuous recordings are available for this day. *Date number with a yellow triangle in top right corner*: Event recordings are available for this day. *Date number with no triangle in top right corner*: No recordings are available for this day.
4.	**Stream type search**: Select to search recorded video files by main stream or substream.
5.	**Playback time**: Enter the start time of the recorded video to search.
6.	**Search button**: Click to search for recorded video files by selected date, playback time, and stream type.
7.	**Download Player**: Click to download the TruVision Player tool to play back recordings on your PC.
8.	**Playback control toolbar**:
	Multiview type: Select how you want the video to be displayed in the viewer (full, quad, 9, and 16).
	Smart search: Select one of the smart types to search recordings. Select Clear, Motion, Cross Line, or Intrusion Detection. See “Smart search” on page 203 for more information. **Note**: Smart search only works for one camera at a time in full screen (1x1) display.
	Transcoding: It is possible to use transcoding during playback. Modify the resolution, maximum bit rate, and frame rate of the transcoded stream.
	Reverse and pause the playback.
	Stop playback.

www.acornfiresecurity.com

www.acornfiresecurity.com

	Description	
		Decrease playback speed
	/	Play/pause playback.
		Increase playback speed.
		Playback one frame at a time
		Show/hide text overly for text insertion
		Stop all playback.
		Capture: Capture a snapshot of a video image. See Figure 5 on page 20 for where the snapshots are to be saved.
		Clipping: Create a video clip, which can be then exported to a backup device. In the pop-up dialog box, enter the start and end times.
		Digital zoom: Stop/start digital zoom to zoom in/out of the selected camera image.
		Audio: Adjust the audio level.
		Download: Download video snapshots and clip files to the selected directory. See Figure 5 on page 20 for more information on how to set up the directory.
		Full-screen mode.
9.		**Synchronous playback**: Click to play back two or more cameras synchronously. Click the asynchronous icon to stop synchronous playback. Selected icon is green.
10.	**Time bar**: Time of actual playback.	
11.	**Timeline**: This bar displays the playback recording. Its color shows the recording type. It allows you to move forwards or backward in time. The timeline moves from left (oldest video) to right (newest video). Place the cursor on the timeline and drag the timeline to the desired posit to where you want playback to start. In 24-hour playback, the time bar shows the actual playback time.	
12.	**Recording type**: Description of the color coding of the recording types that appear in the playback timeline. Green indicates constant recording. Yellow indicates event recording.	

Play back recordings

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

To play back recordings:

1. In playback mode, select the desired camera by stopping the current playback, clicking the desired camera, and then click **Play**.

www.acornfiresecurity.com

www.acornfiresecurity.com

2. Select the desired multiview format.
3. Enter the day and time to search for a recording for the selected camera. Click **Search**.
4. Click **Play** to start playback for each camera.

   Note: If no image appears for a camera, then there is no recording for the selected time/date.
5. Use the playback control toolbar to manually control playback.

Synchronous playback

Synchronous playback allows you to play back two or more recordings synchronously. You can control all cameras with a single set of video controls to play, pause, forward, and reverse.

Note: This function is only available in web mode.

To synchronously play back recordings:

1. In playback mode, click the **Synchronous** button for synchronous playback (the icon is green when enabled). The multiview changes to 2x2, if not already selected.
2. Select the desired cameras by stopping the current playback, clicking the desired camera, and then clicking **Play** to start play back all the cameras in multiview.

   Note: If no image appears for a camera, then there is no recording for the selected time/date.
3. Use the playback control toolbar to manually control playback.
4. Click the **Asynchronous** button to stop synchronous playback.

Smart search

Smart Search allows you to search for events in recorded video during playback, even if the recorder is recording continuously, and no events are set-up. If event recording is used, it can still help you to locate events for areas of the screen where no events have been defined.

Smart search can be done as a search based on a cross line, an intrusion detection area, or a motion detection area.

For cross line and intrusion detection, the smart search can be done without setting up a cross line and/or intrusion detection for the camera.

When a smart search based on motion detection is needed, you must first set up motion detection for the camera, and then select ‘Enable Dynamic Analysis for Motion’ via the webpage.

www.acornfiresecurity.com

www.acornfiresecurity.com

To search events using Smart Search in web mode:

1. Make sure that the VCA information from cameras is stored on the hard drive. In OSD mode, go to **Storage** > **Advanced**. Select **Enable Save Camera VCA Data** and then select **Alarm Storage**.
2. Add an IP camera to the recorder and let it record (if needed, set up motion detection for the camera(s)).
3. Go to playback.
4. Select the camera and you should see a colored timeline that shows that the video has been recorded.
5. Click **Play** to start playback.
6. Click **Smart Search**. Select one of the following options:

	Click to delete the selected smart search function.
	Click to search for motion in the whole frame. A yellow bar will appear below the timeline on the time(s) that motion was detected in the video.
	Click to draw a cross line on the playback screen. A yellow bar will appear below the timeline on the time(s) that the line was crossed.
	Click to draw an intrusion detection area on the playback screen. A yellow bar will appear below the timeline on the time(s) that the intrusion detection zone detected movement.

Note: Smart search is only possible in a 1x1 (full screen) layout.

Create snapshots

Snapshots can be taken at any time during playback.

To configure snapshots:

1. In playback mode, select the desired camera by stopping the current playback, clicking the desired camera, and then click **Play**.
2. When you see a moment in a recording that you want to capture as a snapshot, click the **Capture** button.

   The file is automatically uploaded to the location specified under **Configuration** > **Local** > **Snapshot and Clip Settings**
3. Repeat step 2 for additional snapshots.

www.acornfiresecurity.com

www.acornfiresecurity.com

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. However, you cannot specify in web mode the start and end times of a video clip.

Note: You have more control over the length of a video clip in OSD mode.

To create video clips during playback:

1. In playback mode, select the desired camera by stopping the current playback, clicking the desired camera, and then click **Play** ▶.
2. Scroll the timeline where you want the video clip to start and click the **Start Clipping** button in the playback control toolbar. The icon turns green. Let the recording run-up to the moment when you want to stop the clip then click **Stop Clipping**.

   The file is automatically uploaded to the location specified under **Configuration** > **Local** > **Snapshot and Clip Settings**.

   Note: Video clips in OSD mode can be saved to a USB flash drive.
3. Repeat step 2 for additional clips.

Digital zoom in playback

To digitally zoom in during playback:

1. In playback mode, select the desired camera.
2. Click the **Digital Zoom** button in the playback control toolbar and use the mouse scroll wheel to zoom in and out.

www.acornfiresecurity.com

www.acornfiresecurity.com

Chapter 16
Playback in OSD mode

This chapter explains playback when using OSD mode.

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

- Instant playback of the most recently recorded video (accessed from live mode)
- 24-hour playback of one day's recorded video
- Search videos by different themes such as video, snapshots, events, people, and vehicle (see Chapter 17 "Search recordings" on page 208 for further information)
- Launch playback of a video associated with searched events (see Chapter 17 "Search recordings" on page 208)

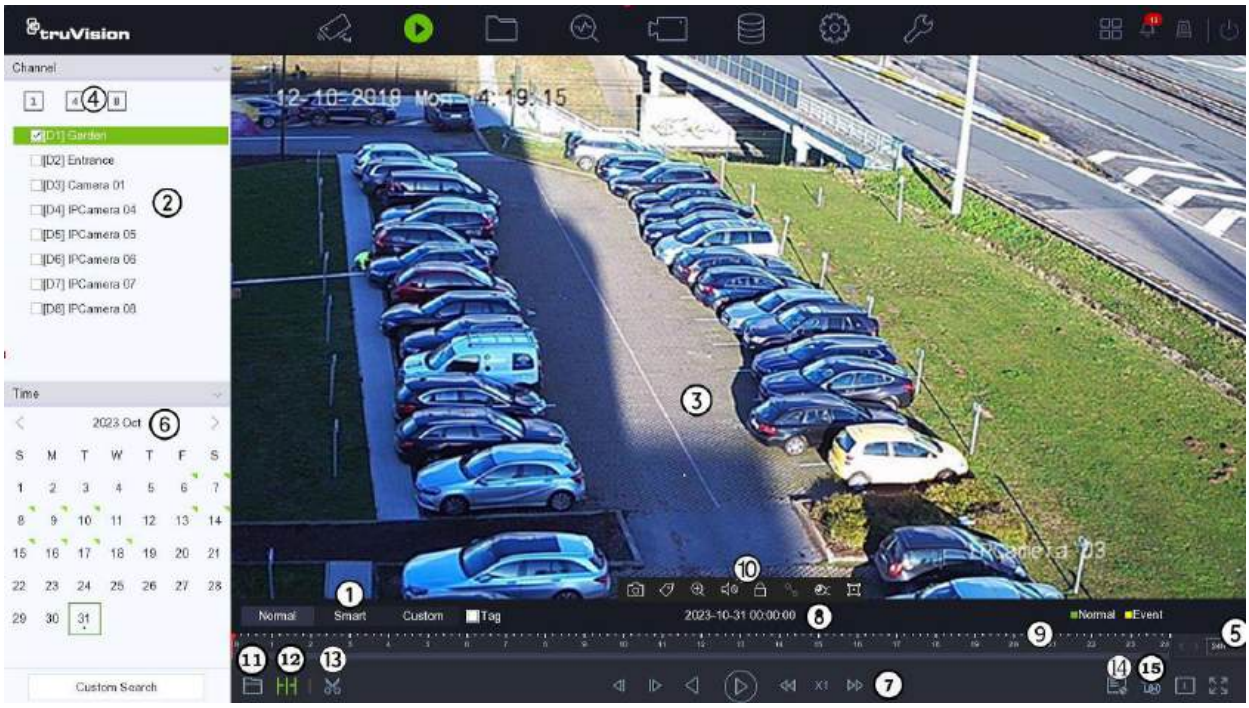
The recorder continues to record the live view from a camera while simultaneously playing back video on that camera display. You must have the access privilege to play back recordings (see "Modify a user's access permissions" on page 67 for more information. This function is only available in web mode).

www.acornfiresecurity.com

www.acornfiresecurity.com

Description of the OSD playback window

Figure 22: 24-hour playback window (OSD mode)



1. **Playback mode**: Select Normal, Smart or Custom playback.

