TruVision Navigator 9.4 SP3 User Manual

P/N 1073689-EN • REV N • ISS 17JUN26

Trademarks and patents

The TruVision Navigator 9.4 SP3 name and logo are trademarks of Kidde Global Solutions.

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

Manufacturer

KGS 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. KGS 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.

Contact information

EMEA: https://firesecurityproducts.com

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

Product documentation

Please scan the QR code to download the electronic version of the product documentation. The manuals are available in several languages.

End-user license agreement

BY DOWNLOADING, INSTALLING OR USING THE SOFTWARE, YOU AGREE TO BE BOUND BY THIS END USER LICENSE AGREEMENT (THE “AGREEMENT”). IF YOU DO NOT AGREE, DO NOT INSTALL, COPY OR USE THE SOFTWARE; YOU MUST DELETE OR DESTROY ANY COPY IN YOUR POSSESSION OR CONTROL. This Agreement is between you (“you” or “your”) and KGS Fire & Security. (“Licensor”) for the Software that accompanies this Agreement, including all associated media, printed or electronic documentation (collectively, the “Software”).

LIMITED ACCESS SOFTWARE: IF YOU HAVE OBTAINED A TRIAL VERSION OF THE SOFTWARE, YOUR ACCESS TO THE SOFTWARE WILL BE LIMITED AND YOU WILL NOT BE ABLE TO TAKE ADVANTAGE OF ALL OF THE SOFTWARE FEATURES UNLESS YOU OBTAIN A FULL LICENSE. TO OBTAIN ACCESS TO ADDITIONAL FEATURES, YOU MUST PURCHASE A FULL LICENSE FROM LICENSOR AND OBTAIN A KEY/CODE TO UNLOCK THE ADDITIONAL FEATURES.

FOR THE SAKE OF CLARITY, THE AGREEMENT SHALL APPLY

TO THE SOFTWARE, WHICH INCLUDES BOTH THE TRIAL VERSION AND THE FULL LICENSED VERSION.

1. License Grants. During the term of this Agreement and conditioned upon your full compliance with all of the Agreement's terms and conditions, Licensor grants to you the following licenses:

1.1. *Software*. Licensor grants to you a personal, nonexclusive, nonsublicensable, nontransferable revocable license to install and use the Software on any computer or similar device, such as a network server used to install or run the Software on other computers over a computer network.

1.2 *Documentation*. Licensor grants to you a personal, nonexclusive, nonsublicensable, nontransferable, revocable license to make and use a reasonable number of copies of documentation provided with the Software for your internal use in connection with your use of the Software; provided that you reproduce all copyright and other proprietary notices that are on the original copies.

2. License Limitations. The license(s) granted in Section 1 are conditioned upon your compliance with the following limitations:

2.1 *Reverse Engineering.* You may not decompile, decipher, disassemble, reverse engineer or otherwise attempt to access source code of the Software, or circumvent any technical limitations in the Software that limit or restrict access to or use of the Software or any content, file, or other work, except as expressly permitted by applicable law notwithstanding this limitation.

2.2 *No Distribution, Rental or Transfer.* You may not distribute, publish, rent, lease, lend, transfer, sublicense, disclose or otherwise provide the Software to any third party, except that the initial user of the Software may make a one-time permanent transfer of this Agreement and Software to another end user, provided the initial user retains no copies of the Software. This transfer must include all of the Software (including all component parts, the media and printed materials, documentation, any upgrades and this Agreement). The transfer may not be an indirect transfer, such as a consignment. Before the transfer, the end user receiving the Software must agree to all the terms and conditions of this Agreement. Prior to any such transfer, you must notify Licensor in writing of the name and address of the new end user.

2.3 *No Modification or Derivative Works*. You may not modify or create derivative works of the Software, in whole or in part.

2.4 *Proprietary Notices.* You may not remove any proprietary notices or labels on the Software or any copy thereof.

2.5 *Non-Permitted Uses*. Without limiting any of the foregoing, you may not make any use of the Software in any manner not expressly permitted by this Agreement.

2.6 *Not for Resale Software*. Software identified as "Not For Resale" or "NFR," may not be sold or otherwise transferred for value, or used for any purpose other than demonstration, testing or evaluation.

3. Reservation of Rights and Ownership. Licensor, its parent or its suppliers own all right, title and interest, including all intellectual property rights, in and to the Software and reserve all rights not expressly granted to you in this Agreement. The Software is protected by copyright and other intellectual property laws and treaties. All trademarks, logos, and service marks (collectively, "Marks") displayed on the Software are the property of Licensor or of their respective holders. You are not permitted to use any of the Marks without the applicable prior written consent of Licensor or such respective holders.

4. Additional Software or Services. This Agreement applies to any updates, supplements or add-on components to the Software as well as any services accessed through the Software or internet-based service components (if any) of the Software that Licensor may, in its sole discretion, provide or make available to you ("Update"). If Licensor provides additional terms along with the Update, those terms will apply to the Update. If Licensor provides you an Update, Licensor may, at its sole discretion, require you to use Update and cease use of early versions. Licensor reserves the right to discontinue any internet-based service (if any) provided or made available to you through the use of the Software.

5. Termination. This Agreement will automatically terminate upon your breach of any of this Agreement's terms and conditions. You may terminate this Agreement by removing the Software from your device(s). In the event of termination, you must immediately destroy all copies of the Software, whether on your device or otherwise in your possession. The following Sections of this Agreement will survive termination: Sections 2, 3 and 5 to 11.

6. WARRANTIES AND DISCLAIMERS.

6.1. Limited Warranty. Licensor warrants that, for a period of one (1) year from the date of receipt of the Software, the Software will perform substantially in accordance with the documentation that accompanies the Software. If the Software fails to comply with this limited warranty, Licensor will at its option either (a) repair or replace the Software or (b) return the price you paid. This limited warranty is void if failure of the Software results from accident, abuse, modification, misapplication, misuse, abnormal use or a virus. This warranty will apply to any replacement Software for the remainder of the original limited warranty period or 30 days, whichever period is longer. You agree that the limited warranty in this Section is your sole and exclusive warranty and remedy with respect to the Software.

6.2 DISCLAIMER OF WARRANTIES. EXCEPT AS SET FORTH IN SECTION 6.1, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW THE SOFTWARE IS PROVIDED *AS IS AND WITH ALL FAULTS.* LICENSOR AND ITS PARENT, AFFILIATES AND SUPPLIERS HEREBY DISCLAIM ALL OTHER WARRANTIES AND CONDITIONS, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING ANY IMPLIED WARRANTIES, DUTIES OR CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION OR NON-INFRINGEMENT, LACK OF VIRUSES OR BUGS, ACCURACY OR COMPLETENESS OF RESPONSES OR RESULTS WITH REGARD TO THE SOFTWARE. LICENSOR AND ITS PARENT, AFFILIATES AND SUPPLIERS DO NOT

WARRANT THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE OR THAT ANY DEFECTS WILL BE CORRECTED. THE ENTIRE RISK ARISING OUT OF THE SOFTWARE REMAINS WITH YOU.

7. EXCLUSIONS OF CERTAIN DAMAGES; Limitations of Liability. In no event WILL Licensor or its parent, affiliates OR suppliers be liable for any special, incidental, punitive, indirect or consequential damages (including damages for loss of profits, DAMAGES TO ANY COMPUTER, DEVICE, OR SYSTEM, LOSS OF DATA, goodwill, use or other losses) arising out of or in any way related to the SOFTWARE or this AGREEMENT, REGARDLESS OF the CAUSE OF ACTION OR THE BASIS OF THE CLAIM and even if Licensor has been advised of the possibility of the damages OR REMEDIES FAIL OF THEIR ESSENTIAL PURPOSE.

LICENSOR'S AND ITS PARENT'S, AFFILIATES' AND SUPPLIERS' ENTIRE LIABILITY UNDER THIS AGREEMENT AND YOUR EXCLUSIVE REMEDY WILL BE LIMITED TO THE ACTUAL DAMAGES YOU INCUR IN REASONABLE RELIANCE ON THE SOFTWARE UP TO THE PRICE YOU PAID FOR THE SOFTWARE. NO ACTION, REGARDLESS OF FORM, relating to the software MAY BE BROUGHT BY YOU MORE THAN ONE YEAR AFTER YOU HAVE KNOWLEDGE OF THE OCCURRENCE WHICH GIVES RISE TO THE CAUSE OF ACTION.

8. (Outside of the USA) Consumer End Users Only. The limitations or exclusions of warranties and liability contained in this Agreement do not affect or prejudice the statutory rights of a consumer (i.e., a person acquiring goods otherwise than in the course of a business). The limitations or exclusions of warranties, remedies or liability contained in this Agreement shall apply to you only to the extent such limitations or exclusions are permitted under the laws of the jurisdiction where you are located.

9. Third Party Software. The Software may contain third party software which requires notices and/or additional terms and conditions. Such required third party software notices and/or additional terms and conditions are available from the third party software provider, and are more a part of and incorporated by reference into this Agreement. Certain items of independent third party code may be included in the Software that is subjected to open source licenses ("Open Source Software"). The Open Source Software is licensed under the terms of the license that accompany such Open Source Software. Nothing in this Agreement limits your rights under, or grants you rights that supersede the terms and conditions of any applicable end user license for such Open Source Software.

10. Indemnification. You agree to defend, indemnify and hold harmless Licensor and its parent, affiliates and suppliers and their respective officers, directors and employees from all claims and expenses (including attorneys' fees and costs) that arise out of or in connection with your use of the Software, any breach of this Agreement, or your violation of any laws or regulations or the rights of any third party.

11. U.S. Government License Rights. Software provided to the U.S. Government pursuant to solicitations issued on or after December 1, 1995 is provided with the commercial license rights and restrictions described in this Agreement. Software provided to the U.S. Government pursuant to solicitations issued prior to December

1, 1995 is provided with “Restricted Rights” as provided for in FAR, 48 CFR 52.227-14 (JUNE 1987) or DFAR, 48 CFR 252.227-7013 (OCT 1988), as applicable.

12. **Compliance with Law; Export Restrictions.** You will comply with all applicable international and national laws, rules and regulations that apply to the Software and your use of the Software, including the U.S. Export Administration Regulations, as well as end user, end use, and destination restrictions issued by U.S. or other governments. You acknowledge that the Software is of U.S. origin and subject to U.S. export jurisdiction.

13. **Governing Law and Jurisdiction.** This Agreement will be construed and controlled by the law of the State of New York, without giving effect to its conflict of law provisions. Each party consents to exclusive jurisdiction and venue in the state and federal courts in the State of New York for any and all disputes, claims and actions arising from or in connection with the Software and this Agreement. The United Nations Convention on Contracts for the International Sale of Goods does not apply to this Agreement. Notwithstanding the above sentences of this Section 13, if you are a state, county, parish, or municipal governmental entity, division or unit within the United States, then this Agreement will be construed and controlled by the laws of your state and each party consents to exclusive jurisdiction and venue in the state and federal courts in your state for any and all disputes, claims and actions arising from or in connection with the Software and this Agreement.

14. **General.** The section titles in this Agreement are used solely for the parties’ convenience and have no legal or contractual significance. Any list of examples following "including" or "e.g.," is illustrative and not exhaustive, unless qualified by terms like "only" or "solely." Licensor’s failure to act with respect to a breach by you or others does not waive its right to act with respect to subsequent or similar breaches. No waiver of any provision of this Agreement will be effective unless it is in a signed writing, and no waiver will constitute a waiver of any other provision(s) or of the same provision on another occasion. If a court of competent jurisdiction holds any term, covenant or restriction of this Agreement to be illegal, invalid or unenforceable, in whole or in part, the remaining terms, covenants and restrictions will remain in full force and effect and will in no way be affected, impaired or invalidated. You may not assign, transfer or sublicense this Agreement or your rights (if any) under this Agreement. This Agreement will be binding upon all successors and assigns. This Agreement constitutes the entire agreement between you and Licensor with respect to the Software and merges all prior and contemporaneous communications and proposals, whether electronic, oral or written, between you and Licensor with respect to the Software. All notices to Licensor in connection with this Agreement must be in writing and will be deemed given as of the day they are deposited in the U.S. mails, postage prepaid, certified or registered, return receipt requested or sent by overnight courier, charges prepaid to the address set forth below.

Licensor information

If you have any questions about this Agreement, or want to contact Licensor for any reason, please direct all correspondence to:

KGS Fire & Security B.V.

Kelvinstraat 7, 6003 DH Weert, The Netherlands

Contents

Important information

Limitation of liability

To the maximum extent permitted by applicable law, in no event will KGS Fire & Security 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 KGS Fire & Security 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 KGS Fire & Security 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, KGS Fire & Security assumes no responsibility for errors or omissions.

Advisory messages

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

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

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

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

Chapter 1
Introduction

Overview

TruVision® Navigator represents the latest advancement in video management. The system delivers powerful software capabilities and allows users to manage their TruVision-based video surveillance systems. TruVision Navigator can be used as a standalone application or can be deployed as a client/server architecture, making it scalable for deployment in either small- or large-scale commercial environments.

TruVision Navigator is a video management system that allows users to monitor, manage, and investigate video surveillance systems.

With TruVision Navigator, you can:

- View live video from cameras
- Search and play back recorded video
- Manage devices such as cameras and recorders
- Respond to events and alarms
- Export video for investigation

The system can be deployed as a standalone application or as a client/server system, allowing it to scale from small installations to large multi-site environments.

TruVision Navigator supports integration with multiple subsystems, including video surveillance devices, access control systems, intrusion detection systems, and analytics-enabled cameras. The system can be deployed in both standalone and client/server architectures, allowing centralized management of devices and users across multiple sites. This scalability makes it suitable for both small installations and large enterprise environments

How to use this manual?

This manual is organized to guide you through installation, configuration, and daily operation of the system.

Chapter 2
Installation

Introduction

This chapter explains how to install TruVision Navigator and prepare the system for first use.

It provides step-by-step procedures for:

- Installing the software in both standalone and client/server environments
- Setting up client workstations
- Activating the system license
- Performing the initial login after installation
- Upgrading or uninstalling the application

Before starting the installation, ensure that the system meets the required hardware and software specifications (see Appendix A — Minimum System Requirements).

Installation options

There are two installation options for TruVision Navigator. The core features and functions remain the same regardless of which of the two installation options are selected.

- **Standalone Mode:** This installation option allows the client and database to reside on the same computer. No other clients on the network can connect to the database on this computer. This installation option is ideal for small, standalone systems. See “Installation – standalone mode” on page 22.
- **Multi-client Mode (traditional client/server):** This installation option allows the client and server to reside on the same or separate computers. It is suitable for larger systems with many geographically dispersed users, computers, and recording devices. See “Installation – client/server mode” on page 2323.

Administrator rights are required to install Navigator on a computer, but the application is available to any user that successfully logs in to a Windows® account on that computer.

Note: You must select the client/server installation, to use the people counting feature on a web browser.

Installation prerequisites

For each computer:

- Download the latest operating system service pack from the Microsoft Download Center.
- Check for Windows updates at http://update.microsoft.com.
- Download the latest video driver.
- For the minimum software and hardware requirements, see Appendix A “Minimum system requirements”.

Network and service requirements

The system relies on network communication and background services to function correctly.

Ensure that:

- Required communication ports for devices (HTTP, command ports, RTSP) are open
- Notification ports (default: 5001) are accessible for event transmission
- Required services, such as database services and local scheduling services, are running

If these requirements are not met, the system may experience issues such as missing video streams, failed connections to devices, or missing event notifications.

Installation – standalone mode

To install a new standalone instance of TruVision Navigator:

1. Double-click the TruVision Navigator Setup.exe installer to begin the installation. Right-click the Setup.exe file and select **Run as Administrator**.
2. If necessary, click **Yes** in the User Account Control window to make changes to the computer.
3. Ensure that the RSTP port used by all recorders is open so that live video can be viewed. The default RSTP port is 554.

4. The *End User License Agreement* window appears. Select the **I Accept these terms and conditions** check box and then click **Next** to continue.
5. The Welcome window appears. Select **Typical** or **Advanced** (to change the default installation location), and then click **Next**.
6. *Advanced installation only*: Accept the default installation folder or click **...** to select a different location and then click the **Next** button.
7. The Confirm Selections window appears. Click **Install**.
8. The WinPcap Setup Wizard appears. Click **Next** to continue.
9. The WinPcap License Agreement window appears. Click **I Agree** to continue.
10. The Installation options window appears. The **Automatically start the WinPcap driver at boot time check box** is selected by default. Click **Install** to continue.
11. Click **Finish** to continue.
12. Click **Close** to complete the installation.

Installation – client/server mode

To install a new client/server instance of TruVision Navigator:

1. Double-click the TruVision Navigator Setup.exe installer to begin the installation. If prompted, right-click the Setup.exe file and select **Run as Administrator**.
2. Click **Yes** to make changes to the computer.
3. The *End User License Agreement* window appears. Select the **I Accept these terms and conditions** check box and then click **Next** to continue.
4. The *Welcome* window is displayed. Select **Advanced** for a client/server installation, and then click **Next**.
5. The *Installation Folder* window appears. Click the **Next** button to accept the default installation folder or click **...** to select a different location.
6. The Configuration window appears. Select **Client/Server Mode** and click **Next** to continue.
7. The Type of Database window appears. Select **Use internal database** (recommended option) and then click **Next**. If the organization requires use of Microsoft SQL Server and it is already installed, select **Use Microsoft SQL Server** and then click **Next**.

   Note: Aritech will not be responsible for SQL Server errors or issues.
8. The Confirm Selections window appears. Click **Install**.
9. The WinPcap Setup Wizard appears. Click **Next** to continue.

10. The WinPcap License Agreement window appears. Click **I Agree** to continue.
11. The Installation options window appears. The **Automatically start the WinPcap driver at boot time check box** is selected by default. Click **Install** to continue.
12. Click **Finish** to continue.
13. Click **Close** to complete the installation.

Note: Recorders connected to the network must be reachable over the network from the Navigator server computer. If there are firewalls between the server computer and the recorder network, make sure to open the following inbound ports into the recorder network:

- The HTTP ports used by all recorders on the network.
- The Command ports used by all recorders on the network.

By default, recorders use 80 for HTTP and 8000 for Command traffic. If the server computers can't connect to the recorders, the following features will not work:

- Automatic Diagnostic Polling.
- Device Health Checking.

WinPcap issues and workaround

The installation of TruVision Navigator will fail, when a different version (to what the software needs) of WinPcap libraries is detected in the Windows System folders.

To fix this, follow these steps:

1. Stop the TruVision Navigator Setup.
2. Uninstall existing WinPcap and install TruVision Navigator again.
3. If the issue still occurs, continue to step 4.
4. Check if the following libraries are found in this location C:\Windows\SysWOW64

   File names: wpcap.dll and packet.dll
5. Rename these libraries.
   - Rename wpcap.dll to wpcap.dll.old
   - Rename packet.dll to packet.dll.old
6. Reboot the PC and install TruVision Navigator again.

Multi-client (client/server) installations

Client download URL

The **Client Download URL** field only appears in client/server installations.

For multi-client installations (client/server), the client download URL is the network location of the Navigator client software package. Administrators can deliver this URL to new users so they can download the client software remotely from the Navigator server. If SMTP is in use, this is done automatically for the administrator during user setup.

For standalone installations (direct database connection), this field is disabled since no other networked Navigator clients can connect to this instance of the Navigator server.

User management and client software delivery

With multi-client (client/server) installations of Navigator, computers on the same network as the Navigator server can download the Navigator client.

Note the following:

- Remote distribution of client software is NOT available for the standalone (direct database connection) installation option.
- The person installing the client software must have administrator rights on the computer to perform the client installation.
- When a new user is added to the system, that user does not have any permissions assigned and therefore cannot log in to Navigator. User permissions must be assigned before the user can log in (see “User management” on page 203).
- After installation of the client software, all items that the user has permission to access appear in the Navigator panel.

Fully automated client software delivery

Note: It is possible to add custom instructions/text to the default email text and decide if the download URL link needs to be included in the email. See “New user email content” on page 204.

Navigator can be configured to use an SMTP server to send automated email messages (with client download URL, username, and password) to new users or when an existing user’s login credentials (username and password) need to be reset in the system by an administrator (see “SMTP setup” on page 202202).

To distribute the client software remotely to a new user, first configure TruVision Navigator with an SMTP server, and then add the new user and grant permission to the new user (see “User management” on page 203).

Partially automated client software delivery

If SMTP capability is not used, there are alternate methods that can be used to deliver the client software.

To deliver client software remotely without access to SMTP, do the following:

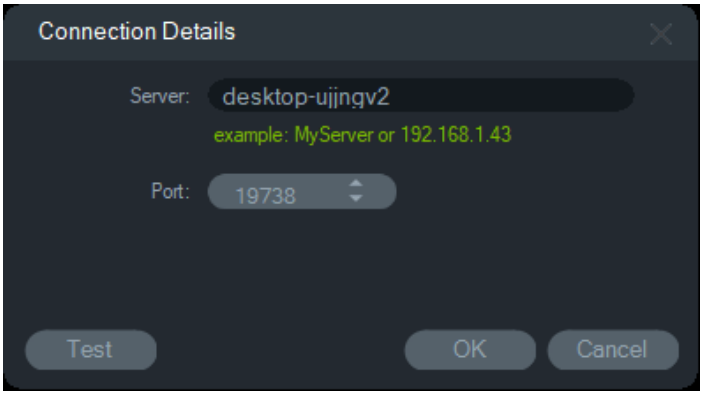
1. Ensure that the **SMTP Server** field is empty in the Settings window **Server** tab.
2. Add the user (see “User management” on page 203).
3. The administrator delivers the user’s login credentials and client download URL to the user via phone or private email. Cut and paste the URL from the **Client Download URL** field in the **Server** tab in the Settings window. Remember to assign the user’s permissions or he/she will not be able to log in.
4. Copy or type the client download URL into a browser or click the link in an email.
5. *Skip this step if you have deployed an SSL certificate from a CA:* Click **Go on to the web page (not recommended)**. See the *TruVision Navigator 8.0 SP2 Software Upgrade for Client Computers Addendum* for details.
6. Follow the instructions in the Client Software Download page to download the ClientOnlySetup.exe file.
7. Run the ClientOnlySetup.exe file (the ClientOnlySetup.exe file is preconfigured to point to the server that it was obtained from) and follow the installation prompts.
8. Launch Navigator and log in with the credentials provided via phone or email.
9. Enter the required information in the Change Password window (see “Task: Log in and secure the system” on page 30 for further information).

To manually install the client software on computers, do the following:

1. Download the ClientOnlySetup.exe file from the Client Installation web page and place it on a thumb drive or other media.
2. Physically deliver the .exe file to the specific computer.
3. Run the ClientOnlySetup.exe file (the ClientOnlySetup.exe file is preconfigured to point to the server that it was obtained from) and follow the installation prompts.
4. Launch Navigator and log in with the user credentials.
5. Enter the required information in the Change Password window (see “Task: Log in and secure the system” on page 30 for further information).

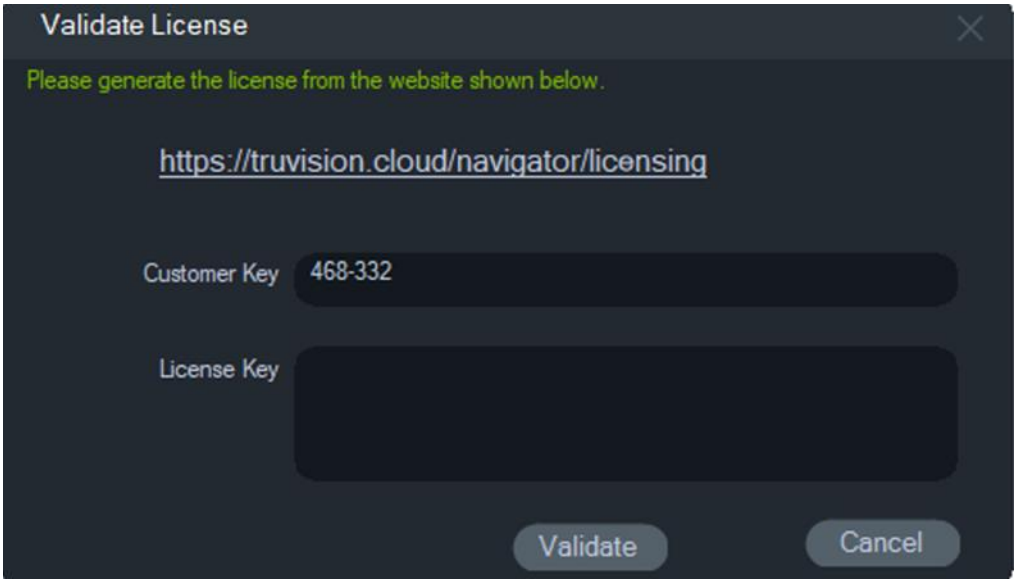
Connection details

Click **Connection Details** in the login screen in client/server mode to view and/or change the default server name and port number, and to test the server connection.

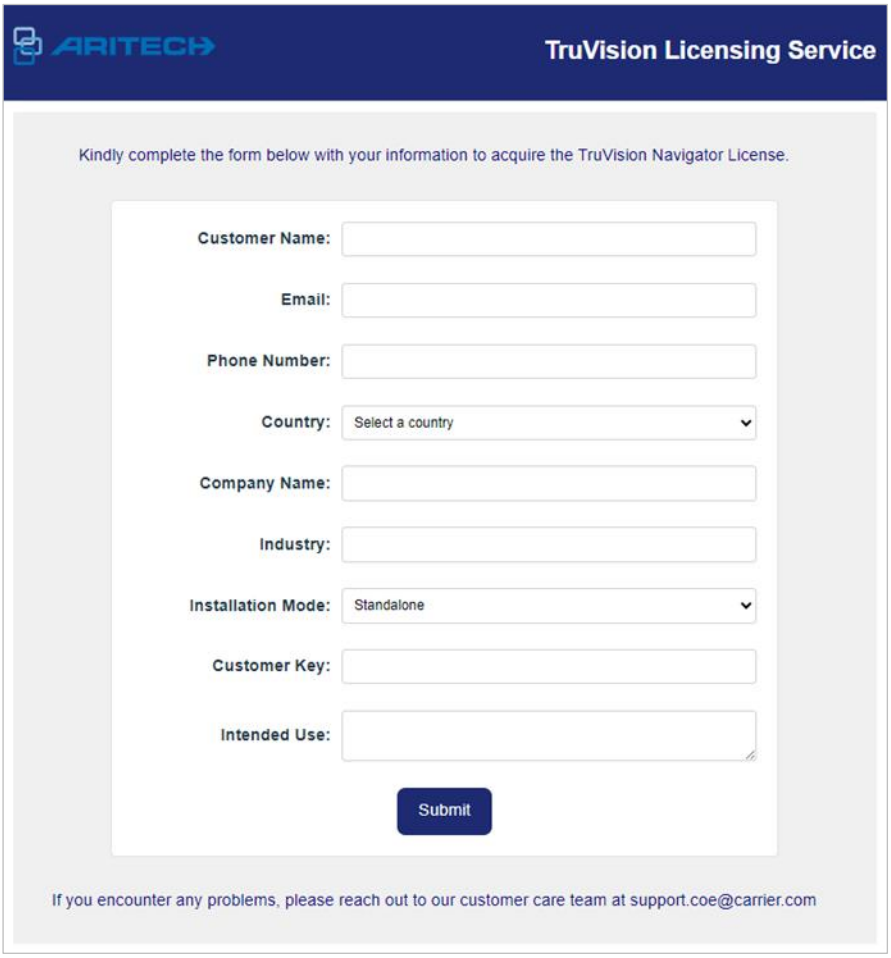


Licensing

After successful installation, launch TruVision Navigator. The application will prompt for a valid license key on the first launch. Click on the provided URL, copy the customer key, and enter the necessary details to generate the license key.

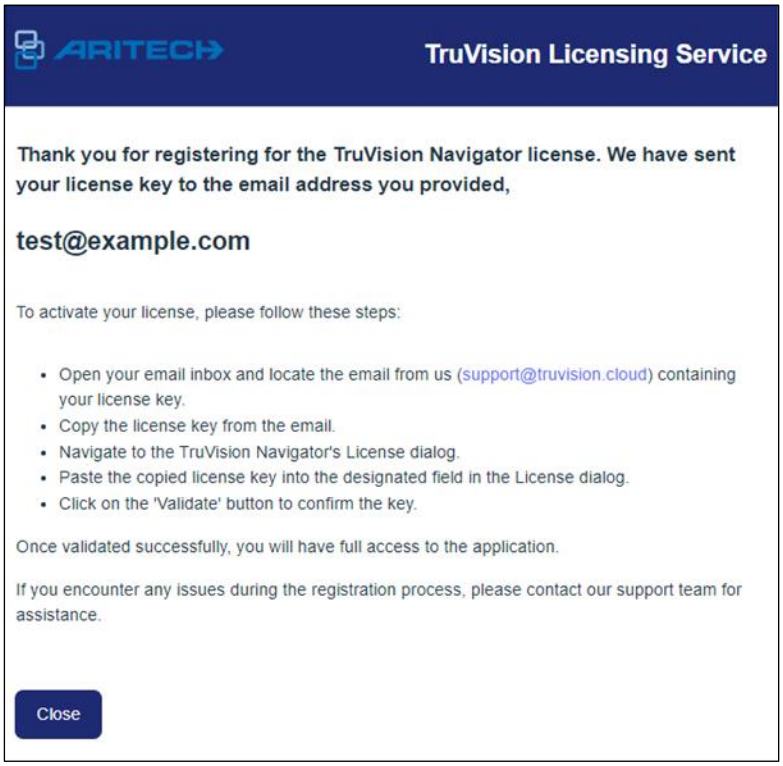


License Key Generation



To generate a license, enter the required customer information in each field, such as **Customer Name**, **Valid Email Address**, **Phone Number**, **Customer Key**, **Company Name**, **Installation Mode**, and **Country of Installation**. The **Customer Key** is a unique ID generated by the TruVision Navigator Application.

Once valid details submitted, TruVision Navigator Licensing system generates License Key as per the given details and sends through email provided.



To activate your license, follow these steps:

1. Open your email inbox and locate the email from us (support@truvision.cloud) containing your license key.
2. Copy the license key from the email.
3. Navigate to the TruVision Navigator’s License dialog.
4. Paste the copied license key into the designated field in the License dialog.
5. Click on the **Validate** button to confirm the key.

Once validated successfully, you will have full access to the application. If you encounter any issues during the registration process, please contact our support team for assistance.

Notes

- If the License Key is invalid or does not match the installation type, the login page will not launch.
- Store the License Key. In case of reinstallation of the TruVision Navigator application on the same machine, the License Key can be reused.

License Key Validation

Paste the copied license key from the webpage into the TruVision Navigator Licensing Page and click on **Validate**. The system will display an appropriate message and, upon validation, will allow the use of the TruVision Navigator.

Task: Log in and secure the system

Purpose
Ensure the system is protected before further configuration.

Default credentials

- Username: **admin**
- Password: **admin**

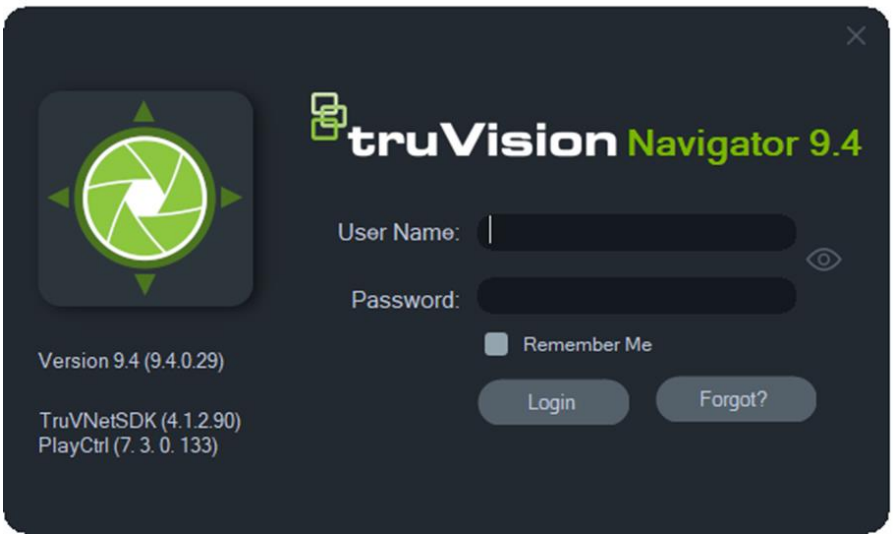
Procedure

1. Launch TruVision Navigator
2. Enter default credentials
3. Click **Login**
4. Enter a new password
5. Confirm the password
6. Select a challenge question
7. Enter the answer
8. Click **OK**

Result

- Administrator account is secured
- System is ready for configuration

Note: The **Remember Me** option is used in combination with the Auto Login function. More information about this option can be found in Chapter 10 “Auto login” and “Remember Me option” on page 139206 and 207.



If you forget the password set up during initial login, click the **Forgot?** button in the Login window to answer the challenge question, change the password, and re-enter the application without calling for assistance.

If the **Challenge Answer** cannot be obtained to recover the password, click the **Forgot?** button again and call the KGS Fire & Security technical support team with the "tech support key" automatically provided in the related field. The technical support team can recover the **Challenge Answer** with this information.

Upgrading an existing installation

Note: We recommend that you back up the database before upgrading.

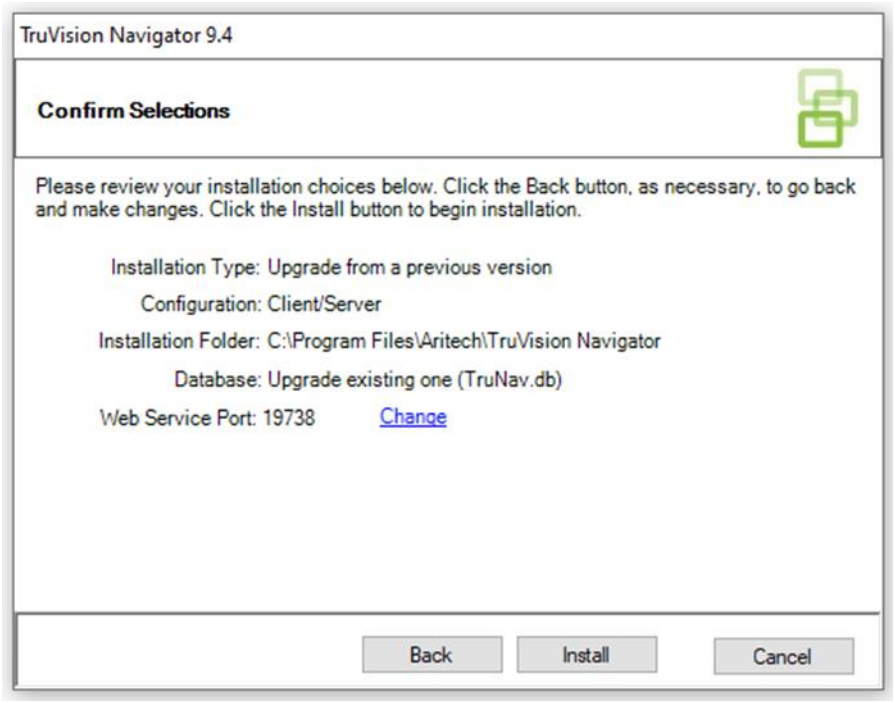
If you are upgrading from TruVision Navigator 9.x version, you can upgrade to the latest released version. If you are upgrading from an older version of TruVision Navigator (for example, 8.x) you must do a fresh installation. This means that you must uninstall the current (older) version before installing a new version.

Check the hardware requirements for the new version and update/upgrade the PC, if needed (see Appendix A "Minimum system requirements"on page 257).

If you need to retain an existing database (for version 8.x), you must contact technical support.

1. Double-click the new TruVision Navigator Setup.exe installer to begin the installation. Right-click the Setup.exe file and select **Run as Administrator**.
2. Click **Yes** to make changes to the computer.
3. The *End User License Agreement* window appears. Select the **I Accept these terms and conditions** check box and then click **Next** to continue.
4. The *Welcome* window appears. Select **Typical** (standalone installation) or **Advanced** (for a client/server installation or to change the default installation location), and then click **Next**.

5. *Advanced installation only:* The *Installation Folder* window appears. Click the **Next** button to accept the default installation folder or click **...** to select a different location.
6. *Advanced installation only:* The Configuration window appears. Select the required configuration mode and then click **Next** to continue.
7. The Select Database window appears. Select the **Use existing database** option (recommended) and then click **Next**. If the organization requires use of Microsoft SQL Server and it is already installed, select **Use Microsoft SQL Server** and then click **Next**.
8. The Confirm Selections window appears. Click **Install**.

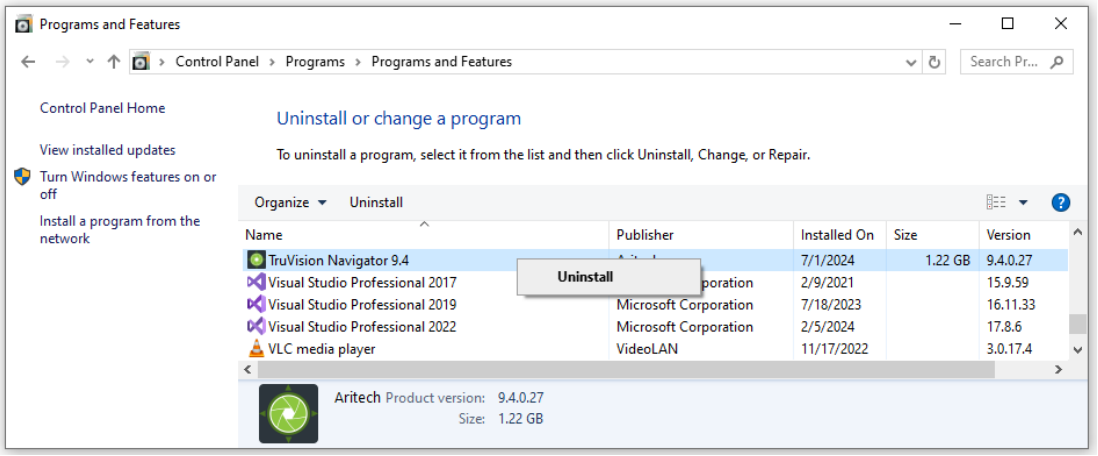


9. Click **Close** to complete the installation.

Uninstall

To uninstall Navigator:

1. Launch the Programs and Features application from the Windows Control Panel.
2. Navigate to TruVision Navigator and click **Uninstall**.



3. Click **Yes** to make changes to the computer.
4. The Uninstaller window appears. If required, select the **Also delete the TruVision Navigator database** check box before clicking **Uninstall**.
5. The Uninstalling Product window appears, followed by the Product Uninstalled window. Click **Close** and restart the computer.

Note: This process removes all TruVision Navigator files and logs from the computer. No registry edits are necessary to remove Navigator from the computer. The NTP service and WinPcap programs should also be uninstalled for complete removal of all files installed during Navigator installation.

Chapter 3
Initial Setup

Overview

This chapter describes the basic configuration steps required after installing TruVision Navigator.

It includes:

- Logging in for the first time
- Activating devices
- Adding and organizing devices
- Verifying live video and recording
- Configuring basic system settings

Some tasks in this chapter use system tools such as Device Manager. Detailed information about Device Manager is provided in Chapter 4.

Some settings apply system-wide (server), while others apply only to the local workstation (client). Refer to Chapter 14 for details.

First-time login

Default credentials

The default credentials for TruVision Navigator are:

- User Name: admin
- Password: admin

See “Task: Log in and secure the system” on page 30 for further information.

Device discovery

Device Manager searches for online devices within the local network and displays network information for the devices. It automatically searches every 15 seconds for the online devices in the computer's local network and then displays the information for the found devices.

IMPORTANT: A wired network connection is required for device discovery. A device cannot be discovered or activated via a Wi-Fi network connection.

Note: Unmanaged devices do not support the discovery feature.

Search for active devices online

After launching Device Manager, click the **Device Discovery** button in the Getting Started window. The Device Manager window appears.

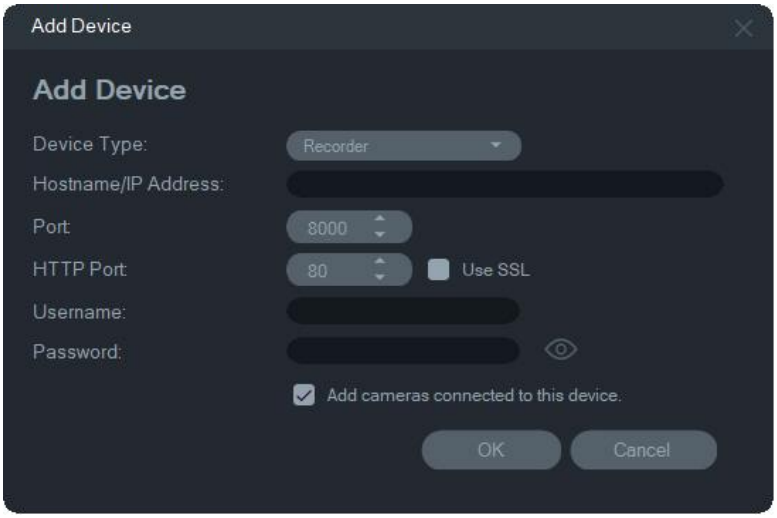
The device information that appears in the **Discovered Devices** tab (shows only the devices that have *not* been added to the Navigator panel) includes the device type, IP address, port number, gateway, firmware version, serial number, MAC address, etc. Discovery results can be filtered by clicking the **Navigator** tab (which shows only the devices that *have* been added to the Navigator panel), and/or by making a selection from the device filter drop-down list (**Camera**, **Recorder**, **TruPortal**, etc.)

Notes

- Click the **Refresh** button to perform a new search for online devices. When the **Refresh** button appears with a yellow dot, it indicates that new devices have been added in the background. Click  to add the newly found devices to the list.
- Click a column heading button to sort the information.

Add device

If a TruVision IP device connected to the network does not appear in the Device Manager's list of discovered devices, add it by clicking the **Add Device** button.



Type in the appropriate device location information along with the device's user name and password. Select **Use SSL** if required by the server. Click **OK**.

Select the **Add cameras connected to this device** check box to add cameras under a recorder in the Navigator panel. Type the user name and password for each camera or select **Use this credential for all devices** in the Credentials Required window.

Activate an inactive device

Newer TruVision devices appear as "Inactive" in the Device Manager window upon initial connection to the network.

IMPORTANT: A wired network connection is required to activate an inactive device. A device cannot be activated via a Wi-Fi network connection.

To activate an inactive device:

1. Click **Activate Device** in the Getting Started window. A list of inactive devices appears in the Device Activation/Change IP Address screen.
2. Follow the steps under "Change IP address" on page 57.

Note: The device is not activated until it is given a new password.

An activate device success message appears.

Verify live video

After adding devices, verify that live video is displayed correctly.

Procedure:

- Select a camera in the Navigator panel
- Open it in the Viewer
- Confirm that live video is visible

Check the following:

- Video is displayed
- Image quality is acceptable
- Video updates in real time

If no video is shown, check:

- Device connection
- Network settings
- User credentials

Configure basic system settings

After verifying the system, configure basic settings required for normal operation.

Procedure:

- Open the **Settings** menu
- Configure the following options:
    - **Client settings:**
        1. Select language
        2. Adjust basic display options
    - **Notifications:**

      Enable event notifications (if required). To receive notifications in TruVision Navigator, you also need to configure the device. See the device's user manual for more details.

      To setup notifications in TruVision Navigator see "Notification settings" on page 222.

Apply the settings to confirm changes. For advanced system configuration, see Chapter 14 — System Settings.

Recommended next steps

After completing the initial setup, additional configuration is required to ensure full system functionality and security.

Administrators should:

- Configure user roles and permissions
- Configure notification handling and filtering
- Configure Event-Actions to automate system responses (see Chapter 14 — System Settings)
- Verify system security settings and authentication policies These steps ensure that the system operates securely and responds correctly to events.

Chapter 4
Device Manager

Overview

The TruVision Device Manager is used to discover and configure TruVision devices on a network, such as IP cameras, DVRs, NVRs, encoders, decoders, network switches, and other supported devices.

This chapter explains how to use Device Manager to add and configure devices, activate them, and perform basic management tasks such as updating firmware and adjusting network-related settings.

Overview of Device Manager

Device Manager provides quick access to common tasks through the Getting Started window, including:

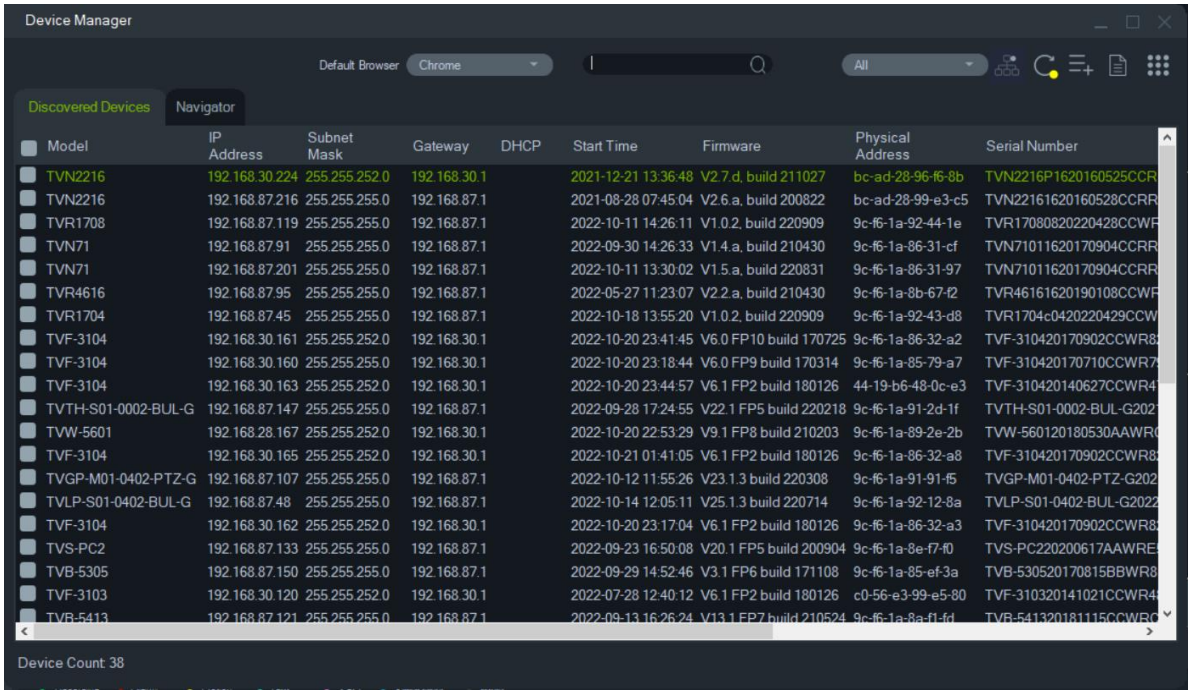
- Activate Devices
- Device Discovery
- Firmware Updates
- Storage Calculator
- Setup Wizard for New Systems

Typical workflow:

1. Discover or add devices
2. Activate devices
3. Verify device connection
4. Configure devices as required

Devices can operate either independently or under the control of a recorder. Cameras connected to a recorder inherit configuration such as recording behavior and event handling from the recorder, while standalone cameras must be configured individually. Understanding this distinction is important when configuring events, notifications, and analytics behavior.

Device Manager window



The Device Manager window contains the **Discovered Devices** and **Navigator** tabs along with the following buttons:

Button icon	Name	Description
	Filter	By typing the model, firmware version, or other options, the user can filter search results.
	SNMP	View SNMP configured devices and SNMP device data. See “**Error! Reference source not found.**” on page 68.
	Refresh	Refresh the list of discovered devices. See “Device discovery” on page 41en page 35.
	Add Device	Add a device manually. See “Add device” on page 41.
	Export to CSV	Export the list of discovered devices to the CSV file format.
	Device Manager Tools	Tools for Device Manager configuration. See “Device Manager tools (advanced)” on page 54.

Note: Select the browser type from the **Default Browser** drop-down list, after double-clicking the discovered devices, open the Device’s configuration window in the selected browser. The device should support the selected browser to open the login and configuration screen after a successful login.

Add devices

Devices can be added automatically using discovery or manually.

See also Chapter 3 “Search for active devices online” on page 35 and “Add devices” on page 41.

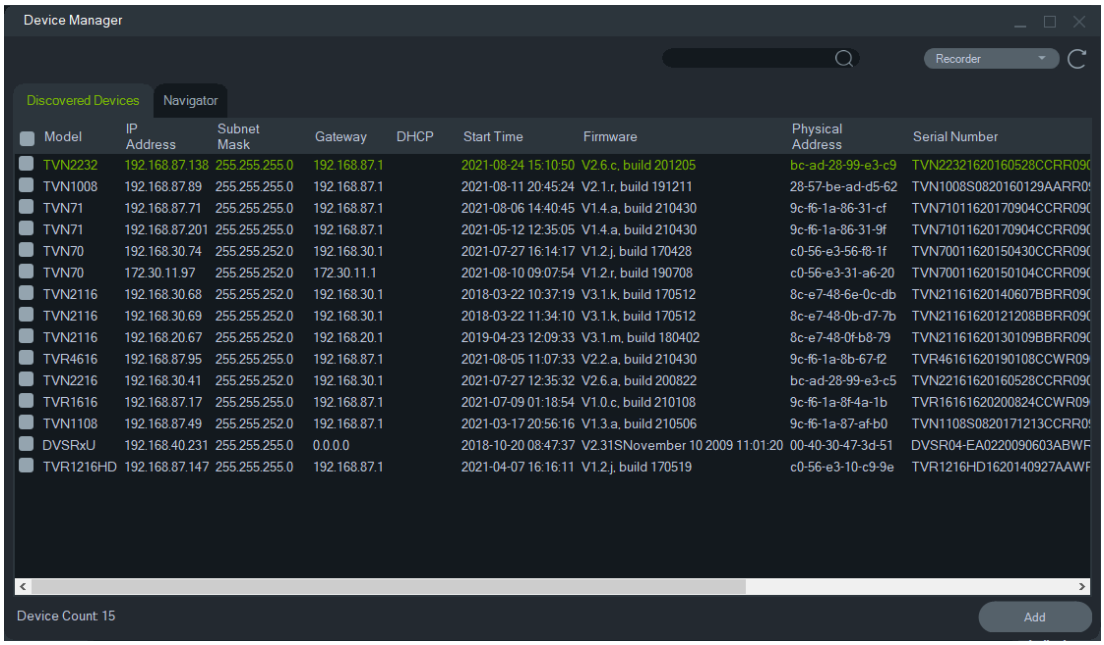
Device discovery

Device Manager searches for online devices on the local network and displays them in the Discovered Devices list.

IMPORTANT: A wired network connection is required for device discovery.

Adding devices using the discovery tool

1. Click the **Add Device** button in the Navigator or right-click the Devices icon, and then select **Add Device** > **Add via Discovery Tool** from the drop-down list.
2. The Device Discovery window displays and provides a list of available devices in the network. You can filter these results by selecting **All**, **Camera**, **Encoder**, **Decoder**, **Recorder**, **TruPortal**, **IFS**, **Intrusion**, or **Other** in the drop-down list.



Note: For recorders, the first two characters after the alpha model number prefix indicates model number, and the last two characters indicate channel count. For example, a TVR4616 model number indicates a 16-channel TVR46 recorder.

The second “Navigator” tab displays the devices that are added already in the application.

3. To add devices to the Navigator, select one or multiple devices from the list using the mouse and Ctrl key, and then click **Add**. The device(s) appear under the Device node in the Navigator panel.
4. Type the **Username** and **Password** and then click **OK**.
5. After the recorder or TruVision camera appears online, expand the Device icon to view all devices added to the system. Upon successful connection, the Navigator populates the respective cameras under the device.

To remove a camera icon from the Navigator panel:

1. Right-click the recorder icon associated with the camera and select **Properties**.
2. Click the camera to be removed and select the **Camera Not in Use** check box.
3. Click **Save**. Repeat these steps, deselect the **Camera Not in Use** check box, and then click **Save** to add the camera back to the Navigator panel.

To remove a recorder or decoder icon from the Navigator panel:

1. Right-click the device icon and select **Delete Device**.
2. Click **Yes**.

Add device manually if a device is not discovered:

1. Click the **Add Devices** button in the Navigator panel and select **Add Manually**, or right-click the Devices icon and then select **Add Device** > **Add Manually** from the drop-down list. The Add Device window appears.

2. Select the appropriate model from the **Device Type** drop-down list.

   Note: Select **TruVision Recorder** or **TruVision Camera** from the drop-down list for any TruVision device. Using one of these drivers enables the device's browser-based configuration page. Some functions do not work as designed if either of these generic device types are selected. We recommend selecting the specific device model if possible.

3. Type a name in the **Device Title** field. Values are alphanumeric.

4. Based on the device type, a selection from the **Streaming Type** drop-down list may be required. For some devices, there is only one option for the **Streaming Type**, so it is selected by default. Streaming types are defined as follows:

- TCP: TCP is a reliable stream delivery service that guarantees delivery of a data stream sent from one host to another without duplication or losing data.

- UDP: The application connects to the device and asks the device to stream video back to the application on a UDP address and port. For this option, the firewall must be configured to allow the device to stream to the application on that specific port.

- Multicast: This type of streaming only requires one stream and one user connection to the recording device and can be connected to many clients. This saves connections and network bandwidth. Multicast is supported in live view only.

5. Type the device's IP address or the EzDDNS URL (e.g., http://hostname.tvr-ddns.net) in the **Device Address** field.

   Note: A recorder can be added using a Domain Name System (DNS) name as well as a static IP address by typing the DNS name in the **Recorder Address** field.

6. The **Port** field is pre-populated with a default value based on the type of device selected. If the port assigned to the device is different from the default value, type the correct port value in this field.

Note: The port number must be added to the device address when using DynDns with a HTTP port other than port 80 (e.g., mydvr.dyndns.org:2222 if the HTTP port being used is 2222). When using No-IP instead of DynDNS, also add the HTTP port number.