2. **Camera panel**. Select the camera(s) for playback. Use the mouse to click on the vertical scroll bar to display the list of cameras available.
3. **Playback viewer**.
4. **Multicamera selection**: Select which cameras to display simultaneously when in normal mode. It can be one camera or a group. The maximum number of cameras that can be displayed will depend on the recorder model.
5. **Playback period**: Select the playback period to display for the selected day: 24-hour, 6-hour, 2-hour, 1-hour, or 30 minutes. Default is 24-hour playback.
6. **Calendar panel**.
   Green square: Selected day of playback.
   Date number with a green triangle in the top right corner: Recordings are available for this day.
   Date number with no green triangle in the top right corner: No recordings are available for this day.
7. **Playback control toolbar**:
   : Reverse the playback by 30 seconds.
   : Forward the playback by 30 seconds.
   / : Play/pause playback.
   : Decrease playback speed: Options available are: ½ speed, ¼ speed, 1/8 speed, and single frame.
   : Increase playback speed. Options available are: X1 speed, X4 speed, X8 speed and X32 speed.
   X 1: Speed of playback.

8. **Time bar**: Time of actual playback.
9. **Timeline**: This bar displays the playback recording. It indicates in color the type of recording. Green is a normal (constant) recording and yellow is an event recording.
10. **Audio and video control toolbar**: This toolbar appears when the mouse cursor is placed on a video tile. See “Audio and video control toolbar” on page 201 for more information.
11. External File playback.
12. Playback subperiods.
13. Clipping.
14. Enable/disable text insertion overlay.
15. Select main or sub stream. This is only possible when dual stream recording is sett-up.

www.acornfiresecurity.com

www.acornfiresecurity.com

Audio and video control toolbar

The audio and video control toolbar lets you quickly access regularly used playback commands. Position the cursor over a video tile to see this control toolbar (see Figure 23 below).

When you are in event playback, a new icon appears in this toolbar that lets you mark the video that has motion, cross line, or intrusion detection in a recording.

Figure 23: Audio and video control toolbar

Icon	Description
	Tage: Create a tag of a scene, which can be then exported to a backup device. In the pop-up dialog box, enter the name of the tag. See “Create ” on page 206 for more information.
	Digital Zoom: Enter digital zoom. See “Digital zoom” on page 187 for further information.
	Audio On: Enable/Disable audio output. The stream type must be set to Video/Audio. See “Camera encoding settings” on page 153 for further information.
	Lock: Lock or unlock a file during playback. Locked files can then be exported to a backup device.
	Smart Search: This command only appears when in smart playback mode. It lets you set the detection areas on screen to find recorded video based on the drawn motion detection areas, cross line, or intrusion detection area. See “Smart search” on page 203 for further information.
	360° camera dewarping: this feature allows to do dewarping in different view modes for TruVision TVF and TVPA 360° cameras.
	Display VCA info: enable/disable the VCA lines as overlay during playback.

Playback modes

There are three types of playbacks, Normal Smart and Custom. This categorization is only available in OSD mode.

Normal playback

In normal playback, you will see all the recorded footage, continuous and event, for the selected camera(s). The recording starts at midnight. Several cameras can be selected for multiscreen display in normal playback mode.

www.acornfiresecurity.com

www.acornfiresecurity.com

To do a normal playback:

1. In playback mode, click **Normal** playback.
2. Select the desired camera. More than one camera can be selected.
3. Hover the mouse cursor on the video tile to display the audio and video control bar.
4. Click the icon for the desired function to carry out (see Figure 23 on page 201).

   Note: Event detection is not available in normal playback.

Smart playback

In smart playback, you can selectively play back the parts of a recording with motion, cross line or intrusion detection events and skip over video that does not have such events. Smart playback mode analyses the video for VCA, smart events and motion events and then marks them.

To be able to play back VCA, smart events, and motion events you must ensure that the function **Save Camera VCA Data** is enabled. This function is only available in OSD mode.

Only one camera can be selected in event playback mode.

Note: Make sure that you have enabled **Dual-VCA** in the camera. See “Dual VCA” on page 95 for further information.

To play back an event:

1. In playback mode, click **Smart** playback.
2. Select the desired camera.
3. Start playback. By default, the recorder will play back only the events (shown in yellow in the timeline). It will skip any non-event recorded video (in green).
4. Press the **Play Strategy** button , to define the playback settings:
   - Enable/disable skipping of normal video.
   - The playback speed for normal and smart video can be setup between x1 and x8, if normal video playback is selected.
5. Go to **Storage** > **Advanced** and confirm that **Save Camera VCA Data** has been enabled.
6. Hover the mouse cursor on the video tile to display the audio and video control bar.
7. Click the event detection icon . Select the desired event rule for motion, cross line, or intrusion detection, and then draw where you want to mark the detection to be done on screen.

— or —

Click **Clear** to delete previous detection rules.

www.acornfiresecurity.com

www.acornfiresecurity.com

8. Click the **Search** icon in the control toolbar to search and play back video with the matched events.

Smart search

Smart Search allows you to search for events in recorded videos during playback. If event recording is used, it can still help you to locate events for areas of the screen where no events have been defined.

Smart search can be done as a search based on a cross line, an intrusion detection area, or a motion detection area.

For cross line and intrusion detection, the smart search can be done without setting up a cross line and/or intrusion detection for the camera.

When a smart search based on motion detection is needed, you must first set up motion detection for the camera, and then select 'Enable Dynamic Analysis for Motion' via the webpage.

To search events using Smart Search via OSD mode:

1. Make sure that the VCA information from cameras is stored on the hard drive. Go to **Storage** > **Advanced**. Enable **Save Camera VCA Data**.
2. Add an IP camera to the recorder and let it record (if needed, set up motion detection for the camera(s)).
3. Go to **Playback** > **Smart**.
4. Select the camera from the list and you should see a colored timeline that shows that video has been recorded.
5. Click **Play** to start playback.
6. Select **Space Rule**. Select one of the following search options:
   a. Draw Motion Detection Rule
   b. Draw Intrusion Detection Rule
   c. Draw Cross Line Detection Rule
7. Select the desired function and draw the area of interest on the video frame.
8. Press the search icon to start the search.

9. The timeline will now display yellow events detected by smart search in the green continuous recording bar. The yellow event lines detected by smart search will look the same as those event lines that already existed in the timeline.

www.acornfiresecurity.com

www.acornfiresecurity.com

Play back recordings with people and vehicles

The new TruVision IP cameras support the detection of people and/or vehicles. In the playback screen of the OSD mode, you can apply a filter on the playback that will identify recordings of people and/or vehicles. The camera must be set up to record people and /or vehicles.

This function is only available in OSD mode.

To search recordings by people or vehicle detection in OSD mode:

1. In playback mode, select **Smart** Playback.
2. Select the desired camera. Only one camera can be selected.
3. Select a date for playback.

   The timeline will then show the recorded video for the camera.
4. In the bottom right of the screen, select a playback period to zoom into the recording.

   5. The timeline will show all recorded events that have been set up. If you want to filter for events with people and/or vehicles, In the bottom left of the screen, click the **People** and/or **Vehicle** icon depending on which the camera has been set up to record.
6. The timeline will display the recorded people/vehicle events in yellow.
7. When people and/or vehicle is selected, you can select to skip the video without events (normal video) as well as the unselected events. This is done via the Playback Strategy button .

   Example: If you select to show the events with people, and select **Skip Normal Videos**, then all videos without events and vehicle events will be skipped.

Custom playback (OSD only)

The third playback mode that is available in the OSD is the Custom Playback.

Recorded video can be played back, based on customized search conditions.

To define the search conditions and playback the results:

1. Click **Playback**
2. Select one or more cameras from the camera list
3. Click **Custom Search**

   Now select the search method. There are three methods available:

   - Search by appearance

www.acornfiresecurity.com

www.acornfiresecurity.com

- Search by tag
- Search by event

Search by appearance:

1. Define the time and date
2. Select the file status (All, Locked, Unlocked) and click **Start Search**.
3. The results will be shown in a table. Click to see a thumbnail of the search result. The result is always for once camera. Click the **Channel** button to select another camera.
4. Click the play button to start the playback of the selected clip.
5. You can also export the clip or lock it to avoid deletion.
6. Click **Exit** to return to the Playback screen.

Search by tag:

1. Define the time and date for the search.
2. Enter the name of a saved tag that you want to look for.

   You need to enter the full name of part of the name.
3. Click the play button to start the playback of the selected clip.
4. You can also export the clip or lock it to avoid deletion.

Search by event:

1. Define the time and date for the search.
2. Select the event type from the dropdown list.

   Some event types might not be available for the used cameras. Make sure that you have setup the desired event type recoridg before doing a search for an event type.
3. Click **Start Search** to display the search results.
4. Click the play button to start the playback of the selected clip.