7. Type the required values in the **Username** and **Password** fields.
8. Select the **Add Device Offline** check box to add the device to the Navigator if it is currently offline. Bring an offline device online by right-clicking the device in the Navigator panel and selecting **Connect**.
9. Click **OK**.

Note: After clicking **OK**, fields highlighted with a red exclamation point indicate rejected values. Move the mouse pointer over the exclamation points for tips on why the values were invalid. All fields must be valid to successfully add a device.

Adding an UltraSync recorder

TruVision Navigator (as of version 9.4 SP2) supports the connection of TruVision recorders via UltraSync.

TruVision Navigator uses a P2P (peer-to-peer) communication method to establish a connection with the recorder.

Prerequisites

1. Run TruVision Navigator as Administrator

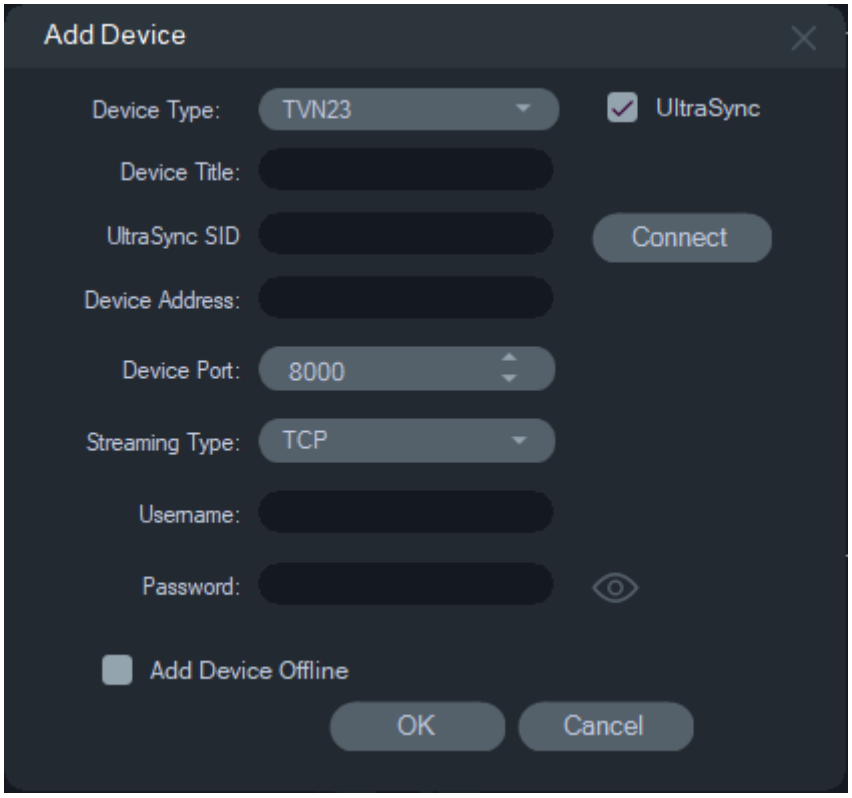
   Required to start UltraSync services and connect to UltraSync-enabled devices.

2. Open Required Ports

   Ensure necessary UDP ports 53 and 1194 for the UltraSync Server are open on the network firewall.

3. Use a TruVision recorder with UltraSync support that runs the following firmware:

- TVN 12: firmware 3.1.3 Build 251017 or newer
- TVN 23: firmware 1.03.004 Build 251017 or newer
- TVR 17: firmware 3.3.1 Build 250818 or newer
- TVR 18: any firmware



To add an UltraSync recorder

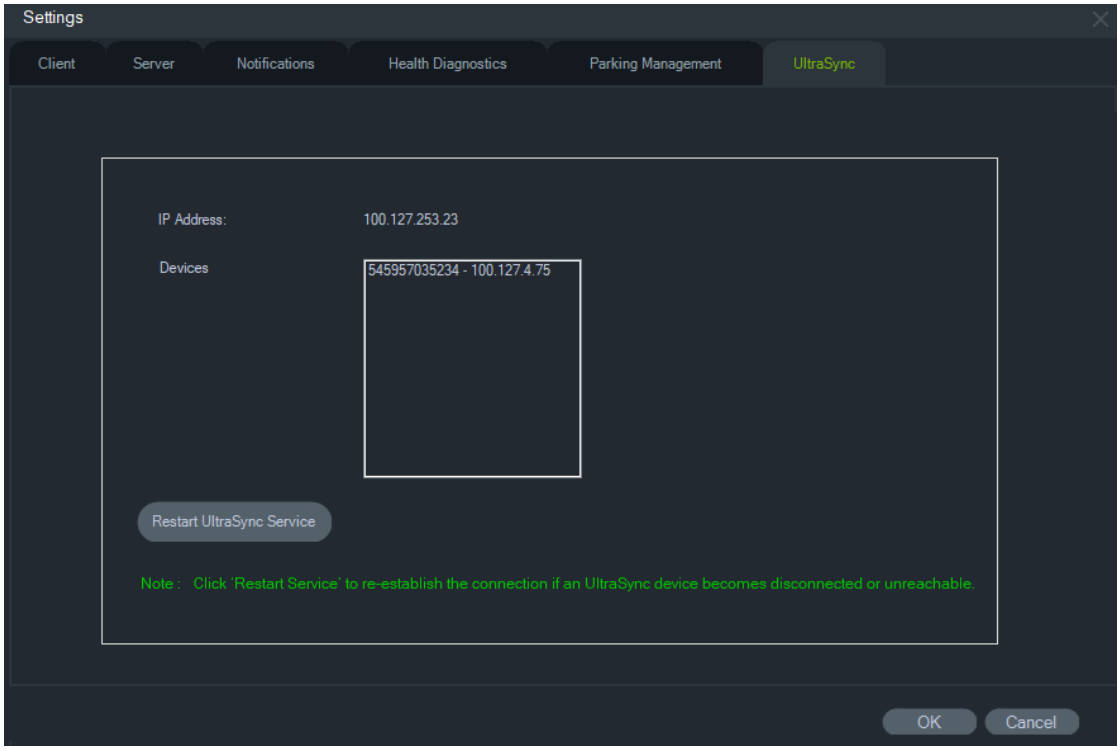
1. In the Device Tree, right-click on **Device**, click **Add Device > Add Manually**.
2. Select TVN12/TVN23/TVR17/TVR18 as **Device Type**.
3. Enter the UltraSync SID

Input the SID of the UltraSync-enabled recorder. This SID must be retrieved from the recorder.

Open the recor webpage, go to the Live page and click the UltraSync icon

4. **Click the "Connect" Button**
   - This initiates the UltraSync services locally.
   - It may take up to 30 seconds for the services to initialize.
   - Once connected, the IP address of the UltraSync recorder will be displayed.
5. **Complete the Connection**
   - Enter the port number (default: 8000) and recorder credentials.
   - Click OK to connect the recorder to TruVision Navigator.

UltraSync information



An UltraSync tab is available in the Settings dialog, accessible only to admin users.

This panel allows:

- Restarting the UltraSync service.
- Viewing the IP address of the local TruVision Navigator machine.
- Displaying the connected UltraSync recorders.

Limitations:

1. HTTP only communication

   All connections use HTTP, regardless of secure communication settings. However, the security of the connection is guaranteed, due to the UltraSync connection mechanism.

2. Alarm Host notifications

   Refer to the application's UltraSync Information section to locate the device's IP address. In the above screenshot the IP address of the alarm host is 100.127.253.23 and thus needs to be entered in the recorder as Alarm Host IP address.

Unsupported features:

Some device management operations are not supported via UltraSync

- IP address changes
- Password updates

Adding a TruVision 360° camera

Navigator supports TruVision 360° cameras. These cameras can be added to TruVision NVRs as a regular IP camera either manually or using the discovery tool.

Each TVF-110x 360°camera provides five streams to the user.

- 1 x Raw 360° image (also contains a substream)
- 1 x Two 180° bands in one video stream
- 3 x 120° streams with digital PTZ capability

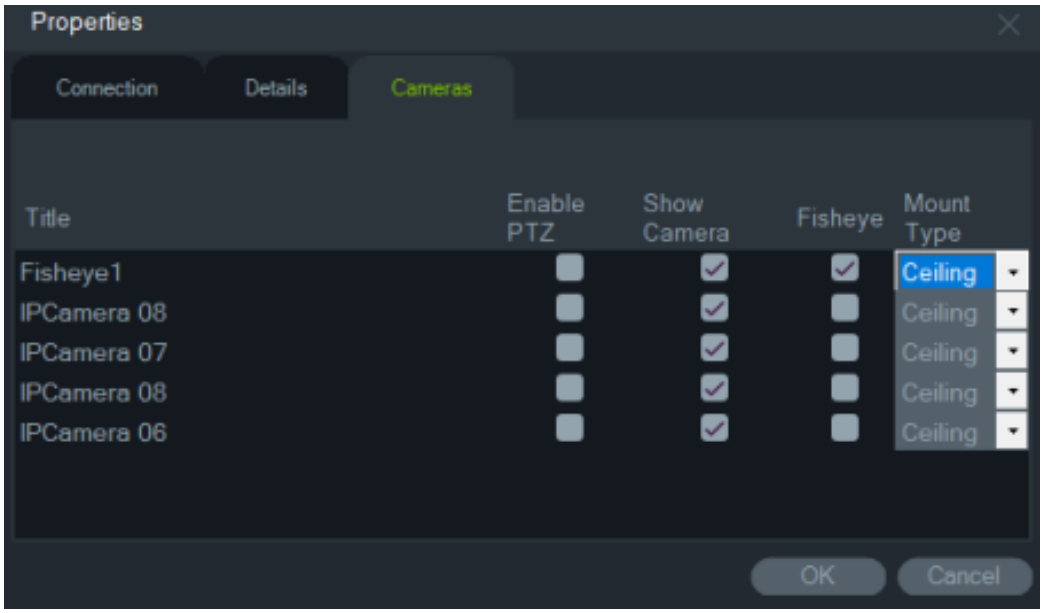
When a 360°camera is added to a device, the camera appears in the Navigator panel and has its own device node with up to five channels listed under it. By default, the 360°camera is added with only the 360° mode enabled.

The TVF-520x 360° and TVPA cameras support more dewarping views. See "Dewarp views" on page 84.

To add the rest of the views:

1. Ensure that the Fisheye Mode in the camera configuration menu is set to Multi Channel Mode. See the camera's user manual for details.
2. Right-click the camera's device node and select **Properties**.
3. In the **Properties** menu, click the **Cameras** tab and select the **Show Camera** check boxes for the views to display.

4. Click **OK**.



For information about dewarping 360° cameras, see “Dewarp views” on page 84.

Adding a TruVision multi-imager 360-degree IP Camera

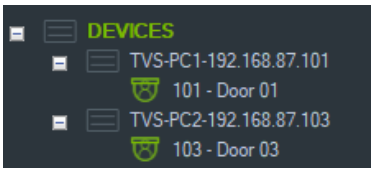
TruVision Navigator supports TruVision multi-imager 360-degree IP cameras (TVS). These cameras can be added to TruVision NVRs as a regular IP camera either manually or using the Discovery tool. Each multi-imager IP camera provides four streams to the user.

When a multi-imager IP camera is added to a device (for example, TVN 22 below), the camera appears in the Navigator panel and has its own device node with up to four channels listed under it.

Adding people counting IP camera

TruVision Navigator supports TruVision people counting IP cameras (TVS-PC). These cameras can be added to TruVision NVRs as a regular IP camera either manually (see “Add device manually if a device is not discovered:” **Error! Bookmark not defined.**42) or using the discovery tool (see “Adding devices using the discovery tool” **Error! Bookmark not defined.**41). Once a people counting camera is added into the Navigator, it displays with a people camera icon.

To configure people counting cameras, see “Adding people counting IP camera” on page 10247.



Adding thermal IP camera

TruVision Navigator supports the TruVision thermal IP cameras. These cameras can be added to TruVision NVRs as regular IP cameras either manually or using the Discovery tool. Some of the S series thermal IP cameras support an optical video stream and a thermal video stream.

When the thermal IP camera is added to a device (for example, TVN 12), the camera appears in the Navigator panel and has its own device node with the optical stream and the thermal stream listed.

Activate devices

Overview

Some devices must be activated before they can be used in the system.

Activation typically involves setting a password and enabling communication between the device and TruVision Navigator.

Task: Activate Devices

Procedure:

1. Open Device Manager
2. Select the device to activate
3. Click Activate Device
4. Enter a password for the device
5. Confirm the password
6. Click Apply

Notes:

- Devices must be activated before they can be used

- A wired network connection is required for activation

After activating a device, continue with verifying the device connection (see section below).

Verify device connection

Overview

After adding and activating a device, verify that it is correctly connected to the system. This ensures that the device is accessible and ready for use.

Task: Verify device connection

Procedure:

1. Open the Navigator panel
2. Locate the device in the device list
3. Check the device status (online/offline)
4. Expand the device to view connected cameras
5. Confirm that cameras appear under the device

Result: The device is displayed as online and its cameras are visible in the Navigator panel.

Troubleshooting:

If the device is offline:

- Check network connection
- Verify IP address and credentials
- Ensure the device has been activated

Organize/manage devices

Download/upload configuration

Devices that support the download/upload function are listed in the “Supported Devices” row in the device details tables (see Appendix B “Device details” on page 263).

Use the **Download Configuration** and **Upload Configuration** selections to transfer recorder configurations between individual devices.

- Right-click the recorder and select **Download Configuration** to save the recorder's configuration in CFG file format.
- Right-click the recorder and select **Upload Configuration** to upload a different recorder configuration to the selected recorder in CFG file format.

Reboot device

1. Right-click a recorder icon in the Navigator panel and select **Reboot** to reboot it.
2. Click **Yes** to confirm reboot of the device. The recorder icon changes to  in the Navigator panel to indicate that it is offline.
3. After the device reboots, right-click its icon in the Navigator panel and select **Connect** to reconnect it.

Restore factory defaults

Devices that support the restore factory defaults function are listed in the "Supported Devices" row in the device details tables (see Appendix B "Device details" on page 263).

1. Right-click a recorder icon and select **Restore Factory Defaults** to have the device default to factory settings (the same settings on the device when it was shipped).
2. Click **Yes** to confirm reboot of the device. The recorder icon changes to  in the Navigator panel to indicate that it is offline.
3. After the device reboots, right-click its icon in the Navigator panel and select **Connect** to reconnect it.

Delete/rename device

- Right-click the recorder icon and select **Delete Device** to remove the recorder from the Navigator panel.
- Right-click the recorder icon and select **Rename Device** to change the name of the recorder in the Navigator panel.

Configure devices

Overview

After adding and verifying a device, basic configuration may be required. Device configuration allows you to adjust settings such as network parameters, video properties, and system behavior.

Advanced configuration and system-wide settings are described in Chapter 14 — System Settings.

Typical device settings include:

- Network settings (IP address, ports)
- Video settings (resolution, frame rate)
- Recording settings
- Time and synchronization settings

Notes:

- Some settings may require administrator rights
- Changes may require a device restart

Discovered devices can be configured either in Navigator or through the device's internal configuration web page.

TruVision recorder browser configuration is currently available for the recorders listed below:

Table 1: Browser configuration compatibility

Recorder Model	Firmware version
TVN 10	2.0 and above
TVN 12	All versions
TVN 21	3.0 and above
TVN 22	1.0 and above
TVN 23	All versions
TVR 12HD	All versions
TVR 15HD	All versions
TVR 44HD	All versions
TVR 45HD	All versions
TVR 16	All versions
TVR 17	All versions
TVR 18	All versions
TVR 46	All versions
TVN 11	All versions
TVN 70	All versions
TVN 71	All versions

To configure a device using the device's internal configuration web page:

1. Right-click a device in the Navigator panel and select **Configure Device** or **Configure Camera**.

   Note: If configuring a device remotely, the device HTTP port must be forwarded through the router, along with the control and RTSP ports. Without HTTP port forwarding, the browser of the device cannot be viewed.

2. If necessary, click **OK** to update the plug-ins.

   Note: The plug-in should already be installed if the device has been connected to and previously configured through the device's internal web browser

3. Follow the instructions in the Setup-UTC Web Components window. When complete, restart Navigator.

   Caution: Close all browser windows when instructed and close Navigator before continuing.

4. Right-click the TruVision device and select **Configure Device**. Navigator opens the device's internal configuration web page.

5. Configure the device with the required preferences. See the device's user manual for all configuration options.

   Note: For cameras not connected to a recorder, enter the camera's login credentials to proceed.

6. When complete, click the **Close** button to save any configuration changes and return to Navigator.

Notes

- Some devices cannot be configured remotely using Navigator.
- The trusted source for camera titles is the device itself. When adding a device for the first time, Navigator does not display the device's configuration information at the time of connection. The cameras in the Navigator panel may display generic camera titles (Camera 1, Camera 2, Camera 3, etc.). Camera names are updated after performing device configuration for the first time. Afterwards, any changes to camera titles through Navigator updates both the Navigator and the device.
- For protocol configuration of analog PTZ cameras attached to an embedded NVR via an encoder, use encoder web administration rather than the embedded recorder configuration menu.

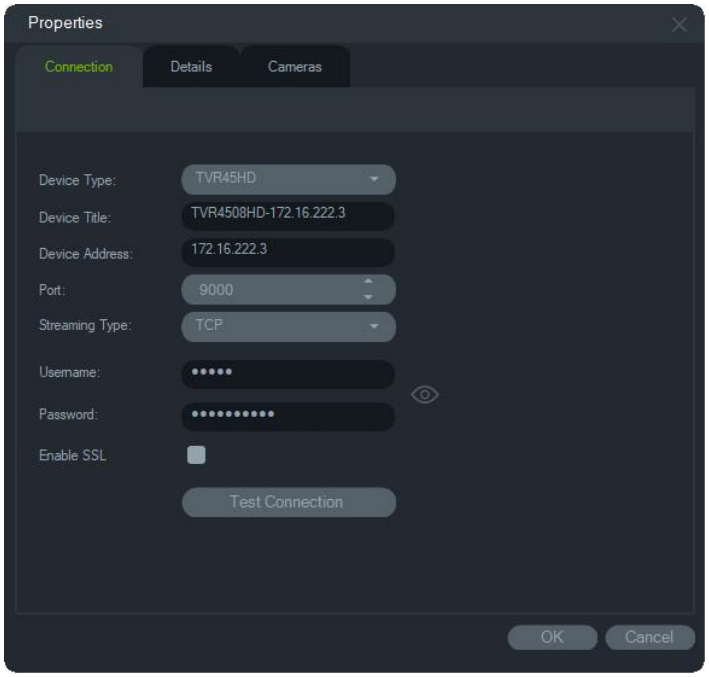
Manage IP cameras (IP camera recorders only)

Right clicking a recorder and selecting **Manage IP Cameras** launches the IP Camera Status page in the Configuration interface. See the recorder's user manual for details about IP camera configuration.

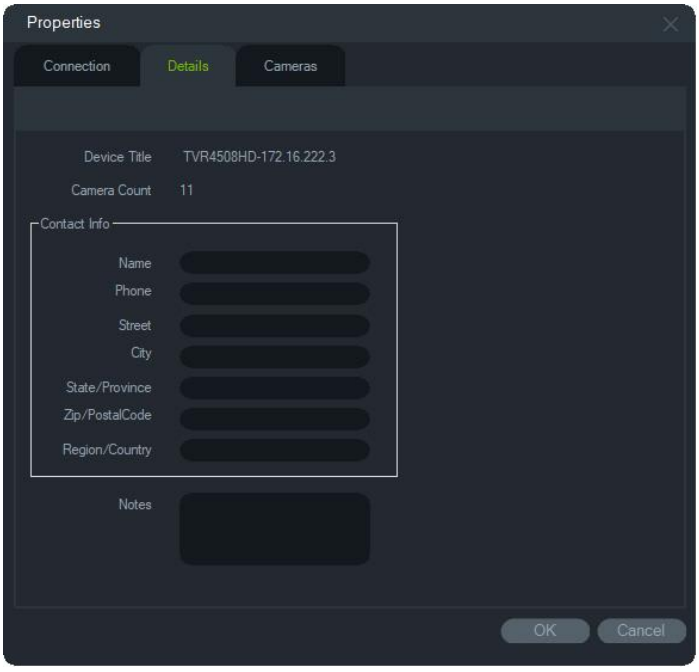
Recorder properties

Right-click the recorder icon in the Navigator panel and select **Properties** to display the Properties window.

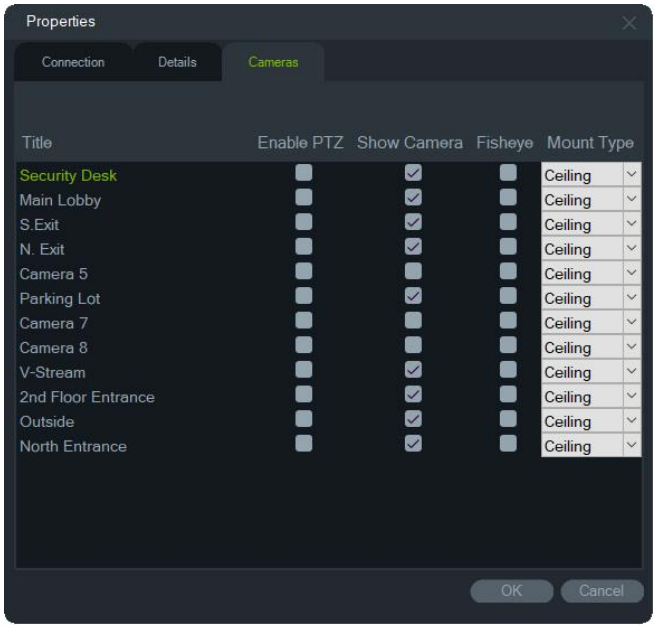
- The **Connection** tab shows all of the information previously entered when adding the device. Make changes as appropriate and click **OK** to save changes.



- The **Details** tab provides an area to type in contact information and notes to help facilitate management of the system. If the device was imported from an address book that contained information in this window, data appears in these fields. Type in data as appropriate and click **OK** to save changes.



- Use the **Cameras** tab to hide or show cameras, enable or disable PTZ and fisheye controls, and set the mount type. When finished, click **OK** to save changes.



Configure an IP camera

Right-click an IP camera and select **Configure Camera** to access the camera configuration menu. See the camera's user manual for further information on camera configuration.

Note: Devices that support the configure camera function are listed in the "Supported Devices" row in the device details tables (see Appendix B "Device details" on page 263).

Device Manager tools (advanced)

Overview

Device Manager provides additional tools for advanced configuration and maintenance of devices. These tools are typically used by administrators to manage device settings, perform updates, and maintain system performance.

Bulk operations

Multiple devices can be managed simultaneously using bulk operations.

Typical tasks include:

- Applying configuration changes to multiple devices

- Updating firmware on multiple devices
- Synchronizing settings

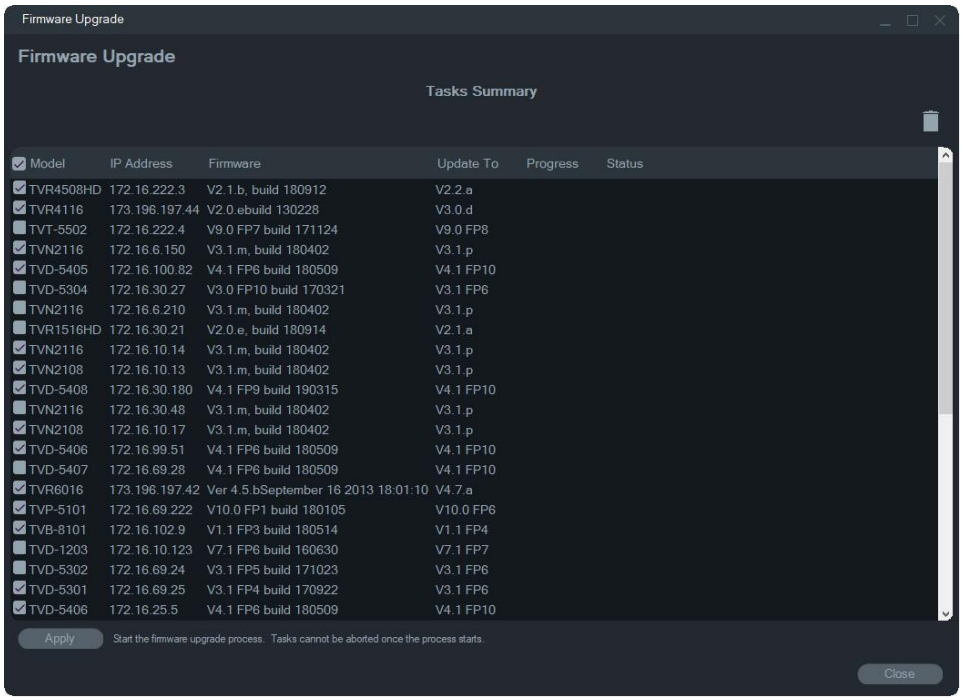
Firmware management

Use the Firmware Upgrade window to upgrade the firmware of the selected device or devices.

Note: The local computer must be connected to the internet to connect with the firmware server.

To select devices for firmware upgrade:

1. Click the **Firmware Updates** button in the Getting Started window. The Updates Available dialog appears.
2. Select **Download All Firmware** to download all firmware files. If this check box is not selected, only firmware files that have not already downloaded will download to the local computer. Click **OK** in the Updates Available dialog to proceed.
3. 6.The Firmware Download screen appears. Wait for the firmware files to download to the local computer.
4. The Firmware Upgrade screen appears. In the Model list, click a device to select it or hold the Ctrl or Shift key to select multiple devices.



5. Click **Apply**, and then click **Yes** to start the firmware upgrade process. The Credentials Required dialog box appears.
6. Type the **User Name** and **Password** for the device(s) (if necessary, select **Use this credential for all devices**), and then click **OK** to begin the firmware upgrade.

Firmware upgrade progress appears in the Firmware Upgrade window. When upgrading is complete, the updated version information of the device(s) appears in the device list.

Manual firmware update

Follow these instructions only if the firmware update file has already been downloaded to the local computer.

To perform a manual firmware update:

1. Select one or more devices for firmware update in the main Device Manager window.
2. Click **Device Manager Tools**, and then click the **Manual Firmware Update** tool button. The Firmware Upgrade window appears.
3. Click **Browse** to locate the firmware file, and then type in the user name and password for the highlighted device in the Device List.
4. Click **Add** to add the highlighted device to the Tasks Summary list or click **Add All** to add all the devices in the Device List to the Tasks Summary list.
5. Click **Apply**, and then click **Yes** to start the firmware upgrade process.

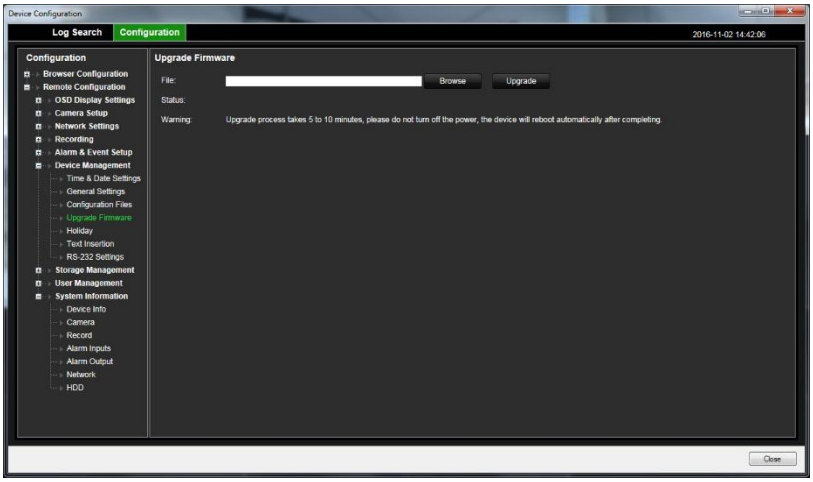
Firmware upgrade progress is displayed in the Firmware Upgrade window. When upgrading is complete, the updated version information of the device(s) is displayed in the device list.

Update a firmware update of a recorder that is already in the Navigator Panel

To upgrade firmware to device(s):

1. Right-click a recorder icon in the Navigator panel and select **Configure Device**.
2. Select **Upgrade Firmware** under Device Management.
3. Click **Browse** to find the applicable firmware file.

   Note: Since TruVision Navigator does not do a file format check on the firmware file, ensure it is in the proper file format for that device type. In addition, the firmware file must reside on the local computer. It cannot be accessed across network paths.
4. Click the **Upgrade** button.



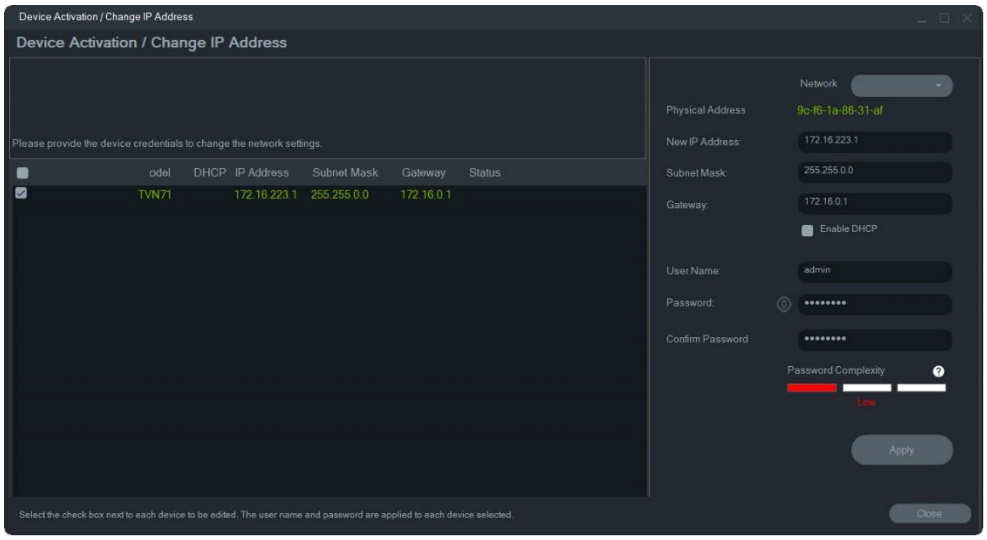
Notes:

- Ensure compatibility before updating firmware
- Do not interrupt the upgrade process
- Restart may be required after update

Change IP address

1. Click the **Change IP Address** tool button to bring up the Device Activation / Change IP Address window.
2. Select one or more devices to continue with setup. If multiple devices are selected, IP addresses are automatically assigned in sequence (in this case, all devices must have the same password). Select individual devices to assign specific IP addresses to each. If a device has one or more Network Interface Cards (NICs) to share the network load when using a number of HD cameras, an IP address can be assigned to each by selecting the corresponding number of the NIC from the **Network** drop-down list. Type in a new IP address, subnet, and gateway manually or click an IP address to use default settings.

Note: Credentials must be entered before assigning an IP address to a NIC card.



3. Click **Test.**
4. If the IP addresses were recognized as available, click **Apply**.
5. Click **Yes** to change the IP address for the selected devices.

Notes:

- Incorrect network settings may disconnect the device

- Ensure network configuration matches system requirements

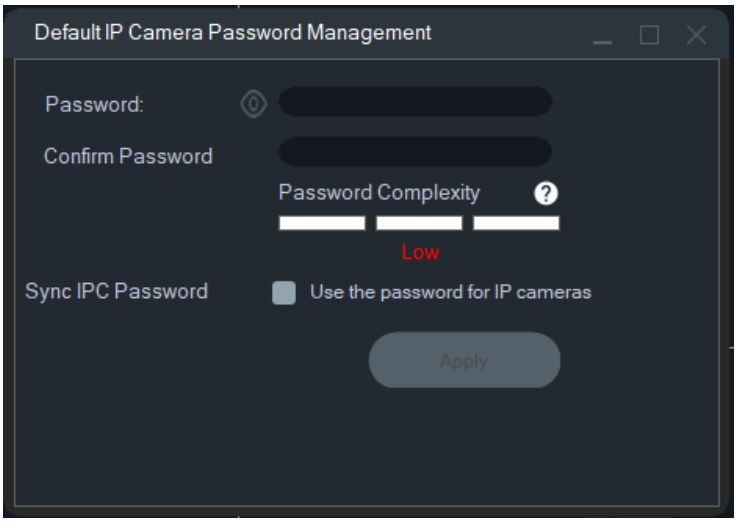
Change password

1. Select one or more devices the main Device Manager window (if multiple devices are selected, all must have the same password), click **Device Manager Tools**, and then click the **Change Password** tool button.
2. Type the correct information in the **Old Password**, **New Password**, and **Confirm Password** fields. Select the **Include cameras connected to this recorder** check box to change the password(s) for connected cameras.
3. Click **Apply**.

Default IP Camera Password Management

Set the same passwords for all the cameras connected to the recorder.

Note: This feature is only supported on TVN 12 and TVR 17 recorders.



Time synchronization

Device Manager can synchronize device time with the system to ensure consistency. Accurate time is important for playback, events, and reporting.

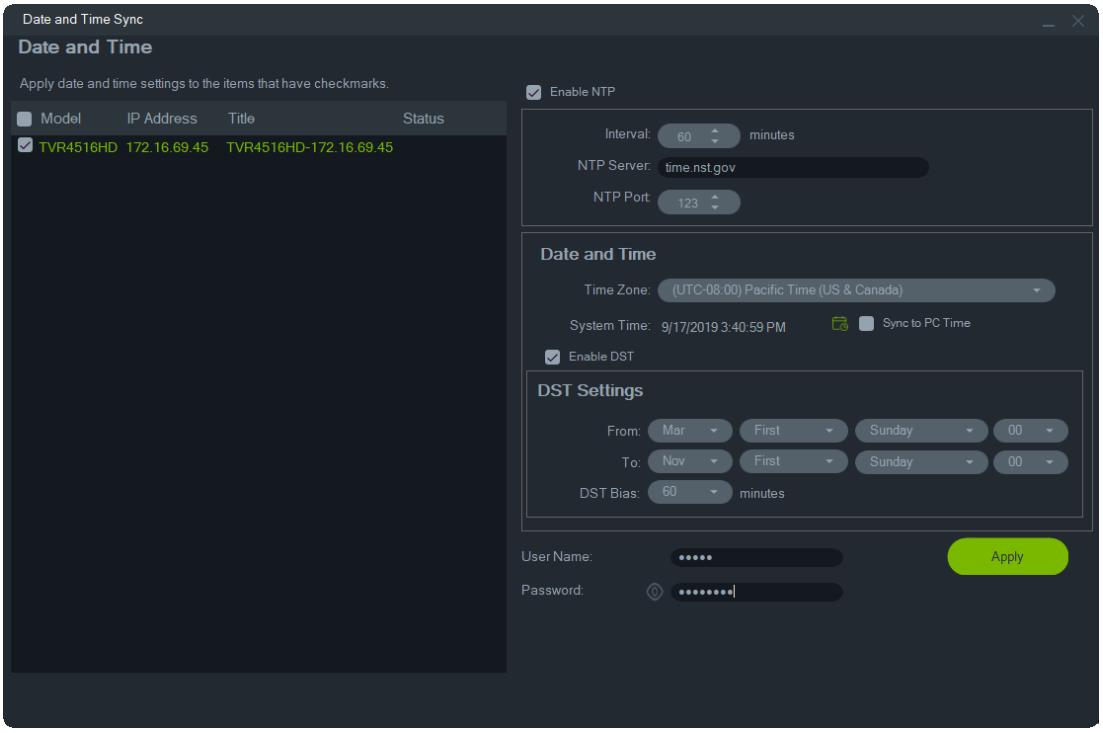
Use this tool to set the time and date across multiple devices.

Network Time Protocol (NTP) is a protocol for synchronizing the clocks of network devices such as IP cameras and computers. Connecting network devices to a dedicated NTP time server ensures that they are all synchronized.

Note: For a list of IFS switches that support date and time sync, see the *TruVision Navigator Compatibility with IFS Switches Addendum*.

To perform date and time sync:

1. Select one or more devices for date and time sync in the main Device Manager window.
2. Click **Device Manager Tools**, and then click the **Date and Time Sync** tool button. The Date and Time Sync window appears.



3. Select **Enable NTP** and then type in an address in the **NTP Server** field, a time interval in the **Interval** field, and an NTP Port number in the **NTP Port** field as necessary.
4. From the **Time Zone** drop-down list, select the time zone that corresponds to the device's location.

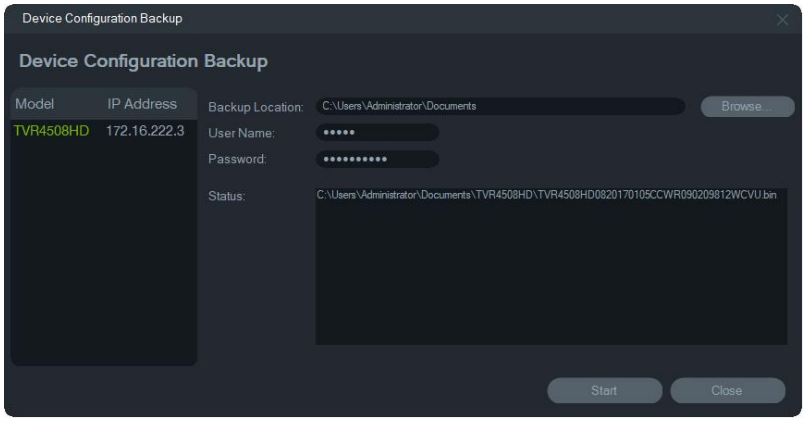
   Note: You can also select the **Sync to PC Time** check box to synchronize the time of the device with the time of the computer.
5. Type in the **User Name** and **Password** credentials for each device or for multiple devices, and then click **Apply** after the credentials are accepted for all the devices in the list.

Device configuration backup and restore

Use these tools to backup and restore device configurations.

To back up a device configuration:

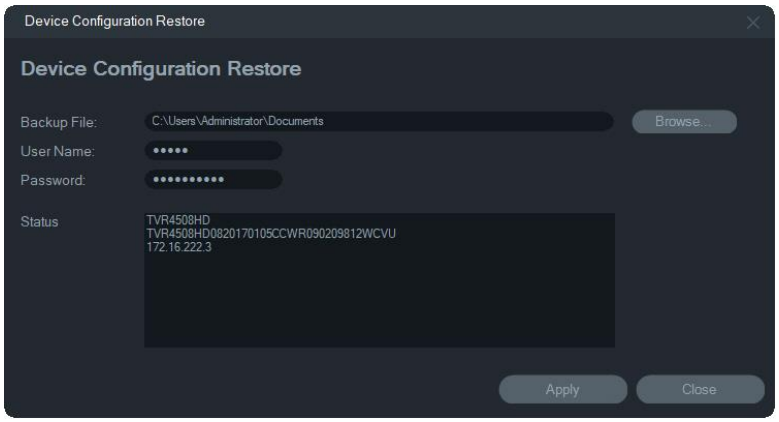
1. Select a device in the main Device Manager window, click **Device Manager Tools**, and then click the **Device Configuration Backup** tool button.
2. If required, click **Browse** to select a new backup location.
3. Enter the device's user name and password and select **Start** to begin the backup process.



4. Click **Close** when backup is complete.

To restore a device configuration:

1. Select a device in the main Device Manager window, click **Device Manager Tools**, and then click the **Device Configuration Restore** tool button.
2. If required, click **Browse** to select the location of the backup file.
3. Enter the device's user name and password and click **Apply**.



4. Click **Yes** to restore the device configuration.

Upload camera information

Use this tool to restore the device configuration for IP cameras only.

Note: Not all cameras support this feature.

The list of recorders that can upload camera information is as follows:

- TVN 11
- TVN 12
- TVN 21
- TVN 22
- TVN 23
- TVN 70
- TVN 71
- TVR 15HD (IP cameras only)

- TVR 45HD (IP cameras only)
- TVR 16 (IP cameras only)
- TVR 17 (IP cameras only)
- TVR 18 (IP cameras only)
- TVR 46 (IP cameras only)

To upload camera information:

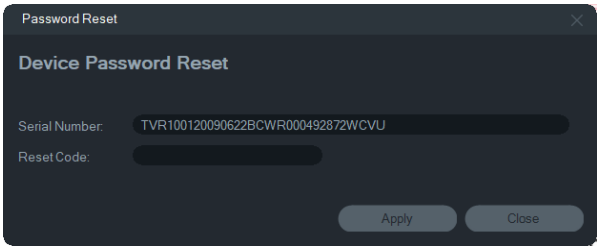
1. Select a supported recorder in the main Device Manager window, click **Device Manager Tools**, and then click the **Upload Camera Information** tool button.
2. Click **Browse** to select the location of the configuration file.
3. Type in the recorder's user name and password and click **Apply**.
4. Click **Yes** to upload the camera information.

Reset password

If an admin (not a specific user) device password is lost, contact Technical Support to restore the password. There are two ways to restore the password. The method to be used depends on the device and its currently installed firmware.

To restore the default password (method 1):

1. Select the device for password reset in the main Device Manager window.
2. Click **Device Manager Tools**, and then click the **Reset Password** tool button.
3. Copy the complete serial number from the **Device Serial No.** field in the Device information panel and paste it into an email to send to Technical Support. Also provide Technical Support with the date shown in Live View. For some devices (e.g., TVR60), the hour shown in Live View is also required. Technical Support will provide a security key by email.

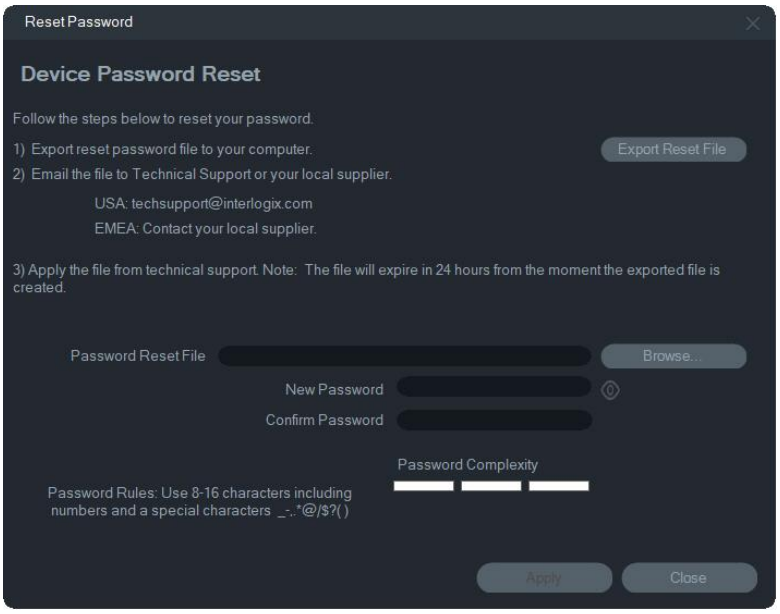


4. Enter the security key received from Technical Support in the **Security Code** field and click **OK** to restore the default password. The default password is **1234**.

Note: The security key provided is related to the date (or hour in the case of TVR60) the serial number was sent to Technical Support and expires the day it was created. We recommend resetting the device password immediately after receiving the reset code.

To set a new password using an XML file (method 2):

1. Select the device for password reset in the main Device Manager window.
2. Click **Device Manager Tools**, and then click the **Reset Password** tool button.
3. Click the **Reset Password** button.



4. Click **Export Reset File** in the Reset Password window to save the XML file, and then email the file to Technical Support. Technical Support will provide a new XML file.
5. Save the XML file received from Technical Support on the computer, click **Browse**, and select the new XML password file.
6. Type a new password and then confirm it in the **New Password** and **Confirm Password** fields. Click **Apply**.

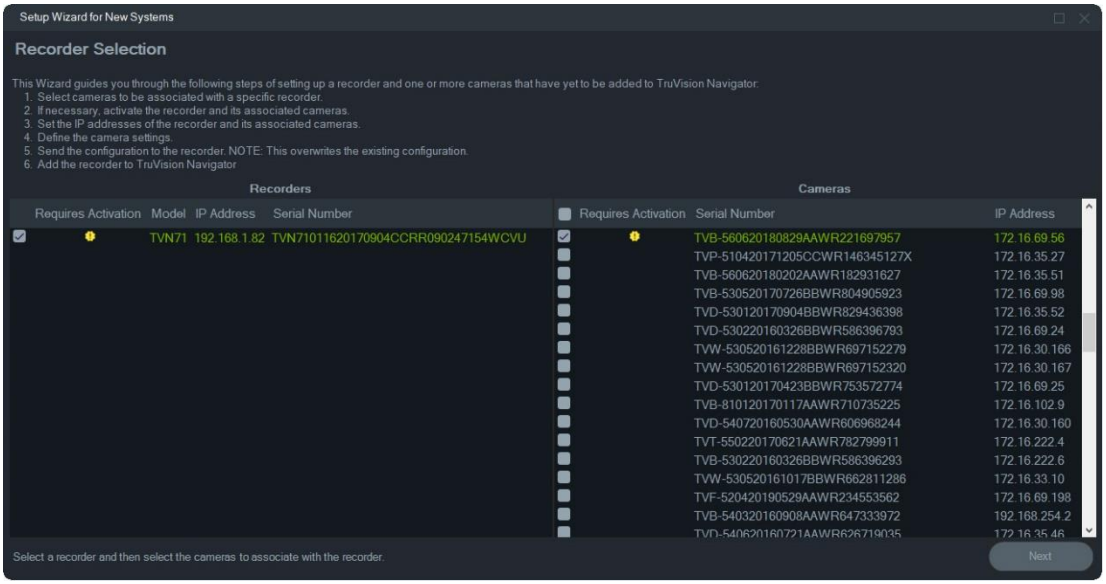
Note: Do not restart the device after the password recovery XML file has been exported, otherwise the steps above must be repeated. The password recovery XML file expires after 48 hours.

New system setup wizard

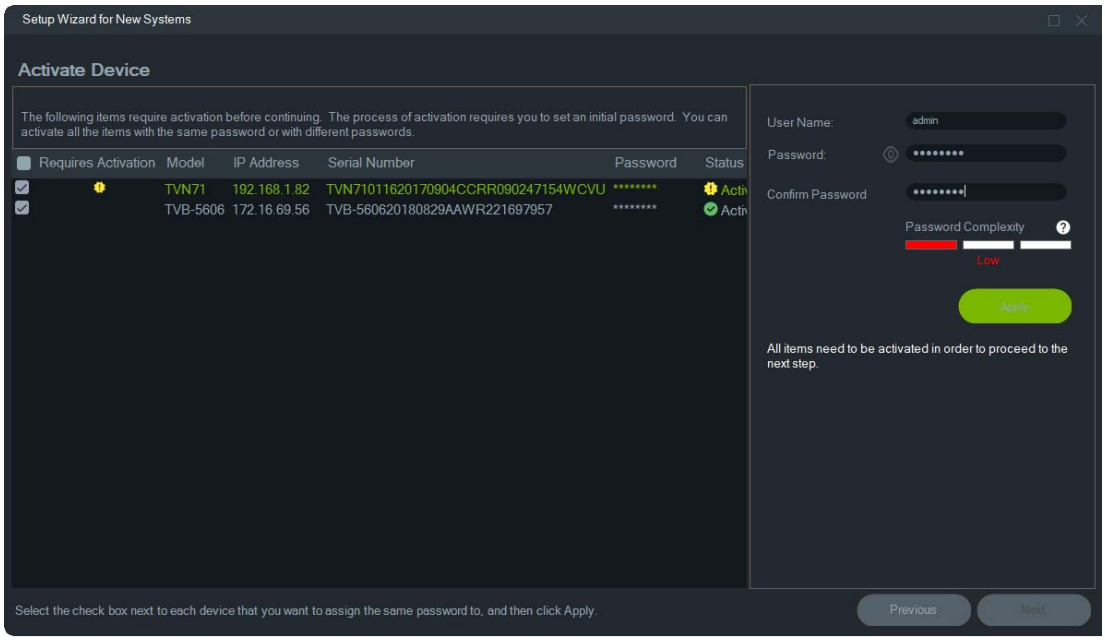
The New System Setup Wizard simplifies the initial setup of new devices.

To set up devices using the Wizard:

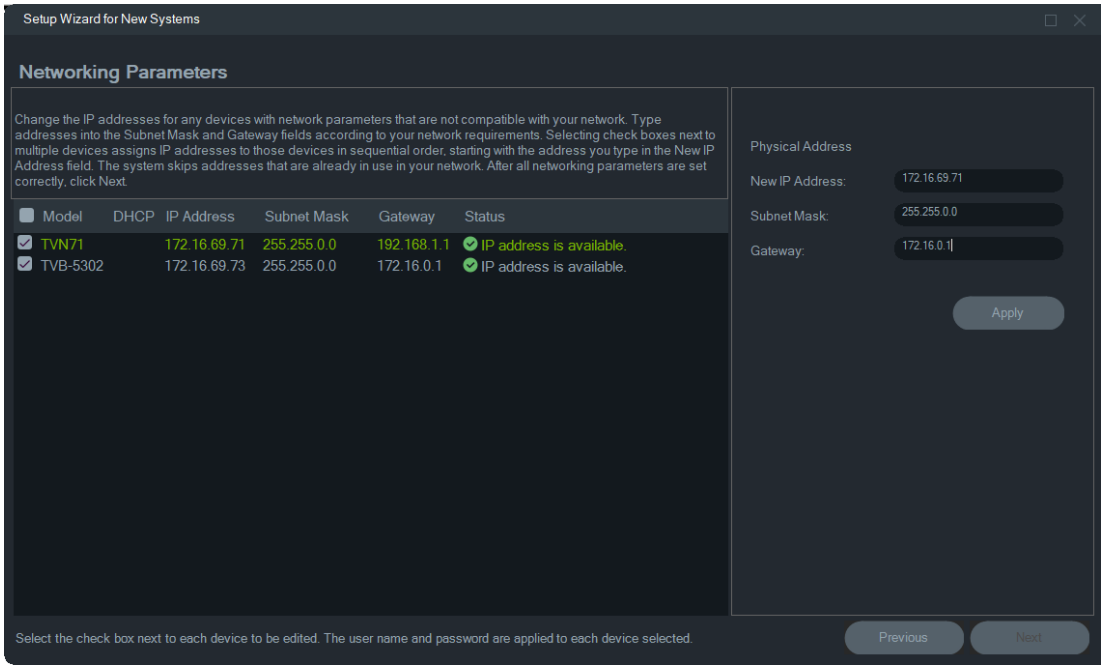
1. Click the **New System Setup Wizard** button in the Getting Started window.
2. Select a recorder and one or more cameras to set up in the Recorder Selection window.



3. In the Activate Device window, select one or more devices to continue with setup. If multiple devices are selected, IP addresses are automatically assigned in sequence (in this case, all devices must have the same password). Select individual devices to assign specific IP addresses to each. Type in a new IP address, subnet, and gateway manually or click an IP address to use default settings.
4. Type ‘admin’ as the user name and type in a new password for the device(s). Click **Apply** to determine if the IP addresses are available. Click **Next** when finished.

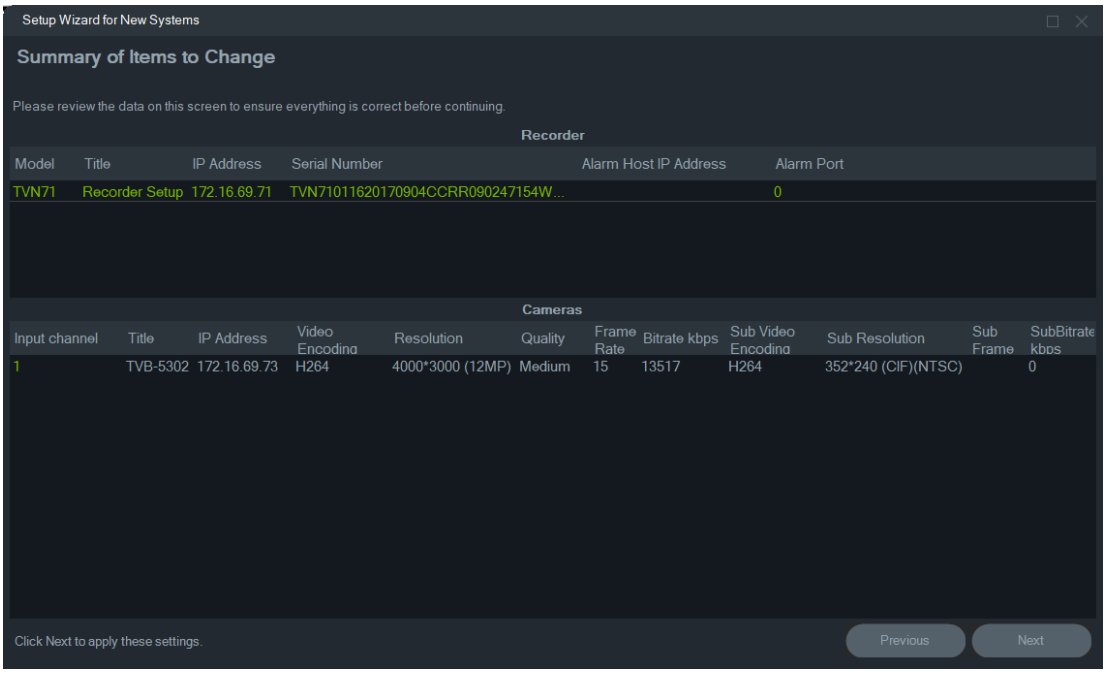


5. The Credentials Required window appears. Select the check box next to each device, type the user name and password, and then click **Apply**. Click **Next** when finished.
6. The Networking Parameters window appears. Change the IP addresses for any devices with network parameters that are not compatible with your network by typing addresses into the Subnet Mask and Gateway fields according to your network requirements. Selecting check boxes next to multiple devices assigns IP addresses to those devices in sequential order, starting with the address you type in the **New IP Address** field. The system skips addresses that are already in use in your network. Click **Apply** after all networking parameters are set correctly.



7. Click **Yes** to confirm the IP address changes. When finished, click **Next** again and wait several seconds for the storage calculator window to appear.
8. Select resolution and frame rate. If necessary, change the camera name and add substream information. The bitrate number auto-calculates and can also be changed if required. See “Storage calculator” **Error! Bookmark not defined.**66 for details. Click **Next**.
9. The Alarm Host Setup window appears. *Optional:* Select **Enable Alarm Host** to set the IP address of the client or server that will receive alarm notifications. The **Alarm Host IP** box is prepopulated with the IP address of the computer that the Wizard is running on. Type a different IP address in the **Alarm Host IP** box if required. If multiple NIC cards are present, the **Alarm Host IP** box has a drop-down list containing the IP address of each NIC card. Click **Next**.

10. The Summary window appears, showing the device information along with the location of the recorder configuration file. Click **Next**.



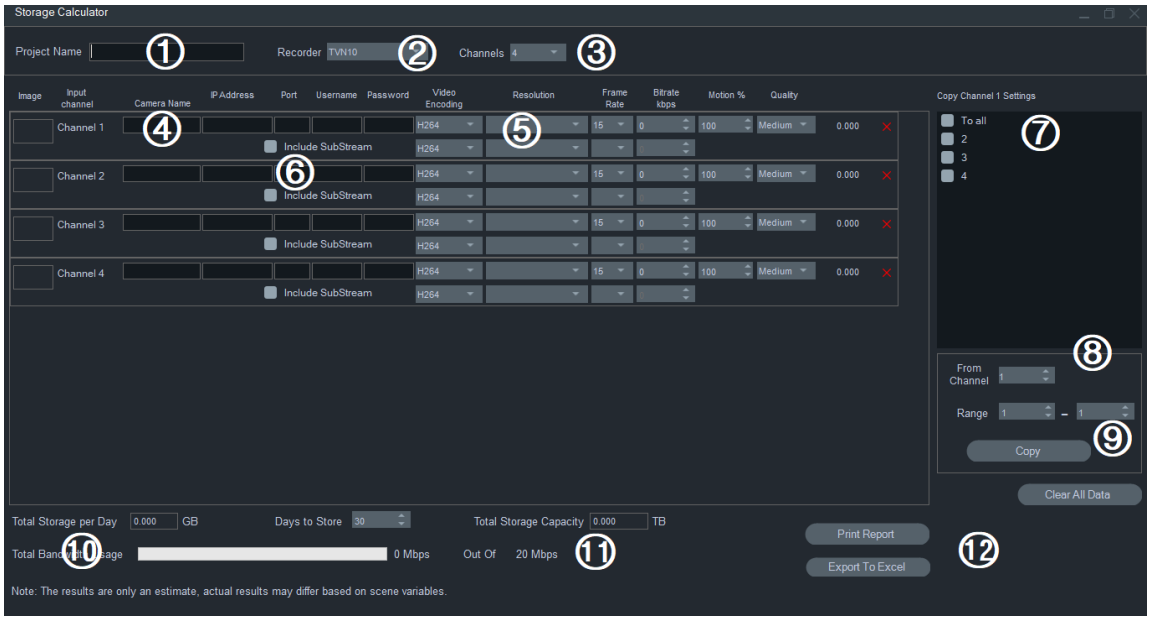
11. Click **Yes** to send the new configuration to the recorder.
12. The completion dialog appears. Click **Complete** to finish setup.

Storage calculator

Storage calculator is a tool that permits the creation of a storage capacity requirement report for TruVision recorders that can be printed or exported to Microsoft Excel (XLS file format).

IMPORTANT: Storage requirement calculations provided by the calculator are only an estimation based on medium quality video settings. More storage capacity could be needed depending on the scene complexity of images captured by the cameras.

Note: Storage calculator only supports the TruVision recorders listed in the **Recorder** drop-down list in the TruVision Storage Calculator window.



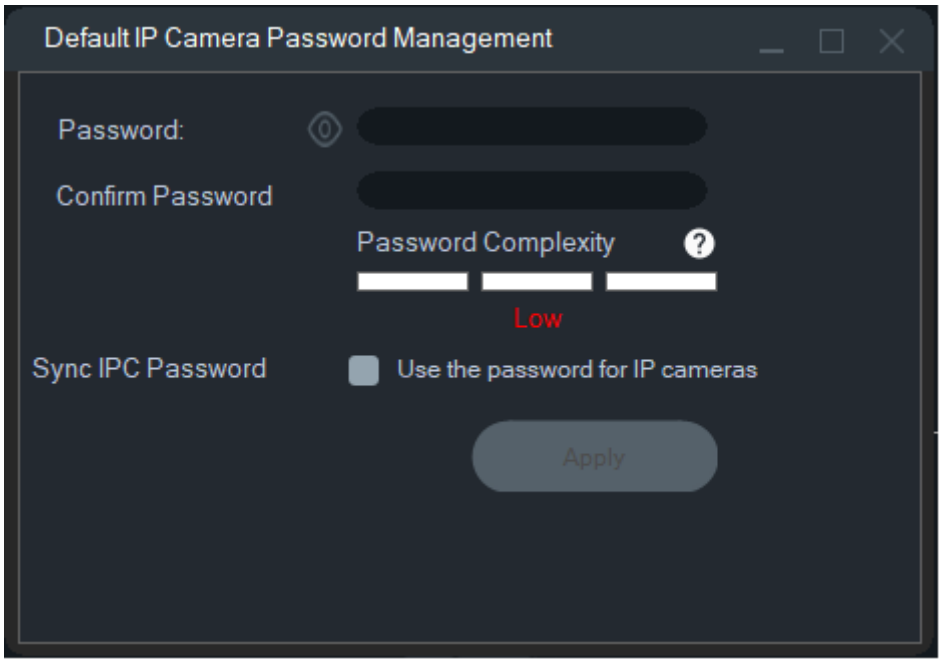
To generate a storage calculator report:

1. Click the **Storage Calculator** button in the Getting Started window.
2. Type a value into the **Project Name** field.
3. Select the recorder model from the **Recorder** drop-down list (2).
4. Select the number of camera channels in the **Channels** drop-down list (3).
5. Type camera names into the Camera Name (4) boxes as necessary and enter values for each camera in the Main Stream (5) and Substream (6) (if applicable) sections. Use the **Copy Channel 1 Settings** (7), **From Channel** (8), and **Range** (9) boxes to copy values between cameras.
6. The **Total Storage per Day** (10) and **Total Storage Capacity** (11) boxes populate with storage requirement calculations. When finished configuring the storage calculator project, click the **Print Report** or **Export to Excel** button (12) to generate a storage calculator report for future reference.

Set camera default password

Set the default password for all cameras after activating the recorder

Note: This feature is only supported on TVN 12 and TVR 17 recorders.



SNMP support (Version 2c)

Note: SNMP v2c has some known vulnerabilities. Take care when enabling it on a public network. Contact your network team and follow best practices before enabling it. Never use default community strings; only use unique community strings. Make sure that all security measures have been taken at your end.

TruVision Navigator supports Simple Network Management Protocol (SNMP). It makes it possible for the user to retrieve some specific data related to the status or health of devices. This works with SNMP Version 2c (which is also supported in TruVision devices).

In Device Manager, the Discovery Devices window allows the user to select discovered devices or devices that are already added in TruVision Navigator. By clicking the SNMP icon , the user opens the SNMP dialog.

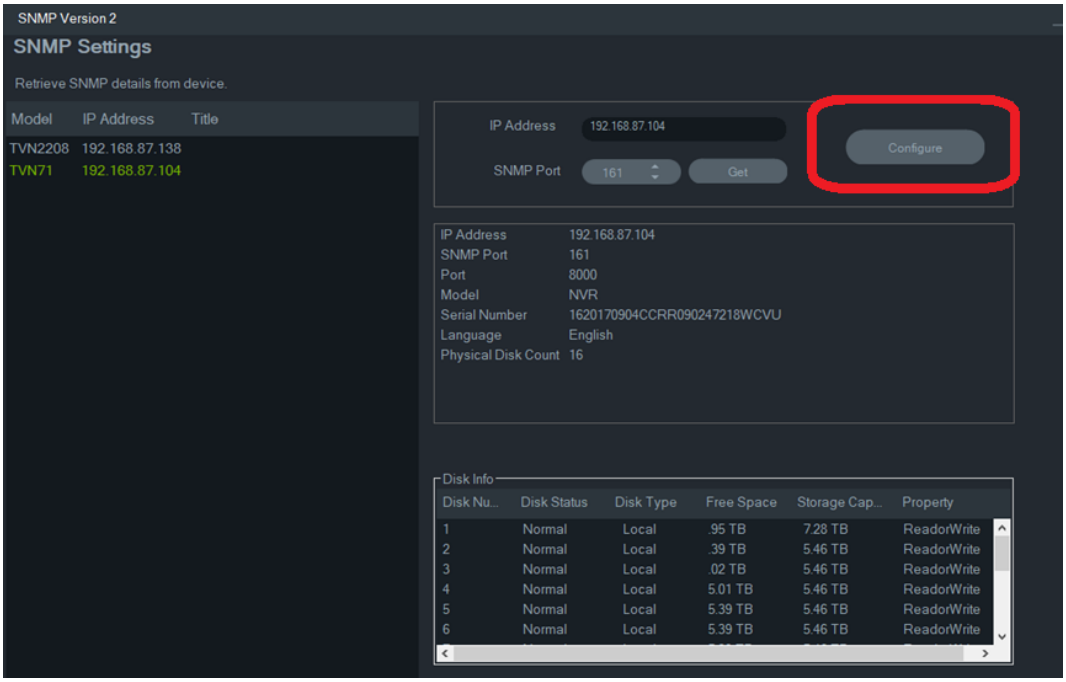
To discover devices using the SNMP icon:

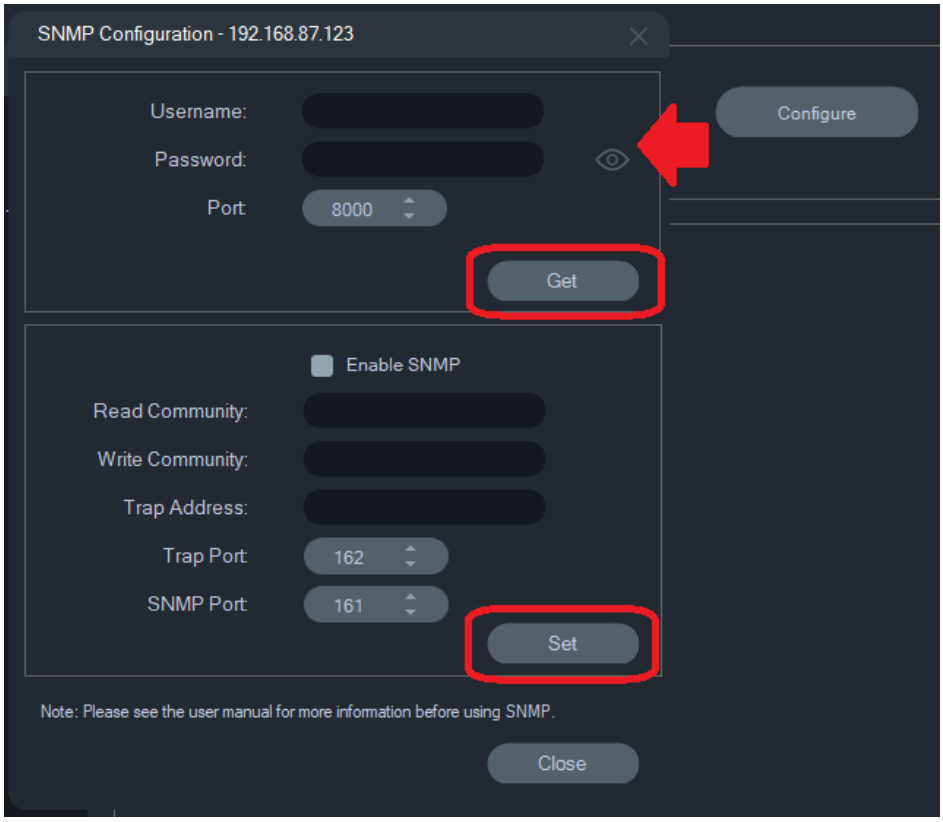
1. Select devices from Navigator tab or Discovered Devices (selection is optional).
2. Click the **SNMP** icon to populate the SNMP dialog in the SNMP Settings window.

To retrieve SNMP data:

1. SNMP dialog shows all the recorders/cameras that were selected in the Device Manager window (see “Device Manager window” on page 40). Navigate to a specific device to get its SNMP data.
2. If the device was not selected and is not displayed, enter the device’s IP address and by clicking the **Get** button retrieve the SNMP data of the device.
3. **Configuration button** allows the user to configure the SNMP settings on the device. Select a device from the left panel or enter the device’s IP address and click the **Configure** button.

Note: Different SNMP data will be displayed depending on the device type (recorder or camera).





To configure SNMP settings:

1. Enter the device credentials to configure the SNMP settings.
2. For devices already added to TruVision Navigator, the device credentials will be automatically populated.
3. For devices added or discovered manually, you must provide device credentials.
4. Click **Get** button to populate SNMP configuration settings.
5. Click **Set** button to change and save the SNMP settings on the device.

Chapter 5
Live view

Introduction

This chapter describes how to monitor live video using TruVision Navigator. It explains how to view camera streams, organize layouts, and interact with cameras during live monitoring.

Open live video

To add an item to a single video tile:

- Double-click a camera, map, or website in the Navigator panel to add it to the next open video tile.
- Drag a camera, map, or website from the Navigator panel to an open video tile.
- Double-click an applicable event in the Notifier or a Collector panel video or snapshot to add it to the next open video tile.
- Drag an applicable event in the Notifier or a Collector panel video or snapshot to an open video tile.

To add items to multiple tiles:

- Drag a recorder or logical view from the Navigator panel to an open video tile.
- Hold down Shift while clicking the right mouse button or hold down Ctrl while clicking the right mouse button to select multiple cameras, maps, or websites in the Navigator panel and drag them to an open video tile.

When adding multiple items, tiles automatically increase in number and the layout adjusts based on how many items are being added, unless the layout has been locked with the **Lock Current Layout** button.

Double-clicking in any single tile enlarges it to full screen. Double-clicking the full screen tile restores the previous tile layout.

Note: To ensure that a web page displays correctly in full screen mode, double-click the green bar at the top of the web page's video tile.

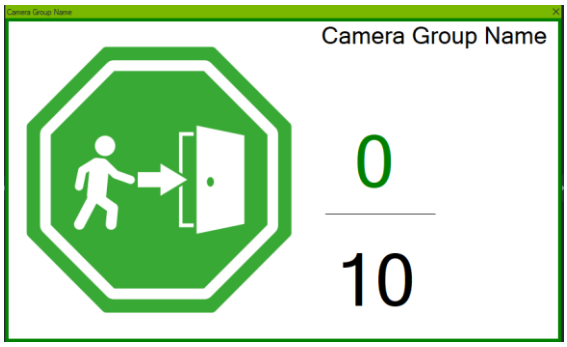
Organize/swap items in the Viewer by dragging a video tile's status bar to another video tile.

To add real-time people counting results into a video tile:

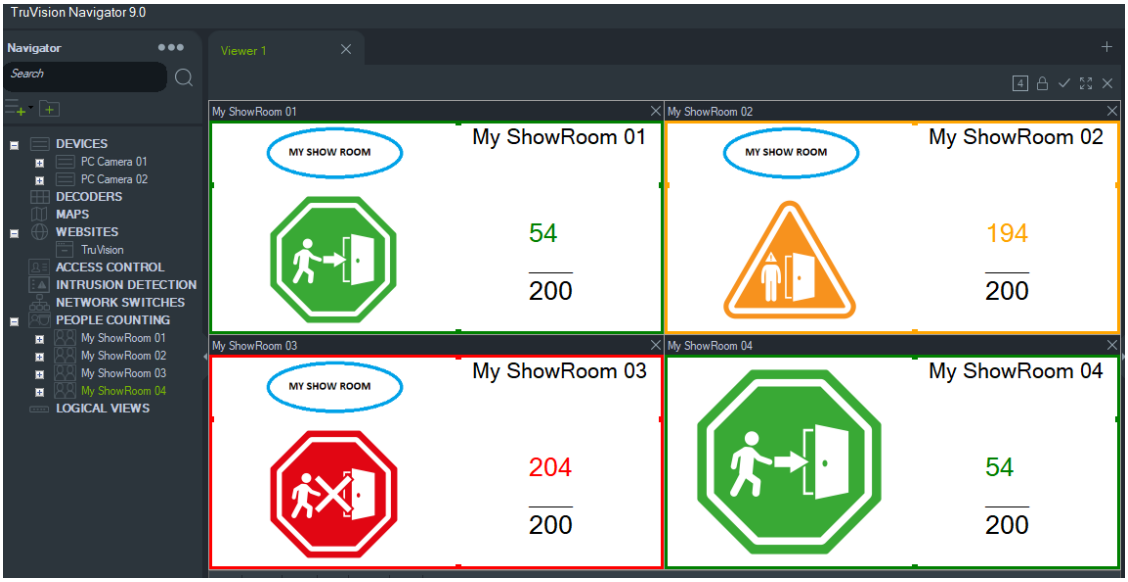
Drag and drop a people counting group from the device tree to one of the available tiles in the live viewer. The real time counting results of that camera group will be displayed.

The camera group name, the traffic sign icon and the actual counting results (and if configured the max. permitted number) will be displayed.

Below is an example of a live people counting displayed on a viewer tile in the Navigator:



Below is an example of the Navigator multi-tile view:



Tabbed viewer panels

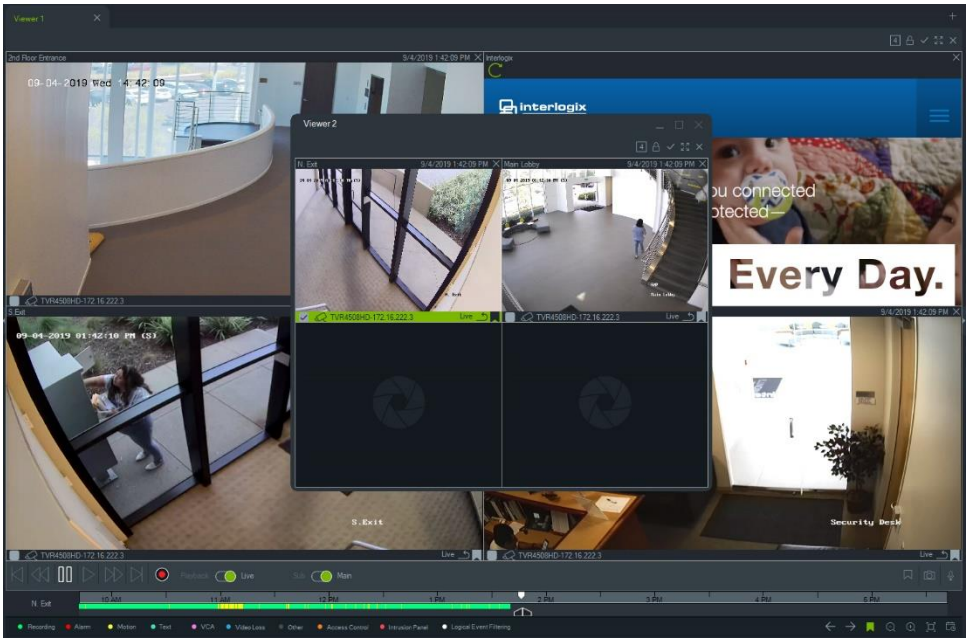
Multiple tabbed viewer panels can be added to the Viewer (up to 10). These additional viewer panels can also be detached and become free floating windows.

Videos in tabs not in the background can be paused to improve system performance. See "Client" on page 199.

Note: The application advises limiting video streams to 64 by using more sub-streams and fewer main streams to enhance streaming efficiency. Running an excessive number of videos in tabbed viewer panels can adversely affect system performance.

To add a tabbed viewer panel:

1. Click the **New Viewer** button to add a new layout panel. A new viewing panel is added as a tab in the Viewer panel title bar.
2. Populate the new viewing panel as described above. Drag a viewer tab out of the Viewer title bar to turn the viewing panel into a free-floating window accessible in the Windows taskbar. Drag the free-floating panel back into the title bar to access it again as a tab.



3. Right-click a viewing panel tab to access the tab's context menu (**Delete Tab** or **Rename Tab**).

Viewer tab button functions

	**Custom/sequence view**. Use custom views to define and save multi-site view templates for future use.
	**Lock Current Layout**. Prevents changes to the current viewer panel setup.
	**Select all**. Select all tiles in the viewer.
	**Toggle**. Toggle between normal view and maximized view.
	**Close All**. Close all tiles in the viewer.
	**New Viewer**. Add a tabbed viewing panel (10 maximum).

Adding a V-Stream

V-Streams combine output from all camera channels in a recorder into a single stream. V-Streams only appear if they are configured in the recorder.

To view a V-Stream, click a V-Stream icon in the Navigator panel and drag it to a video tile in the Viewer panel.

Video stream limits

The TruVision Navigator application recommends utilizing more sub-streams and fewer main streams to optimize the number of videos you can stream. This recommendation helps maintain better performance and resource management. Refer to Appendix A “Minimum system requirements” on page 257 for more details.

- **Recommended limit:** The application recommends streaming up to 64 video streams to maintain optimal performance. Exceeding this limit may result in a decline in application performance.

  Warning message: The application displays the following warning message upon exceeding 64 streams.

  “You have exceeded the recommended limit of 64 video streams. App performance may degrade with more streams. The maximum limit is 100.”

- **Maximum limit:** The application allows streaming up to 100 video streams. Reaching this limit will prevent additional streams from opening.

  Error message: The application displays the following error message upon exceeding 100 streams.

“You have reached the maximum limit of 100 video streams. Please close some streams to continue.”

Note: For streaming multiple cameras, it is recommended to stream from recorders rather than adding each camera individually to the Navigator.

Viewer performance depends on several factors, including:

- Number of active video streams
- Selected stream type (main stream or substream)
- Client hardware capabilities If performance issues occur, adjust client settings to optimize resource usage.

Viewer overview

The Viewer panel is used to display live video, playback video, maps, and other content. Video streams are shown in tiles, allowing multiple cameras to be viewed at the same time.

The Viewer panel consists of:

- Video tiles that display camera streams
- Tabs that allow switching between different views
- Panels such as the Event Monitor and Notifier, used to display events and alerts

The Viewer panel can display different types of content, including:

- Live video from cameras
- Maps and floor plans
- Other system elements such as websites

Content can be opened in the Viewer by dragging items from the Navigator panel or by double-clicking them.

Adding folders

Adding folders provides a way to organize Navigator panel items in a logical manner.

To organize the Navigator panel:

1. Click a top-level node (Devices, Maps, Websites, Access Control, Intrusion Detection, Network Switches, or Logical Views) and click the **Add Folder** button . This creates a new folder.
2. Type a name for the new folder and press Enter.
3. To add a sub-folder within the previously created folder, right-click the parent folder and select **Add Folder**.
4. Click and drag items into folders or folders within folders. Cameras always stay attached to their respective devices.

Manage layouts

Layouts define how video tiles are arranged in the Viewer panel. They allow multiple cameras to be displayed simultaneously in different grid configurations.

The Viewer supports various layout options, such as:

- Single view (1 camera)
- Multi-camera grids (for example, 2x2, 3x3, or 4x4)

To change the layout:

1. Select a layout option in the Viewer panel
2. Choose the desired grid
3. The layout updates automatically

To display cameras in a layout:

- Drag a camera from the Navigator panel into a tile
- Repeat for additional tiles as needed

To replace a camera in a tile:

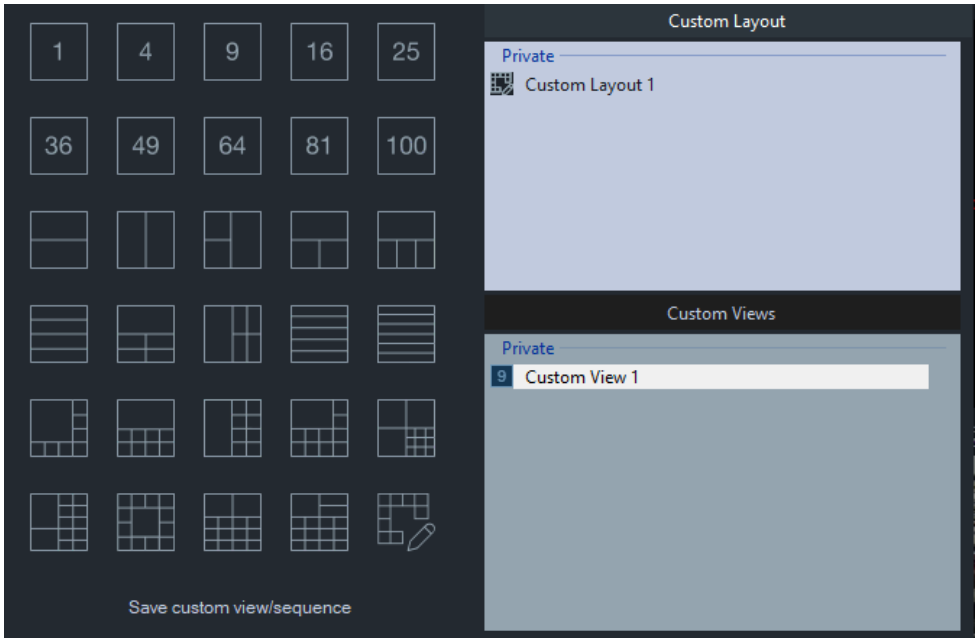
- Drag a different camera into the tile

Custom Views/Logical Views

Custom Views

Custom views allow you to save a specific layout of cameras for quick access. They are useful for monitoring predefined groups of cameras and quickly switching between different viewing configurations.

Note: A maximum of 20-30 custom views can be created. The maximum number depends on the complexity of the custom views (factors such as tile layout, number of videos in the tiles, and names of the custom views).



To create a custom view:

1. Load all the cameras to be included in the custom view into the Viewer.
2. Click the **Custom View** button in the Viewer panel header bar.
3. Select **Save custom view/sequence**.
4. Type a title in the **Title** field.
5. Click **OK**.
6. Close all videos.
7. *Select the Custom View* title in the Viewer panel header bar drop-down list.

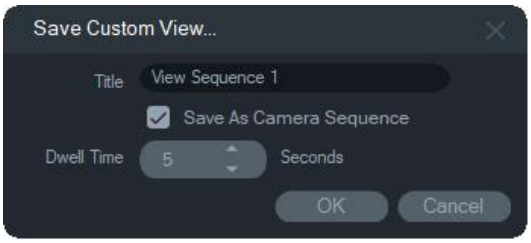
To load a custom view:

- Select the desired view from the list
- The Viewer updates to display the saved layout

To define a custom view as a camera sequence:

1. Load all the cameras to be included in the custom view into the Viewer.

   Note: Maps and websites are ignored in camera sequences.
2. Click the **Custom View** button in the Viewer panel header bar.
3. Select **Save custom view/sequence**.
4. Type a title in the **Title** field.
5. Create a single-screen sequence of each tile from left to right by selecting the **Save as camera sequence** check box.



6. If necessary, type a new value for dwell time in the **Dwell Time** field.
7. Click **OK**.
8. Close all videos.
9. *Select the Custom View* title in the Viewer panel header bar drop-down list. A custom view camera sequence is indicated by the icon. A single video tile displays each camera in sequence in the custom sequence.

To modify a custom view:

1. Right-click a custom view in the Custom View/Custom Layout window and select **Edit**.
2. Type a new title in the **New Title** box and click **OK**. Make changes to the custom view such as adding or removing an object from a tile, moving an object from one tile to another, or editing the layouts of custom views if their layouts are also custom.
3. Click **Save** when finished.

To make a custom view public (client/server installations only):

Right-click a custom view in the Custom View/Custom Layout window and select **Make Public** to make the custom view available across the network.

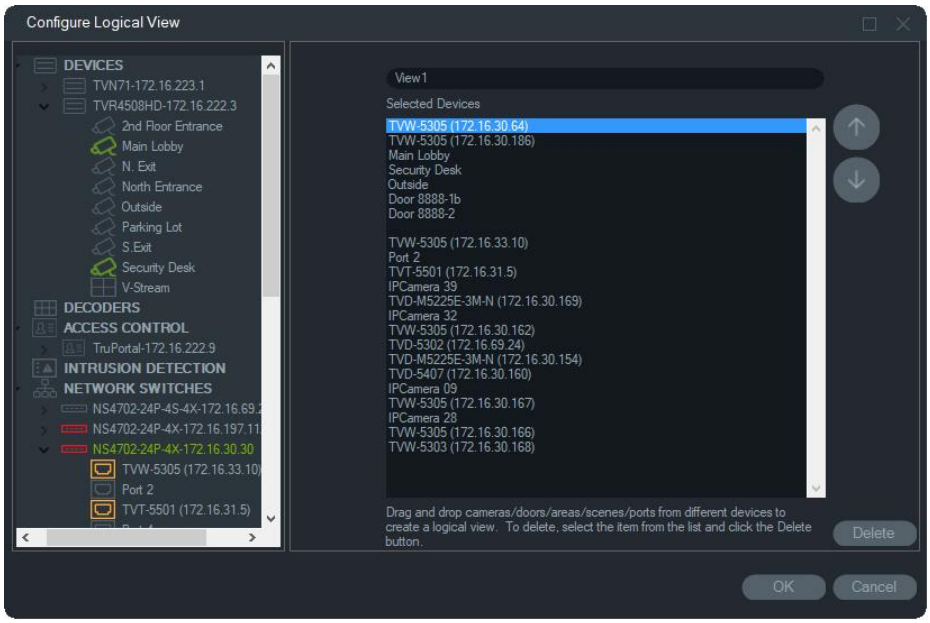
Note: Public custom views cannot be made private, and only the user who created the custom view can delete it.

Logical views

Logical views provide the flexibility to display the physical devices in any configuration required.

To add a logical view:

1. Right-click the Logical View node in the Navigator panel and select **Add Logical View**. The Configure Logical View window appears.
2. Type a title for the view in the **View Name** field, and then drag and drop devices from the Logical View panel into the **Selected Devices** box.



3. Use the up and down arrow buttons to move devices within the list. When finished, click **OK** to create the new logical view. To delete a logical view, right-click the logical view icon in the Navigator panel and select **Delete**.

Custom layouts

In addition to the standard tile layouts provided, you can also create custom tile layouts.

To create a custom layout:

1. Click the **Custom View** button in the Viewer header bar, and then click the  icon. The Custom Layout window appears.
2. The Custom Layout window displays a 5×5 layout by default. This can be changed by selecting 1×1, 2×2, 3×3, etc., up to 10×10.
3. Type a title for the layout in the **Title** box and select cells to merge by clicking and dragging inside the grid.

Note: A merge can only be performed on tiles that form a single square or rectangle.

4. Click  to complete the merge. Note that two previously merged cells can also be merged.
5. Click a merged cell and then click  to unmerge the cell.
6. Click **Save** to save the custom layout.

To edit a custom layout:

1. Ensure that the custom layout to be edited is closed in the Viewer Panel, and then right-click a custom layout in the Custom View/Custom Layout window and select **Edit**.
2. Make the required changes to the custom layout and click **Save**.

To make a custom layout public (client/server installations only):

Right-click a custom layout in the Custom View/Custom Layout window and select **Make Public** to make the custom layout available across the network.

Note: Public custom layouts cannot be made private, and only the user who created the custom view can delete it.

Control Video

Basic controls in the Viewer allow you to interact with live video and adjust how it is displayed.

To view a camera in full screen:

- Double-click the video tile or use the full screen option

To return to the previous view:

- Exit full screen or double-click again
-

To change the camera displayed in a tile:

- Drag a different camera from the Navigator panel into the tile

If supported, additional controls such as zoom and audio playback may be available to enhance the viewing experience.

Digital zoom

Navigator can perform digital zoom in/out functions in the live and recorded view. To zoom in, select a tile and scroll up with the mouse wheel. Scroll down to zoom out. When in digital zoom mode, click and hold the left mouse button to navigate in the zoomed image.

Note: Press Ctrl before scrolling the mouse wheel to enable digital zoom on a PTZ camera.

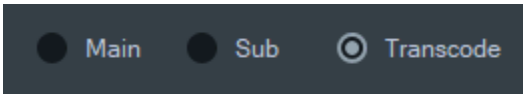
Create a snapshot during live view

Taking a snapshot of a selected video tile containing a camera sends a still image file to the Collector for export.

To take and deploy a snapshot:

1. Click the **Snapshot** button above the timeline or right-click a video tile containing a camera and select **Snapshot**.
2. Right-click the snapshot in the Collector panel to **Print Preview**, **Print**, **Email**, **Rename**, or **Export** the snapshot image. See “Export video” on page 139.

Video streams



Select one of the stream type options **Main**, **Sub** or **Transcode**, or right-click the video tile and select **Stream** and then **Sub**, **Stream** and then **Main**, or **Stream** and then **Transcode**.

Use transcoding when you want to show one camera in a lower resolution than the main or substream resolution. This helps to display a view from a camera over a slow network connection.

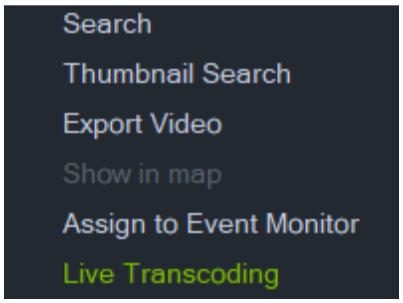
The **Main** setting provides the highest possible resolution. The **Sub** setting activates a substream for a lower resolution video that does not consume as much bandwidth.

The **Transcode** option uses the transcoded stream from the recorder. Transcoding is only supported by these recorders and in the following modes:

Recorder model	Live	Playback
TVR 45HD	Not supported	Supported
TVR 46	Not supported	Supported
TVN 22 (S/P)	Supported	Supported
TVN 23 (S/P)	Supported	Supported
TVN 71	Supported	Supported

Note: Transcoding can only be used for one channel at a time.

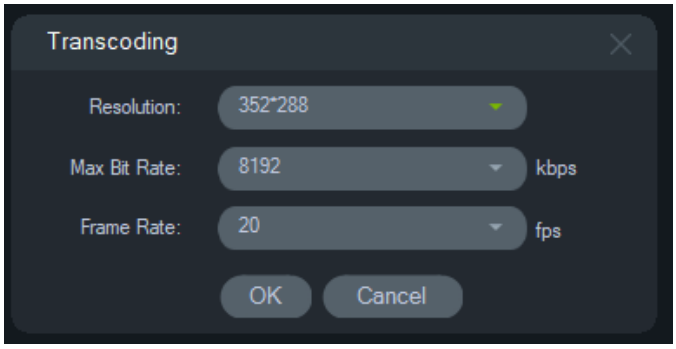
Live Transcoding uses pre-configured stream settings from the recorder, but you can change them from the Navigator Context Menu of the Camera to set the desired configuration.



Some recorders support also transcoding during playback. The user can select the quality of the stream during playback, which is useful when there is limited bandwidth available. The transcoding parameters must be set up before switching to the transcoded stream.

1. Select **Transcode** on the timeline or tile context menu. The Configuration window below appears.

2. Change the transcode playback stream configuration as desired.
3. Use the Transcoding configuration window to set the resolution, maximum bit rate, and frame rate for the transcoded stream. See graphic below:



The following transcoding parameters can be set-up:

- **Resolution**: Selections are: Auto, 4CIF, CIF, or QCIF
- **Bitrate**: Selections are: 32, 48, 64, 80, 96,128, 160,192, 224, 256, 320, 384, 448, 512, 640, 768, 896, 1024, 1280,1536,1792, 2048, 3072, 4096, or 8192
- **Frame rate**: Full frame rate, 22, 20, 18, 16,15, 12, 10, 8, 6, 4, 2, or 1

Event monitoring (basic use)

During live monitoring, events and alarms generated by devices can be displayed in the Viewer using tools such as the Event Monitor and Notifier. These tools allow users to quickly identify and respond to important incidents.

Events are displayed in the Event Monitor or Notifier panels. They typically include information such as the device, time, and type of event.

To view video associated with an event:

- Click the event in the Event Monitor or Notifier panel
- The corresponding video is displayed in the Viewer

When cameras are assigned to the Event Monitor, video from those cameras can be displayed automatically when an event occurs.

The Notifier panel is the central repository for notifications in Navigator. Devices send these notifications over the network via TCP to the IP address of the TruVision Navigator server. See Chapter 7 “Notifier configuration” on page 98 for more details.

Maps (basic)

Maps provide a graphical representation of locations where devices such as cameras are installed. They help users quickly locate and access devices during live monitoring.

Maps or floor plans can be added as PNG, JPEG, GIF, or BMP files.

To add a map:

1. Right-click the Map icon in the Navigator panel and select **Add Map**.
2. The Open Map File window appears. Navigate to the image file for the map required and click **Open**. The map appears in the Navigator panel under Maps.

To open a map:

- Double-click the map in the Navigator panel
- Or drag the map into a Viewer tile

To rename or delete a map:

- Right-click the map name in the Navigator panel and select **Rename Map** or **Delete Map**.

To view video from a map:

- Click a camera icon on the map
- The corresponding video is displayed in the Viewer

To navigate within a map:

- Click and drag to move the map inside the tile
- Use zoom options to adjust the view

Map icons may change appearance to indicate device status or events. When events occur, related devices on the map may be highlighted to help identify their location.

Maps can also include links to other items, such as submaps or websites, which can be opened directly from the map.

Dewarp views

Dewarping provides an alternate view other than the fisheye image normally associated with 360° cameras. This feature only requires one fisheye view (live or playback) from the device. The Navigator dewarps multiple views from a single dewarped view.

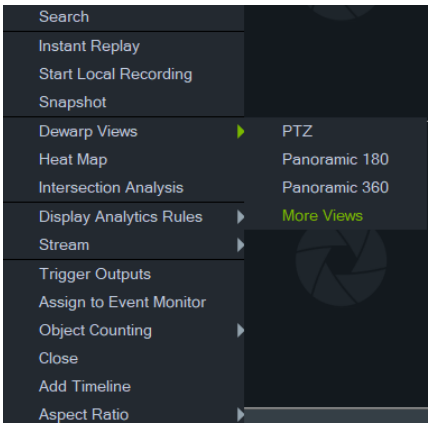
Note: PTZ, Panoramic 180° and Panoramic 360° view is only used for TVF-110x and third-party cameras. For TVF-510x and TVPA cameras, More Views option needs to be used.

To enable dewarping:

1. Right-click the camera recorder and select **Properties**.
2. Select the **Fisheye** check box.
3. The **Mount Type** drop-down list is set to **Ceiling** by default. If required, select **Wall** or **Desktop**.

To access dewarp views:

1. Right-click the camera video tile and select **Dewarp Views**.
2. Select a view from the context menu. A new video tile opens with the dewarped view type indicated in the video tile header bar.



PTZ

A maximum of 31 PTZ views can be dewarped from a single 360° camera.

Click the left mouse button inside the PTZ video tile and drag it in any direction to change the view. A red square inside the camera tile indicates the position of the dewarped view as the four-headed arrow cursor is moved inside the PTZ video tile.

Panoramic 180

This selection displays two 180° views inside a single video tile. Only one Panoramic 180 view can be dewarped from a single 360° camera, and then all other dewarp views become unavailable.

Panoramic 360

This selection displays a 360° view inside a single video tile. Only one Panoramic 360 view can be dewarped from a single 360° camera, and then up to 30 additional PTZ dewarp views become available.

Additional Dewarp Views

TruVision supports additional dewarp views for the TVF-520x and TVPA 360° cameras.

To access additional dewarp views:

1. Right-click the 360° camera in the device tree.
2. Select **Dewarp Views**.
3. Select **More Views**.

— OR —

1. Open the 360° camera view in a video tile.
2. Right-click and select **Dewarp Views**.
3. Select **More Views**.

A new specific dewarp viewer will open for the selected camera.

To select a Dewarp view:

In the top-right of the Viewer go to Dewarp Views buttons to select a dewarp view supported by the specific camera mount type (which has been set up in the Properties menu, see below).

To select a mount type:

Right-click the 360° camera in the device tree and select **Properties**. Go to the camera tab and select the mount type.

Notes

- During dewarping, you can switch between Live & Playback streams and use different Playback operations.
- When the main stream with the 360° view of the camera is closed, the corresponding dewarp viewer will also close.
- Wavy lines are observed when using TVF-520x 360° cameras for the dewarping of the sub stream. This can be avoided by using the same aspect ratio (4:3/16:9) for the main stream and the sub stream.

Tips for live monitoring

- Use layouts to display multiple cameras and adjust the view according to your monitoring needs.
- Create custom views for frequently used camera groups to quickly switch between configurations.
- Limit the number of cameras displayed at the same time to maintain optimal performance.
- Use lower resolution streams when monitoring many cameras simultaneously.
- Assign important cameras to the Event Monitor to ensure that key events are displayed automatically.
- Use maps to quickly locate devices and access cameras by clicking map icons.
- Drag and drop devices from the Navigator panel into the Viewer for quick access.

Chapter 6
Camera control

Overview

This chapter describes how to control cameras during live monitoring.
Camera control includes pan, tilt, and zoom (PTZ) operations, as well as presets and tours.

PTZ controls

PTZ controls allow users to adjust the camera view in real time.

To use PTZ controls, the camera must be identified to the recording device as a PTZ camera.

To activate a camera for PTZ:

1. Right-click the recorder icon in the Navigator panel and select **Properties**.
2. Click the **Cameras** tab and select the **PTZ Enabled** check box next to the PTZ camera.
3. Click **OK**. The camera's icon in the Navigator panel changes from a fixed camera icon to a PTZ camera icon.

To control a PTZ camera using the PTZ controls:

1. Drag a PTZ camera from the Navigator panel into the Viewer and select it.
2. Click the PTZ icon on the Controller toolbar above the timeline to open the PTZ window.

- **PTZ button**: Click and hold the arrows on the PTZ button to move the camera in different directions.
- **Zoom**: Click the − and + buttons to zoom in and out inside the PTZ camera video tile.
- **Focus, Autofocus**: Click the − and + buttons to manually focus the camera, or click the button to autofocus.
- **Iris**: Click the − and + buttons to adjust the size of the camera iris. The amount of light allowed into the camera increases as the iris opening gets larger.
- **Speed**: Set the speed to the appropriate level for the network and operations.

Note: PTZ control responsiveness varies depending on the frame rate, resolution, and quality of the video stream. D1/ 30FPS/Quality 9 provides the most responsive PTZ control over the network. Weigh PTZ control responsiveness against storage requirements to find the best fit. The PTZ speed setting can also be balanced with the stream configuration to find the best fit.

Preset positions

Presets are predefined camera positions that can be saved and recalled.

To create a preset:

1. Move the camera to the desired position.
2. Click the **Preset Positions** tab in the PTZ control window.
3. Type a name into the **Preset Name** field (if required), and then clicking **Set**.

Name or rename a preset by selecting the preset number from the drop-down list and typing a new name into the **Preset Name** field.

To use a preset:

1. Click the **Preset Positions** tab

2. Choose a preset number from the drop-down list
3. Click **Go To**.

Tours

A tour is a series of checkpoints assigned in a specific sequence with times assigned to reach each point.

Go to a tour preset by clicking the **Tours** tab, choosing a preset number from the drop-down list, and then clicking **Go To**.

Record a tour preset by clicking **Record** and performing a series of PTZ control actions. When finished, click **Stop**.

Note: The tours function is not available for all PTZ cameras. See Appendix B “Device details” on page 263 for applicable functionality.

To control a PTZ camera using mouse commands within the video tile:

1. Drag the PTZ camera from the Navigator panel into the Viewer and select it.
2. Place the cursor in the center of the Viewing tile.
3. Left-click and hold the mouse, then drag in any direction. Note that the further from center the cursor is positioned, the faster the camera moves.
4. *Optical zoom*: Scroll up with the mouse wheel to zoom in and scroll down with the mouse wheel to zoom out.
5. *Digital zoom*: Press and hold Ctrl and scroll up with the mouse wheel to zoom in and scroll down with the mouse wheel to zoom out. Press and hold Ctrl and zoom out as far as possible to deactivate digital zoom.

Note: An Aritech camera with a motorized lens can also be controlled as a PTZ camera with the PTZ controls for iris and focus adjustments.

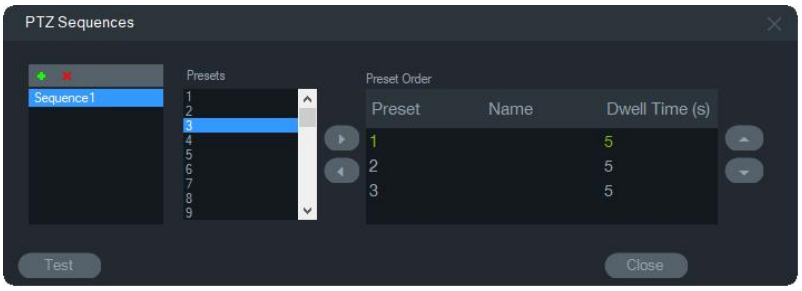
Preset sequences

A PTZ camera’s presets can be built into a sequence based on a specific order and dwell time. These sequences can be created, managed, and tested by right-clicking the PTZ camera in the Navigator panel and selecting **Preset Sequences** > **Manage Sequences**.

To create a preset PTZ sequence:

1. Click the ✚ button to add a sequence.
2. Type a name for the sequence or leave the default name as-is.
3. Click a preset number in the Presets list and then click the right arrow button to add the preset to the Preset Order list.

4. Repeat step 3 as necessary and use the up and down arrows to change the order of presets in the Preset Order list.



To test a preset sequence:

1. Create a preset sequence following the steps above.
2. Click **Test**. The sequence deploys in a video tile in the Viewer.
3. Click **Stop** to finish the test.

To stop or start a preset sequence:

Right-click the PTZ camera icon in the Navigator panel and select **Preset Sequences**, and then the name of the sequence to be stopped or started.

PTZ cameras can also be controlled automatically through Event-Actions.

For example, a PTZ camera can move to a predefined preset position when a specific event occurs, enabling automated monitoring of critical areas.

Use a USB keypad

The TVK-400 keypad can be used to control cameras and perform actions such as PTZ movement and bookmark creation.

Using the keypad:

- Control PTZ camera movement
- Trigger actions such as bookmarks
- Navigate cameras more efficiently

Note: Some functions (such as bookmarks) may require enabling corresponding settings in the client configuration.

Compatible keypads are:

- Aritech TVK-400USB

Connecting the keypad

The keypad must be connected to the client machine's USB port *before* launching the Navigator client. The keypad driver is installed automatically the first time the keypad is connected.

A successful connection of the keypad is indicated by the keypad icon appearing in the bottom right of the Navigator screen.

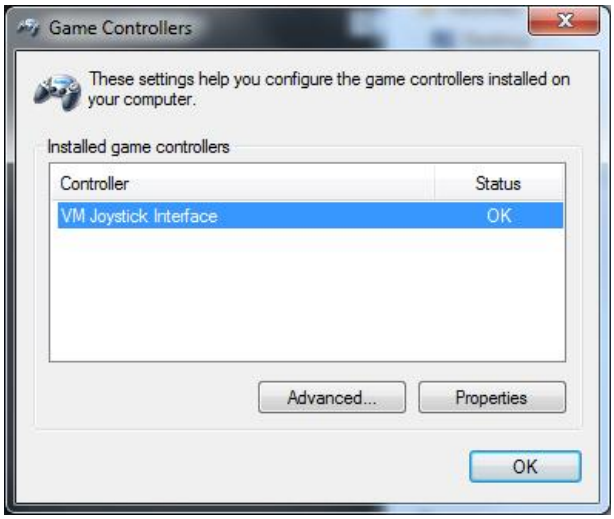
Calibrating the keypad

We recommend calibrating the keypad to avoid erratic PTZ movements.

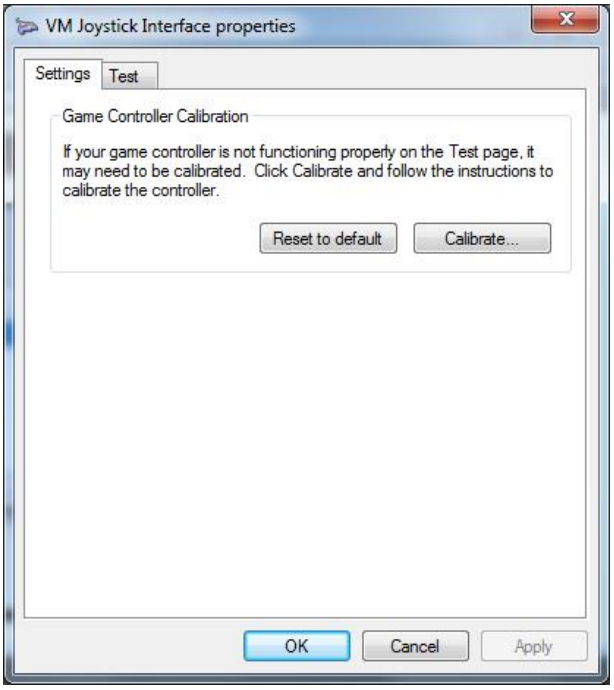
To calibrate the keypad:

Follow the instructions above for connecting the keypad.

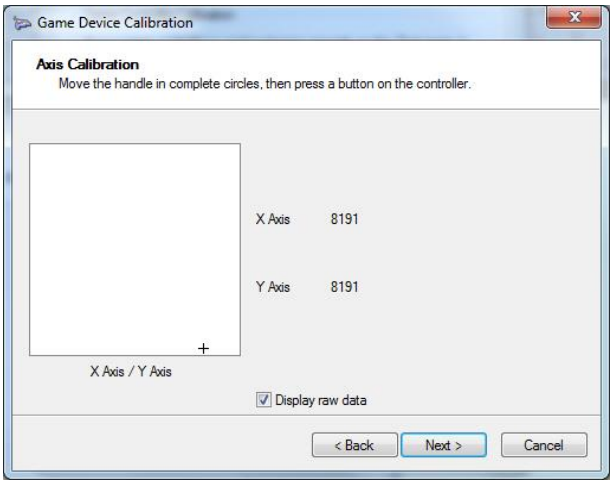
1. Go to **Control Panel** > **Devices and Printers**.
2. Right-click the VM Desktop icon and select **Game controller settings**.
3. The Game Controllers window appears. Click **Properties**.



4. Click the **Settings** tab, and then click **Calibrate**.

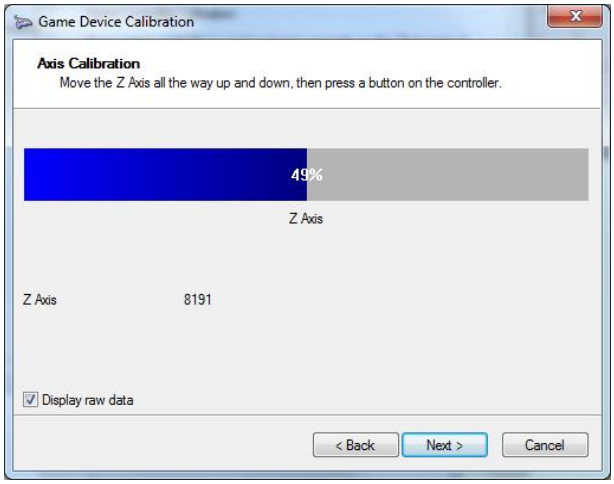


5. The Device Calibration Wizard appears. Click **Next**.
6. The Find Center Point window appears. Leave the keypad handle centered, press a button on the keypad, and then click **Next**.
7. The Axis Calibration window appears. Move the keypad handle in complete circles, press a button on the keypad, and then click **Next**.

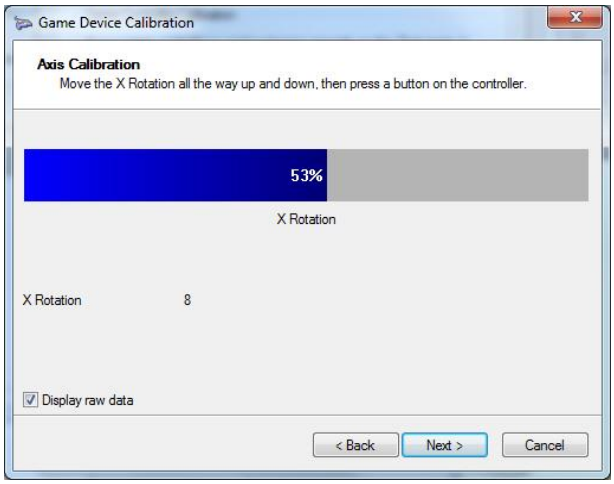


Note: Select **Display Raw Data** to see a numerical value for the current position of the keypad.

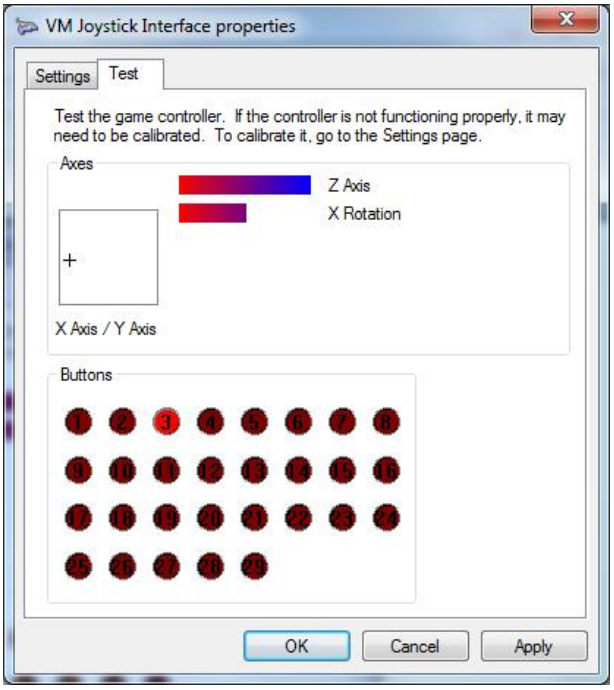
8. The Verify Center Point window appears. Leave the keypad handle centered, press a button on the keypad, and then click **Next**.
9. The Z Axis Calibration window appears. Twist the PTZ knob on top of the keypad handle, press a button on the keypad, and then click **Next**.



10.4 The X Axis Calibration window appears. Move the keypad handle all the way up and down, press a button on the keypad, and then click **Next**.