Thumbnail images to preview a recording

This function is only available in OSD mode and not for all cameras.

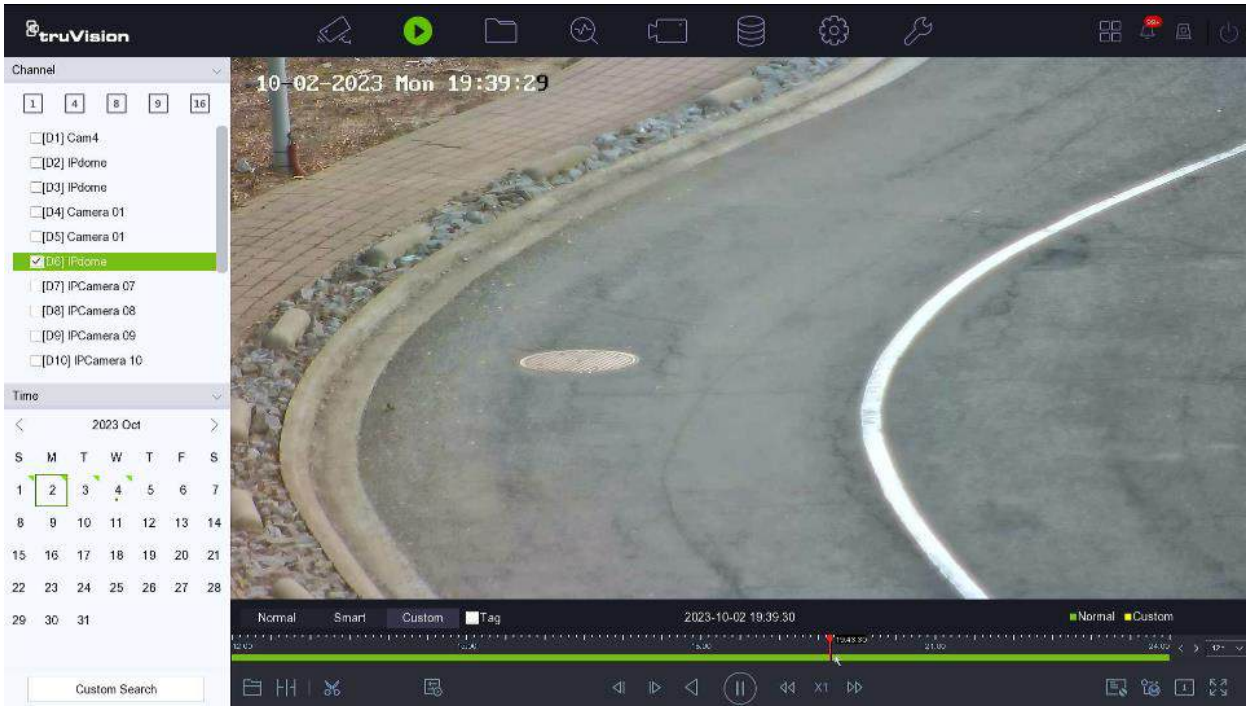
When in normal and smart playback, you can use thumbnail images that appear above the timeline to help guide you to a specific moment in the recording.

www.acornfiresecurity.com

www.acornfiresecurity.com

Hover the mouse on the timeline where you think the video of interest is located. A thumbnail of the video pops up (see Figure 24 below). If you are in Normal playback, play back starts from the spot where you click on the bar. If you are in Smart playback, play back starts from the nearest event on the bar.

Figure 24: Thumbnail image in playback



Instant playback

This function is available from the live view control toolbar in OSD mode (see page 181). When you click the icon, you can play back video recorded from the last five minutes for the selected camera. If no recording is found, then there was no recording made in the last five minutes. The five minutes cannot be adjusted. See “Live view control toolbar” on page 181 This function is not available in web mode.

Create tags

This function is only available in OSD mode.

You can bookmark the important scenes in a recorded file for later reference. A bookmarked recording is 10 seconds long.

To create a tag:

1. In playback mode, select the desired camera.

www.acornfiresecurity.com

www.acornfiresecurity.com

2. In the playback recording, click in the video tile, to see the audio and control toolbar.Move the timeline to where you want the bookmark to start. In the control toolbar, click the button and enter the tag name and click **Save**. The tag is saved.
3. To get a list of the tags saved for a camera, click File Managament > **Video** and then **Search By Tag**. Select the date and time range to search, the camera, and then click **Start Search**.

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.

To create video clips during playback:

1. In playback mode, select the desired camera.
2. Insert a USB flash drive in the recorder to archive the video clips.
3. Click the timeline where you want the video clip to start and click the **Clip** button in the toolbar. You will see that a small area of the timeline is highlighted by default, a clip is 10 minutes long. You can move the start and end line on the timeline to the desired time range. Or press the **Clip Time** button , to specifuy an exact start and end time for the clip. Click Export to export the selected clip to the USB stick. Or press the **Export Clip** button to export the clip.
4. Click **Export Clip** to save the clip. Select how you would like the clip file saved: with Player or as a video with its log. Click **OK**.
5. The Export screen appears. The size of the video clip file is displayed. Under *Device Name*, select the USB flash drive and click **Save**.
6. Repeat steps 3 to 5 for additional clips.

Digital zoom in playback

To digitally zoom in during playback:

1. In playback mode, select the desired camera.
2. Click the **Digital Zoom** button in the audio and video control toolbar. The camera image jumps to full-screen mode.
3. Right-click the mouse to quit the digital zoom mode and return to full-screen playback mode. The playback control toolbar reappears.

www.acornfiresecurity.com

www.acornfiresecurity.com

Chapter 17
Search recordings

This chapter describes how to search and play back recorded videos by different themes: video, snapshots, events, people, and vehicles.

Search in web mode

Search recordings in playback mode. See Chapter 15 “Playback in web mode” on page 193.

Search for recordings in web mode

You can search for recordings via the webpage or the OSD (see page 214 for the OSD).

The search for recordings in web mode will be visual (by clicking on the colored timeline) or can be based on a start time.

To search for recordings in web mode:

1. Click **Playback**.
2. Select a camera for which you want to see recorded video.
3. The timeline will show colors (green (continuous) and/or yellow (event)) to indicate that recordings were made for the camera (according to the configured settings).
4. Move the timeline by holding the left mouse button pressed while moving the mouse and click the play button to start playback.

   - Or –

   Enter a start time and press the enter button to search for recordings starting at that specific time.

   By default, the search will happen on the main stream. When dual stream recording was enabled, you can also search on the sub stream.

www.acornfiresecurity.com

www.acornfiresecurity.com

Search for snapshots in web mode

The recorder can save snapshots of several events.

You can search for stored snapshots via the webpage or the OSD (see page 211 for the OSD).

To search for snapshots in web mode:

1. Click **Snapshot**.
2. Select the camera for which you want to search for snapshots.
3. Select file type.
3. Enter the start and end date and time.

   The result will appear in the list. The snapshots can be downloaded on the PC.

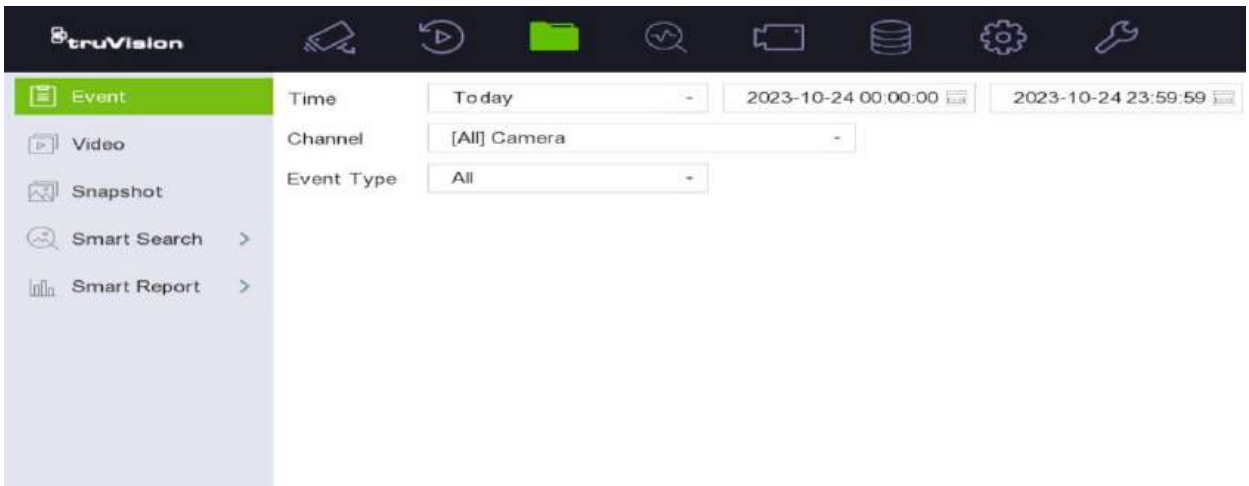
Note: The storage of event snapshots must be configured in the configuration settings for the events. Furthermore, it is also important to ensure that picture storage is enabled in the recorder.

Search recordings in OSD mode

To enter the Search menu in OSD mode, click the File Management icon in the top toolbar.

The window has five submenus that allow you to carry out different searches by theme.