11. Click **Finish** to save the calibration settings.
12. Click the **Test** tab in the VM Joystick Interface properties window.



13. Test the keypad by moving it and observing onscreen behavior. The Axes indicators should indicate a value of 50% after moving the keypad or PTZ knob as far as possible one way or the other.
14. Press buttons on the keypad to test their functionality. Pressing a button should illuminate one of the circled numbers in the Buttons section.
15. Click **Apply**, and then click **OK** when finished.

Keypad functions

TVK400USB keypad

(1)Enter. Enters PTZ camera presets.
(2)Sub/Main stream switching.
(3)Number keys for selecting presets.
(4)Snapshot/Bookmark
(5)Go to playback.
(6)Switch to live.
(7)Scroll. Scrolls between video tiles in multi-up view and scrolls the timeline in one-up view.
(8)Wheel. Rotate right to fast forward and rotate left to rewind.
(9)Fast forward
(10)Pause/resume
(11)Rewind
(12)Keypad. PTZ: Rotate knob to zoom in/out, keypad moves the camera. Non PTZ: Rotate knob to zoom in/out, keypad pans inside the zoom in view.
(13)Zoom. Live: Zooms the camera in/out. Playback: Zooms in/out on the timeline.
(14)Iris open/close
(15)Focus near/far
(16)Set preset. Press this button, a preset number, and Enter to enter a new PTZ preset.
(17)Toggle between one-up and multi-up views.
(18)Local record

Chapter 7
Events and notifications

Overview

This chapter explains how to configure events and notifications in the system. Events are generated by devices and can trigger alerts, video display, or automated actions.

Event sources

Events can be generated by different system components, including:

- Cameras (motion detection, analytics)
- Recorders
- Access control systems
- Intrusion systems

Event configuration

The configuration of the events happens in the configuration menus of the devices. In the device you also need to configure that the event needs to be sent to the TruVision Navigator software.

This is done by adding the IP address of the TruVision Navigator server as Alarm Host IP address in the device.

The standard communication port between device and software is port 5001.

For event the action Notify Alarm Host/Surveillance Center needs to be enabled.

See the user/configuration manual of the device for instructions.

Event processing

Event handling in the system consists of two levels:

- Device-level configuration: defines which events are generated and sent to the system
- System-level processing: defines how the system responds to these events

System-level responses include notifications, Event Monitor behavior, and Event-Actions.

Event-Actions

Event-Actions define automated responses to events received by the system. They allow administrators to configure actions such as:

- Displaying video in the Event Monitor
- Triggering outputs (such as relays or alarms)
- Generating notifications

Event-Actions are configured in System Settings (see Chapter 14) and operate independently of device-level event configuration. They enable automation of system behavior and reduce the need for manual operator intervention.

Event Monitor configuration

Cameras can be assigned to the Event Monitor so that video is displayed automatically when an event occurs.

To assign a camera:

- Right-click the camera
- Select **Assign to Event Monitor**

Notifier configuration

The Notifier displays incoming events and alerts.

Filters can be applied to control which events are shown and how notifications are displayed.

Events received from devices are processed as notifications within the system. These notifications can be:

- Displayed in the Notifier panel
- Filtered based on criteria
- Used to trigger Event-Actions for automated responses

The Notifier panel is the central repository for notifications in Navigator. Devices send these notifications over the network via TCP to the IP address of the TruVision Navigator server. The firewall must be configured on the server to accept these network notifications. Refer to the recorder's or camera's user manual for information on configuring notifications so that they appear in the Notifier panel.

View video for live notifications as they are received by double-clicking the camera name link in the Notifier panel. This launches the video in the Viewer.

Note: Video is indicated by a video icon (with an arrow) next to the notification. If the video icon is not next to the notification, no video for the event is available.

Live notifications can be set to make an audible sound. See "Client" on page 199 for more information on this feature. After 1000 notifications occur in the Notifier panel, the oldest notifications are purged in the system.

Note: User defined notification such as logical events & action events display in the notifier. User activity notifications such as logged in/off & Video Export notifications displays in the notifier in Client/Server mode.

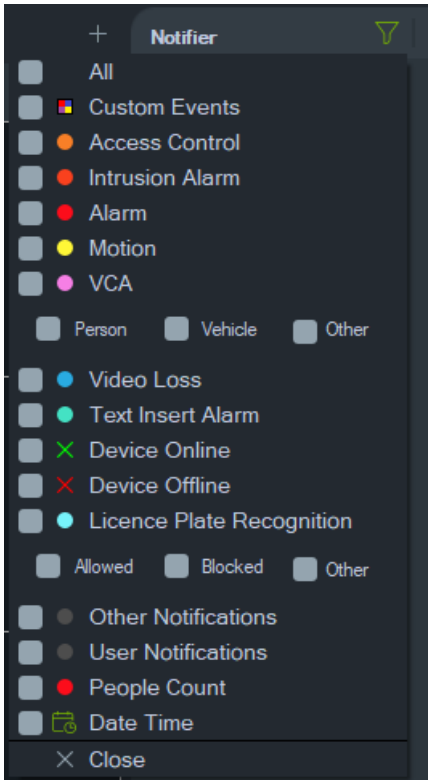
Filters

The Filters feature allows customization of the Notifier panel so that it shows only certain types of notifications.

To set filters in the Notifier panel:

1. Click the **Filters** button in the Notifier panel.

2. Select one or more notification types to show only those types of notifications in the Notifier panel. The **Filters** button turns red when a filter is set.



3. To show the selected events occurring only during a set time period, select **Date Time**, set the date and time range, and then click **OK**.
4. Click **Close**. To remove filters, click the **Filters** button and select **All** or click the individual notification types to remove the check marks.

Chapter 8
Analytics

Overview

Analytics features provide advanced insights based on video data and events generated by cameras.

These features help users detect patterns, monitor activity, and respond more effectively to situations.

Analytics functionality depends on the capabilities of the connected devices and their firmware versions.

Not all analytics features are supported on all devices. Analytics processing may also impact system performance. Use analytics features according to system capacity and operational requirements.

Analytics types

The system supports several types of analytics, including:

- People counting
- Parking management
- License plate recognition (ANPR / LPR)
- Heat maps
- Queue management
- Motion and video content analysis (VCA)

People counting

People counting analytics track the number of people entering and leaving a defined area. This information can be used for occupancy monitoring and flow analysis.

Users can:

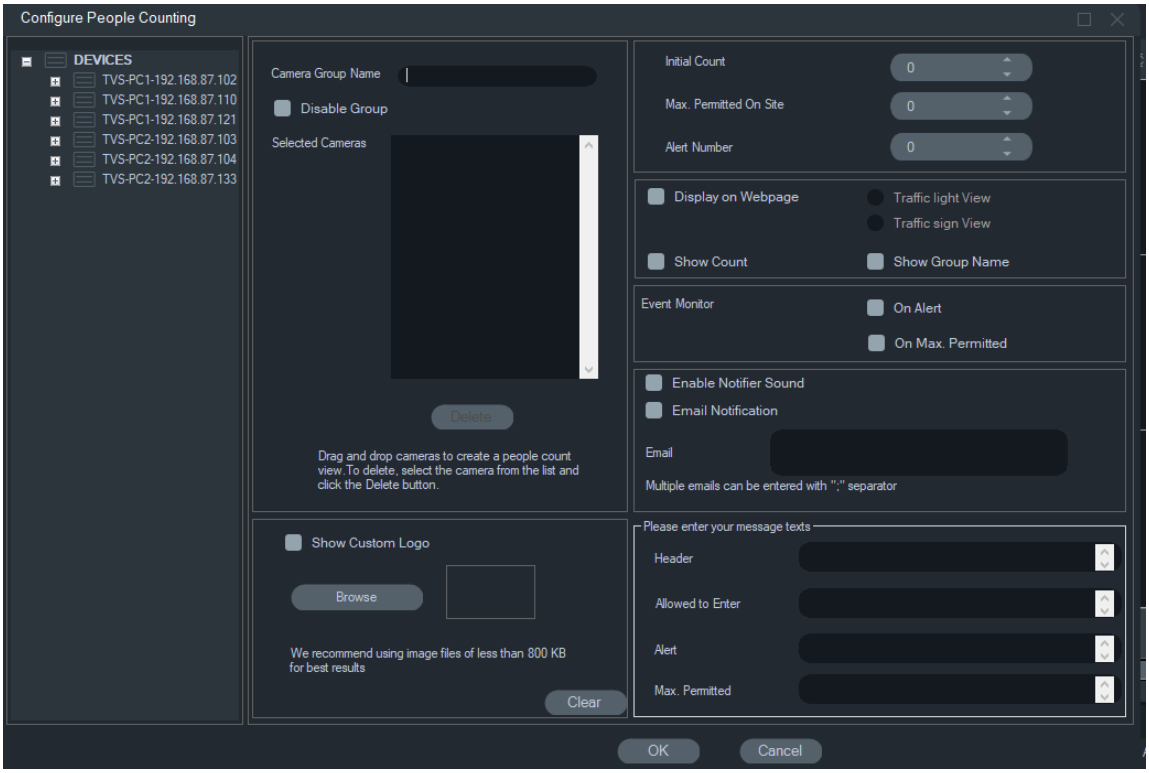
- View real-time counts
- Monitor occupancy levels
- Display counting data on maps

Adding people counting

TruVision people counting cameras can be added to the Navigator panel. The people counting camera is a dual lens camera. The camera is used to monitor entrances and exits, where it can count the number of people entering and leaving the premises.

To add and configure people counting groups:

1. Add people counting cameras into the Navigator, either manually, see “Add device manually if a device is not discovered:” **Error! Bookmark not defined.** or using the discovery tool, see “Adding devices using the discovery tool” **Error! Bookmark not defined.**.
2. In the Navigator tree, go to the People Counting node.
3. Right-click the People Counting node and select **Add People Counting**. The Configure People Counting window opens.



Camera Group Name	The people counting camera group name. This will also be displayed on the web page.
Disable Group	When checked, no count information is provided on this group.
Selected Cameras	People counting cameras selected from the navigator tree.
Initial Count	The initial count value that is used to take into account employees/staff that are already on the premises of the store or shop before it opens (before the actual counting starts). This number can also be added to total count on site, as some employees may enter the site via a different entrance that may not be monitored. When this initial value is not needed, set this value to 0.
Max Permitted On Site	Maximum number of people allowed on the site. When this number is reached, the maximum number is displayed in red. Set to 0 when not required.
Alert Number	The alert number is a number that is lower than the Max. Permitted on site and acts as a warning or alert number. When this number is reached, the alert number is displayed in orange. Set to 0 when not required.
Display on Web Page	A web page can be opened when the application is used in Client/Server mode. Selecting this check box will allow the user to use the web page.
Traffic Light View	Displays the icon of a traffic light on the web page.
Traffic Sign View	Displays the icon of a traffic sign on the web page.
Show Count	When checked, displays the counting data of the group on the web page or the viewer's tile.
Show Group Name	When checked, displays the group name on the web page or the viewer's tile.

Time	Scheduled counting reset time.
Event Monitor – On Alert	When checked and the Alert Number value has been reached, real time counting results will be displayed on the event monitor.
Event Monitor – On Max Permitted	When checked and the Max Permitted value has been reached, real time counting results will be displayed on the event monitor.
Enable Notifier Sound	When checked, the buzzer sound will be used when the counting events that come via the Notifier.
Email Notification	When checked, email notification are sent to the required recipients when Max. Permitted & Alert numbers are reached.
Email	Provide email addresses of the people that will be notified. Separate emails by ';' for multiple email IDs. Any email may be used, not only TruVision Navigator users.
Header	Header Display Text for the web page.
Allowed to Enter	Text displayed on the web page when the people can still enter and the number of people is less than the set value of Max. Permitted on site. The text can be entered by the user.
Alert	Text displayed on the web page when the number of people that have enter reaches Alert Number value. The text can be entered by the user.
Max Permitted	Text displayed on the web page when the number of people that have enter reaches Max Permitted on Site value. The text can be entered by the user.
Show Custom Logo	You can display your preferred logo on the web page or tile. For best results, an image file size of less than 800 KB is recommended.
Browse Logo	You can browse for your preferred logo.
Clear	Clears logo image from the configuration.

4. You can now create a camera group with one or more people counting cameras. For example, you can use a camera group per room, per site, or per area.
5. Provide a relevant name of the camera group. This name will also be visible on the web page.
6. Drag and drop the people counting cameras from the device tree into the list.
7. Setup count values, such as Initial Count, Maximum Permitted on Site, and Alert Number. See table above for more information about these count values.
8. If needed, set other configuration settings, such as web page display, event monitor display, reset counting time, and email notifications.
9. Click **OK**.

People Counting Reporting

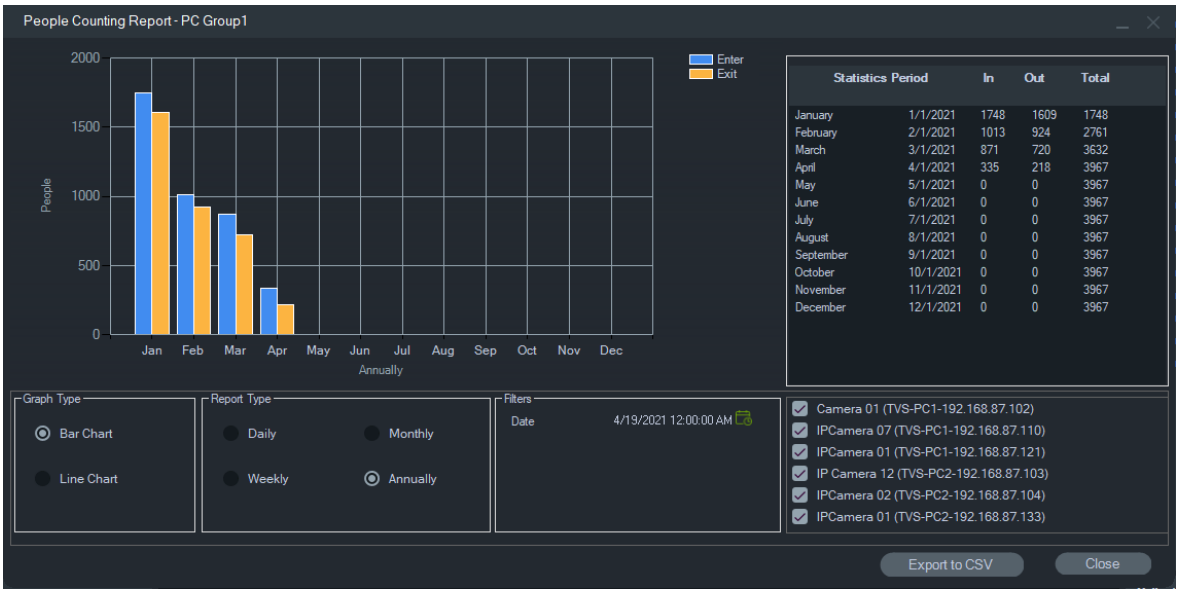
The People Counting Report displays the number of people counted over a defined period.

The report can be created for one or more people counting cameras in a people counting camera group or it can be created with data from different people counting camera groups.

To create a report for one people counting camera group:

Right-click the name of the group in the Device tree and select **Report**.

The People Counting Report window opens.



Graph Type	Select bar chart or line chart.
Report Type	Select Daily, Weekly, Monthly or Annually.
Filters	Define the date and the time range for the report.
Camera selection	Select the cameras to be used for this report.
Statistics table	Shows the number of people that entered/exited, and the total number of visitors for the selected cameras.

You can export the data in CSV format for further processing.

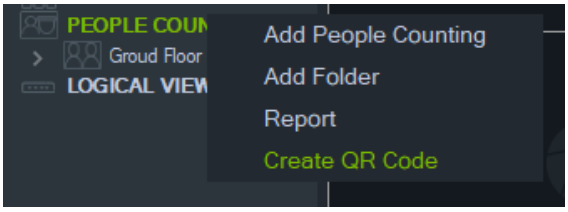
To create a report for multiple people counting camera groups:

1. Right-click the People counting node in the device tree and select **Report**.
2. The report window displays all the possible selections. You can select one or more people counting camera groups for the report.

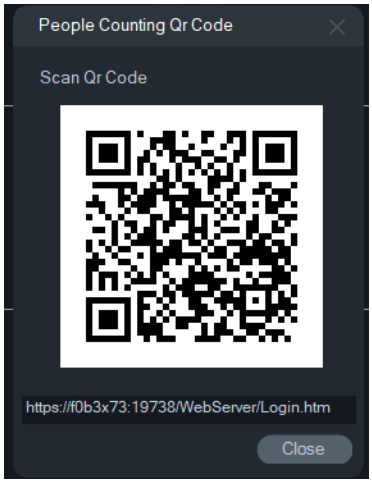
People Counting QR Code

To create a people counting QR code:

1. Right-click the People counting node in the device tree and select **Create QR Code**.



The QR code will be displayed.



2. The user scans it with a mobile device to open the People Counting webpage.

Parking management

Parking management analytics provide real-time and historical information about vehicle occupancy and availability in parking areas.

These features help monitor parking usage, detect available spaces, and improve traffic flow.

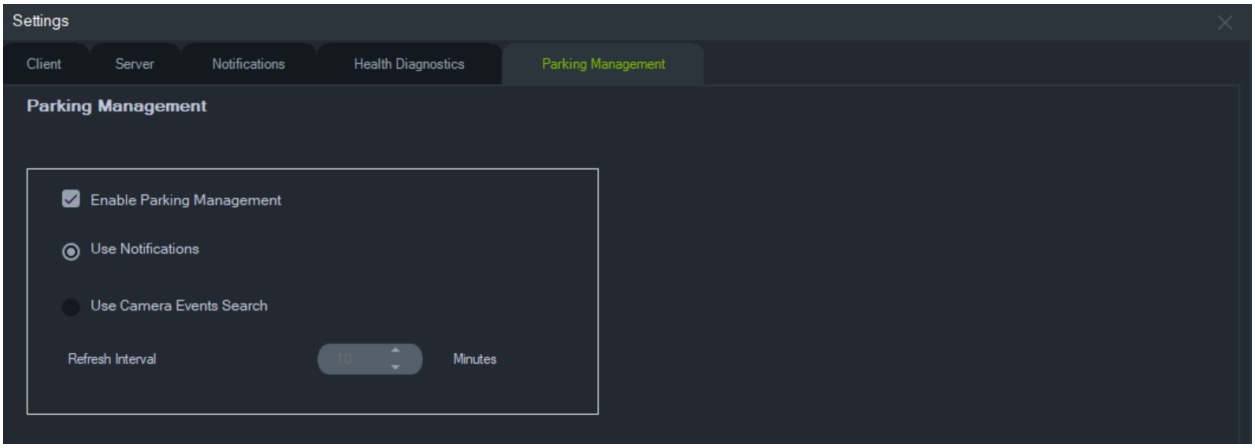
Usage

Users can:

- Monitor the number of occupied and available parking spaces
- View parking occupancy in real time
- Identify high-usage areas
- Analyze parking trends over time

Notes

- Parking management features depend on supported camera models
- Configuration of parking zones and rules is performed in the device configuration



The Parking Management tab in the Settings window provides the following server settings:

- **Enable Parking Management**: Activates Parking Management in the TruVision Navigator Application.
- **Use Notifications**: When enabled, Parking Management utilizes live notification received in TruVision Navigator for the license plate recognition cameras (ANPR Cameras).
- **Use Camera Event Search**: When enabled, Parking Management uses notifications stored in the camera at specified intervals for the license plate recognition cameras (ANPR Cameras).
- **Refresh Interval**: This option is available if Use Camera Event Search is enabled. It specifies the frequency at which data is fetched.

Note: This feature is supported by the ANPR camera models TVLP-S01-0401-BUL-G and TVLP-S01-0402-BUL-G.

Adding Parking Zone

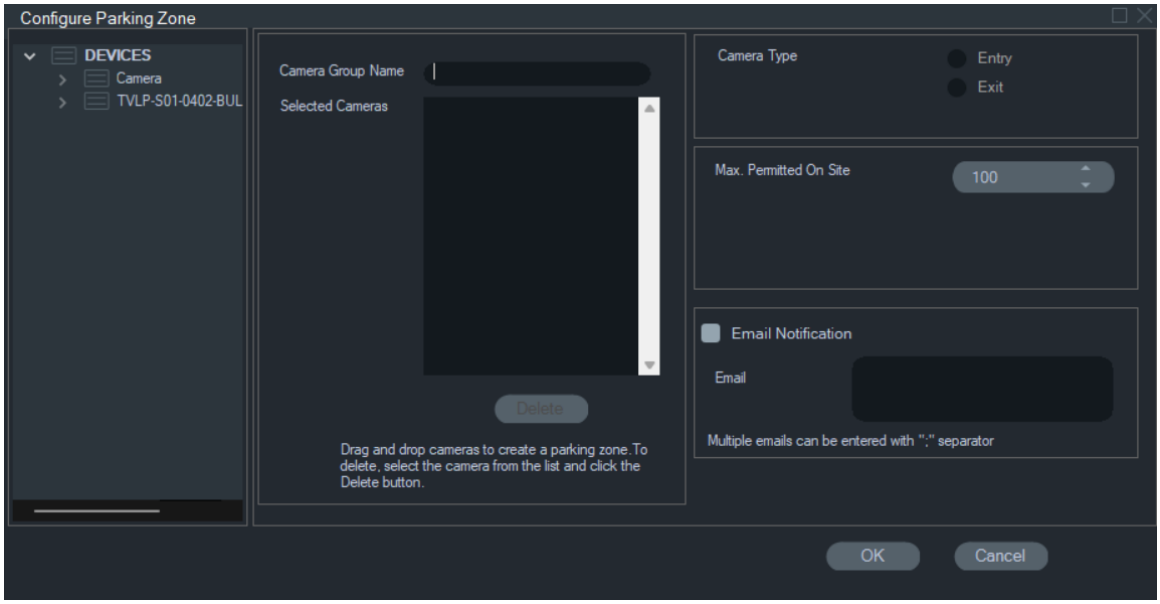
TruVision ANPR cameras can be added to the Navigator panel. The ANPR Cameras generates notification based on vehicle number plates. The camera is used to monitor vehicle number plates, where it can recognize allowed/blocked vehicle numbers and notifies the TruVision Navigator application.

To add and configure Parking Zones:

1. Add ANPR cameras into the Navigator, either manually (see “Add device manually if a device is not discovered:” on page 42) or using the discovery tool (see “Adding devices using the discovery tool” on page 41).

2. In the **Navigator tree**, go to the **Parking Zone** node.
3. Right-click the **Parking Zone** node and select **Add Parking Zone**.

   The Configure Parking Zone window opens.



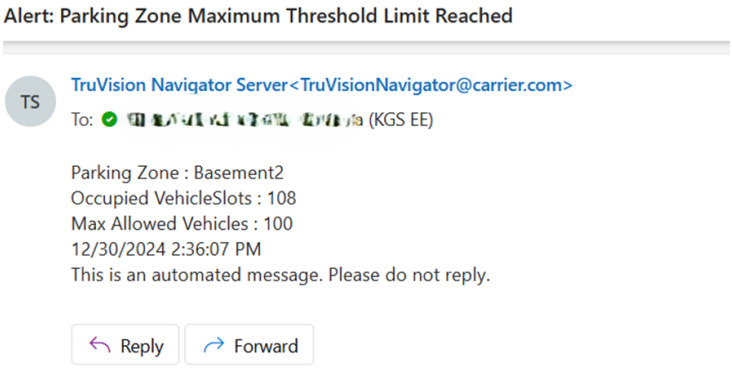
- **Camera Group Name**: The parking zone camera group name.
- **Selected Cameras**: Parking zone cameras selected from the navigator tree.
- **Camera Type**: Each Camera added to the Group, should be set to Entry or Exit. Which means Entry camera covers the entrance of the vehicle into parking zone. Exit camera covers the leaving vehicle from the parking zone.
- **Max Permitted Site**: Each parking zone can have a maximum number of spaces. The default value is 1. The value can be increased/decreased as needed.
- **Email Notification**: When checked, an email notification will be send to the required recipients when Max. Permitted & Alert numbers are reached.
- **Email**: Provide email addresses of the people that will be notified. Separate emails by ';' for multiple email IDs. Any email may be used, not only TruVision Navigator users.

User can create a camera group with one or more ANPR cameras. For example, user can use a camera group per parking area/zone.

1. Provide a relevant name of the camera group, which is the parking zone title.
2. Drag and drop the ANPR cameras from the device tree into the list.
3. Select **Entry or Exit** type for each camera.
4. Set **Maximum permitted on site** value for the parking zone.

5. If people need to be informed about the status of the parking zone, check **Email Notification** and configure the email addresses of the users that need to receive the notifications.
6. Click **OK**.

The configured email addresses will receive emails when the maximum allowed number of vehicles has been reached.

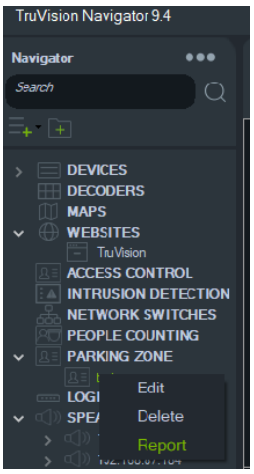


Parking Zone reporting

The Parking Management Report displays the number of vehicles Entry/Exit count over a defined period. The report can be created for one or more ANPR cameras in a parking zone camera group.

To create a report for Parking Zone:

1. Right-click the name of the group in the Device tree and select Report.



2. The Parking Management Report window opens.

- **Graph Type**: Bar graph, shown the total number of vehicles In/Out for the selected Entry Time and Exit Time with hour on X-Axis and Vehicle Count on Y-Axis.
- **Report Type**: Only 24 hours of date time range data can be shown in the graph.
- **Filters**: Define the date and the time range for the report and filter parking duration by hours/by minutes as well as a combination of all list types.
- **Refresh**: Reset all the controls to their default values and update only the Exit Time with the current date time.
- **Export to CSV**: You can export the selected date range of Parking Management Report data to the CSV file format.
- **Search**: To search for a license plate, set the following parameters:

  - **License Plate**: Search License Plate Number using a full/partial license plate number.

  - **License Plate Type**: Search License Plate Type based on a list type, such as Allowed, Blocked and Others.

  - **Entry Time**: Search License Plate Number using vehicles Entry Time.

  - **Exit Time**: Search License Plate Number using vehicles Exit Time.

  - **Duration**: Search License Plate Number using vehicles Duration Time.

  - **Apply:** By default, the Parking Management Report displays data based on the specified entry and exit times without a duration filter. However, you can filter the data by hours or minutes within these durations by clicking the Apply button.

Note: When the Parking Management Report window opens. The default Entry Time and Exit Time range is the latest hour data from the current time, with License Plate Type set to ‘All’ and duration range set to 0 to 24 hours.

License plate recognition (ANPR/LPR)

License Plate Recognition (LPR) identifies and records vehicle license plate numbers.

This feature is used for access control, monitoring, and investigation.

Users can:

- View license plate data in real time
- Search for specific license plates
- Managing license plate information in recorders and ANPR cameras

Show real time LPR

This function applies to TruVision Automatic Number Plate Recognition (ANPR) cameras that feature embedded Optical Character Recognition (OCR) to identify vehicle license plate information in real time.

Note: TruVision ANPR cameras are only available in EMEA and can only read license plates from certain countries (US not included) depending on the firmware version.

Table 2: Supported license plate regions

Firmware V13.x FPx (default loaded FW)	Slovakia, Italy, Spain, France, Germany, Poland, Belgium, France, Czech Republic, Netherlands, Denmark, Luxembourg, Greece, Albania, Bosnia and Herzegovina, Ireland, Malta, Sweden, Switzerland, Portugal, Macedonia, Croatia, Finland, United Kingdom, Romania, Serbia, Bulgaria, Norway, Israel, Hungary, Austria, Vatican City State, Cyprus, Iceland, Slovenia, Turkey, Montenegro
Firmware V14.x FPx	South Africa
Firmware V15.x FPx	Azerbaijan, Belarus, Kazakhstan, Lithuania, Georgia, Estonia, Latvia, Armenia, Russian Federation, Ukraine, Moldova, Belarus, Turkmenistan, Uzbekistan

Note: Make sure to load the proper firmware for the region where the camera is installed.

To activate license plate result (LPR) notifications in Navigator:

1. Set up license detection in the TruVision ANPR camera web UI. See the *TruVision ANPR IP Camera Configuration Manual* for details.
2. Drag a TruVision ANPR camera from the Navigator panel to a video tile in the Viewer panel.
3. Right-click the tile and select **Show real time LPR** > **Show text**. LPR notification information appears on the right side of the video tile.

4. To see LPR notifications in the Notifier panel, select the License Plate Recognition Notifier filter. See “Filters” on page 99 for details.
5. When searching for license plate information in Navigator, a full or partial license plate can be used as a search term. The search is case-sensitive.

License plate search

To search for a license plate:

1. Click the **License Plate** tab in the Search window to search actions for ANPR cameras. You can add these cameras directly (as devices) to the software or they can be added to a recorder.
2. Set the following parameters:

- **License Plate**: Search LPR notifications using a full/partial license plate number.

- **List Type**: Search LPR notifications based on a list type, such as Allowed list, Blocked list and Other List as well as a combination of all list types.

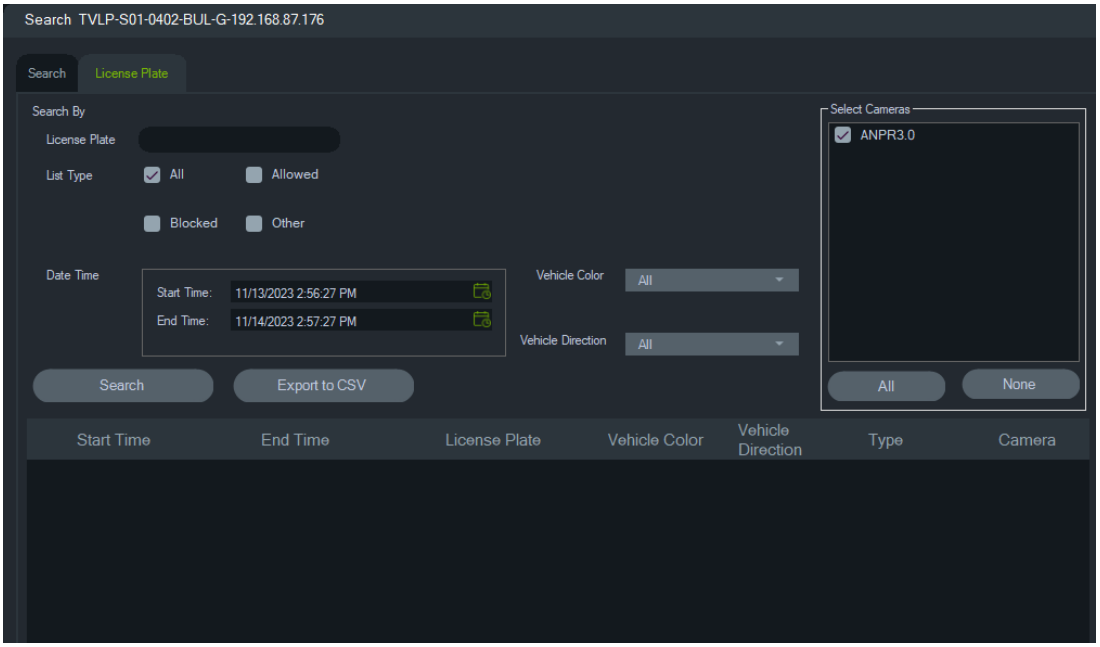
- **Vehicle Color**: Search LPR notification based on the vehicle color drop-down list (white, black, red, etc.). **Note:** The vehicle color-based search feature is only enabled for supported ANPR cameras.

- **Vehicle Direction**: Search LPR notification based on the vehicle direction drop-down list (Forward, Reverse, All). **Note:** The vehicle direction-based search feature is only enabled for supported ANPR Cameras

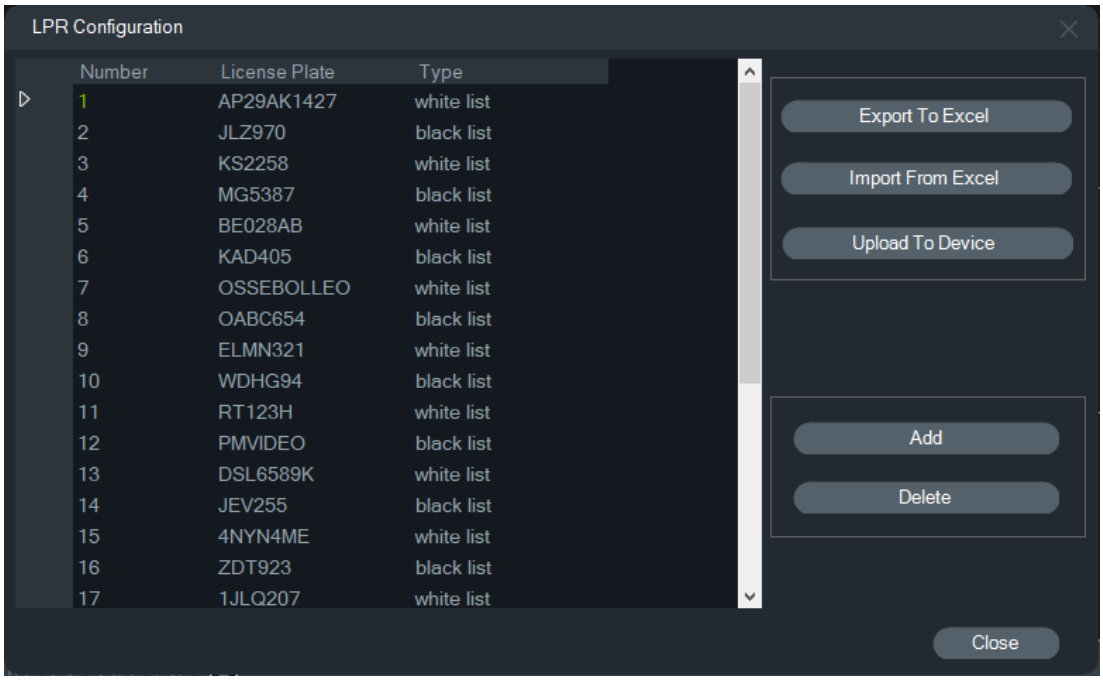
- **Date Time**: Enter start and end times for an LPR notifications search. This field is mandatory.

Note: Select **Cameras** list is only populated with ANPR cameras added to the device.

3. After entering the relevant parameters, click the **Search** button to display the results from the recorder/camera in the grid. The results show the start and end time notifications, notification type, camera, and the vehicle license plate number.



Managing license plate information in recorders and ANPR cameras



ANPR cameras are supported in the TVN 22 and TVN 23 (S/P) recorder series, as well as the TVN 71 recorder series.

Cameras capture the license plate numbers of vehicles. A list is created in a camera, when its used as standalone device, or in a recorder, when the camera is added to a recorder. Lists are used to classify the captured license plates (such as an Allowed list, Blocked list, and Other list).

To manage list using TruVision Navigator:

1. Right-click a recorder name or an ANPR camera in the device tree.
2. Select LPR Configuration.

License plate data is displayed when there is already a license plate list in the recorder or camera.

Note: Before importing a list into the recorder/camera, it is recommended to first export the template from the recorder/camera. The list can then be updated in Excel. Once the list is ready, it needs to be uploaded again in TruVision Navigator and then uploaded to the recorder/camera.

Note: When the ANPR cameras are added to the recorder, the list needs to be in the recorder and not in the camera.

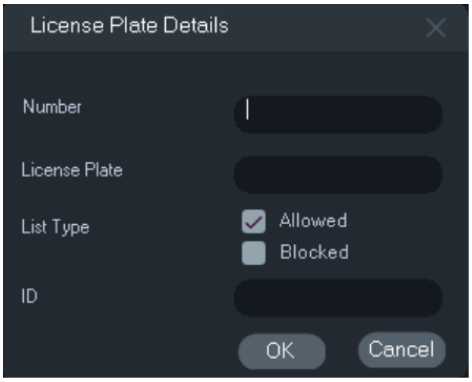
- **Export to Excel**: To export the list from the recorder/camera
- **Import from Excel**: To import the list into the software
- **Upload to Device**: To upload the list to the recorder/camera
- **Add**: To add an extra license plate in the list
- **Delete**: To delete an existing license plate from the list

To add a license plate to a list:

1. Click **Add** to add a license plate.
2. Select LPR Configuration.
3. Enter Number, License Plate, List Type and ID.

- **Number**: A serial number of the item.
- **License Plate**: The vehicle license plate number.
- **List Type**: To add an extra license plate in the list
- **ID**: Any reference ID specific to the license plate.

4. Click OK.



You can double-click the displayed license plate to modify its information. Change the list type by double-clicking the type and then changing its information.

Note: After a recorder has been added, changed or deleted, do not forget to upload the list to the device.

Object counting

Note: The object counting camera must be added by itself to the Navigator panel (so that it has its own device node) and must have a memory card installed to obtain object counting data.

This function can be used with cameras that support object counting. Available selections are as follows:

Statistics

Right-click an object counting camera tile and select **Object Counting** > **Statistics**.

View object counting statistics by Report Type (select from **Daily**, **Weekly**, **Monthly**, or **Annually**), Graph Type (select **Bar Chart** or **Line Chart**), and **Statistics Time**.

Click **Export to CSV** to export statistics data to an external file.

Reset

Right-click an object counting camera tile and select **Object Counting** > **Reset**. This action resets the Enter and Exit numbers in the object counting on-screen counter to zero.

Display counter

Right-click an object counting camera tile and select **Object Counting** > **Display Counter** to display the object counting on-screen counter (Enter and Leave numbers).

Note: This feature does not work for people counting cameras (TVS-PCx)

Heat maps

Note: The heat map function is only supported by TruVision 360° cameras. The 360° camera must be added by itself to the Navigator panel (so that it has its own device node) and must have a memory card installed to obtain heat map data.

Heat maps provide a visual representation of movement and activity within a scene. Areas with higher activity are highlighted using color variations.

Users can:

- Generate heat map reports
- View activity trends over time
- Export heat map data (image or file)

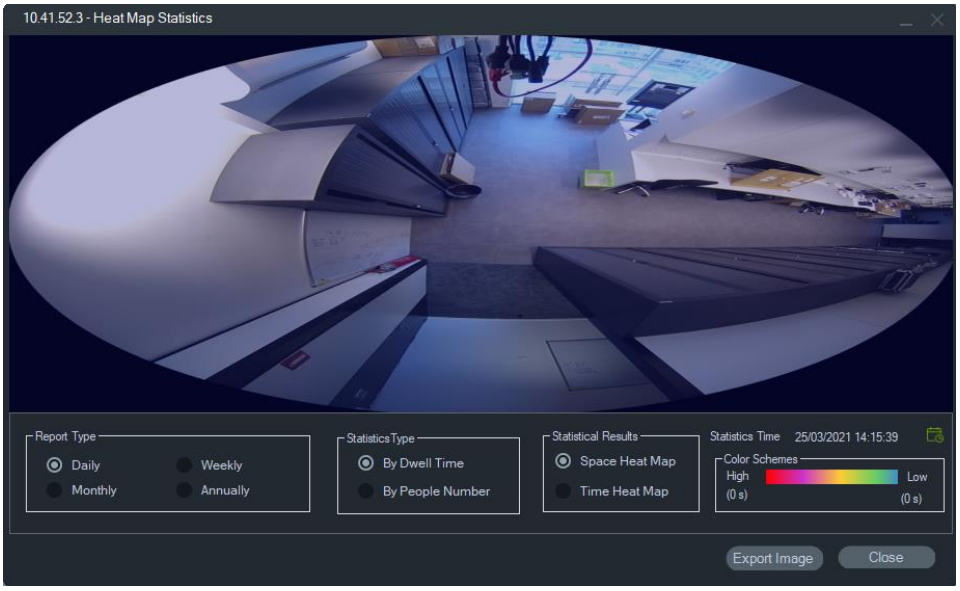
A heat map is a color-coded graphical representation of the movement of objects or people through a scene. The colors correspond to the amount of traffic, and the amount of time spent stationary in the configured scene.

To set up the heat map:

1. In the Navigator panel, right-click the device icon associated with a 360° camera and select **Configure Device**.
2. Type the user name and password and click **Login**.
3. Click the **Configuration** tab and then click **Heat Map**.
4. Select **Enable Heat Map**. For detailed instructions on heat mapping configuration, follow the instructions in the heat map section of the *TruVision 360° Camera Configuration Manual*.

To view heat map statistics:

1. After following the instructions above to set up a heat map, right-click the video tile of a 360° camera and select **Heat Map**. The heat map statistics window appears.
2. Select a Report Type (Daily, Weekly, Monthly, or Annually), and then select a date from the **Statistics Time** drop-down list.
3. With **Image Heat Map** selected under Statistical Results, click **Export Image** to save a heat map image.



4. With **Time Heat Map** selected under Statistical Results, click **Export to CSV** to save heat map statistics in Excel format.

Queue management and flow analysis

Queue management and flow analysis monitor how people move through specific areas. These analytics help identify bottlenecks and waiting times.

Users can:
- Monitor queue length and waiting time
- Analyze traffic flow at intersections
- Generate reports for analysis

Queue management

The queue management statistics are used to show the number of people that are queueing and the average waiting time per person.

Queue management must be setup in the camera and is used to monitor the number of people in an area. For more details about queue management, see the TVPA (Series 2) 360° IP camera configuration manual.

To set up and display the queue management statistics:

1. Setup queue management in the camera and let it run.
2. Check the results of the queue management analysis on the web page of the camera.
3. Add the camera as a device to the Device Tree.
4. Drag and drop the camera in a video tile of the Viewer.
5. Right-click the Tile and select **Queue Management Statistics**.
6. Select the appropriate report type, area, date and other parameters.
7. Verify if the displayed result matches the result from the camera web page.

Example. TruVision Navigator shows the results:

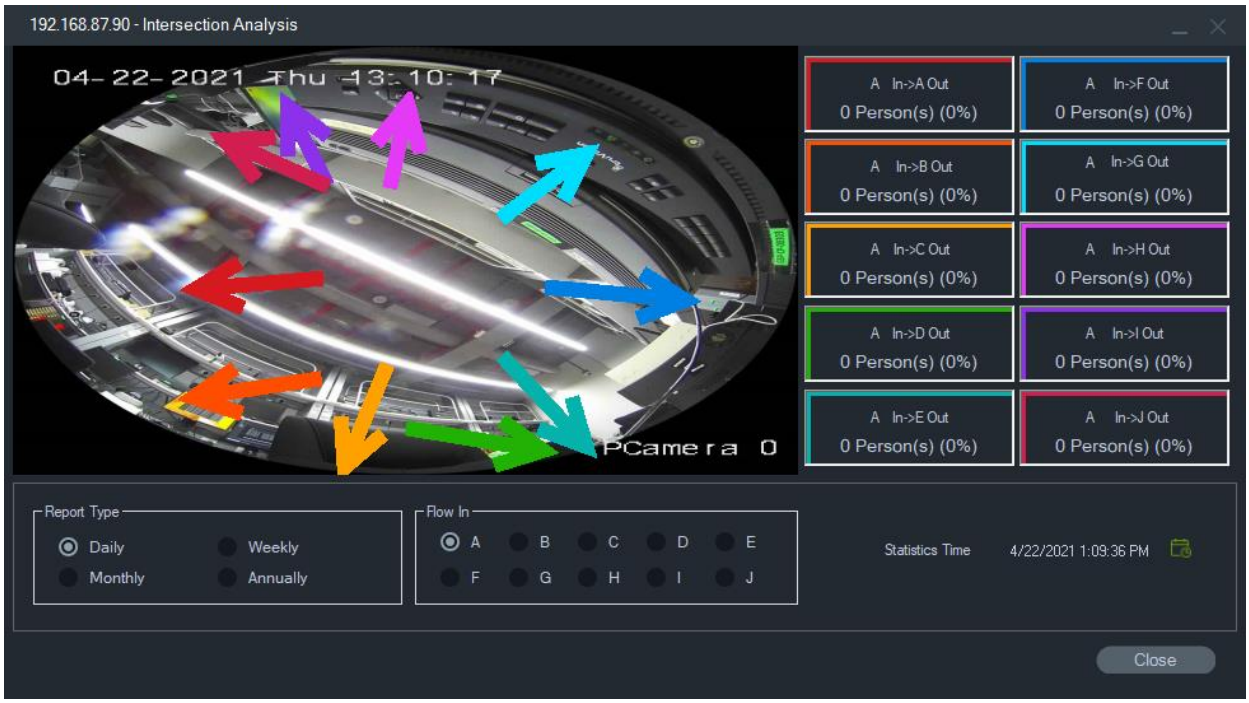
Intersection analysis

The intersection analysis must be setup in the camera and is used to monitor the people flow in any intersection scenario or with intersecting pathways. For more details about intersection analysis, see the TVF or TVPA camera configuration manual.

To set up and display the intersection analysis:

1. Setup the intersection analysis in the camera and let it run for a specific time (minimum 1 day).
2. Check the results of the intersection analysis on the web page of the camera.
3. Check if the results match with the display in TruVision Navigator.
4. Add the camera as a device to the Device Tree.
5. Drag and drop the 360° view in a video tile of the Viewer.
6. Right-click the Tile and select **Intersection Analysis**.
7. Select the appropriate report type, the flow direction, and the date.
8. Verify if the displayed result matches the result from the camera web page.

TruVision Navigator displaying the results:



Face recognition and face picture libraries

Face recognition is an analytics feature performed by supported devices. TruVision Navigator provides tools to manage face picture libraries used by these devices.
The TVR18 recorder series supports face recognition for analog/HD-TVI cameras.
Als the TruVision TVGP-P02 IP PTZ camera supports face recognition.

Face recognition is a function that compares a captured face (in an image or video stream) with the faces of a face picture library and returns its identity information if the face is recognized.

When face recognition is enabled on the device, captured faces from video streams are compared against the face picture library. If a match is found, the system can generate events or notifications depending on the device configuration.

Face recognition processing is performed by the device (recorder or camera), while TruVision Navigator can be used to manage face picture libraries and associated records.

Note:

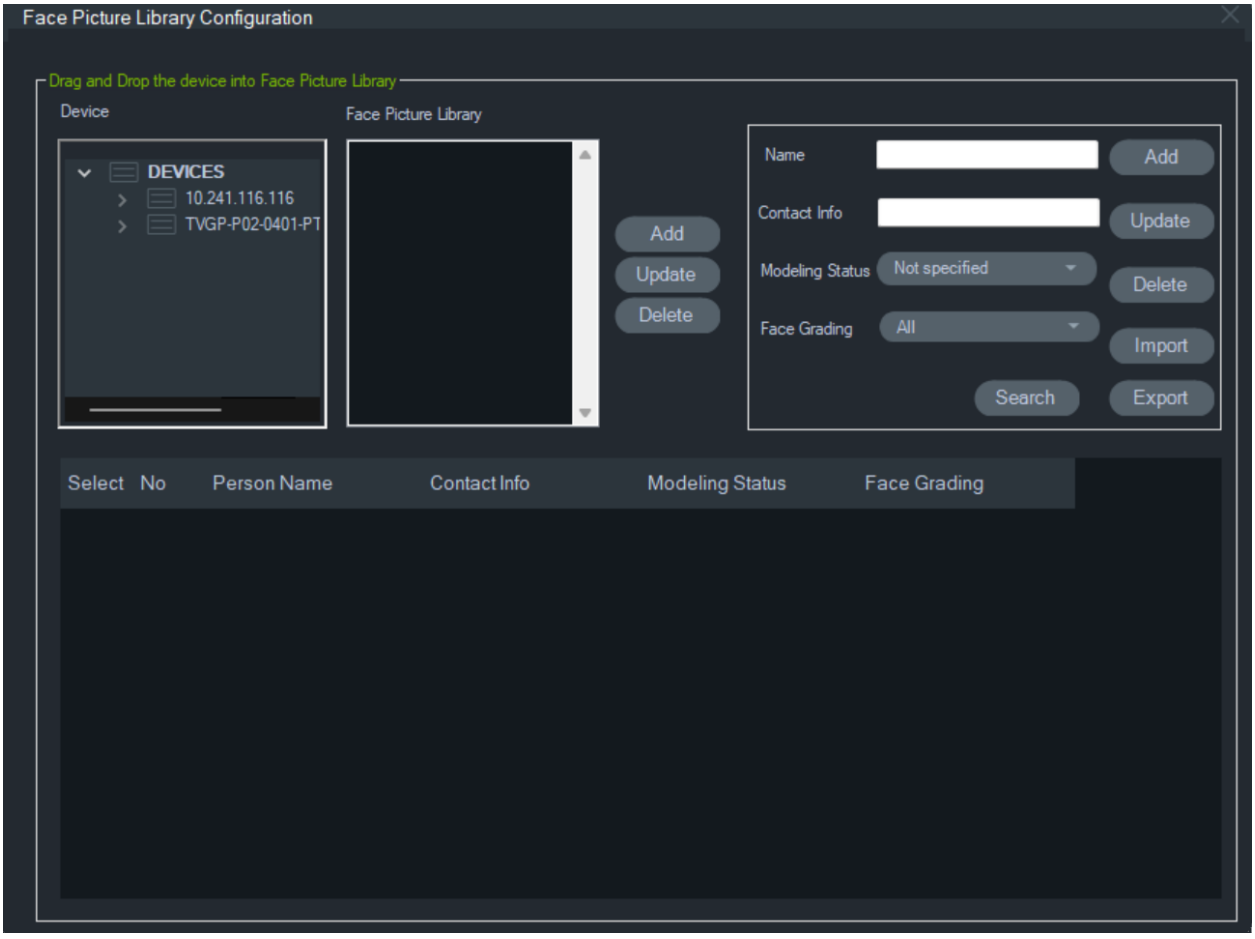
At this moment, it is not possible to receive any face recognition/comparison related events in TruVision Navigator.

The number of supported face records and recognition performance depend on the device model and available system resources.

Support for face recognition in the different TVR18 recorders:

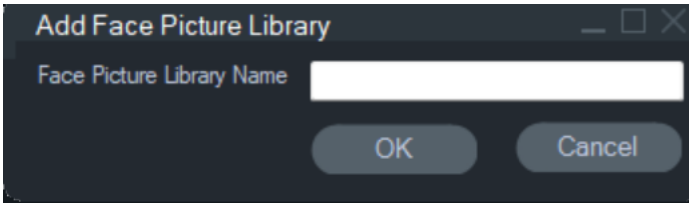
Model	Number of channels
TVR1804C	Max. 2 channels
TVR1808	Max. 4 channels
TVR1816	Max. 4 channels

The recorder stores the pictures of the faces in a picture library in the recorder. Also the TruVision PTZ camera TVGP-P02 IP camera supports face recognition. In TruVision Navigator you can manage the libraries and the content of each library.



In the Device list, you see the device that support a face picture library.
When you drag and drop a device in the field Face Picture Library, it will display the name of the libraries that are already setup in the device.
If the list stays empty, it means that the device doesn't contain a face picture library yet.
Actions:

- Add – Create a new library for the selected device.



Give the library a meaningful name and click OK to save it.

- Edit– Edit the name of the selected library
- Delete – Remove the selected library from the device.

3. When you double-click on the library name, you will see all the records for the persons in the selected library in the table.

- Person Name
- Contact Info
- Modeling Status: Face modeling is the process by which the system analyzes a face image and extracts key features used for recognition. During this process, the system creates a mathematical representation of the face, which is then used to compare against faces detected in video streams.

  Modeling status indicates whether the face image has been successfully processed and is ready for recognition.
  Typical states include:
  - Unmodelled: image has been added but not yet analyzed
  - Succeeded: image is successfully modeled and usable - Failed: image could not be processed due to insufficient quality

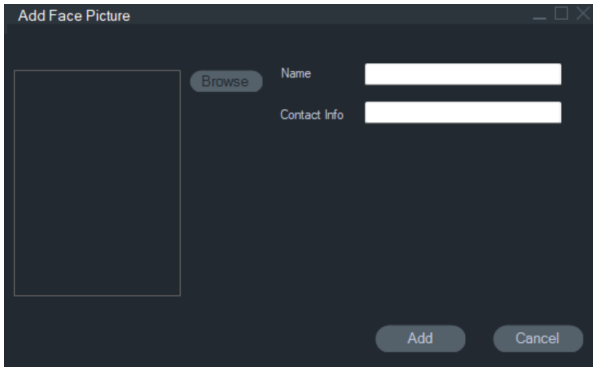
- Face Grading: is a system parameter that evaluates the quality of a captured or uploaded face image based on factors like angle, lighting, and resolution.

You can use the checkbox before each record for bulk selection

Actions:

- Add / Edit / Delete – Manage records

  It is possible to add, edit or delete individual records from the library.
  You can add a face picture in the library:
  For the TVR18:

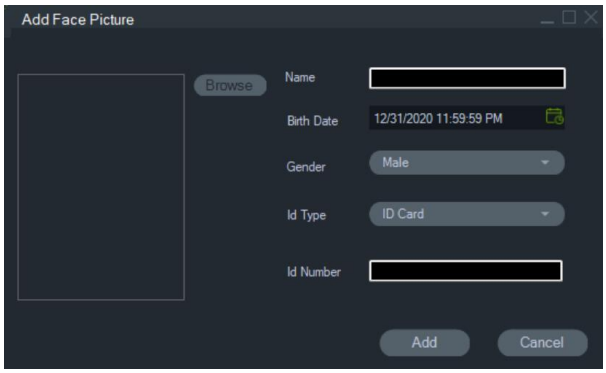


1. Select the library where you want to add the face picture.
2. Click Add to add a face picture.
3. Browse to find a face picture.
4. Click Ok to save the picture in the library.

Note:

- Only JPG and JPEG formats are supported.
- Each picture size should be less than 1 MB.
- The picture resolution shall be between 80 × 80 and 1920 × 1080.

For cameras (TVGP P02 PTZ)



5. Additional options
   - Import / Export: it is possible to import face pictures from the PC in a library. After the pictures are imported, you can edit the information for each person. It also possible to export pictures from a library and store them on the PC.
   - Search – Filter face pictures in the selected library, based on name, contact info, modeling status and face grading.

Video content analysis (VCA)

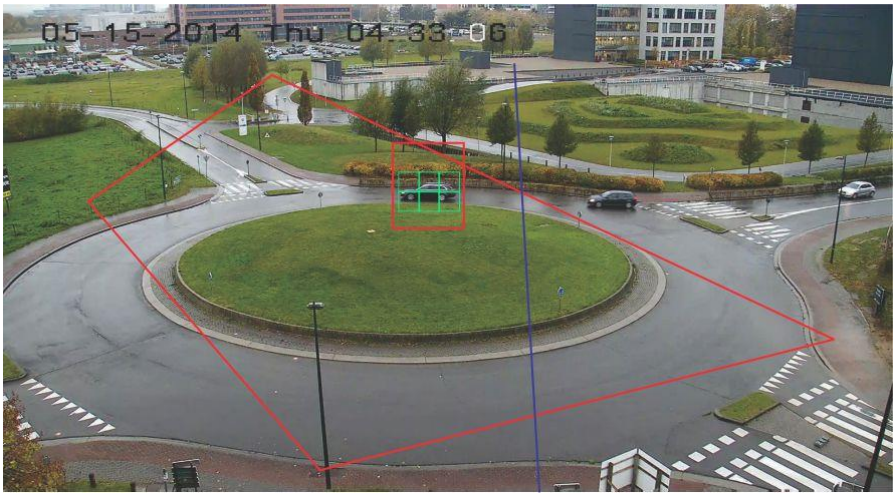
Video Content Analysis (VCA) detects specific events or behaviors within video streams. This includes motion detection and advanced analytics such as intrusion or region-based detection.

Users can:

- Enable or disable analytics overlays
- View detected motion or events directly in the video
- Use analytics to trigger events and notifications

Display analytics rules

Note: Display analytics rules (**Motion**, **VCA**, and **Thermal OSD**) only work with cameras that support this feature. Devices that support display analytics rules are indicated in the “Stream Overlay” row in the device details tables by the “VCA Rules” entry in Appendix B “Device details” on page 263. Enabling analytics rules for motion and VCA provides dynamic display indicators in the video tile for each selection. Motion and VCA indicators, as well as the on-screen drawing that defines a region of interest, differ depending on the model of recorder.



Motion

To enable motion analytics for newer IP cameras:

1. Right-click the camera’s recorder and select **Manage IP Cameras**.
2. Under Camera Setup, click Motion Detection.
3. Select the camera to display motion from the **Camera** drop-down list.
4. Select the **Enable Motion Detection** and **Enable Dynamic Analysis** for Motion check boxes.

5. If necessary, draw a new area setting in the **Area Settings** tab and select **Notify Alarm Host** in the **Actions** tab so that motion notifications display in the Notifier panel. Close the configuration window.
6. Right-click the camera's video tile and select **Display Analytics Rules** > **Motion** to enable or disable motion analytics. Motion analytics may appear as green rectangles in the video tile when they occur.

VCA

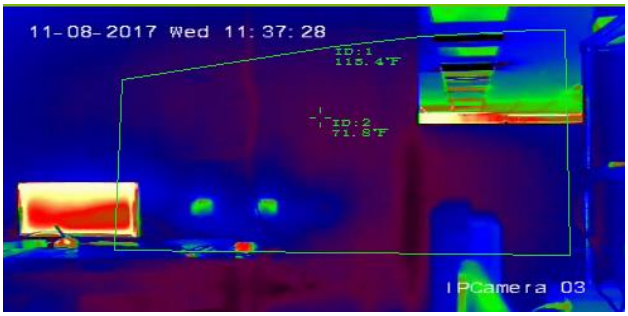
To enable VCA analytics for newer IP cameras:

1. Right-click the camera's recorder and select Manage IP Cameras.
2. Under Camera Setup, click VCA.
3. Select the camera to display VCA analytics from the **Camera** drop-down list.
4. Select the **Enable VCA Alarm** check box.
5. If necessary, select **Notify Alarm Host** in the **Actions** tab to so that VCA notifications display in the Notifier panel. Close the configuration window.
6. Right-click the camera's video tile and select **Display Analytics Rules** > **VCA** to enable or disable VCA analytics. VCA analytics may appear as red rectangles in the video tile when they occur.

Thermal OSD (thermal cameras only)

Note: The thermal camera must be added by itself to the Navigator panel (so that it has its own device node).

Right-click a thermal camera's video tile and select **Display Analytics Rules** > **Thermal OSD** to enable or disable on-screen temperature display.



Analytics on maps

Analytics data can also be displayed on maps.

Examples include:
- People counting summaries
- Device status indicators
- Event highlighting

POS mode

This function enables point of sale (POS) data display (from a device such as a cash register or ATM) in a video tile. The device providing the POS information must work in conjunction with a legacy ProBridge 3 text converter or via the NPCII, a third-party converter of SHL Systems (www.shlsystems.de).

The converter acts as a bridge between the recording device and the Point-of-Sale (POS) device (a cash register or ATM, for example). It feeds the POS text data into the recording device where it is tagged to the applicable video.

The NPCII is compatible with the following recorders:

- TVN 21 (via RS-232)
- TVN 22 (via RS-232 and IP)
- TVN 23 (via RS-232 and IP)
- TVR 45HD (only for analog cameras; via RS-232 and IP)

To activate POS mode:

To display POS data on top of the camera view, right-click the POS-configured camera's video tile and select **POS Mode** > **In Band**.

To display POS data on the side of the camera view, right-click the POS-configured camera's video tile and select **POS Mode** > **Out of Band**.

Tips for analytics

- Ensure analytics features are supported by the camera model
- Configure analytics carefully to avoid false detections
- Use analytics together with events for automation
- Use maps to visualize analytics data effectively

Chapter 9
Playback and search

Overview

This chapter explains how to search for and review recorded video.

Playback and search features allow users to locate specific events, analyze footage, and navigate recordings efficiently.

Search functionality depends on recording configuration and device capabilities.

Advanced search options such as motion-based search or text-based search require corresponding configuration on the device or recorder.

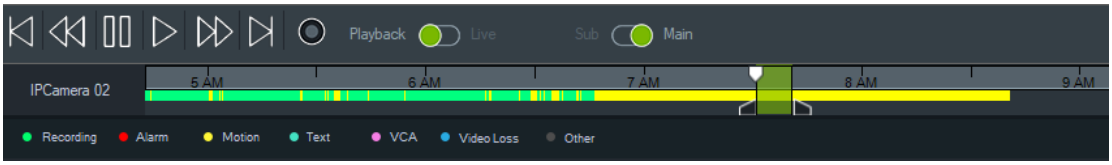
Playback video

To play back video:

- Select a camera in the Viewer
- Switch to playback mode using the timeline or controls
- The video begins playing from the selected time

Timeline navigation

When a specific video tile is selected (indicated by a green outline around the video tile), the timeline functions affect that video tile. See Chapter 13 for more details on the function of each button and the toggle switches in the timeline area. Timeline buttons only appear when they are available to be chosen. For example, the Archive button will not appear until at least one camera is currently in Playback mode.



To find a specific point in time in the timeline:

Search for video at specific points in time using any of the following methods:

- Click the **Zoom In** and **Zoom Out** buttons to locate a date and time in the timeline.
- Click the gray timeline bar and slide it to find a specific point in time.
- Click the **Go To Date** button to specify a date and time in the timeline.

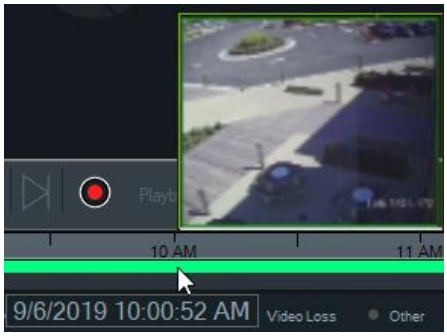
To play back video in the timeline:

- Double-click anywhere on the timeline to automatically play back the selected video at that specific date and time.
- Click and drag the current live/playback cursor, which appears as a green seek triangle icon on the gray timeline bar, to play video from anywhere along the timeline.

To view video thumbnail images in the timeline:

Hover the cursor over a point in the timeline with recorded video to see a thumbnail image of the video.

Note: Devices that support this thumbnail function are listed in the “Get Thumbnail” row in the device details tables (see Appendix B “Device details” on page 263).



Playback controls

Playback controls allow users to control video playback.

Features include:

- Play and pause
- Adjust playback speed
- Synchronize multiple cameras

Search functions

Basic search

Search allows users to locate video based on time and camera selection.

Advanced search

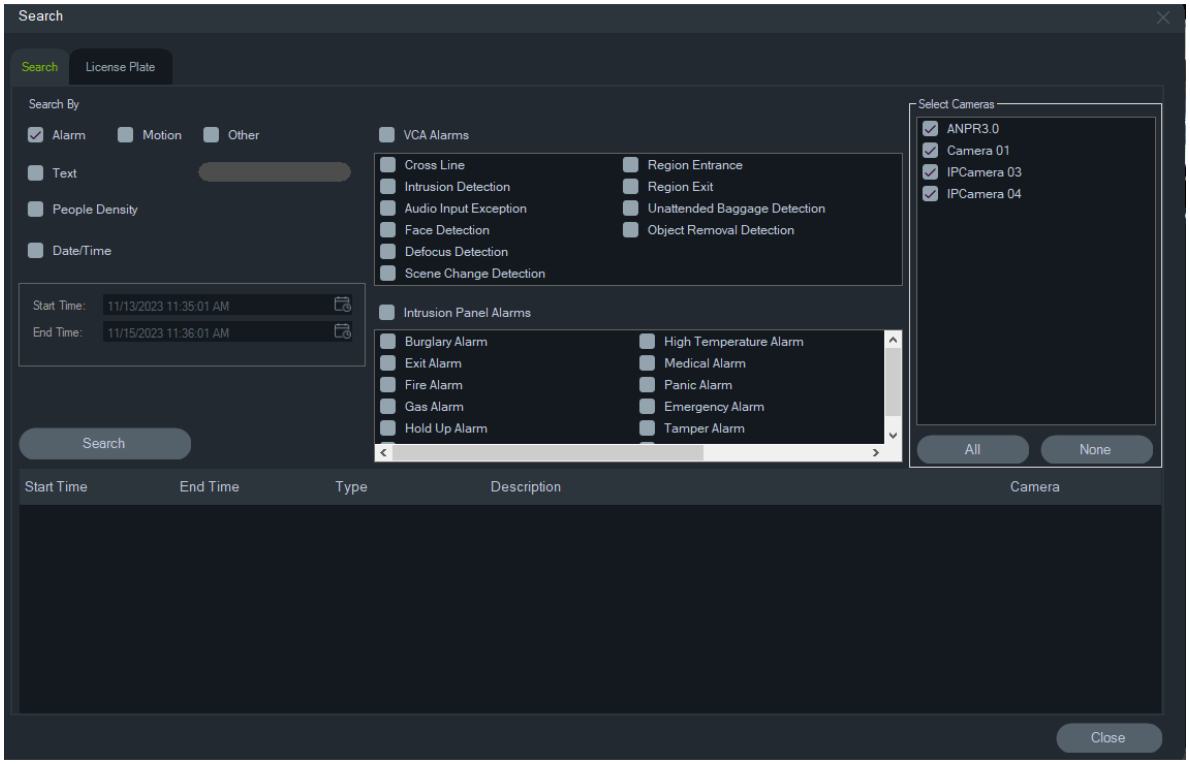
Additional search options include:

- Motion-based search
- Smart search
- Text-based (POS) search

Search multiple cameras for alarms, alarms plus events, motion and point-of-sale text-related video in the Search window. Searchable cameras must be configured for the search criteria specified.

1. Click the **Search** tab.
2. Select check boxes in the Search by and Select Cameras areas to customize a search.
3. Click the **Search** button when finished. If a camera is set to record a substream in Navigator, search criteria can only be located by clicking the **Search Substream** button.

Note: If performing a text search, a case-sensitive value must be typed into the **Text** field if the **Text** check box is selected. After performing a search at the recorder level using a text value, subsequent searches do not permit a **Date/Time**-only search. Close the Search window and launch another search to perform a **Date/Time**-only search at the recorder level.



To search for video tagged with text:

1. Ensure that the device being searched for is working in conjunction with a legacy ProBridge 3 text converter or via the NPCII, a third-party converter. See “POS mode” **Error! Bookmark not defined.** for further details.
2. Click the **Text** check box, type the text string in the **Text** field, and click **Search**.

Select or deselect the text overlay feature in the camera or recorder configuration settings to overlay the text on the video or place it beside the video (see the device’s user manual for details). This check box is dynamic and, if selected or deselected during playback, the text switches from overlay to side-by-side and vice-versa (the switch takes a few seconds).

Different devices support varying levels of search capabilities. See Appendix B “Device details” on page 263 for further details on what types of video data are available for each device.

People Density Search

Click the **People Density** checkbox to automatically activate the **Date/Time** fields. Enter both the start and end times, as this field is mandatory for People Density.

Thumbnail search

Thumbnail search displays images from recorded video over a selected time range.

The range selected can be exported directly to the Collector. It can be played by highlighting the video tile and clicking the play button, which opens the video in the main viewer.

Note: Devices that support the thumbnail search function are listed in the “Thumbnail Search” row in the device details tables (see Appendix B “Device details” on page 263).

To perform a thumbnail search:

1. Select a thumbnail layout view. Options include **9**, **16** (default), **25**, **36**, **49**, and **64**.
2. Select a start time and end time for the thumbnail search (default is 24 hours before the current time).
3. Click **Search**. The thumbnail search window video tiles populate with video thumbnails. Adjusting the search time by double-clicking a thumbnail (except the first one), double-clicking in the timeline, or sliding the beginning and ending timeline markers resets the thumbnails to the new time range specified.

To play thumbnail search video:

1. Click a thumbnail and then click the ▷ button, or right-click a thumbnail and select **Play** to play video beginning at the time specified in the thumbnail.
2. Click the button or right-click in the timeline to export video recorded between the **Start Time** and **End Time** to the Collector. Double-click the thumbnail of this video in the Collector to play it back in the viewer panel.

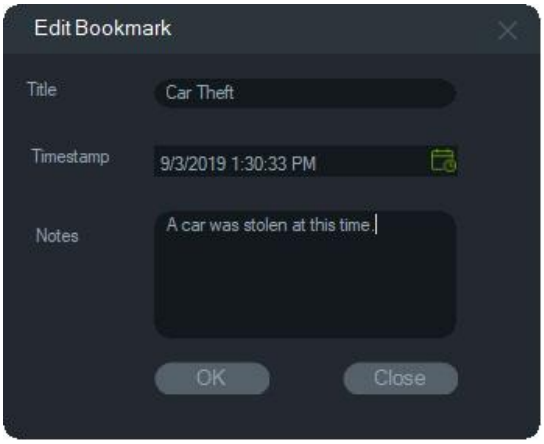
Bookmarks

Adding bookmarks

Add a bookmark to the timeline for quick navigation to an incident.

To add a bookmark, do the following:

1. Select a single video tile.
2. Right-click the timeline and select **Add Bookmark** or click the Bookmark icon in the timeline controls (clicking the icon places the bookmark at the same location as the play cursor). The Edit Bookmark window appears.



3. Type a title for the bookmark (16 characters maximum) in the **Title** field.
4. If necessary, the time stamp can be modified and text can be added into the **Notes** field (256 characters maximum).
5. Click **OK**. The bookmark icon appears in the timeline at the specified time stamp.

Working with bookmarks

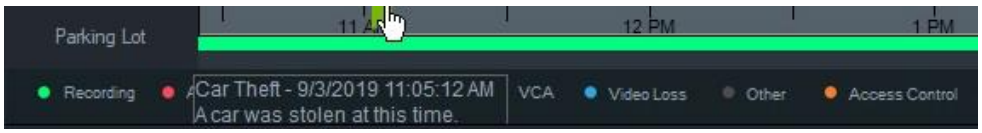
Right-click a bookmark in the timeline to access the bookmark context menu.

- **Edit**: Opens the Edit Bookmark window.
- **Delete**: Deletes the bookmark.
- **Play**: Opens a new tile and starts playing the video from the bookmark time stamp position.

Viewing bookmarks

Click the bookmark show/hide buttons / to hide or display bookmarks.

Hover the cursor over a bookmark icon to display bookmark information, The bookmark title and time stamp appear in the first line and the notes appear in the second line.



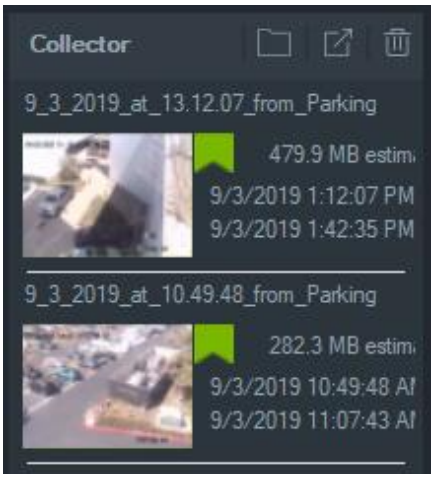
Only bookmarks for the selected video tile are visible on the timeline bar — no bookmarks display if multiple tiles are selected.

It is not possible to create more than one bookmark with the same time stamp on the same camera.

It is not possible to edit a specific bookmark when the timeline is in Zoom In mode and there are multiple bookmarks around the same time stamp.

Bookmarks in exported video

Exported video retains bookmarks if the time stamp of the bookmarks fall within the time range of the video. Bookmarks are retained in videos in the Collector after exiting Navigator. Videos in the Collector that contain bookmarks appear as follows:



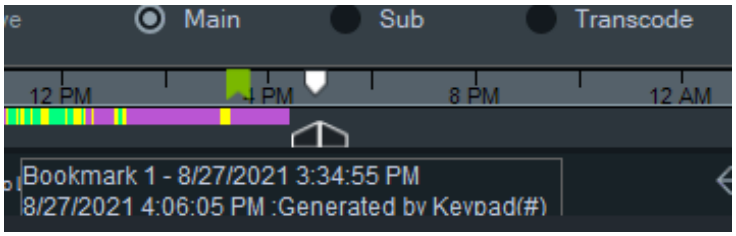
Double-clicking a Collector video with bookmarks opens a video tile. The bookmarks appear in the video playback timeline. Hover the cursor over a bookmark icon to display bookmark information during playback of exported video.

Note: Bookmarks cannot be edited or deleted during Collector video playback.

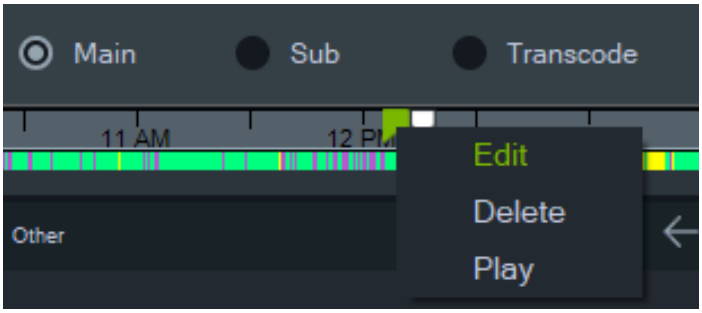
Adding Bookmarks via the keypad (TVK-400-USB)

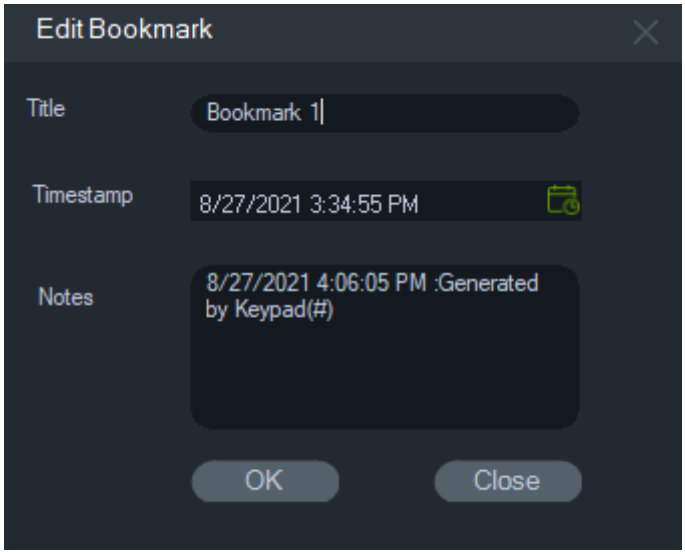
To add bookmarks via the TVK-400-USB keypad go to Client Settings and enable “Enable auto bookmark from keypad # (hash) symbol”. Refer to “Client” on page 199.

While viewing video (Live/Playback), the user can create bookmarks for the selected Video tile by pressing the hash (#) symbol. The bookmarks will have default title, video time and default note.



The user can edit/delete these bookmarks later when necessary.

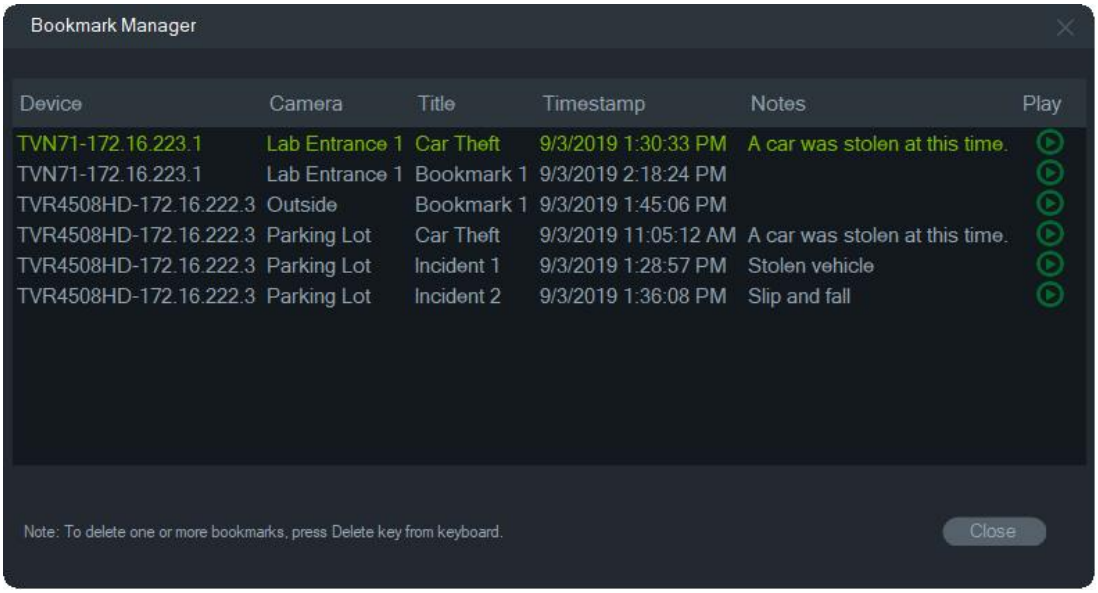




Bookmark manager

The Bookmark Manager window is a central location that contains all device-level bookmarks. When bookmarks are added, edited, or deleted on the timeline, the Bookmark Manager automatically updates. Deleting the device or camera associated with one or more bookmarks removes them from the Device list in the Bookmark Manager.

See “Adding bookmarks” on page 131 for details on adding bookmarks and “**Error! Reference source not found.**” on page 139 for details on exporting bookmarked video.



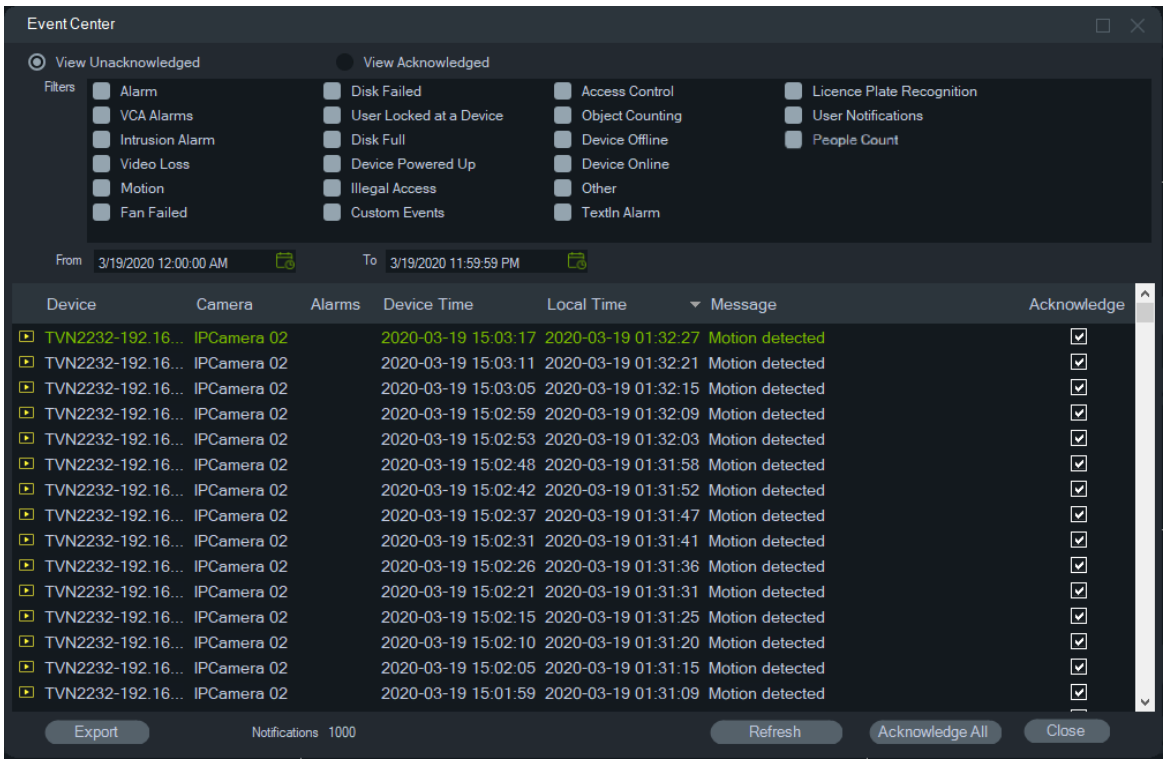
The following operations are available in the Bookmark Manager:

- **Edit**: Double-click a bookmark to edit the title, time, and notes.
- **Delete**: Press the Delete key on the keyboard to delete the bookmark.
- **Play**: Click the bookmark's play icon to play video associated with the bookmark in the timeline.

Note: Bookmarks are saved in the Navigator database, so they are available after Navigator is closed and restarted.

Event Center

The Event Center window provides a record of all events, both acknowledged and unacknowledged, over a specified time range.



To find, view, and acknowledge events in the Event Center:

1. Click the **Event Center** button in the Notifier panel to launch the Event Center.
2. Select **View Unacknowledged** or **View Acknowledged**.
3. Set filters to see only certain event types by selecting the check box next to each event type.
4. Set a date range using the **From** and **To** drop-down lists.
5. Click the top of each column in the list of events to sort events by Device, Camera, Alarms, Device Time, Local Time, or Message.
6. Click the camera link in an event to view it in the Viewer panel.
7. Click **Acknowledge All** to acknowledge all unacknowledged events. After a live notification is acknowledged, it is considered a stored or historic notification that can be searched.
8. Click **Export** to export a list of the events displayed in the Event Center in CSV file format.

Instant replay

Note: It is recommended that this feature is **only used when needed**, because frequent, sequential usage might have an impact on the lifetime of the hard drive.

Right-click a video tile containing a camera and select **Instant Replay** or click the **Instant Replay** button on the video tile to go from Live to Playback by a user-defined and pre-configured period of time (30 seconds is the default setting) for quick viewing of an incident. To set instant replay time, type the minutes and seconds or click the spin wheels to enter the required value in the **Instant Replay Duration** fields and click **OK**.

To start instant replay in a video tile, do one of the following:

- Click the **Instant replay** button in the lower left corner of the video tile.
- Right-click the video tile and select **Instant Replay**.
- Set the Live/Playback toggle switch in the timeline to **Playback**.

To stop instant replay in a video tile, do one of the following:

- Right-click the video tile and select **Live**.
- Set the Live/Playback toggle switch in the timeline to **Live**.

Synced playback

This selection appears in the context menu for cameras in playback mode that are connected to a recorder. Selecting **Sync to this video** plays back all videos in the Viewer (up to a maximum of nine) at the same current playback time/date of the camera being synced to. An “S” icon in the top status bar of the video tile indicates synced videos.

If a synced camera is set to record events instead of a continuous live stream, gaps in recording are indicated by a display of the last frame recorded before the gap occurs. The video resumes when it reaches the time that the next event was recorded.

Note: Certain cameras/conditions cannot be synced for playback:

- Local file playback and recording
- V-Stream
- Cameras connected as devices (using an SD card rather than a recorder)
- No permission for camera playback

Tips for playback

- Use timeline zoom to quickly locate events

- Use bookmarks to mark important footage
- Use synchronized playback to compare cameras
- Use thumbnail search for fast investigation

Chapter 10
Export video

Overview

This chapter explains how to export video and images from the system.

Export features allow users to save recorded video, snapshots, and other data for backup, sharing, or investigation purposes.

Export functionality is controlled by user permissions.

Users must have the appropriate export permissions assigned to perform video or snapshot export operations.

Export video

Export video from one or more cameras either immediately, at a specified time in the future, or on a recurring basis in the Export Video window.

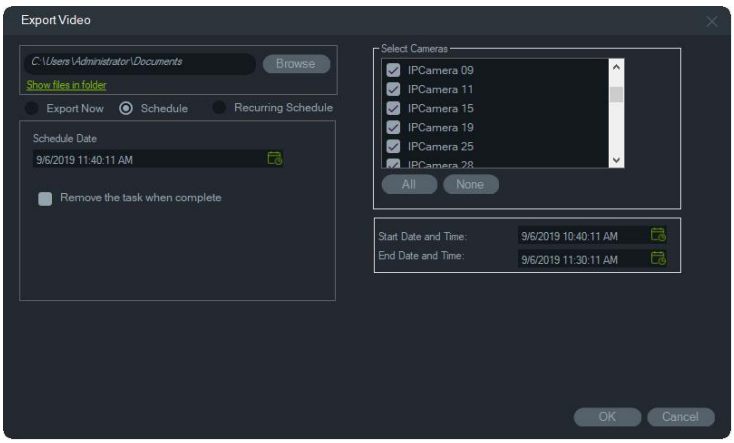
Export Now

To export video from the recorder on a one-time basis:

1. Right-click a recorder icon in the Navigator panel and select **Export Video**.
2. Accept the default location or click **Browse** and specify a destination location for the export.

   Note: Ensure that the destination location for the export has enough disk space capacity to store the exported video. We recommend that this location be different than the location specified for recurring schedule video downloads.
3. Select one or more cameras for video export in the **Select Cameras** list.
4. To start the export process immediately, select **Export Now**. The export task is automatically added to Tasks. Move the mouse pointer over the status column in the **Tasks** window to see detailed progress of the export.
5. To schedule the export process, select **Schedule** and specify a date/time to start the export process. An export task is automatically added to Tasks.

To remove the record of the scheduled export from Tasks, select the **Remove this task when complete** check box.



6. Click **OK**.

When export tasks are complete, the exported video can be found at the location specified along with the TruVision Navigator Player program. See “TruVision Navigator Player” on page 155.

Export using the timeline

To export video from the timeline to the Collector:

1. Slide the beginning and ending timeline markers to highlight a segment of time in green on the timeline bar.
2. Click the **Save Video** button. A green progress bar appears under the exported video that turns blue after exporting is complete.

Note: The **Export video** permission is required to export video from the timeline.

Scheduled export

We recommend creating a separate folder for recurring task video exports, which are downloaded and stored in their own directory. The full download folder structure is as follows:

C:\[VideoDownloadFolder]\AutoArchive\[DeviceTitle]\Cameras\[CameraNames]

When scheduling a recurring task, an alert appears showing the estimated available storage space in the target location. Available space for video export is calculated each day before video download. If there is insufficient space in the target location, a warning alert is sent to the administrator via email if **Video Export Failure** is selected in the **Settings** > **Notifications** window.

To export video from the recorder on a recurring basis:

1. Right-click a recorder icon in the Navigator panel and select **Export Video**.

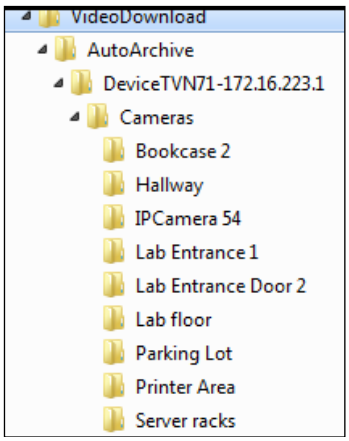
2. Click **Browse** and specify a destination folder for the export.

   Note: Ensure that the destination folder for the export has enough disk space capacity to store the exported video. We recommend that this folder be used exclusively for recurring video downloads.

3. To schedule the export process, select **Recurring Schedule** and select **Everyday** or individual days of the week for the recurring video export.
4. Specify a daily time range for the video export (**24 Hour** or **Custom Time**). Specify the start and end times for each day if selecting **Custom Time**.
5. To remove the record of the scheduled export from Recurring Tasks and Tasks, select the **Remove this task when complete** check box.
6. Select one or more cameras for video export in the **Select Cameras** list.
7. Select the range of recurring dates from the **Recurring Start Date** and **Recurring End Date** drop-down lists.

8. Click **OK**. An export task is automatically added to Recurring Tasks and Tasks.

When export tasks are complete, the exported video can be found in the directory under the download folder in the camera name folders.



Taking snapshots

You can take snapshots from the timeline.

Taking a snapshot of a selected video tile containing a camera sends a still image file to the Collector for export.

To take and deploy a snapshot:

1. Click the **Snapshot** button above the timeline or right-click a video tile containing a camera and select **Snapshot**.
2. Right-click the snapshot in the Collector panel to **Print Preview**, **Print**, **Email**, **Rename**, or **Export** the snapshot image. See Chapter 10 Export video.

Collector panel

The Collector panel contains video and snapshots from the timeline (see “Timeline navigation” on page 127), the camera context menu in the Navigator panel (see “Export video” **Error! Bookmark not defined.**), and the camera tile context menu in the Viewer panel (see “Local recording” **Error! Bookmark not defined.**).

To view a video clip in the Collector, double-click the video's thumbnail to launch it in the Viewer. Double-click a snapshot to play video from the camera that provided the snapshot at the point in time the snapshot was taken.

To delete items from the Collector, right-click an individual item's thumbnail and select **Delete** or click the **Delete All** button at the top of the Collector panel.

Export all collected video and snapshots in the Collector panel to a specific location either on demand or via a schedule.

To export video or snapshots from the Collector:

1. Click the **Export All** button at the top of the Collector panel to export all videos and snapshots, or right-click an item in the Collector panel and select **Export** to export it individually.
2. Click **Browse** and specify a destination location for export. Click the Show files in folder link to view the current contents of the folder (you can also click the **Show files in folder** button in the Collector toolbar to view folder contents).

   Note: Make sure there is enough disk space at the destination location for the export. Use the file size estimate in the Collector as a guideline.
3. To start the export process immediately, click the **Export Now** button. The export task is automatically added to Tasks (see "Tasks" **Error! Bookmark not defined.**). A progress bar appears below each video thumbnail to indicate export progress. Exports in progress appear as green and turn to blue after export is complete.
4. To schedule the export process, click the **Schedule** button and specify a date/time to start the export process. An export task is automatically added to Tasks.

   Note: The Local Scheduling Service must be running to execute these export tasks. Refer to the Services window for status and actions on all services.

When export tasks are complete, exported video and snapshots can be found at the location specified along with the TruVision Navigator Player program. See "TruVision Navigator Player" on page 155.

Collector context menu

Right-click a snapshot to make any of the following selections from the context menu:

- **Print Preview**
- **Print**
- **Email**
- **Rename** (also available in the Collector video context menu)

- **Export** (also available in the Collector video context menu)

TruVision Navigator Player

Exported video files include the TruVision Navigator Player.

The player allows users to:

- Play exported video
- Navigate recordings
- View associated data such as timestamps or bookmarks

To view exported video:

- Open the exported file
- Launch the included player

The player runs independently from the main application and can be used for sharing video with other users.

Viewing exported video

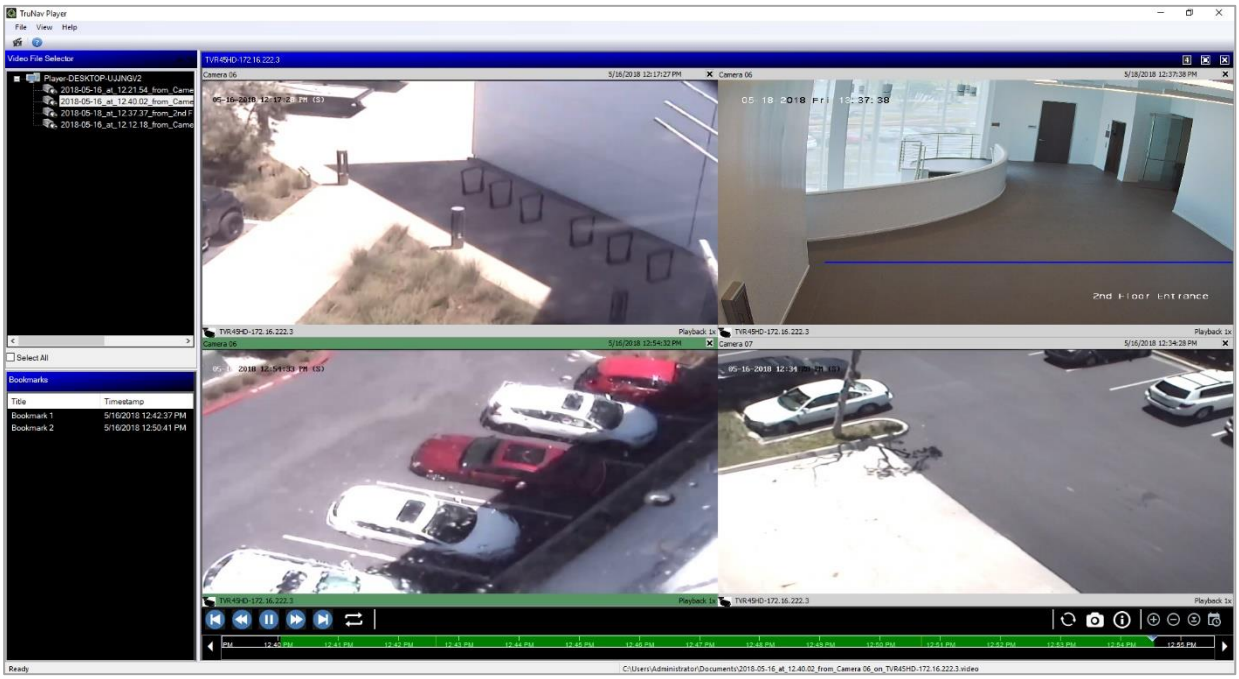
The TruVision Navigator Player is a standalone player that can be used to replay any video clip exported using TruVision Navigator (proprietary file formats include .wvf, .mpc, .asf, .mp4, and .drv). This player should be copied to media along with video clips for authorities. It launches from the media itself and does not require installation to a computer.

To play video with the TruVision Navigator Player:

1. After exporting video clip(s) from the Collector to the user-defined location, launch the TruVision Navigator player by double-clicking the TruVision Navigator Player icon in the file folder where the video clips are located.

   IMPORTANT: The player.bin file must be in the same directory as the TruVision Navigator Player.exe file for the TruVision Navigator Player to work.

2. The player automatically sweeps the directory and loads the associated video clips in the Video File Selector panel from that directory. Double-click a camera icon in the Video File Selector panel to populate the next video tile. The default view is 9-up with a maximum of 16-up. Other custom views are available.



Local recording

Use the **Local Record** button to record live video to the client computer.

Note: Be sure to turn off local recording before it takes up too much storage space on the client computer's hard drive.

To create a local record video file, do the following:

1. Select a camera video tile in the Viewer.
2. Click the **Local Record** button (to the right of the playback controls) or right-click in the tile and select **Start Local Recording** to begin recording. A thumbnail appears with a start time along with a red dot in the Collector.
3. The red **Local Record** button blinks when any camera is recording locally.
4. Click the red **Local Record** button again to stop the recording. An end time for the thumbnail automatically appears in the Collector.
5. Follow export operations as necessary to save the local recording. See "Export video" on page 139.

Tips for exporting

- Ensure sufficient storage space before exporting video
- Use shorter time ranges for faster export
- Schedule exports during low system usage
- Use snapshots for quick evidence capture

Chapter 11
Maps

Overview

Maps provide a graphical representation of locations within the system, such as buildings, floors, or areas.

Devices such as cameras, doors, and intrusion systems can be placed on maps to allow quick navigation and control.

Maps are particularly useful in large systems to quickly locate devices and respond to events.

Maps are configured using the map configuration tools described in this chapter and are used during live monitoring in the Viewer panel.

Maps are not only used for visualization but also function as an operational interface.

Devices represented on maps can respond to system events, allowing users to quickly identify and react to incidents.

Event-driven behavior on maps is typically configured through Event-Actions and device event configuration.

Adding maps

Maps can be added to represent physical locations.

To add a map:

1. Open the Navigator panel
2. Select the Maps section
3. Add a new map
4. Upload or select an image (for example, a floor plan)

Supported image formats (e.g., JPG, PNG)

Maps can be opened in the Viewer by

- Double-clicking the map in the Navigator panel
- Dragging the map into a Viewer tile

Organizing maps

Maps can be organized in a hierarchy to represent multiple locations.

Examples include:

- Buildings
- Floors
- Rooms

Submaps can be used to create multiple levels of detail.

Adding devices to maps

Devices can be added to maps to represent their physical location.

To add a device:

- Drag a device from the Navigator panel onto the map
- Place it in the desired position

After making changes to a map, save the configuration to apply the updates.

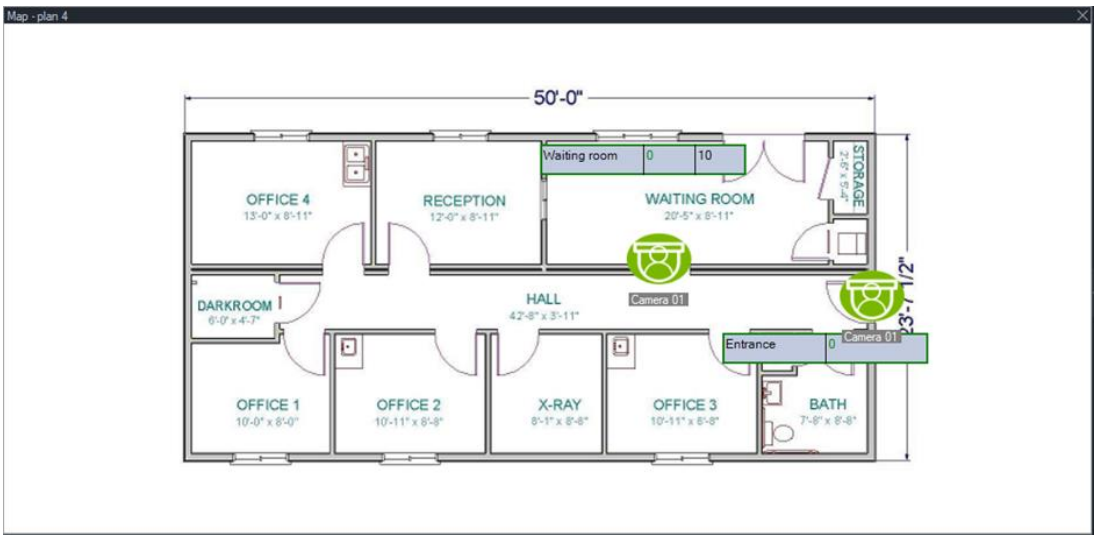
Adding people counting cameras to a map

Note: The display size of the counting summary is related to the resolution of the map. The higher the resolution of the map, the smaller the size of the counting summary.

1. Add people counting cameras and groups to the people counting node in the Navigator tree, see “Adding people counting IP camera” on page 47on page 47 and “Adding people counting” on page 102.
2. Add a map to Navigator, as instructed in “Adding maps” on page 146.
3. Right-click the map that was just added and select **Configure Map**. The configuration window for the map will open.

4. Drag and drop the people counting camera group on the map. A summary window with the real time counting value (and maximum permitted number of people, if setup) will be displayed on the map. You can position the summary where you need on the map. In the example below, a maximum number of people for the waiting room and maximum for the entrance is used. Only one value for the entrance is displayed (equal to the actual number of people on the site).

5. You can also drag & drop the individual people counting cameras on the map, see graphic below.



Device linking

Camera, recorder, access control door, access control panel, intrusion panel, and intrusion sensor icons can be added to maps to represent their physical locations.

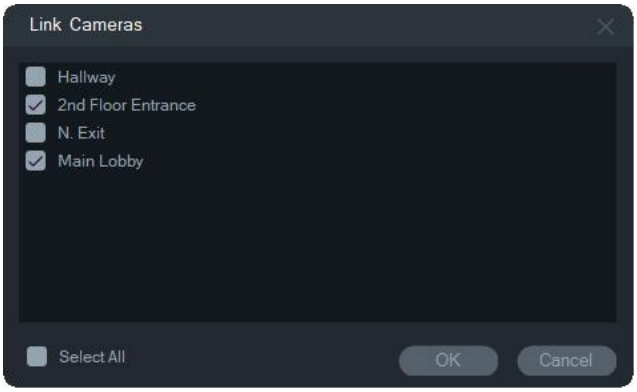
Devices such as cameras can be linked to doors or intrusion sensors. This allows video to be displayed automatically when an event occurs.

Selecting any element in a map while pressing the Alt key highlights other elements associated with the selection. Clicking the map itself while pressing the Alt key highlights all elements on a map. Pressing Ctrl while rotating the mouse wheel permits zooming in to the cursor on a map.

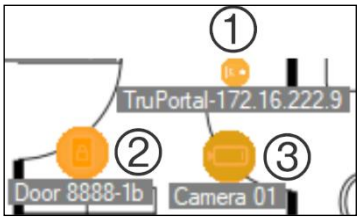
Note: The recommended map image size should be between 800×600 and 1920×1080. Smaller images will cause markers to appear overly large. Conversely, larger images will make markers appear very small.

Link cameras to doors

1. In the Configure Map window, right-click an access control point (door) and select **Link Cameras**.
2. Select all cameras on the map to link to the door (or select **Select All**), and then click **OK**.



3. To see which cameras and access control panels on the map are linked to a door, hold down the Alt key while clicking the panel icon (1) and orange highlighting appears around the door (2) and connected camera (3) icons.



Event behavior

Whenever the door is opened, notifications from linked cameras appear in the Notifier panel (see “Notifier configuration” on page 97). Click the camera notification in the Notifier panel to launch video recorded when the door was opened in the Viewer panel (see “Viewer overview” on page 88). If a linked camera has been assigned to the Event Monitor, video from the camera displays in the Event Monitor if the door’s reader is swiped or if the door is opened.

Open a door from the map

Doors can be opened from maps in the Viewer Panel by double-clicking a door icon.

Configuring map icons

Each device placed on a map is represented by an icon.

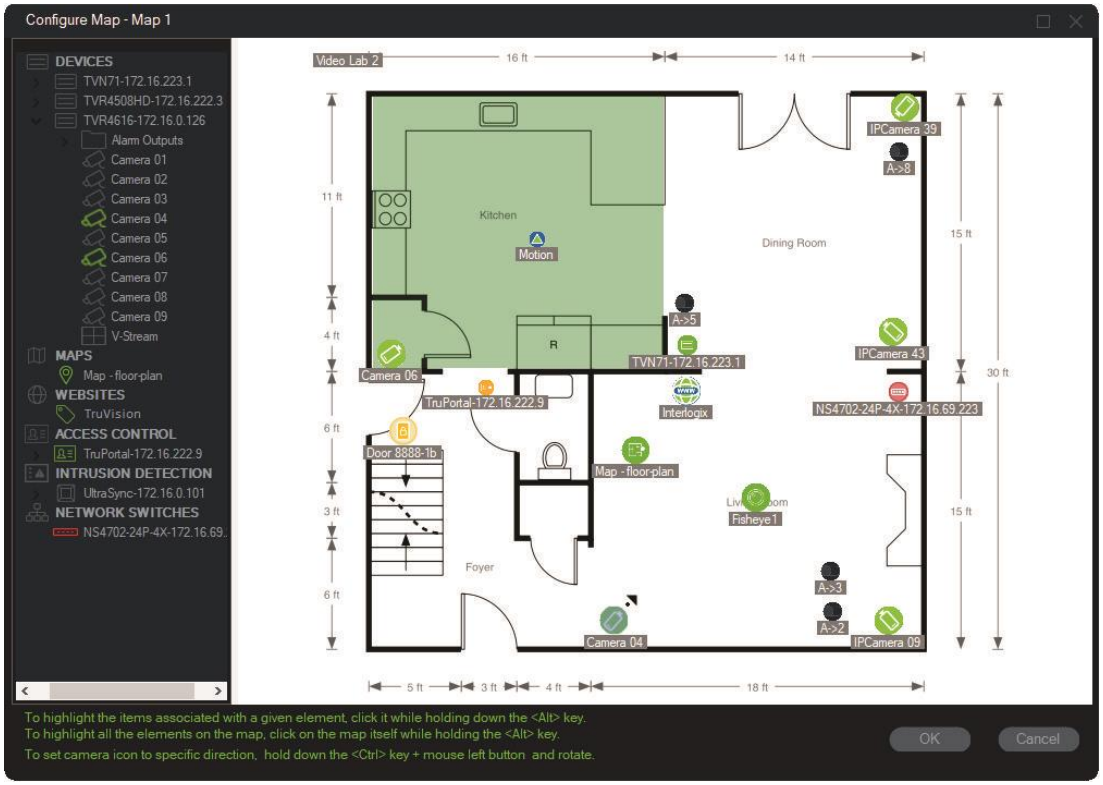
Icons can be positioned and adjusted to reflect the real-world placement of devices.

Each device is represented by an icon.

Icon appearance may change depending on the status. See Chapter 13 for more details.

Adding and positioning icons:

1. Right-click the map name in the Navigator panel and select **Configure Map**.
2. Click and drag a camera, recorder, alarm output, access control panel (if a TruPortal system has been added to Navigator), access control point (door icon), a website, or another map from the Navigator panel to any point on the map.



3. Right-click a camera and select **Orientation** to change the position of the camera to mimic its physical orientation.
4. To manually rotate an IP camera icon, press Ctrl and click the icon. The rotation of the camera icon follows the mouse, and the icon changes color during rotation. The cursor also changes to indicate the direction set for the camera.
5. Click **OK** to save.
6. To remove an icon, right-click it and select **Delete**.

Linking maps and objects

Maps can include links to other elements such as:

- Submaps

- Cameras
- Websites
- Device outputs

These links allow quick navigation between different parts of the system.

Launching maps and websites from a map in the Viewer Panel

In a map in the Viewer Panel that has been configured to include one or more submaps and/or websites, double-click a submap or website icon to launch it in a Viewer Panel tile.

Operating alarm outputs

Alarm outputs can be activated directly from the map.

In a map in the Viewer Panel that has been configured to include one or more recorder or camera alarm outputs, double-click a output icon to turn it on or off. A small green circle appears on the digital output icon when an output is triggered (on).

To delete a digital output from a map, right-click the icon and select **Delete**.

To see which cameras on the map are linked to an output, hold down the Alt key while clicking the output icon and orange boxes appear around the connected camera icons.

Analytics data can also be displayed on maps. See Chapter 11.

Map behavior and interactions

Devices on maps can respond to system events.

For example:

- Icons may change appearance when an event occurs
- Devices may be highlighted to indicate activity

Map behavior may depend on event configuration.

Using maps in the Viewer

Maps can be used in the Viewer to interact with devices.

Users can:

- Click camera icons to display video
- Double-click doors to trigger actions (if enabled)
- Open submaps or websites directly

Map navigation features

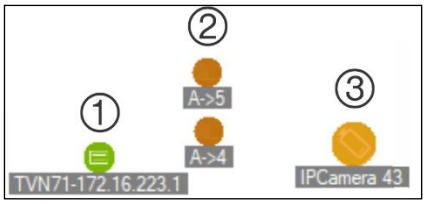
Users can navigate maps using:

- Zoom
- Pan (click and drag)
- Fit-to-screen options

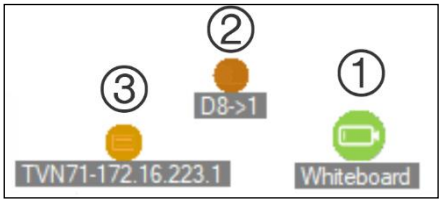
Double-click to open linked items (cameras, maps, websites)

Viewing associated items on a map:

1. Hold down the Alt key and click a recorder icon (1). Orange highlighting appears around all cameras (3) and alarm outputs (2) associated with the recorder.



2. Hold down the Alt key and click a camera icon (1). Orange highlighting appears around all recorders (3) and alarm outputs (2) associated with the camera.



Best practices

- Use clear map images
- Organize maps logically
- Place devices accurately

- Use submaps for large systems
- Avoid overcrowding maps with too many devices
- Use consistent naming for maps and submaps
- Ensure users have the appropriate permissions to access maps and associated devices

Chapter 12
System tools and integrations

Overview

This chapter describes advanced tools and integrations available in the system.

These tools are typically used for system management, diagnostics, and iteration with external systems.

Some features may require additional permissions or supported devices.

System tools and integrations provide advanced management capabilities and connectivity with system components.

These tools support monitoring, diagnostics, and interaction with devices at both the device level and the system level.

PART 1- System tools

System diagnostics

System diagnostics tools provide information about device status and system performance. These tools help identify issues and monitor system health.