Figure 25: The Search menu



www.acornfiresecurity.com

www.acornfiresecurity.com

Search type	Description
Event	Search all videos by time and date of recording and camera. You can search by the following event types: Alarm inputs, motion, face capture, cross line detection, intrusion, region entrance, region, exiting, unattended baggage, object removal, audio loss exception, sudden change of sound intensity, defocus, sudden scene change, fire detection, temperature detection, and temperature measurement pre-alarm, 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), Intrusion Alarm_BV (Verified Burglary), Intrusion Alarm_HV (Verified hold-up), Intrusion Alarm_JA (User code tamper), Panel Heartbeat Alarm, Arming Panel Alarm, and Disarming Panel Alarm. **Note**: Alarm input search: To search for recorded video that is based on an alarm input trigger, select the time and date and the appropriate alarm input. **Th**ere are more event types visible in the list, but they are not supported by the TruVision IP cameras.
Video	Search all videos by time and date of recording and camera. You can also search for tags and locked videos. Locked videos cannot be overwritten.
Snapshot	Search all video snapshots and related video clips by time and date of recording and camera.
Smart Search	Smart Search lets you search for faces, persons, vehicles
Smart Report	See page 130

Search results

A search will usually produce a list of recorded files, which may extend to several pages. The files are listed by date and time for each camera selected. The most recent file is listed first. Double-click a file to play it back on the screen alongside the search list. See Figure 26 below for an example of the results of a search.

You can view the recording of a search result for a selected camera. Double-click a search result and click the Play button. The playback of the file starts (see Figure 26 on page 211).

Each event is stored as a separate recording file.

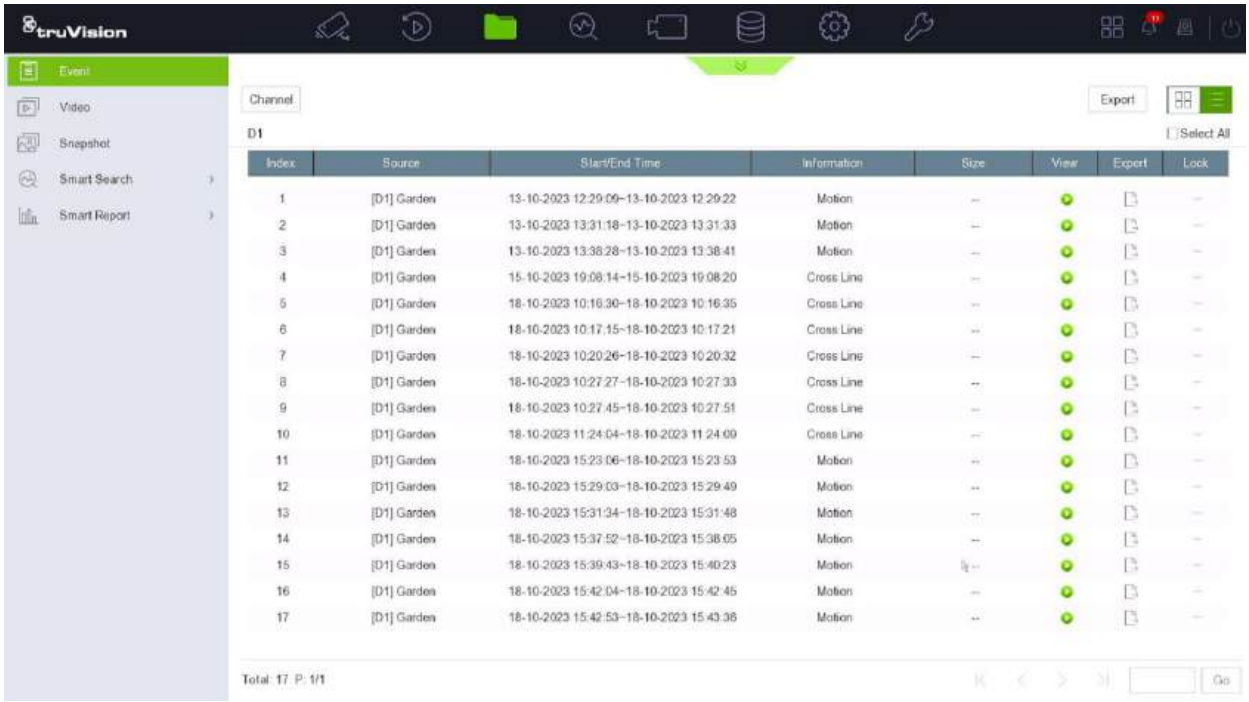
Only one file can be played back at a time.

You can export all or selected files to a backup device.

www.acornfiresecurity.com

www.acornfiresecurity.com

Figure 26: Example of a search result list



1. Click the camera for which you want to see the search results list.
2. Click a recording in the list to play it back on the screen. Click to start the playback.

Search for snapshots, bookmarks, or locked recordings

For information on creating bookmarks, see “Create ” on page 206.

To search for snapshots, bookmarked or locked recordings in OSD mode:

1. Click the **File Management** icon in the top toolbar. The Search menu appears.
2. For bookmarked video: In the File Management menu, click **Video** and then**Search by Tag**.

   For locked recordings: In the **File Management** menu, click Video and then **Search by Appearance**. Select **Locked** as **File Status**.
3. **Optional:** If Search by Tag ” has been selected, enter the name of the tag. The text box can be left empty.
4. Select the start and end times of the recording.
5. Select the desired camera(s).
6. Click **Start Search**. The list of snapshot/tags/locked files appears.
7. Select the desired recording and then click the **Play** button to play back a recording.

Search recordings by event type

You can search recorded videos by event type.

www.acornfiresecurity.com

www.acornfiresecurity.com

To search recordings by event:

1. Click the File management icon in the top toolbar The Search menu appears.
2. In the Search menu, click **Event**.
3. Select the desired event type from the drop-down list or select **All**.
4. Select the start and end times of the recording.
5. Select the desired cameras.
6. Click **Search**. The list of search results appears. The event type is listed for each recording.
7. Select the desired recording and then click the **Play** button to play back a recording.

Smart search

The TVN 23 (S/P) can do smart search for faces, persons and vehicles based on attributes, seen in the video content. This is also based on the intelligence of the connected cameras.

At the moment we have TruVision cameras that support attribute search for faces and vehicles. The attribute search for persons is at this moment not supported by any TruVision camera.

Appearance search for faces

This feature works only with the TruVision P series PTZ camera TVGP-p01-0401-PTZ-G.

This camera has different VCA settings. One of the settings is called Face Picture Comparison.

The camera is able to capture faces. These faces (snapshots and event video) can be recorded by the TVN 23 (S/P) and within the recorder's OSD there is a possibility to do a search based on specific 'attributes' of the recorded face.

This allows the end-user to search for recorded video and snapshots based on:

- Gender: male/female
- Glasses: with/without
- Wearing a mask: yes/no
- (Age)
- (face expression)

www.acornfiresecurity.com

www.acornfiresecurity.com

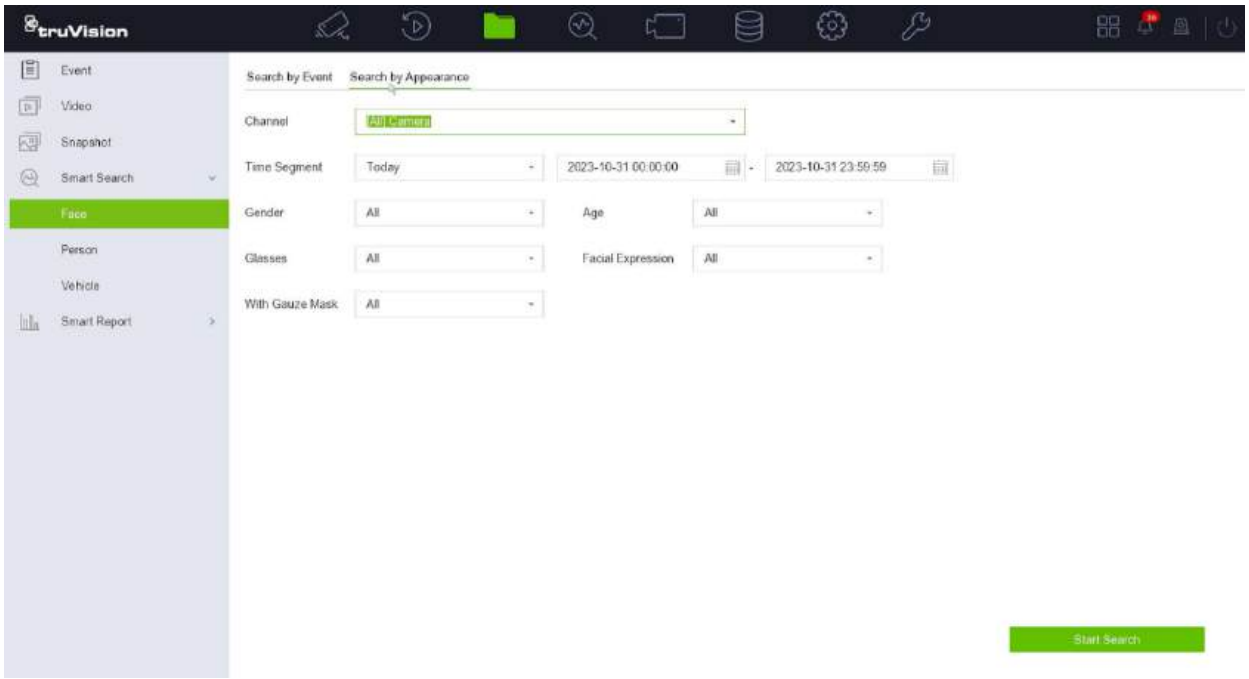
Note:

The age classification doesn't work very accurate.

The face expression is not supported by the TruVision camera.

To use this feature:

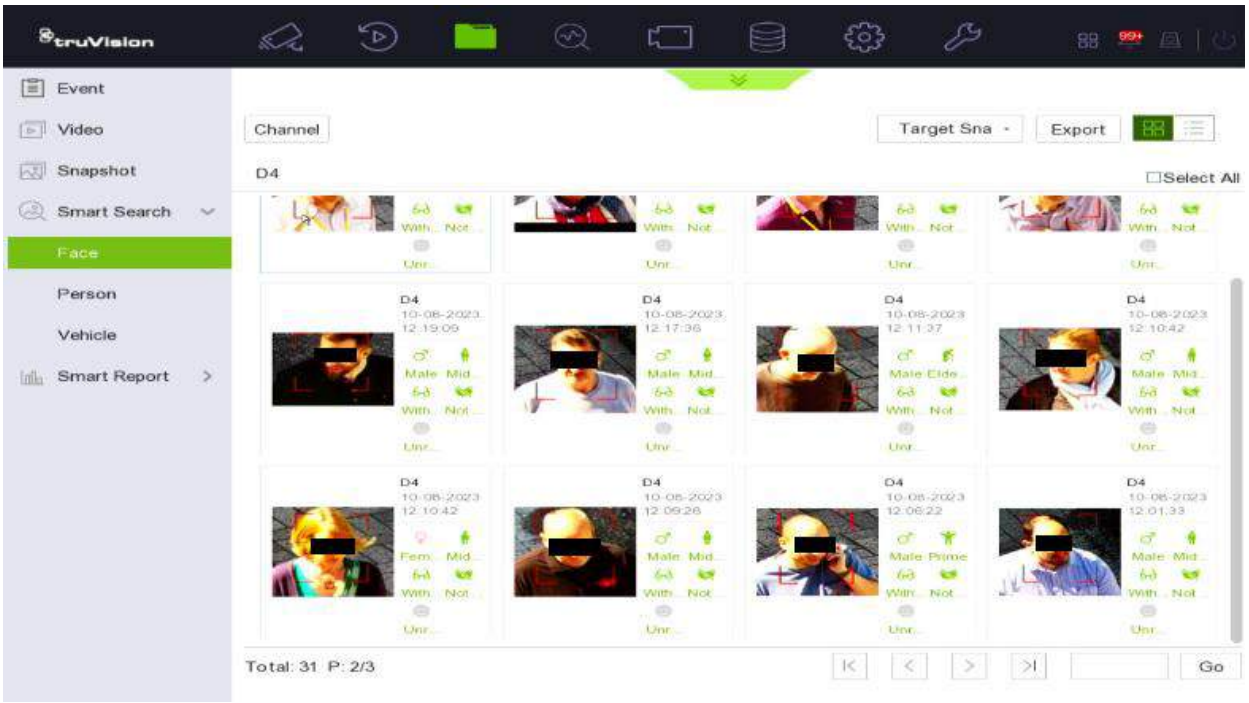
1. Use a TVGP-P01-0401-PTZ-G PTZ camera and make sure the VCA resources are set-up for Face Capture Comparison. Add the camera to the TVN 23 (S/P).
2. Let the camera capture faces.
3. Go to **File Management** > **Smart Search** > **Face** > **By Appearance**.
4. Select the camera from the dropdown list and select the necessary search options (date/time, attributes).



5. Click **Start Search** and the results will be shown as small, cropped face pictures.

www.acornfiresecurity.com

www.acornfiresecurity.com



In this example, the person is seen as a male, middle aged person with glasses an no mask.

By clicking on the cropped image, you will see the recorded video.

Appearance search for vehicles

The following cameras can be used to record license plates and vehicle attributes:

- TruVision S Series ANPR cameras
- TruVision P Series PTZ cameras (with Road Traffic as VCA source)

Besides license plate capturing, these cameras can also detect extra vehicle attributes:

- Vehicle color
- (Vehicle brand)
- (Vehicle type)
- License plat color

www.acornfiresecurity.com

www.acornfiresecurity.com

The vehicle brand and vehicle type can be detected but are not 100% accurate.

To use this feature:

1. Make sure you use one of the supported cameras and connect them to the TVN 23 (S/P). Let them capture some vehicles.
2. Go to **File Management** > **Smart Search** > **Vehicle** > **By Appearance**.

Select the camera from the dropdown list and select the necessary search options (date/time, attributes).

www.acornfiresecurity.com

www.acornfiresecurity.com

Chapter 18
UltraSync related functions

This chapter describes the different UltraSync-related functions and how to use them with this recorder.

Introduction

By connecting the recorder to UltraSync, the recorder can be used with the different UltraSync service levels.

Service levels and functionalities

There are four UltraSync service levels for video.

Core Video

This is the basic service level.

It contains the following features:

- UltraSync connectivity
- Recorder provisioning on the UltraSync portal
- Shows the site details
- Remote web page access for recorders for installers via the UltraSync portal
- Use of the TVRMobile app with UltraSync
- Use of the Advisor Advanced Pro app with video support over UltraSync (standalone video in the app without a link to intrusion panel events.)

UltraSync connection and recorder provisioning

The cloud connection via UltraSync is explained in “Connect the recorder to UltraSync” on page 86.

www.acornfiresecurity.com

www.acornfiresecurity.com

Site details

1. Log in to the UltraSync web portal https://webportal-eu.ultraconnect.com/login.

2. Click the menu icon .
3. Select **Operational Status**.

   A list with all the connected sites is displayed.
4. For each site, click the icon to see more details.

Remote webpage access

An installer can access the webpage of the recorder via the UltraSync web portal to do remote troubleshooting and (limited) remote maintenance.

Remote webpage access cannot be done without the approval of the end-end user.

To get access to the webpage:

1. Log in to the UltraSync web portal https://webportal-eu.ultraconnect.com/login.
2. Click the menu icon .
3. Select **Operational Status**.

   A list with all the connected sites is displayed.
4. Select the site for the remote webpage session.
5. Click to open the operational status screen of the recorder.
6. As an installer, you must first request approval from the end-end user before you can access the webpage. At the bottom of the screen, click **Request** for the **Recorder Webpage Access** function to start the process to access the recorder webpage.

Recorder Functions	
Recorder Webpage Access	Request

   You will be asked to confirm the request. When confirmed, an approval request is sent to the TVRMobile users that have the **Operator** user permission for the recorder.

   Only app users with the Operator permission receive the request. Before the app users can receive the message, they need to have **enabled alarm notifications** in the app.

   Once the end-user has approved, the installer will have 20 minutes access time to the webpage of the recorder.
7. Go to the **Remote Control** tab in the Operational Status webpage and wait until the webpage is loaded. Once the page is open, you can log in to the webpage for the next 20 minutes.

www.acornfiresecurity.com

www.acornfiresecurity.com

Use TVRMobile

See “Add the recorder to TVRMobile” on page 92 for further information.

Core Video Plus

This service level contains all the Core Video features plus:

- Show the operational status of recorders for installers in the UltraSync portal
- Cloud firmware upgrade
- Show system events in the UltraSync portal
- Transfer of system events to a CMS (Control Monitoring Station) over IP

To see the operational status

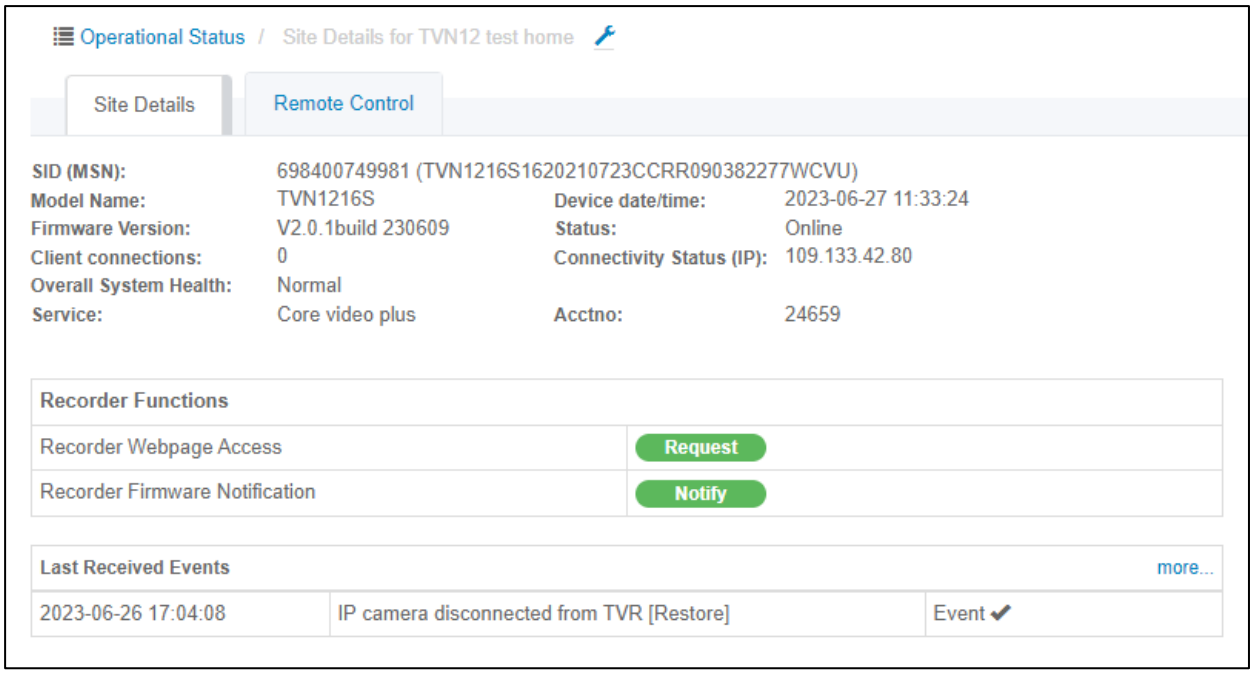
1. Log in to the UltraSync web portal https://webportal-eu.ultraconnect.com/login.
2. Click the menu icon .
3. Select **Operational Status**.