Available diagnostics tools include:

1. Health diagnostics report for a device

- Device reports for health and configuration information
- Network statistics for monitoring bandwidth usage
- Tampering detection for identifying camera interference

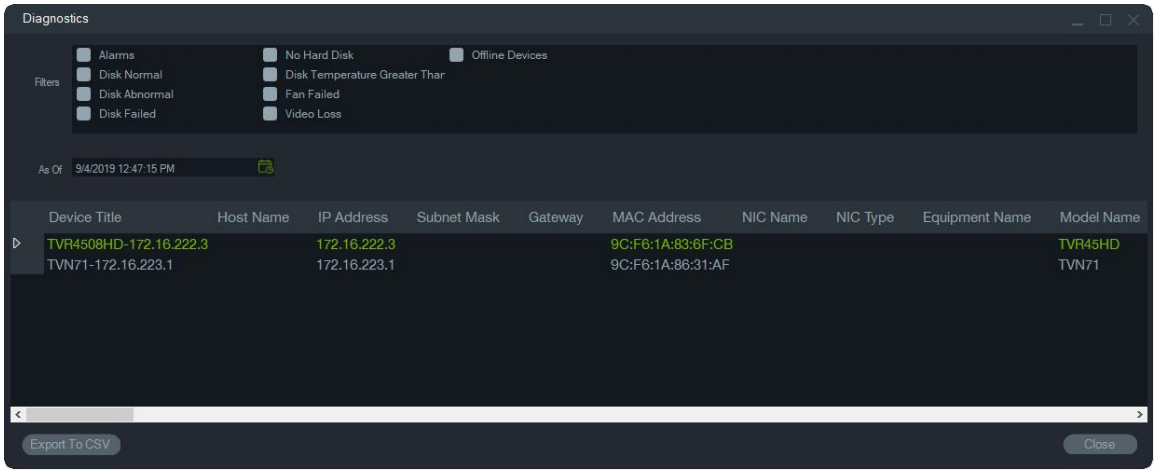
Health diagnostics report

To run a manual health diagnostic snapshot on a single recorder, right-click the device in the Navigator panel and select **Health Diagnostics**.

The Device Diagnostics window appears and displays the full set of health diagnostic data for that specific device. See Appendix B “Device details” on page 263 for more details on the different health diagnostics available for each device.

Right-click the Devices node and select **Health Diagnostics** to review health diagnostic data across all the devices in the system. Move the scroll bar at the bottom of the window to the right to see all health diagnostic information.

Use the filters and date parameters to pinpoint the search. Export the contents of the dialog to the CSV file format for case management, work orders, or issue resolution documentation by clicking the **Export to CSV** button.



Note: For devices to appear in the Diagnostics window, health diagnostics must be run at the device level first. See “Automated diagnostic polling” on page 227 for information on setting automatic diagnostic polling for recorders or “Health diagnostics” on page 226 for manual, device-level generation of health diagnostics.

Device report

Device reports provide detailed information about system devices.

Reports can include:

- Device status and configuration
- Camera health information
- Diagnostic data Reports can be exported for further analysis or record-keeping.

Navigator permits export of health diagnostics information by generating a device report.

To generate the device report:

1. Right-click a recorder icon in the Navigator panel.
2. Select **Device Report**. The device report displays in a new window.

   Note: It may take up to a minute to complete the device report depending on the number of cameras recording to the device and the network connection.
3. Click **Export to PDF** to save the report as a PDF.

As a part of the report, tampering monitor images are also provided at the bottom of the report in the Camera Check section. For more information on the tampering monitor, see “Tampering monitor” on page 160.

Disk analysis

Disk analysis provides a timeline view of video recorded to disk on all connected cameras. Color coded video tags are defined in the bottom of the Disk Analysis window.

Note: Areas in the timeline tagged as Other (gray) may or may not contain recorded video. The device may have been offline or not configured to record video during the period of time indicated.

To run disk analysis and play back video:

1. Right-click the device icon in the Navigator panel and select **Disk Analysis**. The disk analysis window appears.
2. Select a time range of recorded video in the **Start Time** and **End Time** fields.
3. Select cameras for disk analysis in the Select Cameras section and click **Search**.
4. Select check boxes to the left of each camera name as necessary. Video from all cameras selected play back simultaneously in the Viewer during playback.
5. If necessary, click the **Zoom In** and **Zoom Out** buttons or click the timeline and slide it to the left or right to locate a specific point in time.
6. Double-click anywhere on the disk analysis timeline to play video in the Viewer from that point in time.

To export video from the Disk Analysis window:

1. If necessary, click the **Zoom In** and **Zoom Out** buttons or click the timeline and slide it to the left or right to locate a specific point in time
2. Slide the beginning and ending timeline markers to highlight a segment of time in green on the timeline bar.
3. Right-click a disk analysis track and select **Export Video** from the menu or click the **Export Video** button.

To view video thumbnail images in the Disk Analysis window:

Hover the cursor over a point in a camera timeline with recorded video to see a thumbnail image of the video.

Note: Devices that support this thumbnail function are listed in the “Get Thumbnail” row in the device details tables (see Appendix B “Device details” on page 263).

Network statistics

Network statistics allow monitoring of incoming and outgoing bandwidth usage.

Users can:

- View bandwidth consumption
- Monitor active video streams
- Identify potential network issues

Right-click the device in the Navigator and select **Network Statistics** to launch the Network Statistics window. The outgoing and incoming network bandwidth limit and usage appear in a graphical format. The number of open video streams on the system at the device level also appears.

Select or deselect items under Outgoing Bandwidth and Incoming Bandwidth. Click **Close** to exit the Network Statistics window.

Note: Incoming bandwidth statistics do not appear when running network statistics on DVRs.

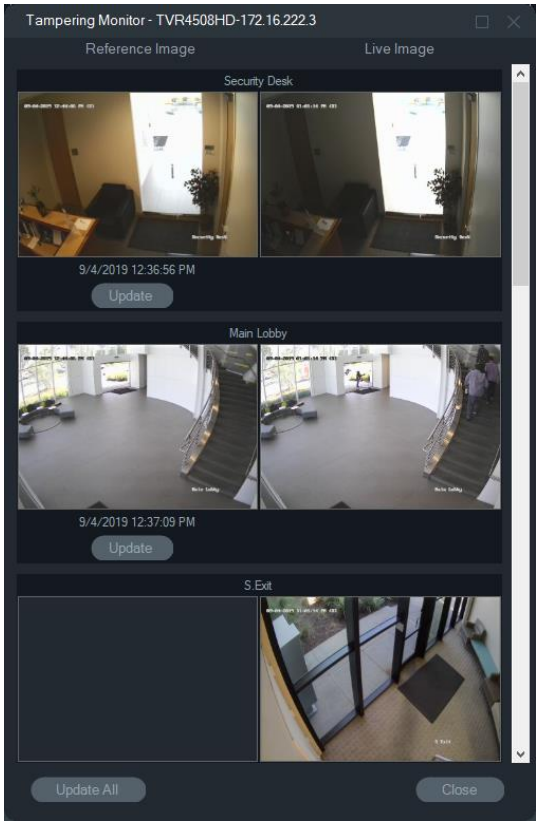
Tampering monitor

Tampering detection compares current camera images with reference images to identify potential camera interference.

Differences between images may indicate obstruction, movement, or tampering.

Navigator is equipped with a tampering monitor that compares the current image with a reference image taken during the installation. The tampering monitor keeps a record of each camera by taking a reference snapshot and storing it in the database.

To open the tampering monitor, right-click a recorder and select **Tampering Monitor**. The Tampering Monitor window appears.



Reference images are listed with the date and time they were taken in the Reference Image column. For the first time applications of this feature, the reference images are empty. In this case, click **Update All** to save the reference images. Tampering activity on each camera can be monitored by comparing reference images with live images located on the right side of the window.

PART 2 – Configuration tools

Device control tools

Device control tools provide options for managing devices.

These tools include:

- Rebooting devices
- Restoring factory defaults
- Exporting and importing configuration

Reboot device

1. Right-click a recorder icon in the Navigator panel and select **Reboot** to reboot it.
2. Click **Yes** to confirm reboot of the device. The recorder icon changes to  in the Navigator panel to indicate that it is offline.
3. After the device reboots, right-click its icon in the Navigator panel and select **Connect** to reconnect it.

Restore factory defaults

Devices that support the restore factory defaults function are listed in the “Supported Devices” row in the device details tables (see Appendix B “Device details” on page 263).

1. Right-click a recorder icon and select **Restore Factory Defaults** to have the device default to factory settings (the same settings on the device when it was shipped).
2. Click **Yes** to confirm reboot of the device. The recorder icon changes to  in the Navigator panel to indicate that it is offline.
3. After the device reboots, right-click its icon in the Navigator panel and select **Connect** to reconnect it.

Firmware management

Firmware management allows devices to be updated with new software versions.

Users can upload firmware files and perform upgrades on supported devices.

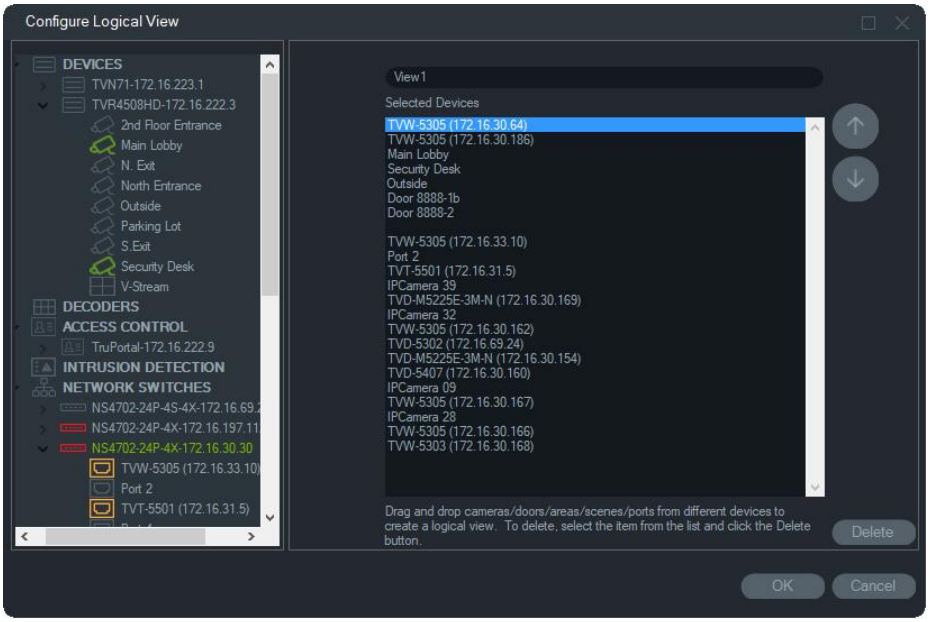
Logical views

Logical views allow devices to be grouped for easier navigation.

These views help organize large systems into meaningful categories.

To add a logical view:

1. Right-click the Logical View node in the Navigator panel and select **Add Logical View**. The Configure Logical View window appears.
2. Type a title for the view in the **View Name** field, and then drag and drop devices from the Logical View panel into the **Selected Devices** box.



3. Use the up and down arrow buttons to move devices within the list. When finished, click **OK** to create the new logical view. To delete a logical view, right-click the logical view icon in the Navigator panel and select **Delete**

To add IP Speaker's audio relays to logical groups:

1. Drag and drop IP Speaker relay(s) to the Logical Views.
2. Right-click an IP speaker device node and select **Play Sound Clips**.
3. You can play various sound clips added from different devices.

Note: To avoid confusion when multiple IP speakers have similar or identical titles for audio relays, the Logical Views display the title of an audio relay in the following format: "Relay Title – IP Speaker Title".

Network devices

Network devices such as switches can be monitored within the system.

This provides visibility into network infrastructure supporting the video system.

Aritech IFS® network switches can be added to the Navigator panel. Port status and statistics for each port on a network switch can be monitored in the navigator panel and/or the viewer panel.

Adding network switches manually

1. Right-click the Network Switches node, and then select **Add Device** > **Add Manually** from the drop-down list. The Network Switch Properties window appears.

   Note: There is only one option for the **Panel Type,** so it is selected by default.
2. Type a name in the **Panel Title** field. Values are alphanumeric.
3. Type the device's IP address in the **Panel Address** field.
4. The **Port** field is pre-populated with a default value based upon the type of device selected. If the port assigned to the device is different from the default value, type the correct port value in this field.
5. Type the required values in the **Username** and **Password** fields. These fields are only required if the device being added has been configured to require a username and password.
6. 4Select the **Enable SSL** check box if required by the server.
7. Click **OK**.

Note: After clicking **OK**, fields highlighted with a red exclamation point indicate rejected values. Move the mouse pointer over the exclamation points for tips on why the values were invalid. All fields must be valid to successfully add a device.

Adding network switches using the discovery tool

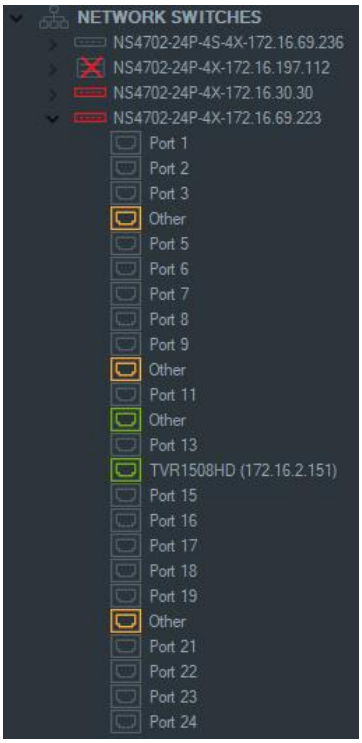
IMPORTANT: A wired network connection is required for device discovery. A device cannot be activated via a Wi-Fi network connection.

1. Right-click the Network Switches node in the Navigator panel, and then select **Add Device** > **Add via Discovery Tool** from the drop-down list or click the **Add Devices** button and then select **Add via Discovery Tool.**
2. The Discovered Devices window displays and provides a list of available network switches in the network.
3. To add network switches to the Navigator panel, select one or multiple switches from the list and click **Add**. The switch(es) appear under the Network Switches node in the Navigator panel.

Note: The discovery tool attempts to add network switches by using their default credentials. If the credentials of a switch are previously changed from default values, the switch still gets added to the Navigator panel, but it is shown as offline. In this case, updated credentials need to be applied manually by right-clicking the panel and selecting **Configure Device**.

4. Expand the Network Switches node to view all switches added to the system. Upon successful connection, the Navigator populates the respective ports under each switch.

Port information and display



Note: An ONVIF-compliant camera or recorder connected to an ONVIF-compliant network switch port displays the model name and IP address in the Navigator panel. If an attached camera is in the Navigator panel, the camera name also appears here.

Network switch icon definitions are as follows:


Switch port active with PoE.


Switch port active.

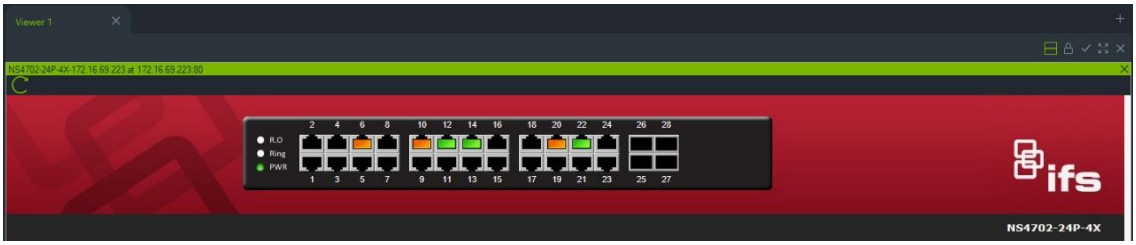

Switch port inactive.


ONVIF-compliant network switch.

To view a network switch front panel in the Viewer panel:

1. Click the **Custom View** button in the Viewer panel and select a one-up or stacked horizontal view (see “Custom Views” **Error! Bookmark not defined.** for details).

2. Right-click a network switch in the Navigator panel and select **Display Front Panel**.
3. Type the user name and password for the switch in the security window and click **OK**. The front panel of the switch appears in the Viewer panel.



To view network switch statistics:

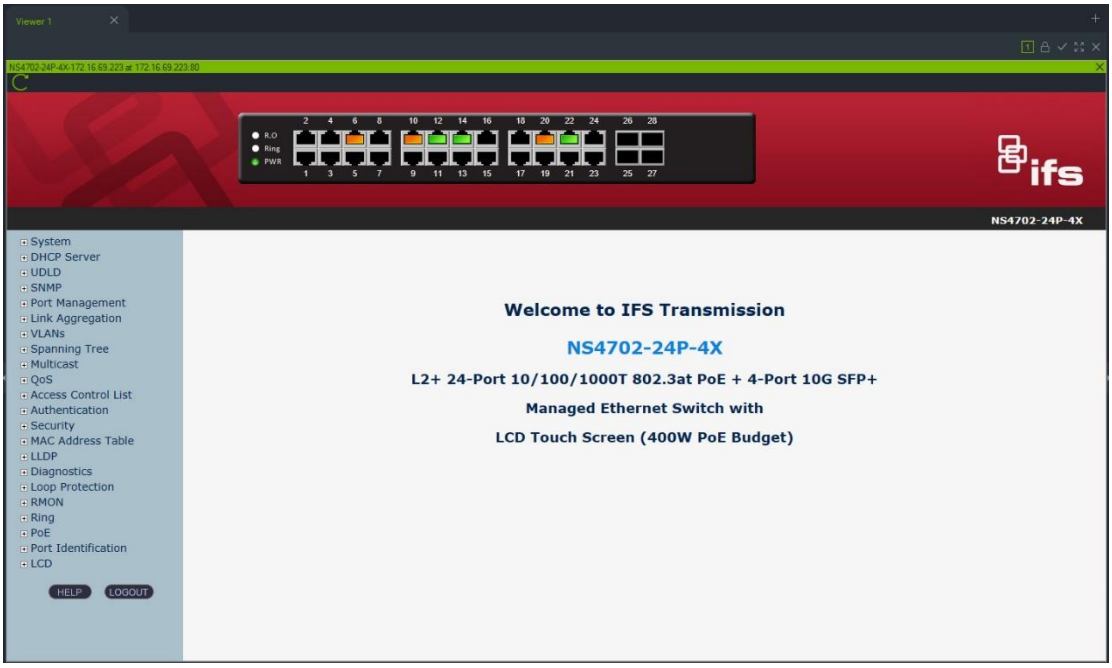
1. Right-click a network switch icon and select **Run Network Statistics**.
2. Select **Bar Chart** or **Line Chart** to view incoming and outgoing bandwidth per port.

To view port statistics:

Right-click a port icon and select **Port Statistics**. A line chart appears that shows incoming and outgoing bandwidth for the port.

Configuring network switches

1. Right-click a network switch icon in the Navigator panel and select **Configure Device**.
2. Type in the user name and password for the switch. The main web page appears. See the user manual for the specific IFS switch model for instructions on how to use the web UI to manage and configure the switch.



Note: If a switch is plugged into a switch via an RJ45 connector, it must be properly configured so that it appears in the Navigator panel. Go to **Port Identification** > **Configuration** in the switch's web UI and select **Switch** from the drop-down list next to the port number that the switch is connected to.

To power cycle a device connected to a PoE port:

Right-click a port in the Navigator panel and select **PoE Reset**. The port color will turn green and then turn orange again after 30 seconds.

To reboot a network switch:

Right-click a network switch icon and select **System Reboot** to power cycle the switch.

PART 3 – Integrations

Access control integration (End of Life)

The system can integrate with the TruPortal access control solution to monitor and control doors.

Users can:

- View door status
- Open doors remotely
- Link cameras to access control events

TruPortal™ is an IP appliance-based access control system that integrates with TruVision Navigator.

After installing the TruPortal SDK, add TruPortal systems to the Navigator panel by choosing one of the following options from Access Control:

- Add manually. See “Adding TruPortal systems manually” on page 168.
- Add via discovery tool. See “Adding TruPortal systems using the discovery tool” on page 168.

Installing the TruPortal SDK

Note: The TruPortal SDK 1.1.54 or later plug-in must be installed before Navigator can communicate with the TruPortal panel.

To download and install the TruPortal SDK plug-in:

1. Go to https://firesecurityproducts.com.
2. Search for TruVision Navigator 9.2, go to the webpage and select Downloads.
3. Download the TruPortal SDK plug-in Zip file and extract the contents to a folder on the local computer.
4. Launch Internet Explorer 9 or later and type the IP address of a TruPortal panel installed in the local network into the Address bar.
5. Log into the system as a user with *Plugins* > *Modification* permissions.
6. Select *System Administration* > *Plugins*.
7. Click the **Install** button.
8. Click the **Select File** button.
9. In the Open dialog box, navigate to the folder containing the plug-in package (the file has an .LFF extension), select the file, and then click **Install**.

Note: Plug-in installation may take up to 10 minutes. The panel restarts after successful installation. The plug-in automatically starts after the panel restarts.

Adding TruPortal systems manually

1. Follow the instructions under “Installing the TruPortal SDK” above.
2. Right-click the Access Control node, and then select **Add Panel** > **Add Manually** from the drop-down list. The Access Control Panel Properties window appears.

   Note: There is only one option for the **Panel Type** so it is selected by default.
3. Type a name in the **Panel Title** field. Values are alphanumeric. The default panel title is My TruPortal.
4. Type the device’s IP address in the **Panel Address** field.
5. The **Port** field is pre-populated with a default value based upon the type of device selected. If the port assigned to the device is different from the default value, type the correct port value in this field.
6. Type the required values in the **Username** and **Password** fields. These fields are only required if the device being added has been configured to require a username and password.
7. Select the **Enable SSL** check box if required by the server.
8. Click **OK**.

Note: After clicking **OK**, fields highlighted with a red exclamation point indicate rejected values. Move the mouse pointer over the exclamation points for tips on why the values were invalid. All fields must be valid to successfully add a device.

Adding TruPortal systems using the discovery tool

Navigator is equipped with an embedded device discovery tool that discovers devices such as recorders, cameras, and encoders in the network and permits the addition of one or more of those devices.

IMPORTANT: A wired network connection is required for device discovery. A device cannot be activated via a Wi-Fi network connection.

---

1. Follow the instructions under “Installing the TruPortal SDK” on page 167.
2. Right-click the Access Control node, and then select **Add Panel** > **Add via Discovery Tool** from the drop-down list. The Discovered Access Control Panels window appears and provides a list of available control panels in the network.
3. To add control panels to the Navigator, select one or multiple panels from the list and click **Add**. The panel(s) appear under the Access Control node in the Navigator panel.

Note: The discovery tool attempts to add access control panels by using their default credentials. If the credentials of a panel are previously changed from default values, the panel still gets added to the Navigator panel, but it is shown as offline. In this case, updated credentials need to be applied manually by right-clicking the panel and selecting **Properties** or **Configure**.

4. Expand the Access Control node to view all panels added to the system. Upon successful connection, the Navigator populates the respective doors under each panel. To unlock a door, right-click the door icon and select **Unlock**.

Access Control configuration requires that Adobe Flash be installed on the computer performing the configuration. See the *TruPortal Software User Guide* for instructions on configuring TruPortal.

Performing lock and unlock operations

Right-clicking the Access Control node provides the following lock/unlock operations:

- **Global Lockout**: Lock out all doors of all panels.
- **Global Reinstate**: Reinstate all doors of all panels.

Right-clicking an Access Control panel provides the following lock/unlock operations:

- **Reinstate All Doors**: Restores all doors to their normal state, unless a designated unlock input is active (see the *TruPortal Software User Guide* for details).
- **Lockout All Doors**: Locks all doors and ignores credentials, so that nobody can enter or exit. After issuing this command, reinstate all doors so that individual doors can be controlled directly.
- **Unlock All Doors**: Releases the locks on all doors, allowing free access and egress. After issuing this command, reinstate all doors so that individual doors can be controlled directly.

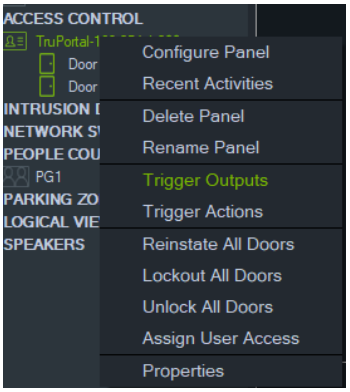
Right-clicking a door icon provides the following lock/unlock operations:

- **Unlock**: Releases the lock on the door, allowing free access and egress until the door state is changed by either a reader schedule or a global (“all doors”) command.
- **Reinstate**: Restores the door to default behavior based on the schedule.
- **Lockout**: Locks the door and ignores credentials so that nobody can enter or exit.
- **Secure**: Locks the door.

Trigger outputs

Select Trigger Outputs in the Access Control panel context menu to view a list of outputs configured in the panel.

Context Menu Option



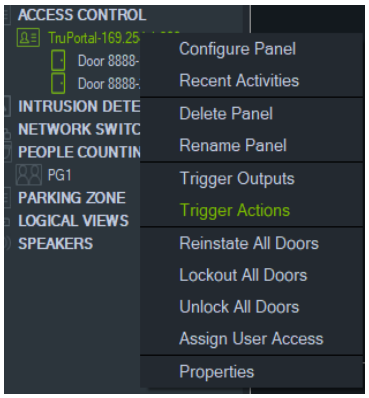
Trigger Outputs window

Toggle the trigger output switches to the on position (green) or off position as needed.

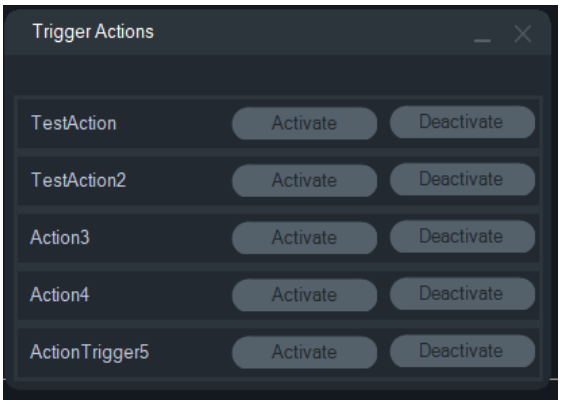
Trigger actions

Select Trigger Actions in the Access Control panel context menu to view a list of Actions configured in the panel.

Context Menu Option



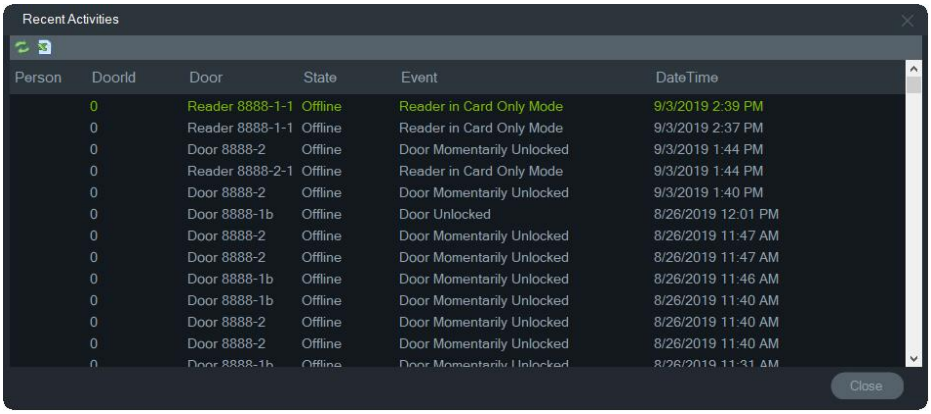
Trigger Actions window



To activate actions, click the **Activate** button. To deactivate actions, click the **Deactivate** button.

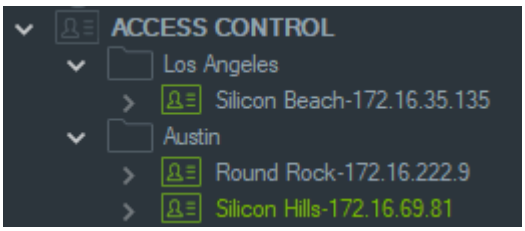
Recent activities

Select Recent Activities in the Access Control panel context menu to view a list of time stamped events associated with each door in the panel. Click the **Export List** button to export the list of recent activities in the CSV file format.



TruPortal multisite configuration

Under the Access Control node, a single user credential can be assigned to multiple TruPortal panels grouped into one site by using folders to separate sites. Using this logic, panels grouped under a folder belong to a single site or group of sites. See the example below:



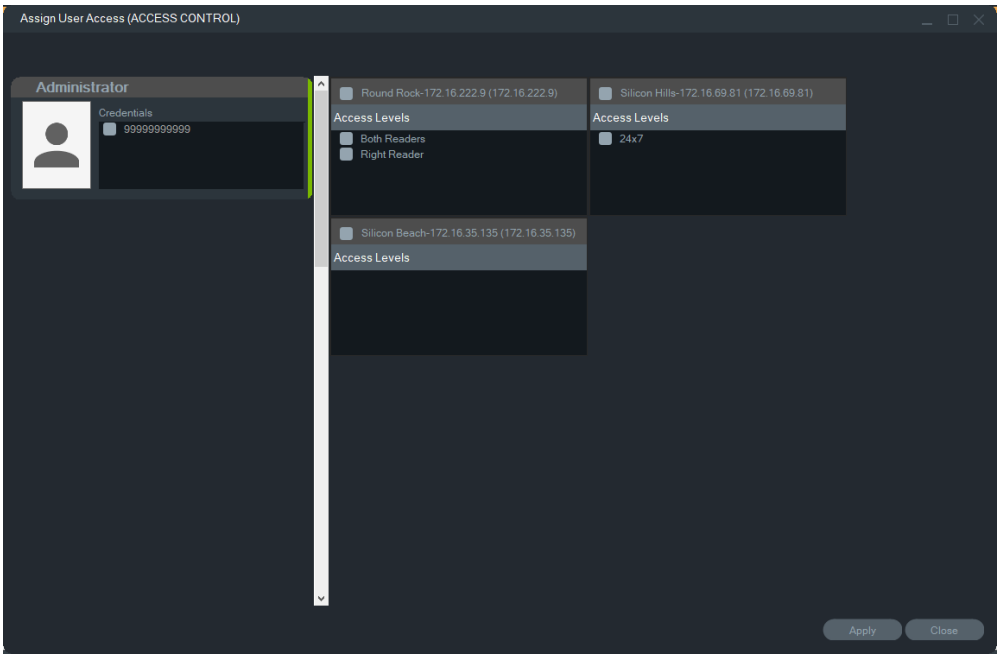
Notes

- The panel or panels under each folder operate as a single system, and each system can accept a maximum of eight card formats simultaneously. Card format refers to the format of data containing credential ID information (standard 26-bit, for example) encoded in door/entrance access cards/badges.
- The name of each card format must be unique within a system since the card format name is the identifier, not the format itself.
- Card formats of the same name are considered the same card format in TruPortal.
- We suggest renaming access control panels in Navigator with site-specific names (see example above) to make user access assignment easier.

To assign user access levels:

Note: Users must be added and configured with credentials in the TruPortal web UI before assigning access levels in Navigator. We suggest that user names be as unique as possible, using a middle name or initial when applicable. See *TruPortal Software User Guide* for instructions on configuring TruPortal.

1. Right-click an access control panel or folder and select **Assign User Access**.
2. The Assign User Access window appears. If necessary, find a user by typing their name into the Search box and click **Search**. Select the check box next to the user image. Only one user can be selected at a time.
3. Select the check box next to the credential number(s) associated with the user. Panels appear in the Assign User Access window, and those associated with the user display a green bar across the top (select **Show Assigned Permission** in the Filter drop-down list to show only these panels).



4. Select individual panels or click the **Select All Panels** button to assign access levels for the user. Click **Remove All Access Levels** to remove all access, or **Refresh** to update recently assigned access levels.
5. When finished, click **Apply**.

To assign an event notification:

Right-click a panel door icon and select **Assign Event Notification**. When the user accesses the door, an access control notification pop-up window appears with the user's name, associated picture, and a notification description such as "Access Granted."

Intrusion detection integration

Supported Aritech intrusion panels can be added to the Navigator panel. Intrusion areas and sensors can be monitored in the Navigator panel and/or the viewer panel.

Setup prerequisites for adding an intrusion panel to Navigator

1. The Aritech intrusion panel must run one of the following firmware versions for interoperability with Navigator:

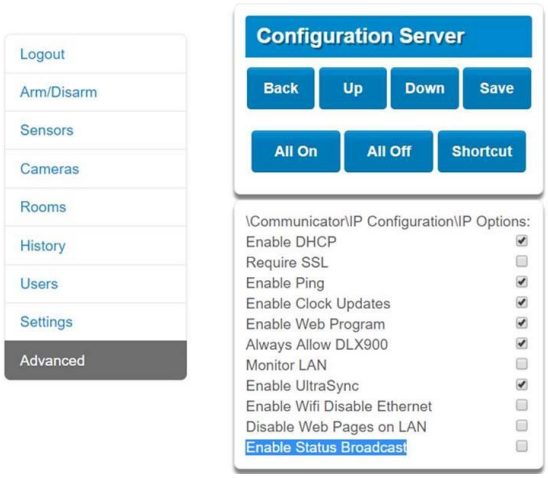
   UltraSync Self-Contained HubB0403001A58P002011-33 or later

   UltraSync Modular HubB0403001A56P002005-01 or later

   ZeroWireB0403001A58P002010-31 or later

   xGenB0403001A56P002005-16 or later

2. The discoverable Aritech intrusion panel (see step 1 for information) must be fully set up and functioning with intrusion areas and sensors installed and/or defined prior to adding it to the Navigator panel. Go to https://firesecurityproducts.com and download the appropriate reference manual and/or installation guide for details.
3. The Aritech intrusion panel web UI must have the **Enable Status Broadcast** setting enabled to communicate effectively with Navigator. See one of the reference manuals listed above for further details.



Adding intrusion panels manually

1. Right-click the Intrusion Detection node, and then select **Add Panel** > **Add Manually** from the drop-down list. The Intrusion Panel Properties window appears.

   Note: There is only one option for the **Panel Type** so it is selected by default.

2. Type a name in the **Panel Title** field. Values are alphanumeric.
3. Type the device's IP address in the **Panel Address** field.

Note: The **Port** field is pre-populated with a default value based upon the type of device selected. If the port assigned to the device is different from the default value, type the correct port value in this field.

4. Type the required values in the **Username** and **Password** fields. These fields are specific to intrusion detection and unique to each individual, and must be assigned by the intrusion panel administrator. The user name must begin with “TruNav-.”
5. Select the **Enable SSL** check box if required by the server.
6. Click **OK**.

Note: After clicking **OK**, fields highlighted with a red exclamation point indicate rejected values. Move the mouse pointer over the exclamation points for tips on why the values were invalid. All fields must be valid to successfully add a device.

Adding intrusion panels using the discovery tool

IMPORTANT: A wired network connection is required for device discovery. A device cannot be activated via a Wi-Fi network connection.

1. Right-click the Network Switches node, and then select **Add Panel** > **Add via Discovery Tool** from the drop-down list.
2. The Discovered Devices window displays and provides a list of available intrusion panels in the network.
3. To add intrusion panels to the Navigator panel, select one or multiple panels from the list and click **Add**.
4. Type the required values in the **Username** and **Password** fields. These fields are specific to intrusion detection and unique to each individual and must be assigned by the intrusion panel administra0tor. The user name must begin with “TruNav-.”
5. Expand the Intrusion Detection node to view all panels added to the system. Upon successful connection, the Navigator populates the respective sensors under each switch.

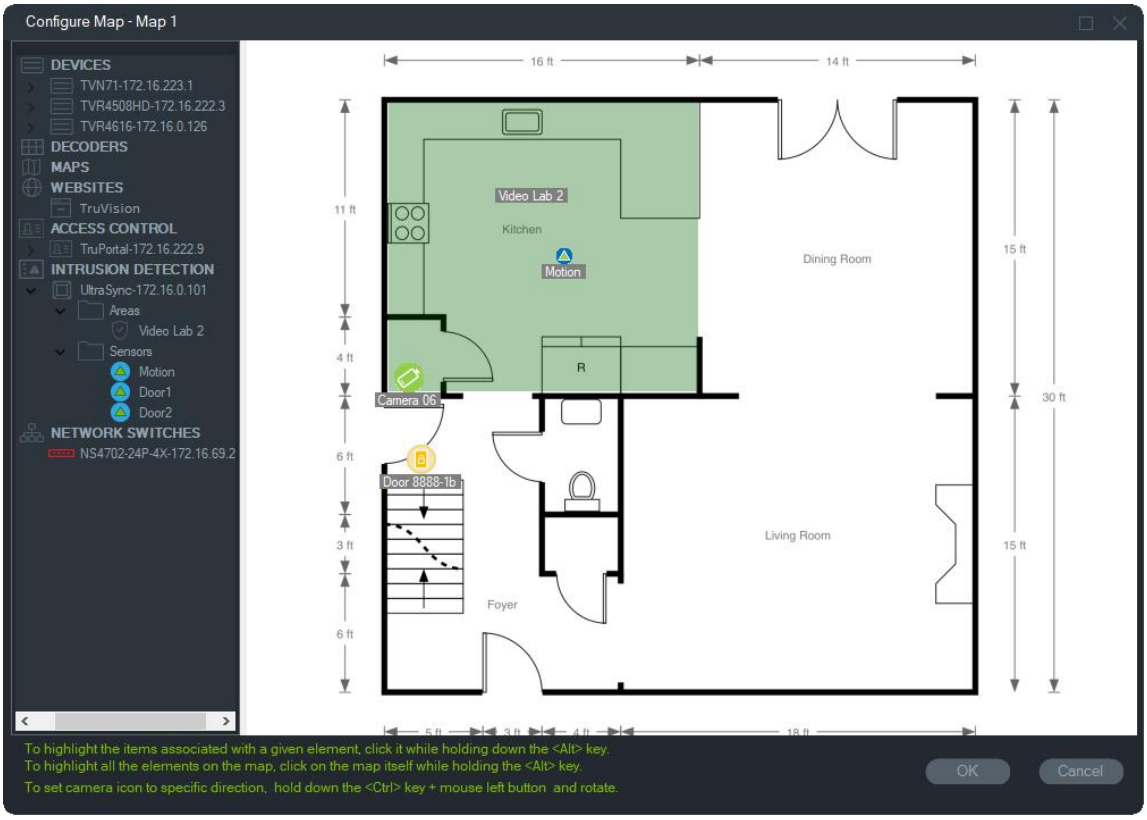
Configuring a map for intrusion notifications

A map can be configured for intrusion notifications that will appear in the Notifier (see “Notifier configuration” on page 97) and the Navigator panel. Notifications from cameras linked to intrusion sensors or areas appear in the Notifier as video links.

To add an intrusion area to a map:

1. Right-click a map in the Navigator panel and select **Configure Map**.
2. Expand the Areas folder under the intrusion panel name, and then drag and drop an intrusion area icon onto the map.

3. Resize and move the intrusion area as needed. The fill color of the intrusion area can be changed by right-clicking the area and selecting **Color**.



To add an intrusion sensor to a map:

1. Right-click a map in the Navigator panel and select **Configure Map**.
2. Expand the Sensors folder under the intrusion panel name, and then drag and drop an intrusion sensor icon onto the map. A green icon appears on the map.
3. Move the intrusion sensor on the map as needed. Sensors should be placed within a defined intrusion area.

To link a camera to an intrusion area or sensor:

1. In the Configure Map window, right-click an intrusion area or sensor and select **Linked Cameras**.
2. Select the cameras to link to the intrusion area or sensor (or click **Select All**) and then click **OK**.
3. To see which cameras on the map are linked to an intrusion area or sensor, hold down the Alt key while clicking the area or sensor icon and orange boxes appear around the connected camera icons.

To configure a sensor:

Right-click a sensor icon on a map in the Viewer panel and make the following selection:

- **Bypass**: Permits arming of the panel while ignoring this sensor.

To arm/disarm an intrusion area:

- Right-click an intrusion area in either the Navigator panel or a map in the Viewer panel and select **Arm** > **Away** or **Arm** > **Stay** to arm the area.
- Right-click an intrusion area in either the Navigator panel or a map in the Viewer panel and select **Disarm** to disarm the area.
- Right-click the Intrusion Detection node and select **Global Arm** > **Away** or **Global Arm** > **Away**, or **Global Disarm** to apply settings to multiple intrusion areas and/or panels.

Intrusion area status

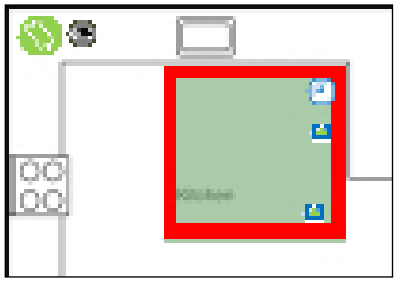
Intrusion area icon definitions are as follows:

Disarmed

Armed in Stay mode. The area will be ignored by the intrusion panel.

Armed in Away mode.

In addition to the icon changing in the Navigator panel, intrusion area status is also shown on maps in the Viewer panel. The border around the intrusion area changes according to the armed or disarmed state. For example, an intrusion area armed in the Away mode appears as follows:



Configuring the intrusion panel

1. Right-click an intrusion panel and select **Configure Panel**. A video tile containing the intrusion panel interface appears in the Viewer panel.
2. Type in the required name and password and click **Sign In**. Go to firesecurityproducts.com and download the appropriate reference manual and/or installation guide for details on using the intrusion panel web UI.

Audio integration

Audio devices such as IP speakers can be integrated with the system.

Users can:

- Play audio clips
- Trigger audio based on events

Adding IP speakers

TruVision Navigator supports IP speakers from Zenitel (see Appendix D “Configure Zenitel IP speakers” on page 311 for supported models). Add IP speakers to the Navigator panel by choosing one of the following options:

- Add manually. See “Adding IP speakers manually” below.
- Add via discovery tool. See “Adding IP speakers using discovery tool” on page 178.

By adding IP speakers users can upload a wide range of announcement and warning audio clips. These clips can be played by users while they are viewing live video from cameras. This functionality allows relevant audio cues or messages to be added with conjunction with the visual feed or specific actions.

IP speakers context menu

Right-click on any of the three available nodes: Speakers, Speaker device, and Audio relay, to bring up a context menu. The available selections in the context menu are described below.

Adding IP speakers manually

1. Follow the instructions in Appendix D “Configure Zenitel IP speakers” on page 311.
2. Right-click the **Speakers** icon, and then select **Add Speaker** > **Add Manually** from the drop-down list. The Discovered Speakers window appears.
3. Type a name in the **Speaker Title** field. Values are alphanumeric.
4. Type the device’s IP address in the **Address** field.
5. The **Port** field is pre-filled with a default value based upon the type of device selected. If the device's assigned port differs from the default value, manually enter the correct port value in the **Port** field.
6. Type the required values in the **Username** and **Password** fields. These fields are only required if the device being added has been configured to require a username and password.
7. Click **OK**.

8. Upon successful connection, the TruVision Navigator populates the respective audio relays for each IP speaker. To play audio relay, see below.

Adding IP speakers using discovery tool

TruVision Navigator includes a built-in device discovery tool that automatically detects devices, such as recorders, cameras, and encoders on the network. This tool allows you to easily add one or more of these devices.

1. Follow the instructions in Appendix D “Configure Zenitel IP speakers” on page 311.
2. Right-click the **Speakers** icon and select **Add Speaker** > **Add via Discovery Tool** from the drop-down list. The Discovered Speakers window appears and displays a list of available IP speakers in the network.

   Note: Discovered Speakers window only displays limited information.
3. To add IP speakers to the Navigator view tree, select one or multiple panels from the list and click **Add**. The panel(s) appear after clicking the **Speakers** icon in the **Navigator** panel.
4. A credential dialog is displayed, where you need to enter username and password (if needed) of the IP speaker. Enter the details and click the **OK** button.
5. Click the **Speakers** icon to view all IP speakers added to the system. Upon successful connection, the TruVision Navigator populates the respective audio relays for each IP speaker. To play audio relay, see “Play sound clip”.

Play sound clip

After adding the IP speaker manually or via discovery (using the right credentials), the IP speaker will be added to Navigator view tree and populated with audio relays. To play a sound clip:

1. Right-click the required audio relay and select **Play Sound Clip**.

Renaming audio relay titles

The titles for the audio relays are populated with default values from the IP speakers configuration. However, you have the option to edit these titles with the appropriate labels. Modifying the relay titles will not affect the configuration of the IP speakers' relays in any way.

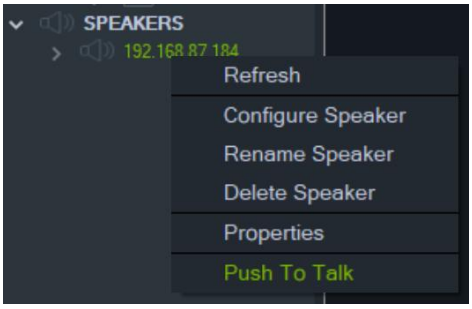
1. Right-click the required audio relay populated under IP speakers.
2. Select **Rename**.
3. Change the title as required and click **OK**.

Push To Talk

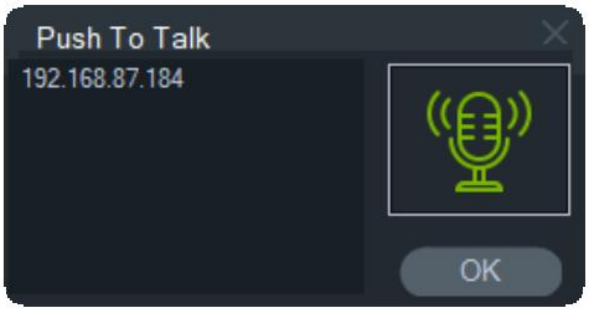
The TruVision Navigator allows live audio streaming from the application to IP speakers. The “Push To Talk” context menu opens a dialog with the selected speaker(s). When a user needs to send live audio from the microphone connected to the PC running the TruVision Navigator, they can click & hold the MIC button icon (see the image below) to talk over the IP speaker.

If the user has multiple speakers and needs to talk over all of them simultaneously, they can open the Push to talk menu from the SPEAKERS node. Users can individually add each speaker to the Push to talk window from the menu and use it to talk over multiple speakers.

Context Menu



Push To Talk – Window



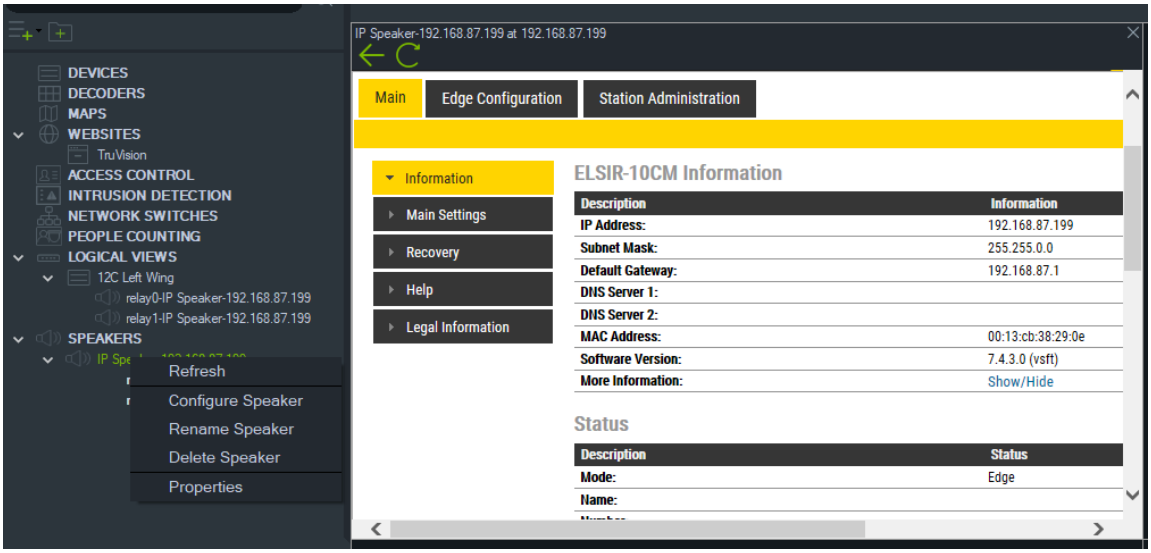
There are the following limitations:

- Push to Talk supports only one connection at a time; multiple connections are not supported.
- Playing an audio clip and simultaneously talking over the speaker may result in unclear audio on the IP speakers.

IP speaker configuration

The TruVision Navigator makes it possible to configure an IP speaker in a web browser.

1. Right-click the IP speaker node and select **Configure Speaker**.
2. An IP speaker configuration window is opened in a web browser. After providing credentials, you can modify the configuration of the IP speaker.



Refresh audio relays after IP speaker configuration

After adding new audio relays or deleting existing ones in a configured IP speaker (in the Navigator), a refresh is required to reload the updated audio relays. Right-click the IP Speaker device node and select **Refresh**. This reloads entire audio relays of the IP Speakers.

Logical views support

To group sound clips, audio relays can be added to Logical Views, see “Logical views” on page 79. To add IP Speaker’s audio relays to logical groups:

1. Drag and drop IP Speaker relay(s) to the Logical Views, see “Logical views” on page 79.
2. Right-click an IP speaker device node and select **Play Sound Clips**.
3. You can play various sound clips added from different devices.

Note: To avoid confusion when multiple IP speakers have similar or identical titles for audio relays, the Logical Views display the title of an audio relay in the following format: “Relay Title – IP Speaker Title”.

Event-actions support

You can add IP Speaker audio relays as an action for specific events originating from the Recorder, Camera, Intrusion/TruPortal panel, or a combination of multiple notifications. See “Event-Actions” **Error! Bookmark not defined.** for more details.

1. In the Event-actions window, drag and drop IP speakers audio relay(s) into the **Actions** pane.
2. Configure the required events and other settings. See “**Error! Reference s ource not found.**” **Error! Bookmark not defined.** for more details.
3. When a configured event is triggered, it activates the playback of an audio clip on the designated IP Speaker.

Map control support

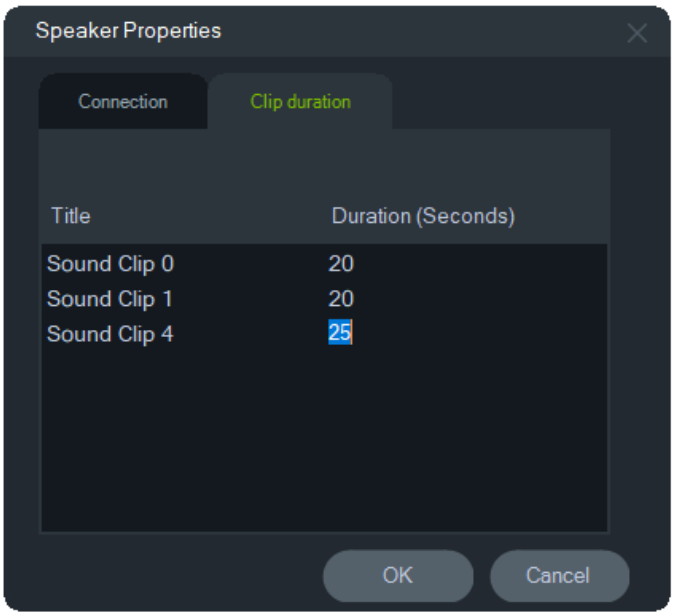
IP Speaker devices can be placed on floor maps according to their physical locations. See “Adding maps” **Error! Bookmark not defined.**.

1. Drag and drop IP Speaker devices on the floor map at their actual location and save the floor maps.
2. Open the floor maps on the Viewer tile, right-click IP Speaker device icon displays configured audio relays, select any audio relay triggers audio on the IP Speaker.

IP speaker audio clips duration setting

To ensure sequential playback of audio clips when playing multiple audio clips from Logical Views and/or Event-Actions, the following configuration needs to be implemented if the Logical View/Event-Actions contain more than one audio clip from the same speaker:

1. Right-click **IP Speakers** and open **Properties**.
2. Switch to second tab – **Clip duration**.
3. Update the duration (in seconds) for each clip and click the **OK** button.



Web and external integrations

External resources such as websites can be integrated into the system.

This allows users to access additional tools or information directly from the application.

Adding websites

Websites can be added to the Navigator panel for viewing and navigating in the Viewer panel.

To add a website:

1. Right-click the Websites node in the Navigator panel and select **Add Website**. The Add Website window appears.
2. Type a title for the website in the **Title** field, and then type or copy/paste the website's URL into the **URL** field.
3. Double-click the website icon or drag it to a tile in the Viewer panel to view and navigate the website.

Navigate the website in the Viewer panel tile using the pointer, scroll bar, and the icons in the top menu (**Forward**, **Back**, and **Refresh**). To delete a website, right-click the website icon in the Navigator panel and select **Delete Website**.

To configure a website in the Navigator:

1. Right-click the website icon in the Navigator panel that requires configuration and select **Configure Website**. The Configure Website window appears.
2. Type a new title for the website in the **Title** field or type or copy/paste a new URL into the **URL** field.

Launching maps and websites from a map in the Viewer Panel:

In a map in the Viewer Panel that has been configured to include one or more submaps and/or websites, double-click a submap or website icon to launch it in a Viewer Panel tile.

PART 4 – Advanced tools

Tasks and background processes

Certain operations, such as video export, run as background tasks.

Users can monitor task progress and status within the system.

Many system operations, such as video export, configuration backup, and firmware updates, are executed as tasks. These tasks can be monitored through the Tasks interface, which provides status, progress, and results of each operation.

Tasks represent asynchronous system operations that are executed in the background. Each task progresses through stages such as pending, running, and completed, and may succeed or fail depending on the operation. Administrators can monitor and review task results to verify system operations.

System limitations and considerations

System performance depends on factors such as:

- Number of devices
- Network bandwidth
- Video resolution

Proper configuration helps maintain optimal performance.

Chapter 13
User interface reference

Overview

This chapter provides a reference for the user interface elements used in the system.

It describes the main panels, buttons, icons, and indicators that appear in the application. This information helps users understand the meaning and function of interface elements during operation.

This chapter is intended as a reference and does not provide step-by-step instructions. For task-based procedures, refer to the relevant sections in earlier chapters.

Navigator panel

The Navigator panel displays the system structure and provides access to devices, maps, and other system resources.

The panel uses a tree structure to organize items, allowing users to expand and collapse folders to navigate through the system.

Common items include:

- Devices such as recorders and cameras
- Maps
- Custom views
- Other system elements

Each item is represented by an icon that indicates its type and status. Icons may also reflect current conditions, such as device availability or active events.