   A list with all the connected sites is displayed.
4. For sites/recorders that are subscribed to the Core Plus Video service, you can see if the recorder is online/offline in the table. The recorder details will be shown in green when the recorder is online and in red when the recorder is offline.
5. To see further details for an online recorder, click to open the operational status screen of the recorder. Once the screen opens, the actual status of the recorder is being retrieved and shall be displayed.

   You will see a similar screen like this:

www.acornfiresecurity.com

www.acornfiresecurity.com



The screen contains the following information:

1. **SID (MSN):** the SID number of the recorder and the recorder's serial number
2. **Model Name:** the recorder's model name
3. **Firmware Version:** the recorder's firmware version
4. **Client connections:** the number of mobile application connections that are currently being used
5. **Overall System Health:** an overall system status for the recorder, defined on the information that is received by the portal.
6. **Device date/time:** the date and time of the recorder at the moment the status was retrieved.
7. **Status:** Online/Offline. The network connection status of the recorder at the moment the data was retrieved.
8. **Connectivity Status (IP):** the WAN IP address used by the recorder.

Cloud firmware update

There are two ways to update the firmware via UltraSync.

- The firmware can be upgraded by a technician who is on-site or who is doing a remote session via the UltraSync portal.
- The firmware can be upgraded by the end-user that receives an information message via TVRMobile.

Firmware upgrade by a technician

See "Upgrade system firmware" on page 32 in this manual.

www.acornfiresecurity.com

www.acornfiresecurity.com

Firmware upgrade by an end-user

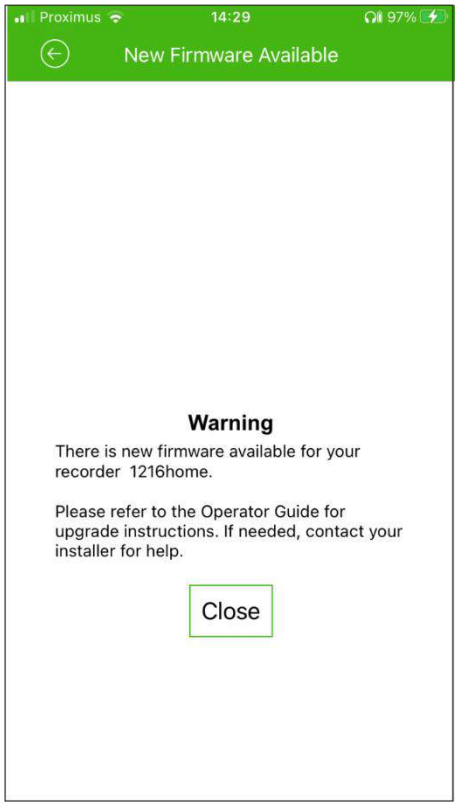
1. The end-user can upgrade the recorder too.
2. The installer can send an information message to the TVRMobile app for Operator users of the recorder.
3. The end-users do not need to acknowledge this message.

To inform the end user to upgrade the firmware:

1. Log in to the UltraSync web portal https://webportal-eu.ultraconnect.com/login
2. Click the menu icon .
3. Select **Operational Status**.

   A list with all the connected sites is displayed.
4. Select the site for the remote webpage session.
5. Click to open the operational status screen of the recorder.
6. At the bottom of the screen, click **Notify** to send a notification to the end user.

The Operator users of the TVRMobile app will receive a message in the app that a new firmware is available for the recorder.



www.acornfiresecurity.com

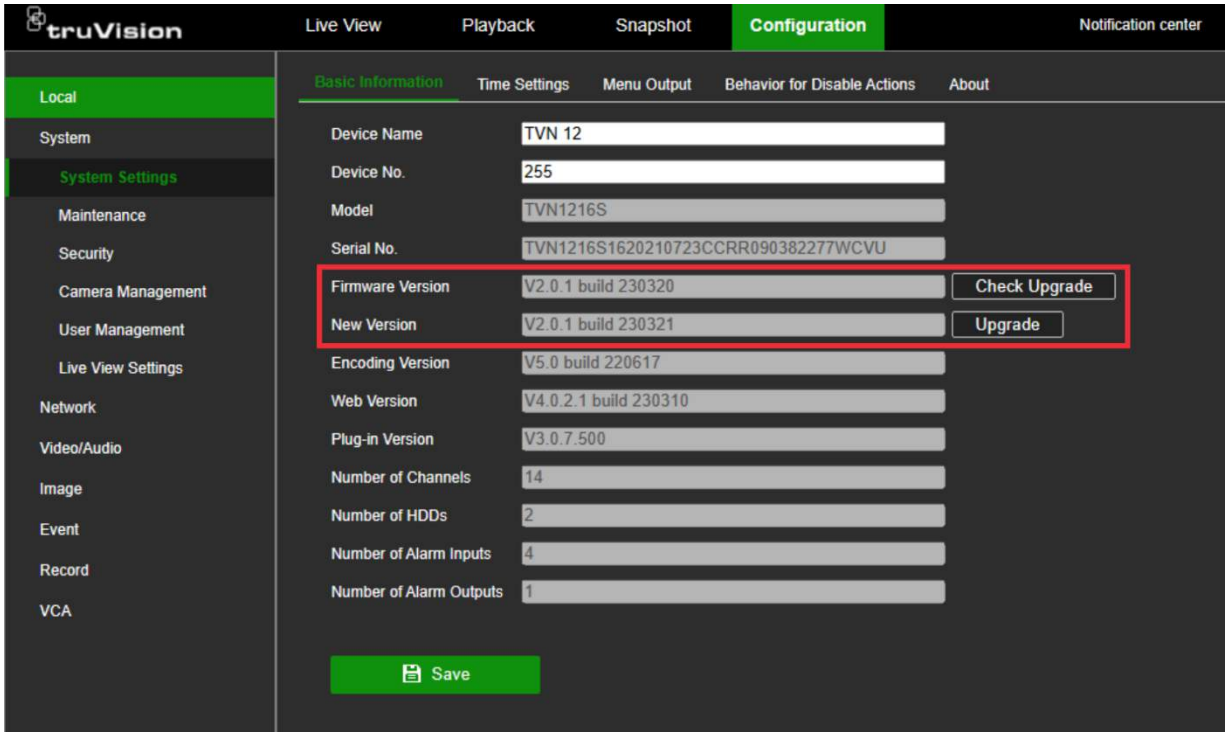
www.acornfiresecurity.com

The end-user can upgrade the recorder. The end-user can find instructions in the Operator guide, which is available on our website.(https://firesecurityproducts.com)

Upgrade by the end-user via the recorder's webpage:

1. Log in to the recorder's webpage
2. Go to **Configuration** > **System** > **System Settings**.
3. You see the current firmware version and a line called **'New version'** with the details of the new firmware.

   Note: The "New Version" information will appear for one minute when you open the screen. After one minute the line with the new firmware version will disappear. Click **Check Upgrade** again to see the new version again (and the Upgrade button).

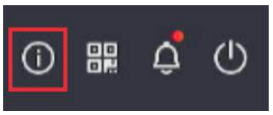


4. Press **Upgrade** to start the upgrade of the recorder. You will see a message that the device cannot be operated during the upgrade process.

   Press **Yes** to start the upgrade. After the upgrade, the recorder will reboot automatically.

Upgrade by the end-user via the recorder's OSD menu:

1. Right click in the live view and select **Menu**.
2. Log in to the menu with the username and password.
3. Click the Information icon at the top right of the screen:

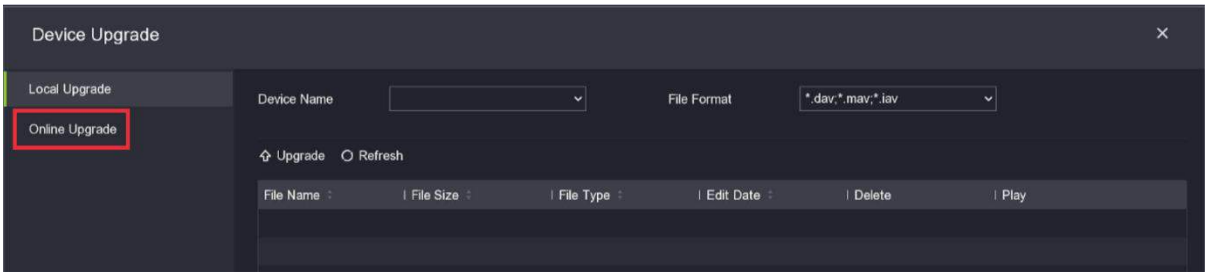


   The recorder information window appears.

www.acornfiresecurity.com

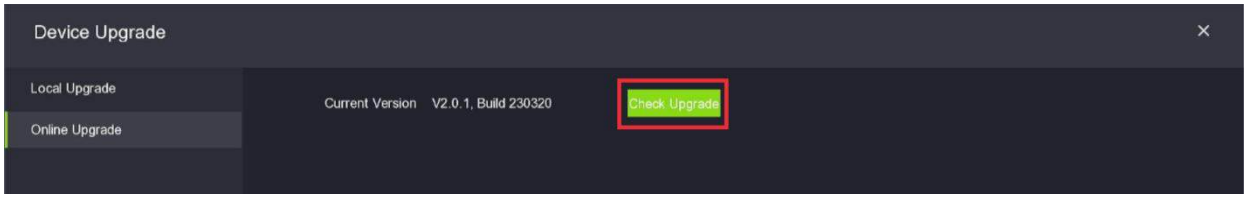
www.acornfiresecurity.com

4. Click the upgrade icon to open the **Device Upgrade** screen.
5. Select **Online Upgrade**.



The current firmware version is shown.

6. Press the **Check Upgrade** button.



7. If a new firmware version is detected on the UltraSync server, then it will appear on the screen.
8. Click **Upgrade** to start the upgrade process.

You will see a message that the device cannot be operated during the upgrade process. Press **Yes** to start the upgrade.

9. After the upgrade, the recorder will reboot automatically.

Recorder system events reporting

The recorder is able to send specific system events to UltraSync that can be seen in the portal or forwarded to a control monitoring station (CMS).

The following events can be reported:

- Specific recorder events:
  - Hard drive errors
  - Illegal login/invalid user credentials
  - PoE power exception (for recorders with PoE ports)
  - Network disconnection
  - Unexpected reboot
- Camera event:
  - Video loss (via the Video Loss event)/IP camera disconnection

www.acornfiresecurity.com

www.acornfiresecurity.com

NOTE: to setup a recorder in the portal to report the system events to a CMS, see the portal documentation in the Content Library that can be accessed via the main menu of the portal.

Recorder settings to receive the system events in UltraSync and/or report the events to a CMS:

1. Make sure that firmware 2.0.1 is used by the recorder and the recorder
2. The service level for the recorder will have to be minimum Core Plus Video
3. For all the recorder events, no extra set-up is needed. They will be pushed to UltraSync when they appear.
4. For the video loss event, make sure you setup the video loss event for the required cameras and enable at least the 'Notify Surveillance Center' action. See page 98-99 for more details.

The recorders need at least the Core Plus Video service level to show the last received event in the Operational Status page when the operational status is requested.

UltraSync will retrieve the status of every recorder every 2 hours and will show the last update in the **Last Received Events** table.

When a system event is shown in the Operational Status page, you can manually refresh the status by pressing the **Request** button for the **Recorder System Events Status function**.

Recorder System Events Status	Request

If you want to see previous reported events (received over 24 hours), click on '**more…**' button.

Last Received Events		more...
2023-06-29 18:07:55	Camera connected	Event ✔

Enhance Video

This service level contains all the Core Plus Video features plus:

- Remote 'admin' password reset method
- Extra health diagnostics information and dashboard view

Remote 'admin' password reset method

A temporary password will be created by UltraSync and sent to the recorder upon request of the installer. An on-site technician can enter this temporary password as 'admin' password. If the temporary password matches the password that was received by the recorder, the technician will be able to create a new 'admin' password via the OSD or webpage (LAN connection).

www.acornfiresecurity.com

www.acornfiresecurity.com

In case the technician remembers the admin password after the temporary password was created, he can still use the admin password to login to the recorder.

To create a temporary admin password:

1. Log in to the UltraSync web portal https://webportal-eu.ultraconnect.com/login.
2. Click the menu icon .
3. Select **Operational Status**.

   A list with all the connected sites is displayed.
4. Select the site for the remote admin password.
5. Click to open the operational status screen of the recorder.
6. You see a screen such as shown below:

www.acornfiresecurity.com

www.acornfiresecurity.com

Operational Status / Site Details for TVN12 test home

Site Details | Remote Control

SID (MSN):	698400749981 (TVN1216S1620210723CCRR090382277WCVU)		
Model Name:	TVN1216S	Device date/time:	2023-06-27 11:36:00
Firmware Version:	V2.0.1build 230609	Status:	Online
Client connections:	0	Connectivity Status (IP):	109.133.42.80
Overall System Health:	Normal		
Service:	Enhance Video	Acctno:	24659

Camera Name	Channel Number	IP Address	Camera Status
Garden	1	192.168.0.10	Online
IPCamera 03	3	192.168.254.4	Offline
IPCamera 04	4	192.168.254.5	Offline
IPCamera 05	5	192.168.254.6	Offline
IPCamera 06	6	192.168.254.7	Offline
IPCamera 07	7	192.168.254.8	Offline
IPCamera 08	8	192.168.254.9	Offline
IPCamera 09	9	192.168.254.10	Offline
IPCamera 10	10	192.168.254.11	Offline
IPCamera 11	11	192.168.254.12	Offline
IPCamera 12	12	192.168.254.13	Offline
IPCamera 13	13	192.168.254.14	Offline
IPCamera 14	14	192.168.254.15	Offline
IPCamera 15	15	192.168.254.16	Offline
IPCamera 16	16	192.168.254.17	Offline

Recorder Functions	
Password	Reset
Recorder System Events Status	Request
Recorder Webpage Access	Request
Recorder Firmware Notification	Notify

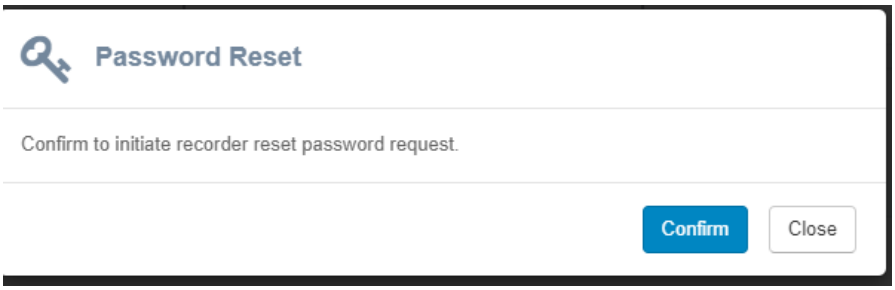
Last Received Events		more...
2023-06-26 17:04:08	IP camera disconnected from TVR [Restore]	Event ✔

7. At the bottom of the screen, you see the extra recorder functions that are available for the Enhance Video service.
8. Press **Reset** to initiate the ‘admin’ password reset process.

   You will see a confirmation pop-up message:

www.acornfiresecurity.com

www.acornfiresecurity.com



9. Press **Confirm**.

   A 12-digit random temporary password will be created and will be sent to the recorder.

10. Click the ‘eye’ icon to display the password.

   You can copy this temporary password to the clipboard so that it can be shared via email with a technician onsite.

11. Enter the temporary password as password for the admin user in the recorder’s UI (OSD or webpage). The recorder will then ask you to create a new admin password.

   The temporary password is valid for 30 minutes, after it is created.

   If the code is not used within 30 minutes, a new code will need to be created.

Note:

- A maximum of <u>three password resets</u> can be done <u>for the same recorder</u> within 24 hours. The 24 hours starts counting as soon as the first temporary code is created.
- During the time that a temporary password is valid (30 minutes), no remote webpage access request can be done via the UltraSync portal.

Extra health diagnostics information and dashboard view

Extra health diagnostics information

The status of the connected cameras (green = online, offline = red) is shown on the Operational Status page along with the camera name and their (LAN) IP address.

www.acornfiresecurity.com

www.acornfiresecurity.com

Site Details | Remote Control

SID (MSN):	698400749981 (TVN1216S1620210723CCRR090382277WCVU)		
Model Name:	TVN1216S	Device date/time:	2023-07-01 10:52:23
Firmware Version:	V2.0.1build 230609	Status:	Online
Client connections:	0	Connectivity Status (IP):	109.133.42.80
Overall System Health:	Normal		
Service:	Enhance Video	Acctno:	24659

Camera Name	Channel Number	IP Address	Camera Status
Garden	1	192.168.0.10	Online
Parking lot	2	192.168.0.250	Online
IPCamera 03	3	192.168.254.4	Offline
IPCamera 04	4	192.168.254.5	Offline
IPCamera 05	5	192.168.254.6	Offline

Dashboard view

The dashboard gives you general information about the installed base and its status.

To see the dashboard

1. Log in to the UltraSync web portal https://webportal-eu.ultraconnect.com/login.
2. Click the menu icon ☰.
3. Select **Dashboard.**

Note: the dashboard is common for recorders and intrusion panels. So some numbers/graphs will be more relevant for intrusion panel than for recorders.

At the top of the dashboard, you can see general information for the installed products:

- Total number of sites
- Number of deactivated products
- Number of recently registered products
- Number of devices with low signal (not relevant for recorders)
- Number of sites for which no (system) events were received.

www.acornfiresecurity.com

www.acornfiresecurity.com

You can click on each of these numbers to see the table with the recorders behind the number.

Below the numbers, you find a set of graphs:

- Pie chart with information about the service levels
- Pie chart with information about the monitoring type (self-monitoring or reporting to a CMS)
- Bar chart with the number of sites that were added in the last 30 days
- Pie chart with activated/deactivated sites
- A bar chart with an indication of the number of recorders with a network issue/network restore

For more information about the service levels and signing up as an installer to use the UltraSync services, please contact your Aritech sales manager.