The Navigator panel allows users to browse and select items for viewing or management. Basic interactions include expanding folders, selecting items, and navigating through the system hierarchy.

Note: The Navigator panel is permission-based, so if a user does not have rights to perform certain actions, they will not see the options.

Viewer panel

The Viewer panel displays live video, playback video, maps, and other content.

The panel is composed of tiles arranged in a layout. Each tile represents a camera stream, map, or other item. Multiple tiles can be displayed at the same time.

Each video tile includes a header and footer that provide information and controls.

Top bar:

- Camera name
- Date and time
- Synchronization status
- Close button

Bottom bar:

- Tile selection checkbox
- Device/camera type icon
- Recorder name
- Video status (live, playback, paused)

Tile color indicates its state:

- Green: Selected
- Gray: Not selected
- Yellow: Local file playback

A selected tile determines which controls are applied. Viewer tiles can display different types of content, including live video, recorded video, maps, and websites.

Viewer panel controls and buttons

The Viewer panel includes a set of controls used to manage video display, layouts, and playback. These controls allow users to interact with video tiles and adjust how information is displayed.

Viewer tab buttons

	**Custom/sequence view**. Use custom views to define and save multi-site view templates for future use.
	**Lock Current Layout**. Prevents changes to the current viewer panel setup.
	**Select all**. Select all tiles in the viewer.
	**Toggle**. Toggle between normal view and maximized view.
	**Close All**. Close all tiles in the viewer.
	**New Viewer**. Add a tabbed viewing panel (10 maximum).

Tile controls

Each video tile includes controls for managing the displayed content.

Common tile controls include:

- Close tile
- Select tile
- Open context menu

Playback controls

The following table describes each playback control in the Navigator application.

Button	Description
	**Frame Step Reverse**. Go to previous frame.
	**Rewind**. Rewind video.
	**Pause**. Pause video.
	**Play**. Play back video. Clicking the **Play** button multiple times increases playback speed.
	**Fast Forward**. Fast forward video.
	**Frame Step Forward**. Go to next frame.
	**Local Record**. See “**Error! Reference source not found.**” on page **Error! Bookmark not defined.**.

Playback controls allow interaction with recorded video.

They include:

- Basic playback
  - Play
  - Pause
  - Stop
- Navigation
  - Timeline cursor
  - Jump forward/backward
- Speed
  - fast forward
  - Rewind

PTZ controls

PTZ controls allow users to adjust the position and view of supported cameras directly from the Viewer panel.

PTZ control. Launches the PTZ window.

PTZ controls include:

Movement:

- Pan: Move the camera left or right
- Tilt: Move the camera up or down

Zoom:

- Zoom in: Increase magnification
- Zoom out: Decrease magnification

Focus:

- Manual focus: Adjust sharpness manually
- Autofocus: Automatically adjust focus

Iris:

- Adjust brightness by controlling the lens opening Speed:
- Set the movement speed of the camera

Mouse-based control

PTZ cameras can also be controlled directly within the video tile.

Available interactions include:

- Click and drag to move the camera
- Mouse wheel to zoom in and out

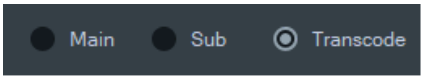
Preset and tour references

Additional PTZ-related functions such as presets and tours may also be available, allowing cameras to move to predefined positions or follow predefined paths.

See Chapter 6 for more details about the PTZ use and controls.

Stream and display controls

Live and **Playback** stream toggle control.

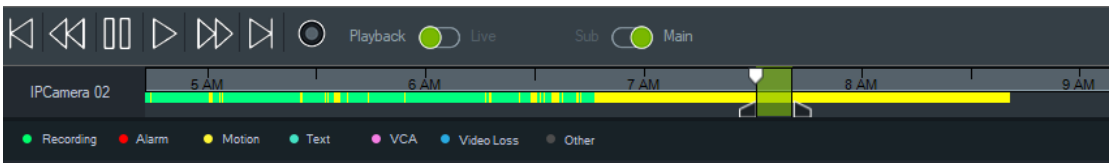


Switch between Main, Sub and Transcode streams.

Timeline indicators

The timeline displays recorded video across a time range and includes visual indicators that represent recording activity and playback position.

The timeline bar represents the available video for the selected camera. Recorded segments indicate periods where video is available, while gaps represent times with no recording.



The current playback position is shown using a cursor on the timeline, indicating the exact time being viewed.

Time selection markers may appear on the timeline to define a selected range of video.

Thumbnail previews may be displayed when hovering over recorded segments, providing a visual snapshot of the video at a specific point in time.

Bookmarks are shown as markers on the timeline and identify important events for quick reference.

When multiple cameras are used, additional timelines may appear to allow comparison of recordings. Synchronization indicators may be shown when playback is aligned across multiple video tiles.

Icon reference tables

Overview

This section provides a reference for icons used throughout the application.

Icons indicate device types, system status, and other information displayed in the user interface.

Device icons used on maps

Device icons and other icons used on maps

Icon	Description
Video icons (green)	
	IP camera
	PTZ dome camera
	360° camera
	People counting camera
	Recorder
Network switch icons (red)	
	IFS network switch

Access control & intrusion icons used on maps

Icon	Description
Access control icons (gold)	

Icon	Description
	TruPortal access control panel
	Access control panel door closed and locked
	Access control panel door closed and unlocked
	Access control panel door closed in lockout state
	Access control panel door open
Intrusion icons (blue)	
	Intrusion control panel
	Intrusion sensor ready
	Intrusion sensor not ready
	Intrusion sensor alarm
	Intrusion sensor bypass

Status icons and indicators

Icon	Description
Green indicator	Active/normal state
Gray indicator	Inactive
Re indicator	Alarm or failure
Yellow indicator	Warning or special state

Specific intrusion area icon definitions are as follows:

 Disarmed

	Armed in Stay mode. The area will be ignored by the intrusion panel.
	Armed in Away mode.

Map and navigation icons

Icon	Description
	Website. Double-click to launch a web site from a map.
	Submap. Double-click to launch a secondary map.

Special function icons

Icon	Description
	Alarm output trigger on
	Alarm output trigger off
	Right-click to open Play Audio Clips menu.

Context menu and additional actions

Additional actions are available through context menus by right-clicking a video tile or other elements in the Viewer.

These actions provide access to functions that depend on the selected item and current mode.

Context menu actions may include:

- Playback-related functions
- Export and snapshot options

- Analytics display features
- Camera-specific controls
- System or device-related actions
- Examples of context menu actions include instant replay, snapshot capture, stream selection, and analytics display options.
- The availability of these actions depends on the selected device, current video mode, and user permissions.

Application menu

The application menu provides access to system-wide tools and settings.

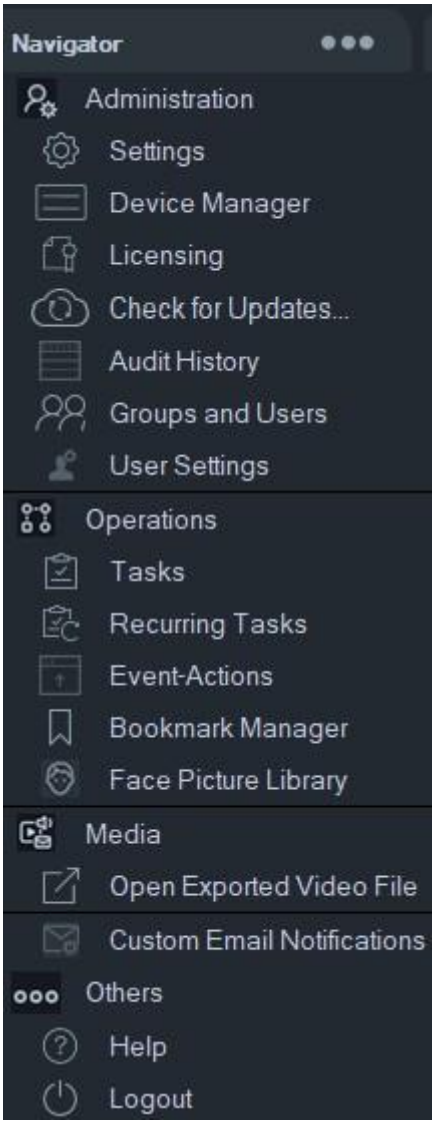
These include:

- Administration settings & tools
- Operational tools
- Media related settings and tools
- Others: help function and logout

Viewer panel

	**Add Bookmark**. Add a bookmark with notes to the camera timeline for quick navigation to a marked incident. See “**Error! Reference source not found.**” on page 131.
	**Save Video**. Send a video segment of the time range selected and highlighted in green in the timeline to the Collector for export. See “**Error! Reference source not found.**” on page **Error! Bookmark not defined.**.
	**Snapshot**. See “Create a snapshot during live view” on page 81.
	PTZ control. Launches the PTZ window. See “PTZ controls” on page 88.
	**Push to Talk**. Speak through an attached microphone into a selected recorder or camera that has speakers installed.
	Move to previous/Move to next bookmark on the timeline.
	Show/Hide bookmarks on the timeline. These icons only appear when a single video tile is selected.
	Zoom In/Out on the timeline. Zoom out to the date level and zoom in to the minute level.
	Center the timeline to the location of the green timeline cursor.

	Go To Date of recorded video
Notifier panel	
	**Filters**. Select color coded notification filters to see notifications in the Notifier based on specific criteria.
	**Event Center**. Launches the Event Center, which contains a list of notifications sent from Navigator devices.
Collector panel	
	**Show files in folder**. Opens the folder where the files are located in Windows Explorer.
	**Export**. See “Export video” on page 139.
	**Delete All Collector Items**. Delete all items in the Collector.
Admin	
	**Server Online**. Indicates that the server is online in a client/server installation.
	**Server Offline**. Indicates that the server is offline. See “Server offline mode” on page 241.
	**Keypad status**. Indicates that the keypad is connected to the client computer.
	**Keypad Not Connected**. Indicates that the keypad is not connected to the client computer.



The following table describes the function of each button and indicator in the top-level view of the Navigator application.

Note: Not all buttons and indicators listed are supported by all devices.

Button	Description
	Navigator menu drop-down list contains the following options:
	Settings. See Chapter 14.
	Device Manager. See Chapter 4 “Device Manager” on page 40.
	Bookmark Manager. Edit and delete bookmarks or play back bookmarked video. See “Bookmarks” on page 131.
	Tasks. Monitor scheduled tasks such as video exports, database backups, and database restores. See “Tasks” on page 246.

Button	Description
	**Recurring Tasks**. Monitors video exports created according to a recurring schedule. See “Recurring tasks” on page 247.
	**Open Exported Video File.** Browse for and launch an exported video in the Viewer.
	**Check for Updates** Downloads the latest language pack and standalone player from the cloud. Language pack requires a restart. Click **Restart Navigator** to restart the application and apply updates.
	**User Settings:** Allows the user to change password and/or change the Challenge Question. See “User management” on page 203.
	**Groups and Users**. Add new users and user logins, add a challenge question, assign permissions, and create groups
	**Audit History.** Set event filters and a time range for viewing user activity
	**Event-Actions**. Permits the user to cause an action on any device in the Navigator panel triggered from any number of devices reporting notifications.
	**Help**. Includes a Help file as well as version, copyright, and end user license agreement information. Custom Help or training links can be added to this menu for specific uses..
	**Logout**. Log out of the Navigator program. Logging out permits another user to log in on the same machine
	**Add Device**. Add recorders and cameras to the device panel. See “Add device” on page 36
	**Add Folder**. Organize devices in the device panel by adding folders. See “Adding folders” on page 76.

Chapter 14
System Settings

Overview

This chapter describes system-wide configuration settings used to manage users, behavior, and overall system operation.

These settings control how the system functions, how users interact with it, and how data is handled across the application.

System settings apply globally unless otherwise specified and may vary depending on user permissions and system configuration.

System settings include both server-level and client-level configuration.

- Server settings apply system-wide and affect all users and devices
- Client settings apply only to the local workstation

Understanding this distinction is essential when configuring system behavior and troubleshooting issues.

General settings

General settings define the overall behavior and appearance of the application.

Typical general settings include:

- Language and regional settings
- Date and time format
- Application startup behavior
- Display preferences

Changes to general settings affect the user experience but do not impact system functionality or device behavior.

Configuration summary

To configure general settings:

1. Open the **Application** menu and go to **Settings > Client**
2. Set the preferred language and regional settings

3. Define startup and interface behavior
4. Adjust display preferences as required

Notes / best practices

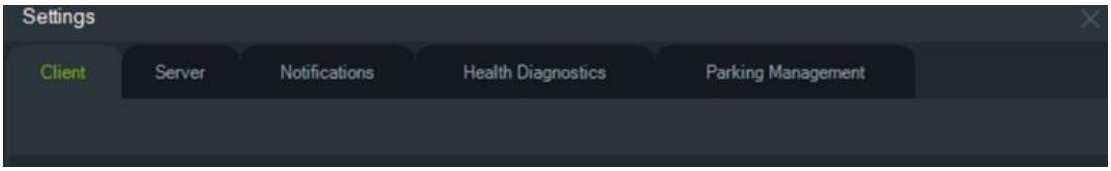
- Settings changes may require a restart depending on the configuration
- Use consistent regional settings across all clients for operational clarity

For both the standalone and multi-client installation models, the TruVision Navigator client and server can be configured for specific features using the Settings window.

To access the Settings window, click the Navigator menu button in the Navigator title bar and then select **Settings**.

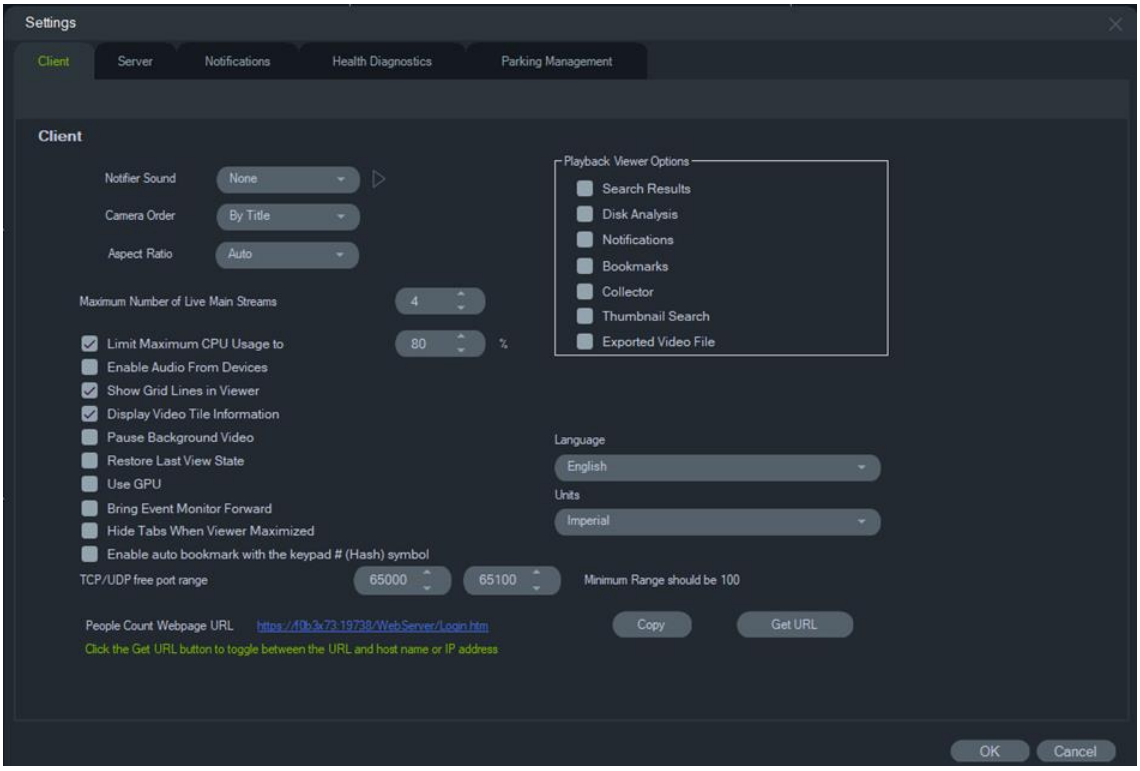
Note: User and/or group permissions are required to see all tabs in the Settings window. See “Permission models” on page 213 for further information.

The following configuration tabs are available in the Settings window:



- **Client:** Includes a variety of settings that apply to each client station. See “Client” **Error! Bookmark not defined.**.
- **Server:** Includes the SMTP server settings, permission settings, instant replay duration custom help link settings, and server/client URL information. See “Server” **Error! Bookmark not defined.**.
- **Notifications:** Includes the port settings necessary to receive events from each device, email notification settings, and a filter of specific notification types. See “Notifier configuration” **Error! Bookmark not defined.**.
- **Health Diagnostics:** Includes a filter of diagnostics to be received, as well as email settings to receive notifications of diagnostics information. Automatic diagnostic polling can also be scheduled from this menu. See “Health diagnostics” **Error! Bookmark not defined.**.
- **Parking Management:** The Parking Management tab allows you to enable and configure parking management data processing using live notifications or events stored in the camera. Users can choose their preferred method based on their requirements. See “Parking management” **Error! Bookmark not defined.**.

Client



Client settings apply to each client station. These settings include:

- **Notifier Sound**: Enable the alert sound when new device notifications are received in the Notifier panel. Click the ▷ button next to the **Notifier Sound** drop-down list to preview the selected sound.
- **Camera Order**: Arrange cameras in the Navigator panel by title or number.
- **Aspect Ratio**: Enable aspect ratio (1:1, 4:3, 9:16, 16:9, or 21:9) for live and playback video in the Viewer. Although this option is available at the Tile level, please note that tile-level settings will override this property.
- **Maximum Number of Live Main Streams**: Set the maximum number of live main streams. When set to 0 (zero), only substreams display.
- **Limit Maximum CPU Usage to**: Set the maximum CPU threshold to prevent the client machine CPU from reaching 100% during video rendering.
- **Enable Audio From Devices**: Turn on audio from applicable devices.
- **Show Grid Lines in Viewer**: Remove/show gridlines between video tiles in the Viewer.
- **Display Video Tile Information**: Remove/show camera title and time and date.
- **Pause Background Video**: Pause video not running in the current view in Navigator. This selection closes the video streams that are not currently

being viewed. Use this setting if bandwidth usage is an issue. There will be a slight delay when switching to the background views.

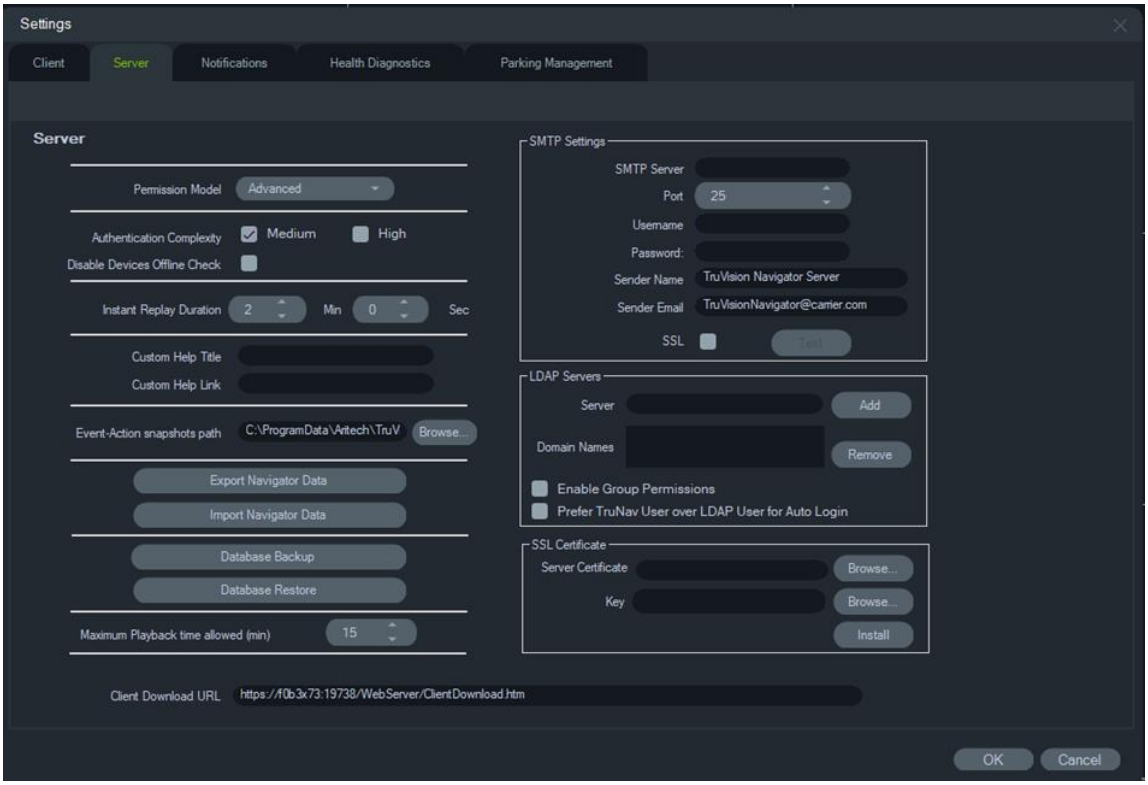
Note: Background video remains active for 30 seconds before pausing.

- **Restore Last View State**: Cameras, views, and tile layouts are restored to their previous state after exiting and restarting Navigator.
- **Use GPU**: Use the computer's video card to decode video.
- **Bring Event Monitor Forward**: Displays the Event Monitor tab in the Viewer panel in front of the current view whenever an event occurs. When the application or the Event Monitor viewer is minimized, it maximizes the application when an event occurs. See "**Error! Reference source not found.**" on page 98 for details.
- **Hide Tabs When Viewer Maximized**: Use this option to hide the tabs when the viewer has been maximized. **Note**: When this option is selected, the switching between Viewers is disabled when the Viewer is maximized.
- **Enable auto bookmark on keypad # (hash) symbol**: Use this option to create bookmarks via the TVK-400-USB keypad. When this feature is enabled, press the # key in the keypad to create a bookmark.
- **Language**: Select the preferred language for the user interface in this drop-down list.
- **Units**: Select **Imperial** or **Metric units** of measure.
- **People Counting Webpage URL**: The default web page URL that contains a link to the server that can display people counting information on a web browser. Click the Copy button to copy the URL. Click the Get URL button to toggle between the URL with a host name or an IP address.

  Note: To display the web page on a mobile device, a URL with an IP address may be needed.
- **Playback Viewer Options**: TruVision Navigator makes it possible to open recorded video from recorders in a specific viewer, called Playback Viewer. The user must enable the required options to open the recorded video in the Playback Viewer. Playback Viewer displays videos related to search results, disk analysis, notifications, bookmarks, the collector, thumbnail search, and exported video files.

The instant replay video, recorded video searched via the Go To time/date, and playback shown via a selection on the time line, will be played in the current viewer.

Server



The **Server** tab includes the following server settings:

- SMTP Setup (**SMTP Server**, **Port**, **Username**, **Password**, **Sender Name**, **SSL**, **Test**).
- **Permission Model** (see “Permission models” on page 213).
- **Authentication Complexity**
- **Disable Devices Offline Check**: Checks if recorders are offline. If selected, no notifications will be received.
- **Instant Replay Duration**
- **Custom Help Title** and **Custom Help Link**
- **Database Backup** and **Database Restore**
- **Server URL**: Multi-client installations (client/server) only.
- **Client Download URL**: Multi-client installations (client/server) only.
- **Export Navigator Data** and **Import Navigator Data**
- **LDAP Servers**: **Add** and **Remove** LDAP servers. See “LDAP servers” on page 208.
- **SSL Certificate**: Permits secure communication between a client and server (client/server installations only). **Browse** for a Certificate Authority (CA) **Server Certificate** and **Key** and **Install** the certificate.

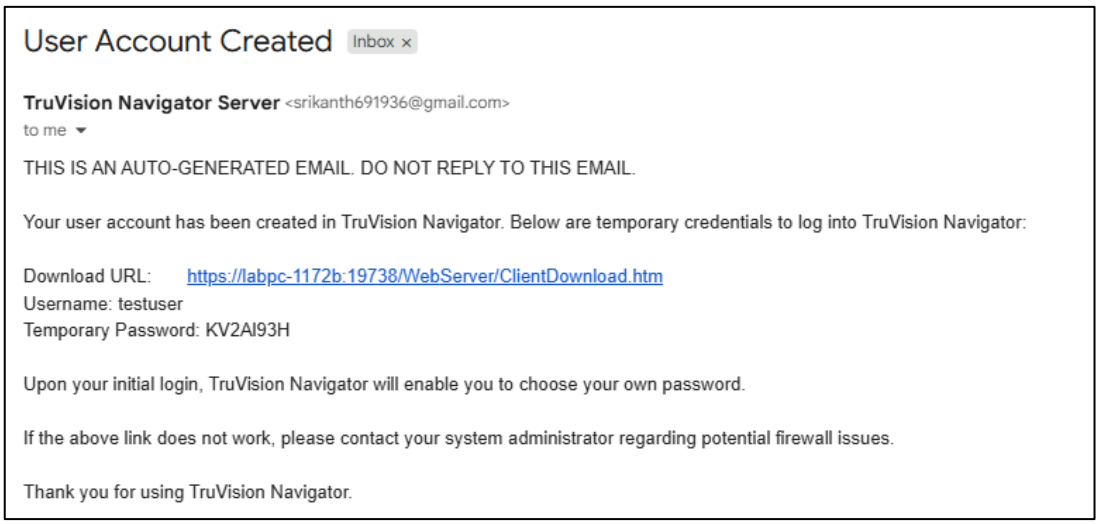
- **Event-Action snapshot path**: Allows the user to select the location where the generated snapshots will be stored for the Event-Action triggers.
- **Playback time allowed (min)**: Restricts the start time of recorded video for users who have the “Watch playback by time” permission.

SMTP setup

Simple Mail Transfer Protocol (SMTP) is a de facto standard for email transmissions across the Internet. The Navigator server can be configured to use an SMTP server to send automated email messages (with client download URL, username, and password) to users when they are created in TruVision Navigator and when their login credentials (username, password) need to be reset in the system by an administrator. If SMTP is not set up, this information must be delivered via an alternative method such as phone or personal email.

To set up SMTP:

1. Type the **SMTP Server** IP address, the **Port**, and any **Username** and **Password** credentials required by the SMTP server.
2. The default email sender name is “TruVision Navigator Server.” If necessary, change the sender’s name.
3. The default sender’s email ID is “TruVisionNavigator@kgsolutions.com”. If necessary, change the sender’s name and select **SSL** if required by the server.
4. Test this setup by clicking **Test** and typing a destination email address for the test message. Check the application status bar for feedback on the test. Also check the email account to ensure there is a test message from the Navigator server confirming proper setup of the SMTP server.
5. An email like the one below is sent. If not received after several minutes, check the Junk Mail folder to see if the email was classified and stored there.


User Account Created Inbox ×

TruVision Navigator Server <srikanth691936@gmail.com>
to me

THIS IS AN AUTO-GENERATED EMAIL. DO NOT REPLY TO THIS EMAIL.

Your user account has been created in TruVision Navigator. Below are temporary credentials to log into TruVision Navigator:

Download URL: https://labpc-1172b:19738/WebServer/ClientDownload.htm
Username: testuser
Temporary Password: KV2AI93H

Upon your initial login, TruVision Navigator will enable you to choose your own password.

If the above link does not work, please contact your system administrator regarding potential firewall issues.

Thank you for using TruVision Navigator.

User management

User management allows administrators to control access to the system by creating, modifying, and organizing user accounts.

Users can be managed individually or grouped to simplify administration and permission assignment.

User accounts

Users can be added to the system using local credentials or through LDAP integration. User accounts define access to the system and can be managed by administrators.

User management includes:

- Creating and deleting users
- Assigning usernames and passwords
- Defining user groups
- Managing user authentication settings

To configure user accounts:

1. Create user accounts (local or LDAP)
2. Assign authentication credentials
3. Define recovery options (challenge questions)
4. Assign appropriate permissions

Note: Adding or assigning permissions to a user requires that the individual performing those functions has the “Manage user permissions” permission assigned to them in Navigator.

To add a regular user:

1. Click the **Groups and Users** tab in the Settings window.
2. Right-click the Users node in the Navigator and select **Add User** or click the **Add User** button. The Add User window appears.
3. Type the required user information in each field. The **Username**, **Password**, and **Confirm Password** fields are disabled if SMTP is configured in the system.
4. Click **OK**. The new user is added under the Users node in the Navigator panel.

5. *To install Navigator on the new user's client computer*: If SMTP is set up in the system, follow the instructions under "Fully automated client software delivery" on page 25. For systems without SMTP set up, follow the instructions under "Partially automated client software delivery" on page 25.

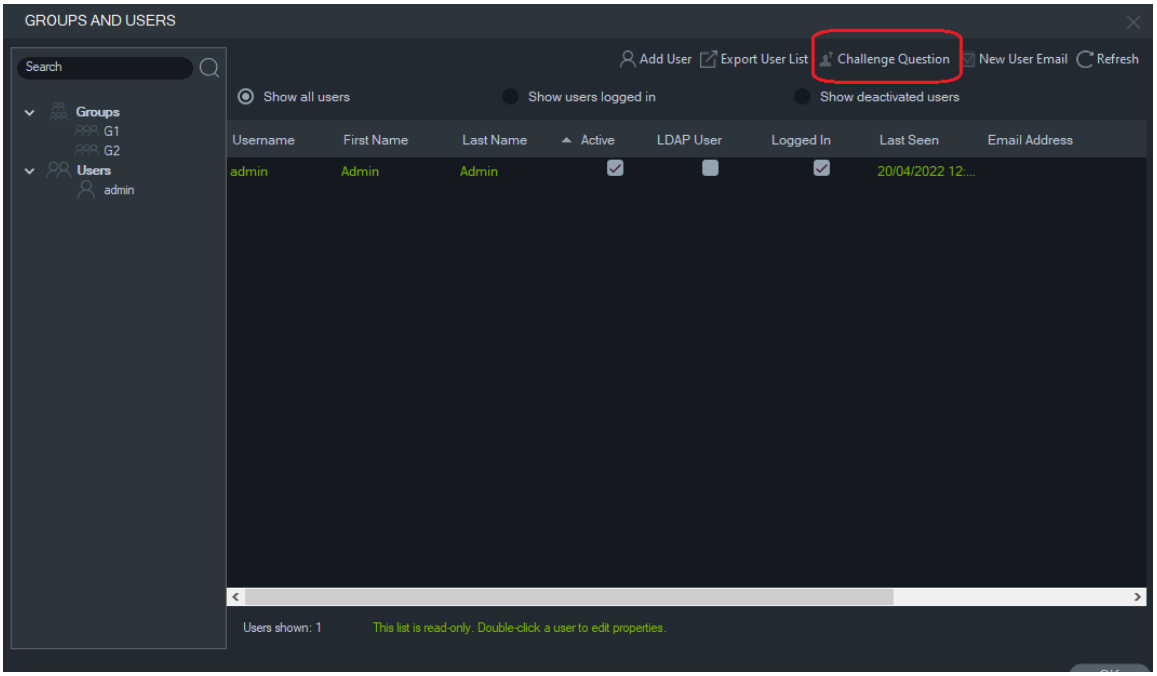
Notes / best practices

- Users cannot access the system until permissions are assigned
- Define user roles before creating accounts to ensure consistent access control

Challenge question

In the Groups and Users tab by clicking the **Challenge Question** button, you can add/delete/modify challenge questions.

Note: When the challenge question is in use, it cannot be deleted.



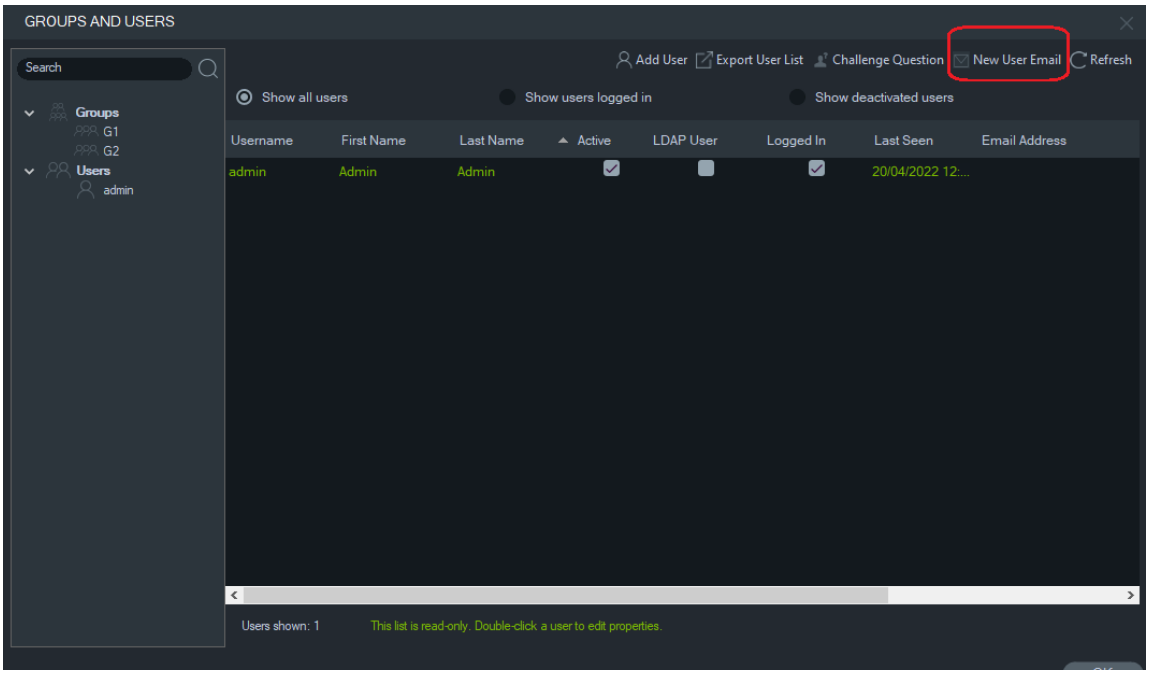
New user email content

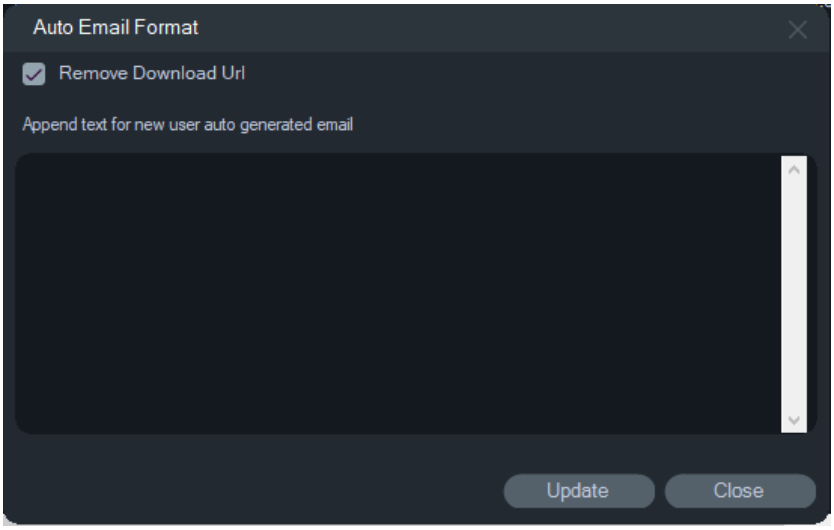
An administrator or user with permission to access Groups & Users can partially modify the email content before the email is send to a new user.

To modify the email content

1. Open the **Group and Users** window in the main menu.
2. Click **New User Email** to open the Auto Email Format window.
3. Select **Remove Download URL** to not include the download location and the associated note for installing the client software.

4. Additional text can be added in the text field. The text will be appended in the email.
5. Click **Update** to save the setting and the text in the database.





Search

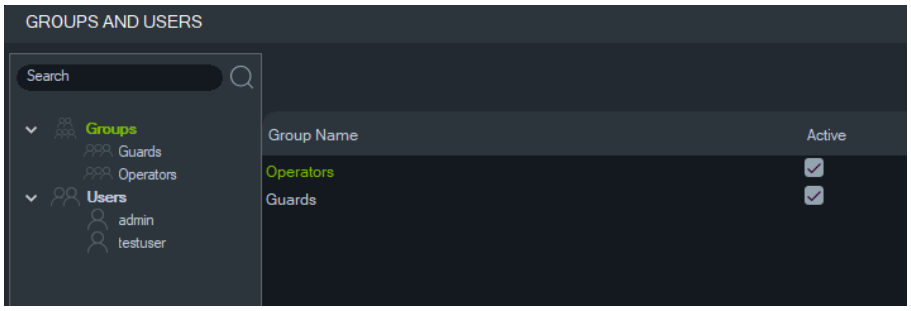
Use Search to find any user or group in the Groups and Users panel.

To perform a Groups and Users search:

1. Type any alphanumeric string into the **Search** field at the top of the Navigator panel and press Enter. Focus goes instantly to the user or group that matches the string.
2. Press Enter again to move to the next object that matches the string until each item matching the search criteria has been found. Type a different alphanumeric string into the **Search** field to perform another search.

Group summary

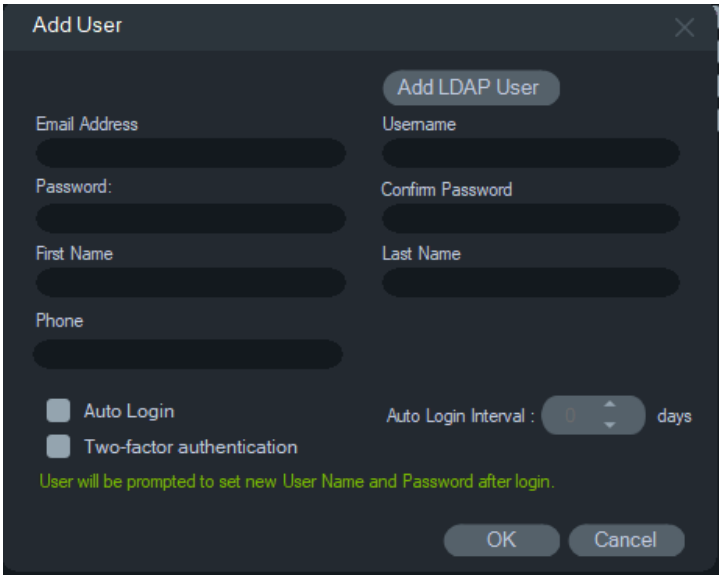
After one or more groups have been created, click the **Groups** node to view a list of all groups and their Active status. Click a group name to rename a group.



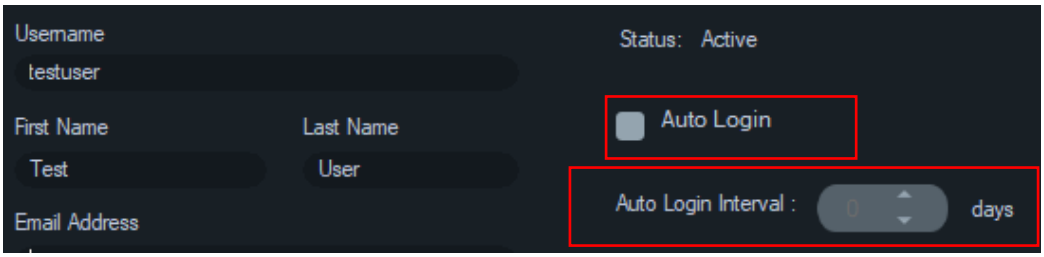
Auto login

By default, Auto Login is disabled for new users.

To enable Auto Login, select the **Auto Login** check box. You can also specify the number of days you will have access the application without providing credentials (default interval is 14 days). After 14 days you must log in again. When the interval is set to 0 days, the Auto Login function will never expire.

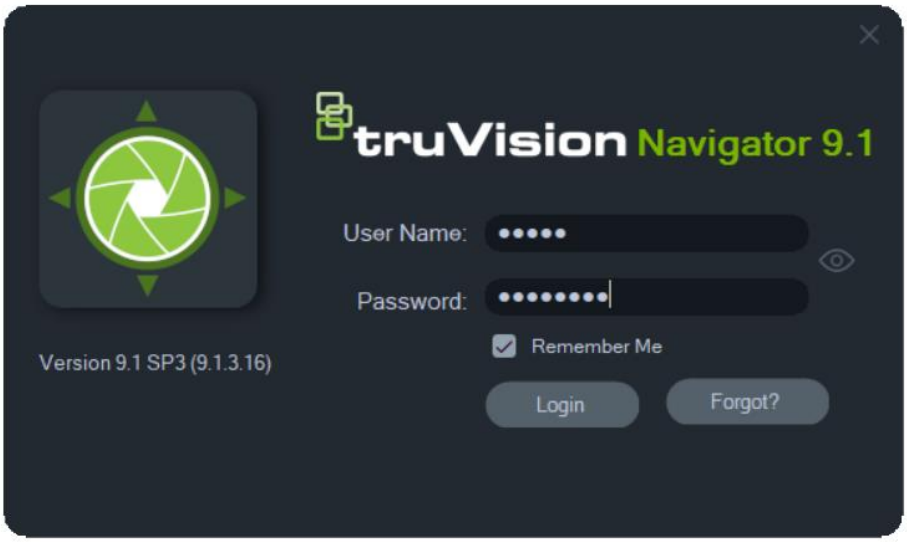


The administrator can edit the Auto Login details on the Users details page, as shown in the graphic below.



Remember Me option

You must select the **Remember Me** option to be able to log in directly from the next login until the interval time specified by the administrator.



Feature behavior

- Users can clear their stored credentials by using the **Logout** option of TruVision Navigator. This will clear the auto login credentials for the user and redirects the user to the Login screen.
- When a password is changed or an account is reset, the user can no longer automatically log in. The empty login screen will reappear at the next login.
- The **Remember Me** option does not work for administrators.
- Changes made by the administrator to the auto login settings for a specific user will be applied when the user next logs in.
- When auto login is enabled, the default value of the time interval is 14 days. The minimum value is 0 days. If the time interval is set to 0, the user will always be able to automatically log in.

LDAP integration

The Lightweight Directory Access Protocol (LDAP) is commonly used to provide a repository for storage of user names and passwords. Adding an LDAP server to Navigator provides a way to validate users that permits them to bypass the Navigator login window.

LDAP integration allows:

- Centralized authentication using directory credentials
- Automatic validation of users without local password management

- Mapping of directory users and groups into the system

When LDAP is used:

- Users authenticate through the directory service
- Permissions must still be configured within the system
- Optional group mapping allows LDAP group membership to define access rights

LDAP server connectivity and domain configuration must be established before importing users

To configure LDAP integration:

1. Configure LDAP server connection and domains
2. Enable LDAP authentication in the system
3. Import users and/or groups
4. Assign permissions within the system
5. (Optional) Enable group mapping

LDAP servers

To add an LDAP server and enable settings

1. Go to **Settings** window and click **Server** tab
2. Type the LDAP server domain name in the Server box, and then click **Add** to test the server connection. This can be done for multiple domain names. The domain name must be reachable from the computer used to add the LDAP server.
3. Click a domain name in the Domain Names box, and then click **Remove** to remove an LDAP server.
4. Click **OK** in the Settings tab when finished to add the LDAP server(s) to Navigator.

LDAP users

LDAP users can access Navigator with adequate permissions in a LDAP environment, with minimum configuration. This allows LDAP users to get their associated LDAP group and compare them with Navigator groups and to allow supported permission to the LDAP User.

Enable Group Permissions: Use this option when the **LDAP** user needs to load LDAP group permissions into the TruVision Navigator system.

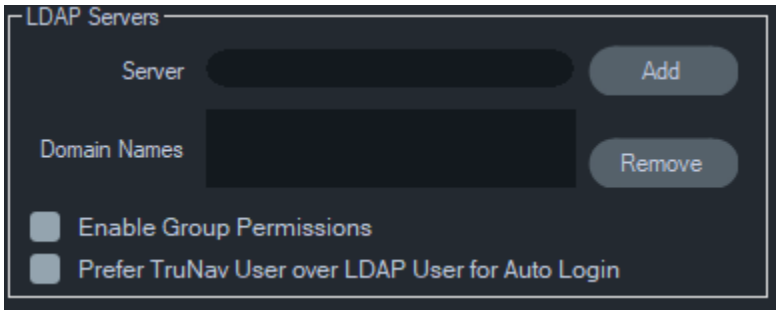
Note: When this option is unchecked, the association between LDAP Groups and Users is removed.

Prefer TruNav User over LDAP User for Auto Login: This option is needed when auto login is enabled for non-LDAP users and LDAP users also exist in the same TruNav system.

To add LDAP server details and enable settings

1. Go to **Settings** window and click **Server** tab
2. Add server/domain information. See above.
3. As the administrator, you must enable LDAP group permissions by selecting the **Enable Group Permissions** check box.

Note: When any LDAP user logs into TruVision Navigator, and if **Enable Group Permission** is enabled, the software will validate the LDAP user groups with the software groups and will load the group permissions associated with the user. If **Enable Group Permission** is disabled, the LDAP user will have the LDAP user permissions that are setup in the software.



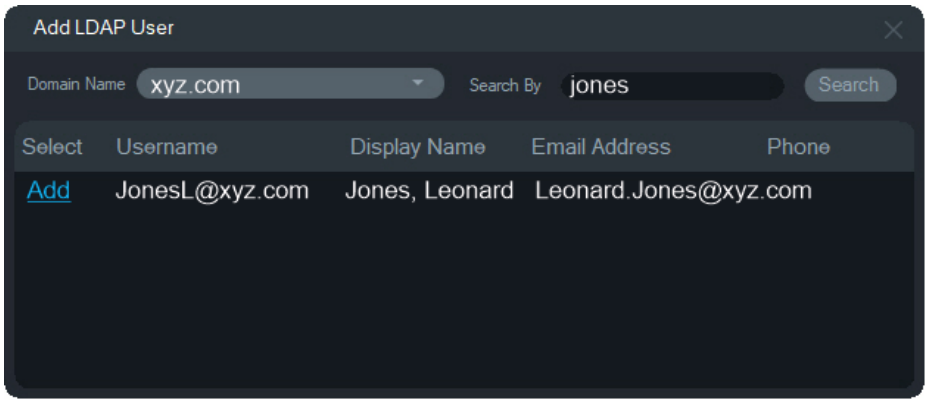
Configure a LDAP server

TruVision Navigator allows LDAP users to log in without credentials and TruVision Navigator users to use auto login for non-LDAP users. If the Auto Login option is enabled on the application and if the application has LDAP users, by default the application allows LDAP login.

Administrators can change the preference for TruVision Navigator users by selecting **Prefer TruNav user over LDAP User for Auto Login** check box in the server settings.

To add an LDAP user:

1. Click the **Groups and Users** tab in the Settings window.
2. Right-click the Users node in the Navigator and select **Add User** or click the **Add User** button. The Add User window appears.
3. Click **Add LDAP User**.
4. The Add LDAP User window appears. Select a domain name from the **Domain Name** drop-down list (see “LDAP servers” on page 208on page 208 for details).
5. Enter the user’s name in the **Search By** box and click **Search**. All matching data appears as shown below.

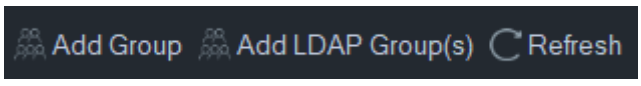


6. Click the Add link next to the user name to add an LDAP user. The Add User window reappears with the user information automatically populated.
7. Click **OK** to add the LDAP user. The user now appears in the **Show all users** list as an LDAP user.
8. If necessary, assign at least one permission to the LDAP user so that they can use Navigator (see “To assign permissions to a user” below).

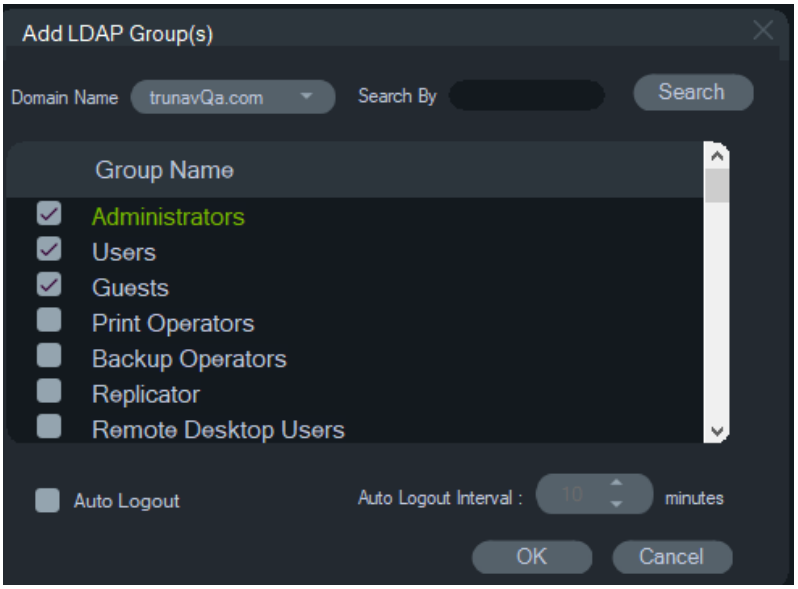
Note: LDAP users are automatically logged in to Navigator when opening the application. An LDAP user must log out of Navigator to log in as a different user.

To add an LDAP group

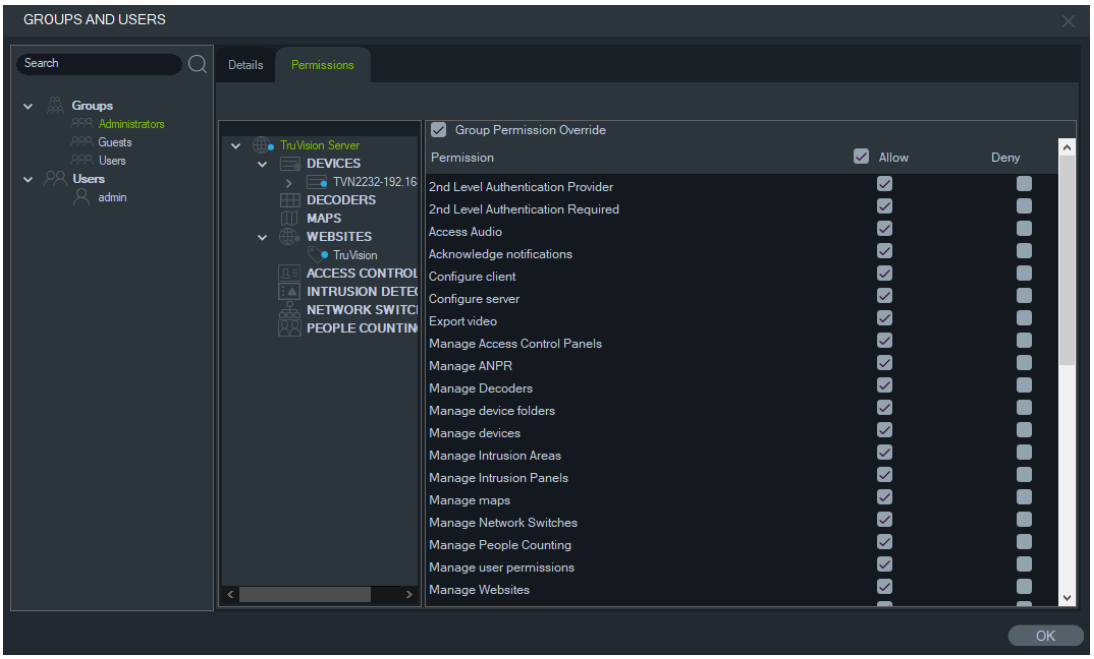
1. Click the **Groups and Users** tab in the **Settings** window.
2. Click **Add LDAP Group (s)**.



3. Select Domain Name and search with a name if needed. Select the group(s) you want to add.

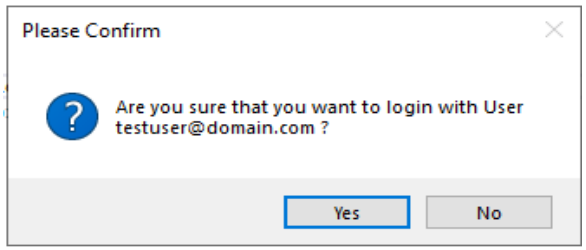


Once the administrator adds the LDAP Groups, they will be populated under Groups. See the graphic below.



4. As the administrator you must provide the required permissions to the selected LDAP Groups
5. When finished, click **OK**.

When a LDAP User logs into the application for the first time, the user will be asked to confirm the login. When the user clicks **Yes**, the application will launch depending on the group permissions associated to the LDAP User. From next time onwards, the application will be launched without asking this question.



Note: If the administrator adds LDAP users into Navigator, this message will not be displayed.

Feature Behavior

- The loading of group permissions will only work if the permission model is set to **Advanced** in the Settings tab.
- If a user is a normal user (non-LDAP user), and the **Enable Group Permissions** is checked or unchecked, it will check permissions on the user/associated group level and act accordingly to the selection.
- If a user is an LDAP user and **Enable Group Permissions** is unchecked, it will check the permissions on the user/associated group level and act accordingly.
- For LDAP users with **Enable Group Permissions** checked, the application considers the user's LDAP group and corresponding Navigator group permissions.

Notes / best practices

- LDAP users still require permissions in the system to function
- Enable group mapping only if LDAP structure matches system groups
- LDAP users may automatically log in based on configuration

User lifecycle management

User accounts can be managed throughout their lifecycle.

Administrative actions include:

- Activating and deactivating users
- Restoring previously deactivated users
- Resetting user accounts after lockout
- Forcing user logout

These actions allow administrators to maintain control over user access and availability.

To manage user lifecycle:

1. Activate or deactivate user accounts
2. Reset accounts after lockout
3. Restore access when needed
4. Force logout for active sessions if required

Notes / best practices

- Deactivation is preferred over deletion to preserve audit data
- Use forced logout in security-sensitive environments

Permissions and roles

Permissions define what users can do and what resources they can access within the system.

Permissions control access to devices, features, and system configuration.