For more information about the use of the UltraSync web portal, open the main menu and select Content Library. The content library contains portal documentation and other useful information.

www.acornfiresecurity.com

www.acornfiresecurity.com

Appendix A
Specifications

	TVN 2308S	TVN 2316(S)	TVN 2332
Recording			
Video compression	H.265+/H.265/H.264+/H.264		
Encoding resolution	32 MP*/24 MP*/12 MP/8 MP/6 MP/5 MP/4 MP/3 MP/1080p/UXGA/720p/VGA /4CIF/DCIF/ 2CIF/CIF/QCIF (*) Current TruVision IP cameras support up to 12 MP)		
Decoding Capacity	2-ch@32 MP (25 fps)*/3-ch@24 MP (25fps)*/6-ch@12 MP (25 fps)+1-ch@8 MP (25fps)/10-ch@8 MP (25 fps)/20-ch 4 MP (25fps)/40-ch 1080P (25fps) (*) Current TruVision IP cameras support up to 12 MP) (		
Stream type	Video, Video & Audio		
Dual Stream Recording	Supported		
Audio compression	G.711ulaw/G.711alaw/G.722/G.726/AAC/MP2L2		
Video & audio			
IP video input	8-ch	16-ch	32-ch
	Up to 32 MP resolution (Current TruVision IP cameras support up to 12 MP)	Up to 32 MP resolution (Current TruVision IP cameras support up to 12 MP)	Up to 32 MP resolution (Current TruVision IP cameras support up to 12 MP)
Incoming bandwidth	128 Mbps	256 Mbps	320 Mbps
Outgoing bandwidth	256 Mbps	256 Mbps	400 Mbps
HDMI 1 output	8K (7680 × 4320)/60Hz, 4K (3840 × 2160)/60Hz, 4K (3840 × 2160)/30Hz, 2K (2560 × 1440)/60Hz, 1920 × 1080/60Hz, 1600 × 1200/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz		
HDMI 2 output	4K (3840 × 2160)/60Hz, 4K (3840 × 2160)/30Hz, 2K (2560 × 1440)/60Hz, 1920 × 1080/60Hz, 1600 × 1200/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz		
VGA output	1920 × 1080/60Hz, 1600 × 1200/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz		
Video output mode	HDMI1/VGA simultaneous output, HDMI2/VGA independent output		
BNC output	1-ch, BNC (1.0 Vp-p, 75 Ω), resolution: PAL: 704 × 576, NTSC: 704 × 480		

www.acornfiresecurity.com

www.acornfiresecurity.com

	TVN 2308S	TVN 2316(S)	TVN 2332
Audio output	1-ch, RCA (Linear, 1 kΩ)		
Bi-directional audio	1-ch, RCA (2.0 Vp-p, 1 KΩ, using the audio input)		
Synchronous playback	8-ch	16-ch	16-ch
Auxiliary interface			
USB interface	Front panel: 2 × USB 2.0; Back panel: 1 × USB 3.0		
eSATA	1 eSATA interface		
Serial Interface	2 RS-485 (half-duplex), 1 RS-232		
Alarm In/Out	16/9		
Ctrl 12V	Controllable 12 VDC, 1 A power output for external alarm device; The power will be turned on when the alarm output is triggered. *: The Ctrl 12V power is controlled by alarm output 9.		
DC 12V	12 VDC, 1 A power output		
Hard drives			
SATA	4 SATA interfaces		
Capacity	Up to 10 TB capacity for each disk		
Network			
Remote connection	128		
Network protocol	TCP/IP, DHCP, IPv4, IPv6, DNS, DDNS, NTP, RTSP, SADP, SMTP, SNMP, NFS, UPnP™, HTTP, HTTPS, UltraSync		
Network interface	1, RJ-45 10/100 Mbps self-adaptive Ethernet interface	TVN 2316S: 1, RJ-45 10/100 Mbps self-adaptive Ethernet interface TVN2316: 2, RJ-45 10/100/1000 Mbps self-adaptive Ethernet interfaces	2, RJ-45 10/100/1000 Mbps self-adaptive Ethernet interfaces
PoE			
Interface	8, RJ-45 10/100 Mbps self-adaptive Ethernet Interface	TVN 2316: NA TVN 2316S: 16, RJ-45 10/100 Mbps self-adaptive Ethernet interface	NA
Power	≤ 150 W	TVN 2316: NA TVN 2316S: ≤ 200 W	NA
Standard	IEEE 802.3 af/at	TVN 2316: NA TVN 2316S: IEEE 802.3 af/at	NA
General			
Power supply	100 to 240 VAC, 50 to 60 Hz		

www.acornfiresecurity.com

www.acornfiresecurity.com

	TVN 2308S	TVN 2316(S)	TVN 2332
Power consumption (without HDD)	≤ 15 W (without HDD and PoE off)	≤ 15 W (without HDD and PoE off)	≤ 15 W (without HDD)
Operating temperature		-10 to +55 ºC	
Relative humidity		10 to 90%	
Dimensions (W x D x H)		445 × 400 × 75 mm	
Weight (without HDD)		≤ 5 kg (without HDD)	

	TVN 2316P	TVN 2332P	TVN 2364P
Recording			
Video compression		H.265+/H.265/H.264+/H.264	
Encoding resolution		32 MP*/24 MP*/12 MP/8 MP/6 MP/5 MP/4 MP/3 MP/1080p/UXGA/720p/VGA /4CIF/DCIF/ 2CIF/CIF/QCIF (*) Current TruVision IP cameras support up to 12 MP	
Decoding capability		2-ch@32 MP (25 fps)*/3-ch@24 MP (25fps)*/6-ch@12 MP (25 fps)+1-ch@8 MP (25fps)/10-ch@8 MP (25 fps)/20-ch 4 MP (25fps)/40-ch 1080P (25fps) (*) Current TruVision IP cameras support up to 12 MP	
Stream type		Video, Video & Audio	
Dual Stream Recording		Supported	
Audio compression		G.711ulaw/G.711alaw/G.722/G.726/AAC/MP2L2/PCM	
Video & audio			
IP video input	16-ch	32-ch	64-ch
	Up to 32 MP resolution (Current TruVision IP cameras support up to 12 MP)	Up to 32 MP resolution (Current TruVision IP cameras support up to 12 MP)	Up to 32 MP resolution (Current TruVision IP cameras support up to 12 MP)
Incoming bandwidth	256 Mbps	320 Mbps	400 Mbps
Outgoing bandwidth	256 Mbps	400 Mbps	400 Mbps
HDMI 1 output		8K (7680 × 4320)/30Hz, 4K (3840 × 2160)/60Hz, 4K (3840 × 2160)/30Hz, 2K (2560 × 1440)/60Hz, 1920 × 1080/60Hz, 1600 × 1200/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz	
HDMI 2 output		4K (3840 × 2160)/60Hz, 4K (3840 × 2160)/30Hz, 2K (2560 × 1440)/60Hz, 1920 × 1080/60Hz, 1600 × 1200/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz	
VGA 1 output		1920 × 1080/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz	
VGA 2 output		1920 × 1080/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz	
BNC output		1-ch, BNC (1.0 Vp-p, 75 Ω), resolution: PAL: 704 × 576, NTSC: 704 × 480	

www.acornfiresecurity.com

www.acornfiresecurity.com

	TVN 2316P	TVN 2332P	TVN 2364P
Video output mode	HDMI 1 and VGA 1 provide simultaneous video output, and work as the main output; HDMI 2 and VGA 2 provide simultaneous video output, and work as the auxiliary output		
Audio output	2-ch, RCA (Linear, 1 KΩ)		
Bi-directional audio	1-ch, RCA (2.0 Vp-p, 1 KΩ, using the audio input)		
Synchronous playback	16-ch	16-ch	16-ch
Auxiliary interface			
USB interface	Front panel: 1 × USB 2.0; Back panel: 1 × USB 2.0		
eSATA	1 eSATA interface		
Serial Interface	1 RS-485 (full duplex), 1 RS-232		
Alarm In/Out	16/9		
Ctrl 12V	Controllable 12 VDC, 1 A power output for external alarm device; The power will be turned on when the alarm output is triggered. *: The Ctrl 12V power is controlled by alarm output 9.		
DC 12V	12 VDC, 1 A power output		
Hard drives			
SATA	8 SATA interfaces		
Capacity	Up to 10 TB capacity for each disk		
RAID			
RAID Type	RAID0, RAID1, RAID5, RAID6, RAID10. The minimum disk size for RAID is 4 TB/disk. It is recommended to use Enterprise hard drives.		
Network			
Remote connection	128		
Network protocol	TCP/IP, DHCP, IPv4, IPv6, DNS, DDNS, NTP, RTSP, SADP, SMTP, NFS, UPnP™, HTTP, HTTPS, UltraSync		
Network interface	2 RJ-45 10/100/1000 Mbps self-adaptive Ethernet interfaces		
General			
Power supply	100 to 240 VAC, 50 to 60 Hz		
Power consumption (without HDD)	≤50 W	≤ 50W	≤ 50W
Operating temperature	-10 to +55 ºC		
Relative humidity	10 to 90%		
Dimensions (W x D x H)	445 × 465 × 93 mm 385 × 315 × 52 mm		
Weight (without HDD)	≤ 10 kg		

www.acornfiresecurity.com

Appendix B
Port forwarding info

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. Used to record video remotely.
Port: 7681	WebSocket (HTTP)	Use for live view on non-IE browsers.
Port: 1024	RTSP Port for 3G/4G	Use with mobile apps. 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.

www.acornfiresecurity.com

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 router, please contact your router manufacturer or internet service provider for further assistance.

www.acornfiresecurity.com