Permission models

The system supports two permission models:

- **Simple model (default)**: Permissions are assigned directly to users
- **Advanced model**: Permissions are managed through user groups

The advanced model allows scalable management by assigning permissions to groups instead of individual users.

When multiple permissions apply (for example through group membership), the effective access is determined by the combination of assigned permissions. It is recommended to test permissions using a representative user account before deployment.

Table 3: Permission matrix

Permission	User Interface Impact	Dependent Permissions
2nd Level Authentication Provider	Enables 2-step authentication for Playback, Export video and access to System Settings	2nd Level Authentication Required
2nd Level Authentication Required	Enables 2-step authentication for Playback, Export video and access to System Settings	2nd Level Authentication Provider
Access Audio	Enable/disable Audio on recorder	
Acknowledge notifications	Show/hide Acknowledge All button in Notifier dialog	

Permission	User Interface Impact	Dependent Permissions
Configure client	Enable/disable Client tab in Settings	
Configure server	Enable/disable right-click options on TruVision Navigator Server node (i.e., Properties and Database Backup and Restore)	
Export video	Enable/disable Local record button in Controller	Watch live video Watch playback video
	Enable/disable Snapshot and Video buttons in the Controller	
	Show/hide Collector Panel	
	Show/hide Tasks Panel (panel may also be visible due to other permissions)	
View access control panel notifications	Enable/disable notifications from TruPortal in the Notifier	
Manage access control panels	Enables/disables access control context menus	Operate access control panels
Manage ANPR	Show/hide ANPR context menus	
Manage decoders	Enables/disables configuration of scenes	Operate decoders
Manage device folders	Show/hide Add Folder button and context menus in Navigator	
	Show/hide Folder (folder may also be visible due to other permissions or parent/child permissions)	
	Show/hide Address Book Import context menu for Devices node	
Manage devices	Show/hide Add Device button and context menus (rename and delete) in Navigator	
	Show/hide Folder (folder may also be visible due to other permissions or parent/child permissions)	
	Show/hide Device (device may also be visible due to other permissions or parent/child permissions)	
	Show/hide Camera (camera may also be visible due to other permissions)	
	Show/hide Bulk Tasks (Firmware Upload and Configuration) context menus for Devices node	
	Enable/disable Device Properties (Connection, Details, Capabilities) dialog on device	
	Show/hide Camera Search and Configuration context menus	
	Show/hide Firmware Upload context menu for device	

Permission	User Interface Impact	Dependent Permissions
	Show/hide Tasks Panel (panel may also be visible due to other permissions)	
Manage intrusion areas	Show/hide intrusion area context menus	Operate intrusion areas
Manage intrusion panels	Show/hide intrusion detection context menus	Operate intrusion panels
Manage network switches	Show/hide network switches context menus	Operate network switches
Manage Parking	Show/hide parking zone context menus	Set-up and operate parking
Manage people counting	Show/hide people counting context menus	Set-up and operate people counting
Manage maps	Show/hide map context menus	View maps
Manage speaker	Add, Play Audio Relays (Sound Clips), Rename, Configure, Properties and Delete operations allowed	Operate speaker
Manage user permissions	Show/hide Users and/or Groups nodes in Navigator	
Manage website	Show/hide website context menu	View website
Operate access control panels	Show/hide door icon context menu	
Operate decoders	Enable/disable scene activation	
Operate intrusion areas	Show/hide arm/disarm selections in context menus	View intrusion panels
Operate intrusion panels	Show/hide intrusion panel context menu	View intrusion panels
Operate network switches	Show/hide network switch context menu	
Operate Parking	Show/hide parking zone context menus	
Operate people counting	Show/hide people counting context menus	Operate people counting
Operate speaker	Play Audio Relays (Sound Clips)	
Pan tilt zoom	Enables/disables PTZ control in camera tile	Watch live video
	Show/hide PTZ button in timeline (PTZ settings access)	
Trigger outputs	Show/hide Trigger Outputs selection in device context menu	
View device diagnostics	Show/hide Run Health Diagnostics in Device node and specific device context menus in Navigator	
	Show/hide Folder (folder may also be visible due to other permissions or child permissions)	

Permission	User Interface Impact	Dependent Permissions
	Show/hide Device (device may also be visible due to other permissions or child permissions)	
View disk analysis	Show/hide Disk Analysis context menu for device	Watch live video Watch playback video
	Show/hide camera row in Disk Analysis dialog	
View intrusion areas	Show/hide intrusion areas in maps	View intrusion panels
	Show/hide intrusion areas in the Navigator panel	
View intrusion panel notifications	Show/hide intrusion panel notifications in Notifier dialog	View intrusion panels
View intrusion panels	Show/hide the intrusion detection node	
View maps	Show/hide the map node	
View notifications	Show/hide Folder (folder may also be visible due to other permissions or child permissions)	
	Show/hide Device (device may also be visible due to other permissions or child permissions)	
	Enable/disable Notifier icon in application status bar	
	Show/hide Device Notification in Notifier dialog	
	Show/hide Camera Notification in Notifier dialog for permissioned device	
View websites	Shows/hides the website node	
Watch live video	Show/hide Folder (folder may also be visible due to other permissions or child permissions)	
	Show/hide Device (device may also be visible due to other permissions or child permissions)	
	Show/hide Camera (camera may also be visible due to other permissions)	
	Allow/Disallow Open Video from Camera (all methods: double-click and drag-and-drop operation in Navigator)	
	Show/hide PTZ and in-tile mouse controls	
Watch live video main stream	Enable/disable Main/Sub switch in playback controls	Watch live video Watch playback video
Watch playback video	Show/hide Folder (folder may also be visible due to other permissions or child permissions)	Watch live video

Permission	User Interface Impact	Dependent Permissions
	Show/hide Device (device may also be visible due to other permissions or child permissions)	
	Show/hide Camera (camera may also be visible due to other permissions)	
	Enable/disable Controller Playback controls including Go To, Playback, Live, double-click timeline)	
	Enable/disable notifications in Notifier dialog	
Watch playback video main stream	Enable/disable Main/Sub switch in playback controls	Watch live video Watch playback video
Watch Playback by time	Allows the user to view recorded video for a defined period, starting from the live time for both main stream and substream. **Note:** Select the Server settings for Play time allowed option.	When **Watch playback by time** is selected along with **Watch playback permissions**, The **Watch playback by time** option will not be affected.

To configure permission models:

1. Select Simple or Advanced model
2. If using Advanced, create groups
3. Assign users to groups
4. Apply permissions at user or group level

Notes / best practices

- Use the Advanced model for systems with multiple users
- Define groups before assigning permissions to simplify management

Groups

Groups simplify permission management by allowing multiple users to share the same permission set.

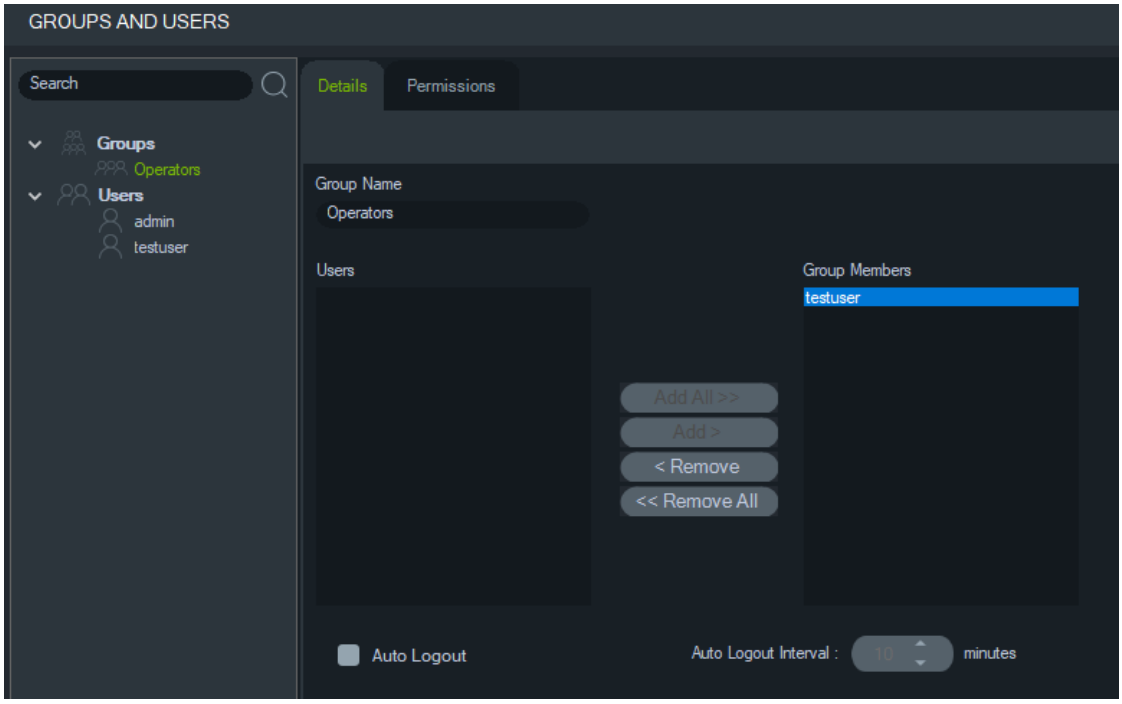
Users assigned to a group inherit the permissions associated with that group.

To configure groups:

1. Create groups
2. Assign users to groups
3. Define permissions at group level
4. Override permissions for specific users if needed

To create a group:

1. Click the **Server** tab in Settings and ensure that the **Permission Model** drop-down list is set to **Advanced**.
2. Click the **Add Group** button or right-click the Groups node in the **Groups and Users** tab and select **Add Group**.
3. Type a name for the group in the Add Group window and click **OK**.
4. Click the group name and then click the **Details** tab to change the group name and add users to the group.

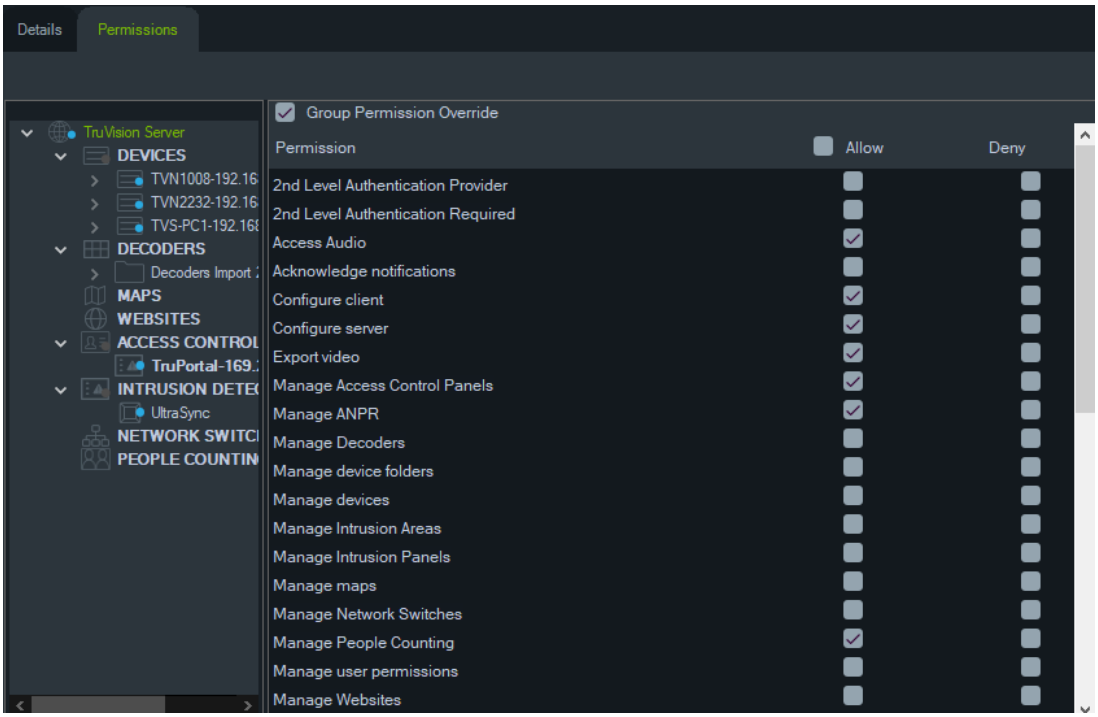


5. When finished, click **OK**.

To assign permissions to a group:

1. Click the group icon in the **Groups and Users** tab and then click the **Permissions** tab.
2. Highlight the TruVision Server node or any sub nodes, folders, devices, or other items in the permissions panel and allow/deny permissions for the

group in the **Permissions** tab. Group permissions affect all of the specific users that are members of the group.



3. When finished, click **OK**.

To add a user to a group:

1. Click the group icon in the **Groups and Users** tab and click the **Details** tab.
2. Select one or more users in the **Users** field and then click **Add All** or **Add** to add users to the **Group Members** field.
3. When finished, click **OK**.

Group permission override

Users with group permissions can have the permissions overridden by the administrator. In this way, the administrator can customize the permissions of a group member.

To override group permissions for a user:

1. Click the user icon in the **Groups and Users** tab and click the **Permissions** tab.
2. If necessary, add the user to a group by selecting one or more group check boxes in the Groups panel.
3. Highlight the TruVision Server node or any sub nodes, folders, devices, or other items in the permissions panel and allow/deny permissions for this user in the **Permissions** tab.

Notes / best practices

- Use groups to avoid repetitive configuration
- Keep group structure simple and role-based

Permission inheritance

Permissions can be assigned at different levels of the system hierarchy.

Permissions assigned at a higher level are inherited by lower-level elements, such as folders, devices, and cameras.

This enables efficient management of access rights across large systems.

To configure permission inheritance:

1. Assign permissions at the appropriate hierarchy level
2. Use higher-level assignments for consistent access
3. Apply exceptions only where needed

Notes / best practices

- Assign permissions at higher levels to reduce complexity
- Review inherited permissions to avoid unintended access

Permission categories

Permissions control access to system features such as:

- Viewing live and recorded video
- Exporting video and snapshots
- Accessing devies and maps
- Using analytics features
- Managing system configuration

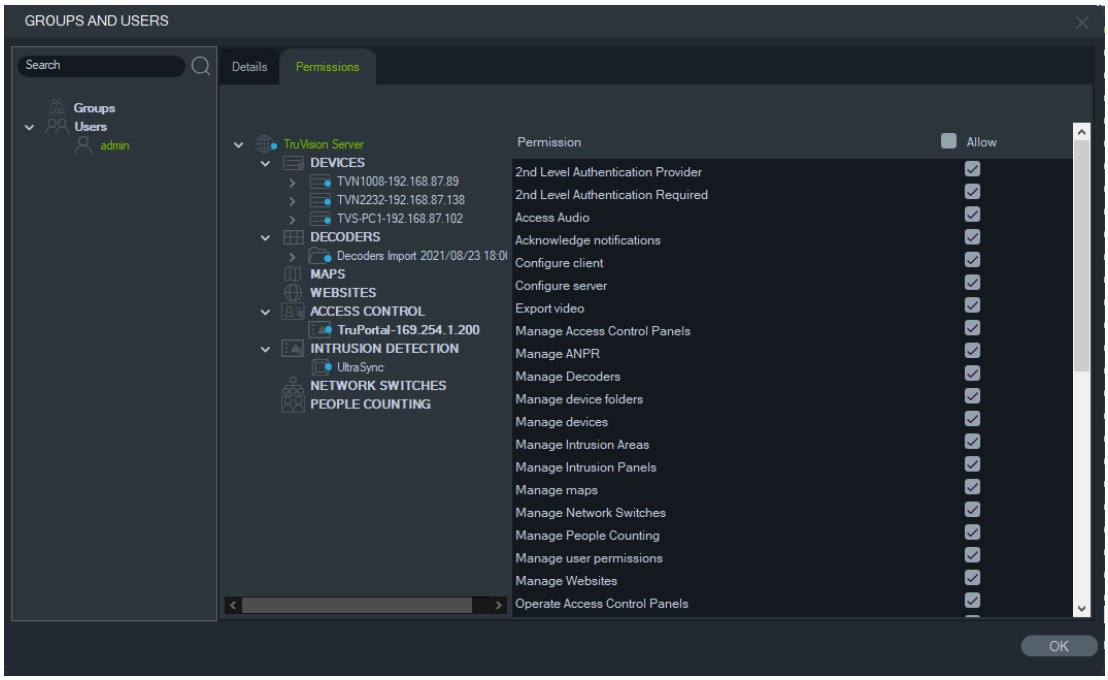
Permissions may also control visibility of interface elements and availability of specific features.

To configure permissions:

1. Define required system actions per role
2. Assign permissions for video, devices, and features
3. Validate access behavior for each user/group

To assign permissions to a user:

1. Click the user icon in the **Groups and Users** tab and click the **Permissions** tab.
2. Highlight the TruVision Server node or any sub nodes, folders, devices, or other items in the permissions panel and allow/deny permissions for this user in the **Permissions** tab. If the Permission Model is set to **Simple** (only users), only the Allow column appears. If the Permission Model is set to **Advanced** (both users and groups), both the Allow and Deny columns appear.



3. When finished, click **OK**.

Permission indicators

When assigning permissions, specify whether the permission is applied at the parent or child node. Granting permissions at a parent node cascades those permissions down to the child nodes.

For example, granting permissions at the Navigator server level cascades down over all folders, devices, and cameras beneath it. These are indicated by a blue dot. Conversely, granting permissions at the child node does not change permissions at the parent node. In this case, the child node displays a blue dot and the parent displays a gray dot.

Table 4: Permission indicators

Permission Indicator	Description
Blue	A blue dot indicates express permissions granted on that node. These permissions are inherited by the children nodes underneath the parent node.

Permission Indicator	Description
Gray	A gray dot indicates express permissions assigned to a child of the parent node, but not at the parent node itself. This serves as a quick visual cue for the administrator to find express permissions granted to a user on devices in the permission panel. If all of the gray dot nodes are expanded, the camera or device with one or more express permissions appears, indicated by a blue dot.

Notes / best practices

- Test permissions with a sample user before deployment
- Avoid granting unnecessary access rights

Notification settings

Notification settings control how system events are received, processed, stored, and delivered to users.

The system receives notifications from devices such as alarms, motion detection, or video loss events.

These notifications can be processed and displayed within the application or sent externally through configured channels.

Notifications can also be triggered by Event-Actions, which define automated responses to events beyond basic notification handling

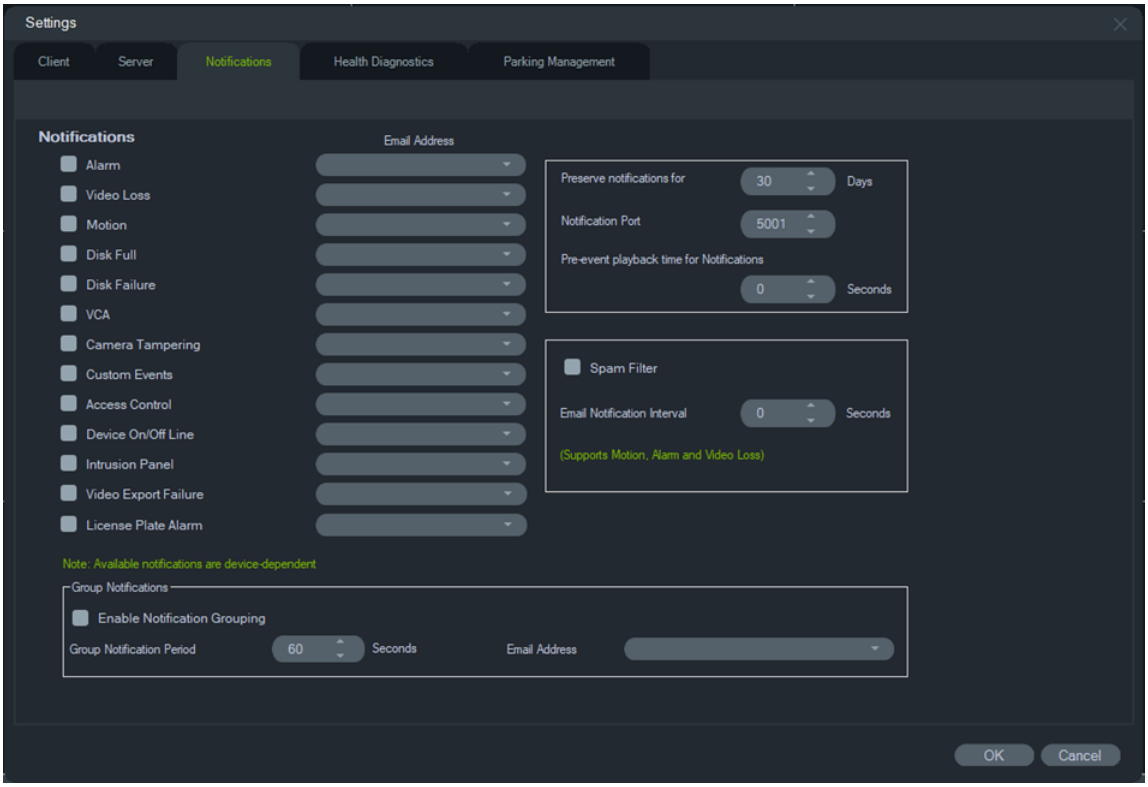
Notification sources and processes

Devices generate notifications and send them to the system using configured network settings. The system must be configured to receive these notifications on the same communication port.

Notifications may include events such as:

- Motion detection
- Video loss
- Alarm inputs
- Device status changes

Network components such as firewalls or routers may require configuration to allow notification traffic.



The Notifications tab in the Settings window includes the following server settings:

- **Notifications**: Select events for notifications by email and text (US only) to send to specific Navigator users.
- **Preserve notification interval**: The length of time the notifications are archived.
- **Notification Port**: The port used for notification throughput.
- **Pre-event playback time for notifications**: While playing recorded video from Notifier and Event Center, recorded video is played prior to the notification time based on the time selected.
- **Email Notifications Interval**: The Email notifications interval will allow the user to define a time interval (in seconds), during which time the same type of notification (for motion, alarm, and video loss) will not generate a new email and is skipped. For example, if a user configures the threshold for 1 minute, once the motion notification email is triggered on a camera, an email will be sent, but the subsequent motion notifications emails will not be sent (for the same camera) for 1 minute.
- **Spam Filter:** Enable the Spam Filter so that there will be only one start and one stop notification for any Motion, Alarm input, and Video loss event.

  Note: TruVision Navigator will consider the first notification it receives as the Start after the application/service has started.
- **Group Notifications**: By enabling Notifications Grouping, all email notifications received within a defined period are grouped into a single

notification email. The user can set a period (in seconds), during which time notifications are grouped in one email message. During the interval no notifications will be ignored.

To configure notification flow:

1. Configure devices to send notifications to system IP and port. See the device's manual for more details.
2. Configure system to listen on the same port
3. Ensure network connectivity between devices and system
4. Configure firewalls/routers if required

Notifications and notifier

Devices can push notifications out to an IP address and port for proactive issue resolution. These notifications typically include alarm, video loss, motion, etc. See Appendix B "Device details" on page 262on page 263 for details on which notifications are supported by each device.

To receive notifications from devices in the Notifier panel, configurations are required at both the device and Navigator service level.

Device configuration: Each device must be set up to push its available notifications to the IP address and port of the Navigator server. See Appendix B "Device details" on page 262.

Navigator service configuration: The TruVision Navigator service or TruVision server settings must be configured to listen on that same port for those notifications.

Notes / best practices

- Device and system ports must match for notifications to work
- Veriify connectivity before troubleshooting notification issue

Notification storage and retention

The system stores notification data in the database for later review.

Retention settings control:

- The duration notifications are stored
- Automatic removal of older notifications

This is setup via the **Preserve notification** interval setting.

These setting helps to manage the database size and system performance.

If any of these values are changed, restart the Navigator program (standalone installations) or restart the TruVision Navigator service (client/server installations) for the changes to take effect.

Notes / best practices

- Set retention based on operational needs and storage limits
- Excessive retention may impact performance

Notification delivery

Notifications can be delivered using different mechanisms:

- Display in the Notifier panel
- Email notifications (if configured)
- Grouped or filtered notifications

Email notifications can be configured to reduce repetition using time intervals and grouping behavior. This ensures that repeated events do not generate excessive notifications.

To configure delivery:

1. Configure SMTP server for email notifications
2. Enable or disable notification types
3. Configure filters and grouping
4. Define notification intervals

Notes / best practices

- SMTP must be configured for email functionality
- Use grouping to reduce notification overload

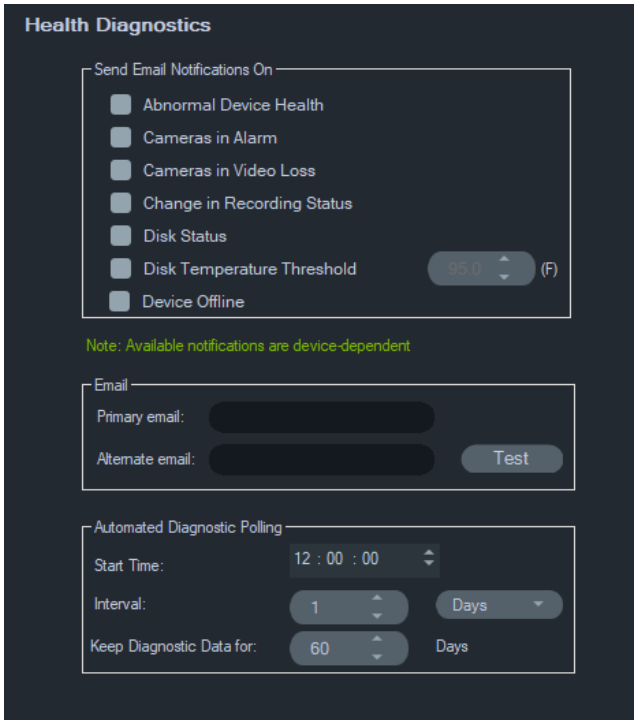
Notification filtering and behavior

Notification behavior can be customized using filtering and control options:

- Filtering by event type
- Grouping notifications within time intervals
- Spam filtering to limit repetitive alerts
- Pre-event playback time for reviewing events

These configurations allow users to focus on relevant events and improve operational efficiency.

Health diagnostics



The **Health Diagnostics** tab in the Settings window provides server settings:

- Select health events for email notification
- Primary and alternate email addresses
- Automated diagnostic polling

Note: Changes made in the **Health Diagnostics** tab won't take effect until a restart of the Navigator program (standalone installations) or the TruVision Navigator server (client/server installations).

Email notifications

Select check boxes for any of the following notifications to receive them via email:

- **Abnormal Device Health**: This notification indicates that either the hard drive is corrupted, or the device cannot encode or record video (DVRs only).
- **Cameras in Alarm**: Any cameras that are in an alarm state.
- **Cameras in Video Loss**: Any camera that is not transmitting video.
- **Change in Recording Status**: A recording has stopped or started.
- **Disk Status**: Health status of the hard drive.
- **Disk Temperature Threshold**: Temperature has exceeded the set threshold.
- **Device Offline**: A device is offline during polling after having previously been online.

Email addresses

Enter valid email addresses in the **Primary email** and **Alternate email** fields. If SMTP has been set up in the system, click **Test** to send test emails.

Automated diagnostic polling

To run automated health diagnostic polling on an interval across all of the devices in the system, the diagnostic polling service must first be configured.

To configure the diagnostic polling service:

1. From the **Health Diagnostics** tab in the Settings window, type the Automated Diagnostic Polling **Start Time** and **Interval** (retention period).
2. Select **Days** or **Hours** for the length of time to keep the health diagnostic polling data in the database.
3. Restart Navigator to begin the automated polling. If any of these values are changed, restart the Navigator program (standalone installations) or restart the TruVision Navigator server (client/server installations) for the changes to take effect.

After manual snapshots or automated health diagnostic data have been captured, the data is stored in the Navigator database. The data is now searchable by users to aid in maintaining system up-time.

Client settings

Client settings control how the application behaves on the local workstation. These settings affect performance, interaction, and local features.

Display and interface settings

Client display settings control how information is presented in the Viewer and Navigator:

- Camera ordering (by name or number)
- Grid display and tile layout
- Video tile information (camera name, time, date)
- Language and unit preferences

These options allow users to tailor the interface to their operational needs.

Configuration summary

1. Configure camera ordering
2. Enable/disable grid and tile info

3. Set language and units

Notes / best practices

- Standardize display settings across operators

Video and playback behavior

Video-related settings control playback and viewing behavior:

- Aspect ratio settings for video tiles
- Number of simultaneous live streams
- Playback viewer configuration
- Background video handling (pause inactive streams)

These settings help optimize video rendering and bandwidth usage.

Configuration summary

1. Set max number of streams
2. Configure aspect ratio
3. Configure playback behavior
4. Set background video handling

Notes / best practices

- Reduce streams to improve performance

Performance settings

Client performance settings help manage system resources:

- Maximum CPU usage limits
- GPU acceleration for video decoding
- Video rendering optimization

These options prevent performance degradation and ensure stable operation of the client system.

Configuration summary

1. Set CPU usage limits
2. Enable GPU decoding

3. Adjust performance thresholds

Notes / best practices

- Use GPU when available for better performance

User interaction settings

Client settings also define interaction behavior:

- Notifier sound alerts
- Event monitor behavior
- Automatic restoration of previous layout and views
- Keypad integration for actions such as bookmark creation

These settings allow users to control how they interact with the system and respond to events.

Configuration summary

1. Configure notification sounds
2. Set event monitor behavior
3. Enable layout restore
4. Configure keypad actions

Notes / best practices

- Enable layout restore for operational continuity

Security settings

Security settings define how access to the system is protected and controlled.

Authentication policies

The system supports configurable authentication complexity levels to enforce password requirements.

Authentication policies may define:

- Minimum password length and complexity
- Maximum login attempts before lockout
- Password reuse restrictions
- Password expiration intervals

Higher security levels require stricter password policies and regular credential updates.

TruVision Navigator has two authentication complexity standards – Medium and High. The default authentication for a new installation is **Medium**. To change the authentication complexity, select an option from the drop-down list and click **OK**.

All new users are required to meet the new authentication complexity standard. However, existing users of the application are not prompted to change their credentials to meet the new standard once it is changed. Therefore, the administrator must reset each of the existing user accounts for the standard to take effect. This reset only affects the password for that user, not the username. To avoid resets, we recommend setting the authentication complexity before any users are created in the system.

Table below table outlines the components of each of these standards.

Table : Authentication complexity

Authentication complexity	Maximum login failure attempts	Username complexity	Password complexity	Password reuse	Password expiration
Medium	3	At least six characters	At least eight alphanumeric characters	n/a	n/a
High	3	At least 12 characters	At least eight characters with at least: One Upper-case letter One lower-case letter One numeric One special character (~, !, @, #, $, %, ^, &, +, =)	Cannot use the last password	User must change password every 60 days

Configuration summary

1. Select authentication complexity level
2. Define password policy
3. Apply settings before user creation

Notes / best practices

- Changing complexity requires resetting existing users

Account lockout and recovery

Users may be locked out after repeated failed login attempts.

Account recovery mechanisms include:

- Challenge questions
- Administrative account reset
- Password reset procedures

These features ensure secure recovery of user access

Configuration summary

1. Configure login attempt limits
2. Enable challenge questions
3. Define reset procedures

Notes / best practices

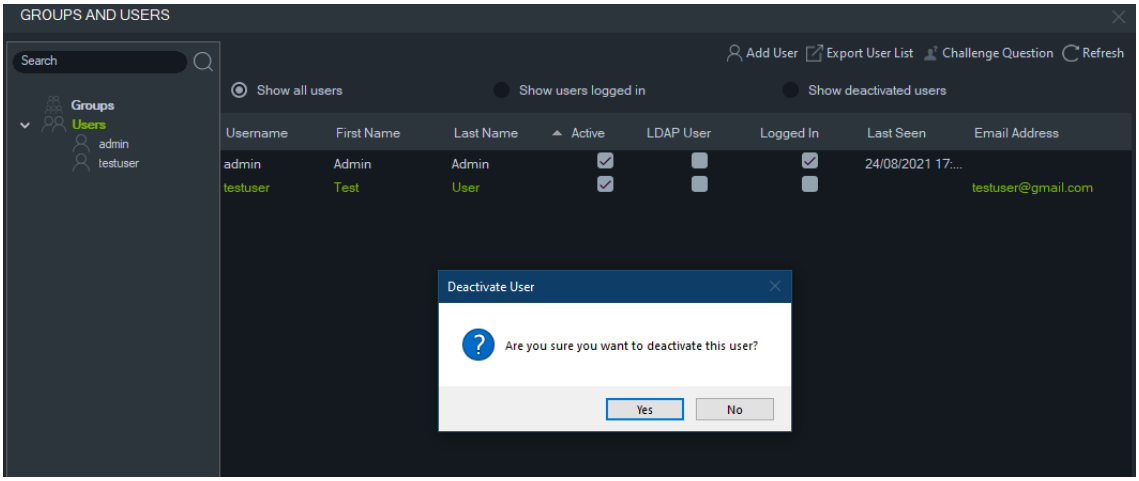
- Document recovery process for administrators

Deactivate a user

Deactivation revokes all user rights to the system but does not delete users from the database.

To deactivate a user:

1. Right-click the user under the Users node and select **Deactivate User**.
2. Click **Yes** when prompted with “Are you sure you want to deactivate this user?”
3. Deactivated users are removed from the Users node in the Navigator unless **Include Deactivated Users** is selected by right clicking the Users node. The Inactive User icon is shaded gray while the Active User icon is shaded blue.
4. To view all active or deactivated database users in a list, click the Users node and select **Show all users**. The Users screen appears. All the columns in this dialog are sortable. Double-click any user row to view that user’s details dialog. **Note**: You can also deactivate a user by clicking the Active check box in this dialog.

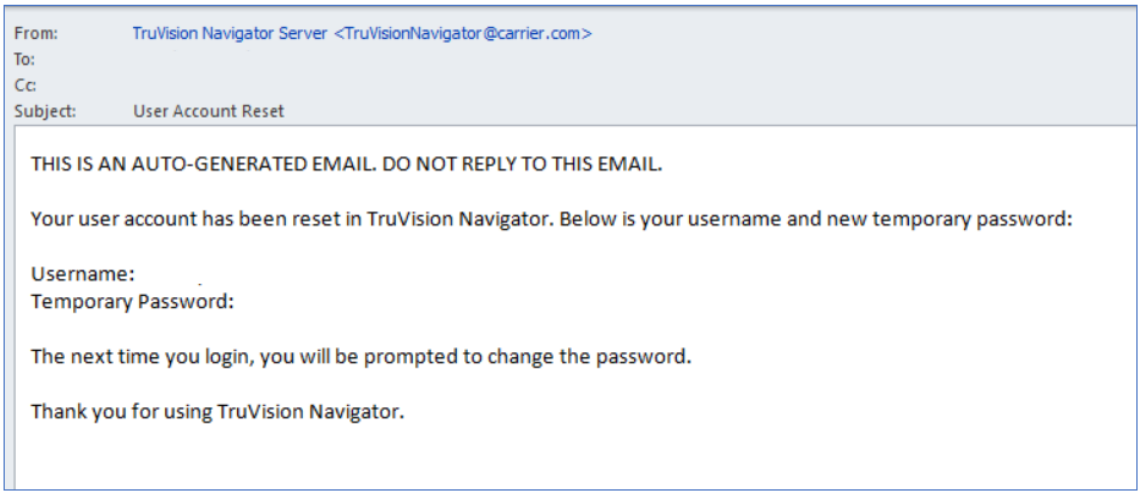


Restore a deactivated user

To restore a deactivated user in the system (three possible methods):

- Right-click the deactivated user under the Users node and select **Activate User**.
- Right-click the deactivated user under the Users node, select **Properties**, and click the **Reset Account** button on the **Details** tab.
- From the user list, double-click the user icon to launch the **Details** tab, and then click the **Reset Account** button.

If SMTP is in use, the user automatically receives an email with a temporary login password. The user is prompted to change this password upon initial login.



If SMTP is not in use, the administrator must provide the user with a new temporary password in the Change Password window. These temporary credentials must be delivered to the user via phone or email.

Reset a user after lockout

If a user forgets the username or password and the challenge question, that user can be locked out of the system. If a user has been locked out for login failures, they must answer the challenge question in the *User Account Challenge* window.

If a user cannot remember the challenge question, the administrator must reset the account.

Force a user to log out

From the user list, double-click the user icon to launch the **Details** tab, and then click the **Force Logout** button. This logs the user out immediately. The user making the change must have the Manage Users Permissions permission granted to execute this function.

Two-level authentication

Two-level authentication adds an additional verification step for sensitive actions.

This mechanism requires approval from an authorized user before allowing access to:

- Recorded video playback
- Video export
- System settings

Different user roles can require or provide second-level authentication.

Configuration summary

1. Assign required roles
2. Enable 2nd-level authentication permissions
3. Test access behavior

There are two levels of authentications available:

- 2nd Level authentication required

  When this permission is assigned to a TruVision Navigator user, they cannot directly access the recorded video (playback) and application settings, and export videos unless an authorized user with **2nd Level authentication provider** permission also enters their credentials.

- 2nd Level authentication provider

  When this permission is assigned to a TruVision Navigator user, they can permit access to playback, export video, and settings for users who have the **2nd Level authentication required** permission.

Notes/Best practices

- Use for sensitive operations only
- Users assigned the **2nd Level Authentication Required** permission must have playback, export video and settings permission to access them.
- If both permissions are enabled for a user, the user can access the allowed features without the two-level authentication.

Limitation:

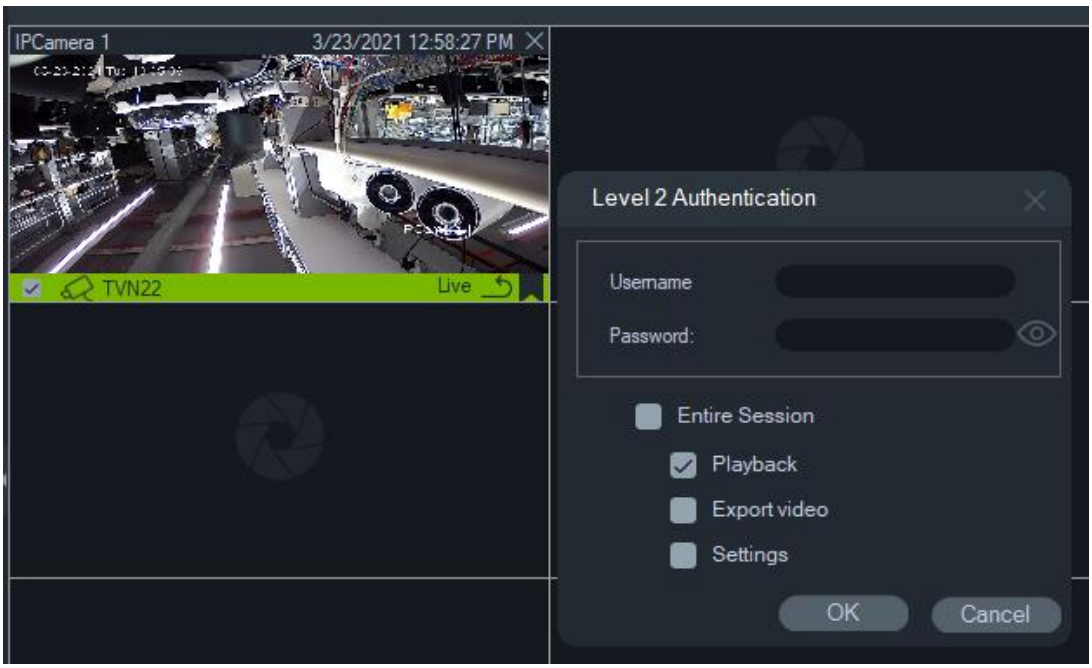
LDAP users cannot assign **2nd Level authentication provider** permission to another user.

For example:

A user is created with the permission access playback, and/or Export Video and/or access the settings and is assigned the **2nd Level authentication required** permission.

If this user then tries to access any of the above-mentioned features (do playback/export or access the settings menu), the application will request a second-level authentication.

In the following scenario, when this user tries access playback, because they require second-level authentication permission, a window will pop-up requesting credentials of a user with the **2nd Level authentication provider** permission. By default, the playback option is selected.



Any user with **2nd level authentication provider** permission can enter their credentials to allow this user to access the selected feature(s).

Entire Session: This option is disabled by default. When selected, the user can access the selected feature until they log off.

The option Entire Session works only for the selected features. If the user then needs to access another feature for which authorization was not provided, this pop-up window will appear again, and again a second-level authentication must be provided. When this happens, it overrides any existing selection for the entire session.

Group management

The advanced permission model permits group management in Navigator. Groups allow the scaling of user permissions across many users. For instance, users can be placed into a single group, and that single group can be assigned permissions against folders, devices, and other items in the system. Without groups, the administrator would have to grant permission to each user against those same devices.

Secure communication for client/server environments

System behavior settings define operational limits and background processing logic.

Configuration summary

1. Install SSL certificate
2. Configure secure communication
3. Validate connectivity

Notes / best practices

- Required for secure client-server environments

Performance and operational limits

The system applies limits to ensure stable operation, including:

- Maximum CPU usage thresholds
- Limits on active video streams
- Notification storage limits

These limits prevent resource exhaustion and maintain system responsiveness.

Configuration summary

1. Configure CPU usage limits
2. Set stream limits
3. Define notification limits
4. Configure timing parameters

Notes / best practices

- Adjust limits based on hardware capacity

Secure communication between devices and TruVision Navigator

The communication between TruVision devices and the software can be fully encrypted.

This secure communication is possible for TruVision recorders TVN 12, TVN 23(S/P), TVR 17 and TVR18 and TruVision IP cameras TVGP-M, TVGP-P, TVFC, TVTH and TVPA cameras.

To create a secure communication path, do the following:

1. Add the TruVision device to the software via the discovery tool.
2. In the device webpage:

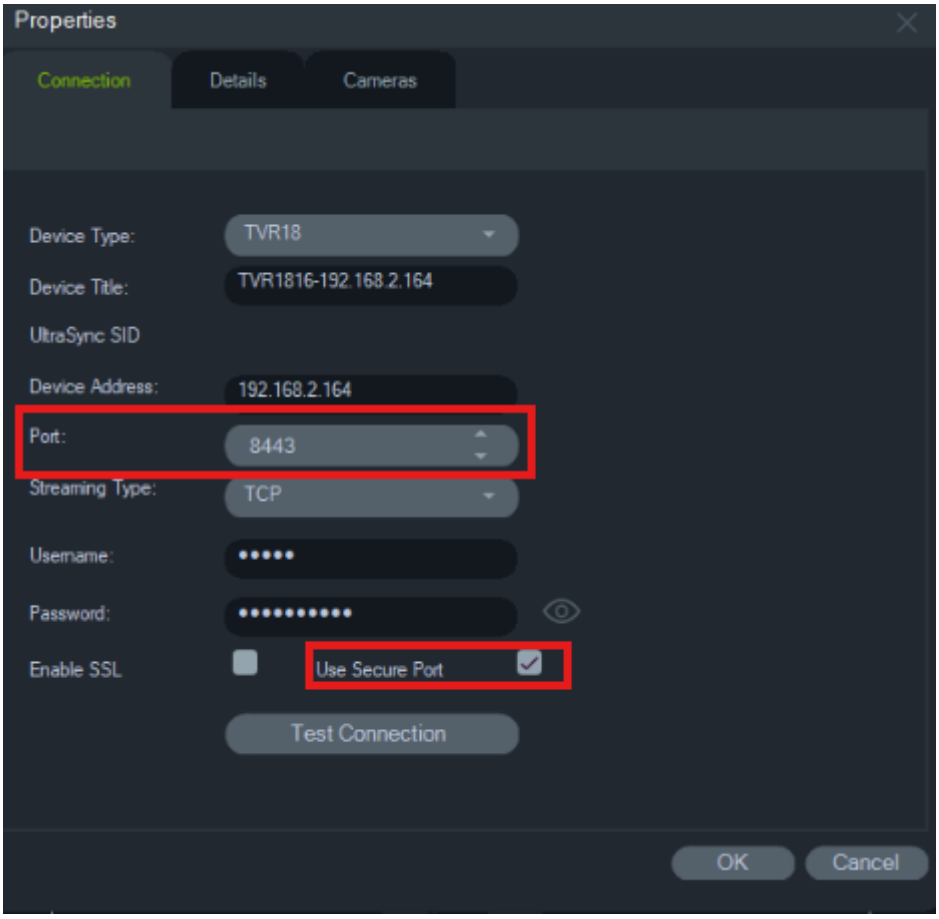
   Open the Configuration menu and go to **Network > Advanced Settings > Network Service** and enable the function **Enable Enhanced SDK Service** and click **Save.**.

   For recorders: enable also the function **Enable Stream Over TLS** for also securing the video stream.

   Go to **Network > Basic Settings > Port** and make a note of the **Enhanced SDK Service Port** (Default = 8443).
3. In TruVision Navigator: Right-click on the device in the device tree and select **Properties**.

   Enable the function **Use Secure Port** and enter the **Enhanced SDK Service Port** number as **Port.**

Example:



Use HTTPS for web browsing

It is advisable to also use HTTPS in the devices for web browsing.

In the webpage of the device:

Go to **Configuration > Network > Advanced Settings > HTTPS** and select **Enable HTTPS**. Save the setting. The webpage will now be opened in HTTPS.

In TruVision Navigator:

Right-click on the device in the device tree and select **Properties**. Select **Enable SS**L and click **OK**.

Updates and maintenance

The system provides tools for software maintenance and system administration.

Software updates

Users can check for and download updates such as:

- Language packs
- Player components

A system restart may be required to apply updates.

Configuration summary

1. Check for updates
2. Download updates
3. Restart application

Notes / best practices

- Always restart after updates

Database management

The system allows database backup and restore operations.

These operations:

- Preserve system configuration data
- Enable recovery after failures
- Restore system functionality without reconfiguration

Backups must be stored safely and are intended for use with the same software version.

Database backup and restore (standalone installations only)

Navigator database backup should be backed up in a separate location by an administrator for safekeeping. If there is a problem with the computer where the TruVision Navigator database resides, the administrator can install that same version of TruVision Navigator and restore the database with the backup file. This brings the system back into operation quickly without manual re-entry of device, user, group, permission, or other system configuration data.

Note: Data backup and restore is not intended for use when upgrading to a newer version of Navigator. It will only work with the same version of Navigator used for the database backup.

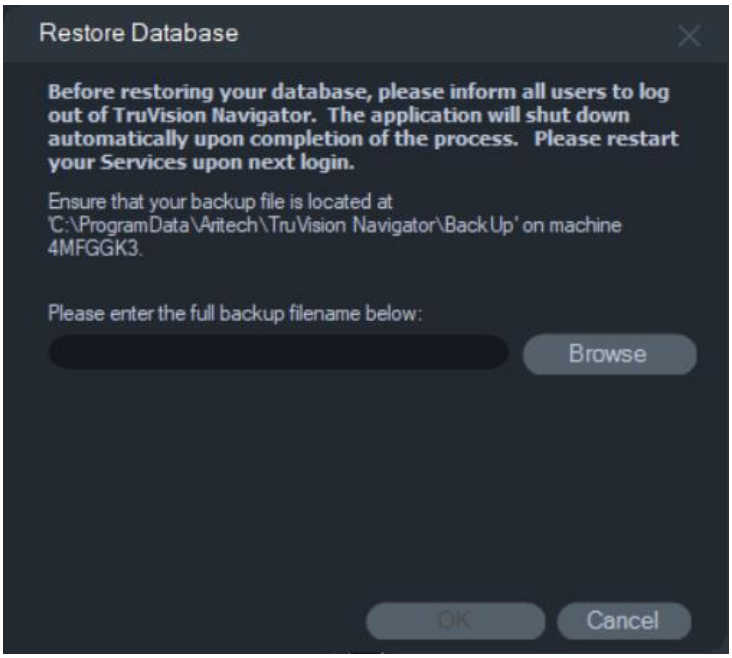
To back up the Navigator database:

1. Select the **Server** tab in the Settings window and then click the **Database Backup** button. The Backup Database window appears.
2. Type a database backup name (no file extension is necessary) and take note of the path where the database backup file will reside. The administrator should copy or move this file to a safe location.
3. Click **Schedule** to schedule the backup or click **Backup Now**. Upon initiation of the backup, refer to the Tasks window for status (see “Tasks” on page 246)

After successful completion, the database backup file resides at the designated location.

To restore the Navigator database:

1. Select the **Server** tab in the Settings window and then click the **Database Restore** button. The Restore Database window appears. Ensure that a copy of the backup database file has been placed in the directory listed.



2. Type the exact name of the file in the text field provided. If restoring the database to a SQL instance that requires SQL authentication credentials, enter them here. Otherwise, use the default setting.
3. Upon initiation of the restore, refer to the Tasks window for status. After Restore Task appears in the Task window, log out of the application. Log back in and the database is restored.

Configuration summary

1. Schedule backups
2. Store backups securely

3. Perform restore when needed

Notes / best practices

- Backup and restore must use same software version

Data import and export

System configuration data can be exported and imported using structured formats.

This includes:

- Device configurations
- System structure and settings

This functionality supports system migration and backup scenarios.

Import/export Navigator data

A Navigator address book stores the title, IP address, and credentials of recorders and cameras, as well as website pages, TruPortal panels, Aritech intrusion panels, IFS network switches, and logical views in the Navigator panel. This data can be imported or exported into Navigator as needed to save and restore these settings.

- Click **Export Navigator Data** to save Navigator settings in the CSV file format.
- Click **Import Navigator Data** to import previously configured Navigator panel settings in the CSV file format.

Configuration summary

1. Export system configuration
2. Import configuration when required

Notes / best practices

- Use export for backup and migration

Email configuration

Email services can be configured to support automated messaging.

SMTP settings enable:

- Sending user credentials

- Sending notifications and alerts
- Delivering system-generated messages

If email services are not configured, information must be delivered manually.

Configuration summary

1. Configure SMTP server
2. Test email functionality
3. Enable notifications

Notes / best practices

- Configure SMTP before creating users

See “SMTP setup” on page 202.

Server offline mode

Server offline mode defines how the client behaves when the connection to the server is unavailable. When the server is offline, the client may continue to operate with limited functionality depending on the system configuration and available local data.

A dialog appears when starting Navigator with the server offline. It states: “While you’re offline, you’ll be able to access video normally. Changes to the system configuration will be disallowed.”

Server offline mode is indicated by the  icon next to Admin in the Navigator screen. The Notifier is empty, and notifications do not appear when in server offline mode.

Note: The Navigator client can take up to five minutes to recognize the Navigator server after the TruVision Navigator service is started.

Available options, server online, and server offline mode:

Function	Online	Offline Mode
Navigator main menu	Settings Device Manager Bookmark Manager Tasks Recurring Tasks Open Exported Video File Check For Updates User Settings Help Logout	Settings Bookmark Manager Recurring Tasks Storage Calculator Open Exported Video File Check For Updates Help Logout
Settings window	Client tab Server tab Notifications tab Health Diagnostics tab Groups and Users tab Audit History tab Event Actions tab	Client tab
Add Folder menu	Enabled	Disabled
Add Devices menu	Enabled	Disabled
Devices menu	Add Device Add Folder Health Diagnostics Open Exported Video File	Open Exported Video File
Device folder menu	Add Device Add Folder Delete Folder Rename Folder	Disabled
Device offline menu	Connect Delete Device Rename Device Properties	Connect Properties

Function	Online	Offline Mode
Device online menu	Run Tampering Monitor Run Device Report Run Health Diagnostics Run Network Statistics Run Disk Analysis Trigger Outputs Manage IP Cameras Search Export Video Configure Device Reboot Device Delete Device Rename Device Properties	Run Health Diagnostics Run Disk Analysis Trigger Outputs Search Export Video Reboot Device Properties
Export Video window	Export Now Schedule	Export Now
Properties window	Enabled	Device or camera detail are visible but cannot be changed.
Camera menu (camera icon)	Search Export Video Assign to Event Monitor	Search Export Video
Camera menu (device icon)	Run Tampering Monitor Run Device Report Run Health Diagnostics Trigger Outputs Search Configure Device Reboot Device Delete Device Rename Device Properties	Run Health Diagnostics Trigger Outputs Search Reboot Device Properties
Multi selection menu, devices	Delete Devices	Disabled
Multi selection menu, folders (devices, maps, websites, access control)	Delete Folders	Disabled
Maps main menu	Add Map Add Folder	Disabled
Maps folder menu	Add Map Add Folder Delete Folder Rename Folder	Disabled

Function	Online	Offline Mode
Map menu	Configure Map Rename Map Delete Map	Disabled
Multi selection menu, maps	Delete Maps	Disabled
Websites main menu	Add Website Add Folder	Disabled
Website menu	Configure Website Delete Website	Disabled
Website folder menu	Add Website Add Folder Delete Folder Rename Folder	Disabled
Multi selection menu, websites	Delete Websites	Disabled
Access Control main menu	Add Panel Add Folder Global Lockout Global Reinstate	Global Lockout Global Reinstate
Access Control panel menu	Configure Panel Recent Activities Delete Panel Rename Panel Reinstate All Doors Lockout All Doors Unlock All Doors Properties	Reinstate All Doors Lockout All Doors Unlock All Doors Properties
Access Control panel menu	Enabled	Enabled
Multi selection menu, access control panels	Delete Panels	Disabled
Intrusion Detection main menu	Add Panel Add Folder Global Arm Global Disarm	Disabled
Intrusion Detection panel menu	Configure Panel Delete Panel Rename Panel Arm All Disarm All Properties	Disabled
Network Switches main menu	Add Device Add Folder	Disabled

Function	Online	Offline Mode
Network Switch menu	Configure Device Delete Device Rename Device Display Front Panel Run Network Statistics System Reboot Refresh Properties	Run Network Statistics System Reboot Refresh
People Counting main menu	Add People Counting Add Folder Report	Disabled
People Counting menu	Edit Delete Show in Map Reset Counter Report	Disabled
Logical View main menu	Add Logical view Add Folder	Disabled
Logical View folder menu	Add Folder Add Logical View Rename Folder Delete Folder	Disabled
Logical View menu	Edit Delete	Disabled

Audit and activity logs

Audit logging provides visibility into system activity and user actions.

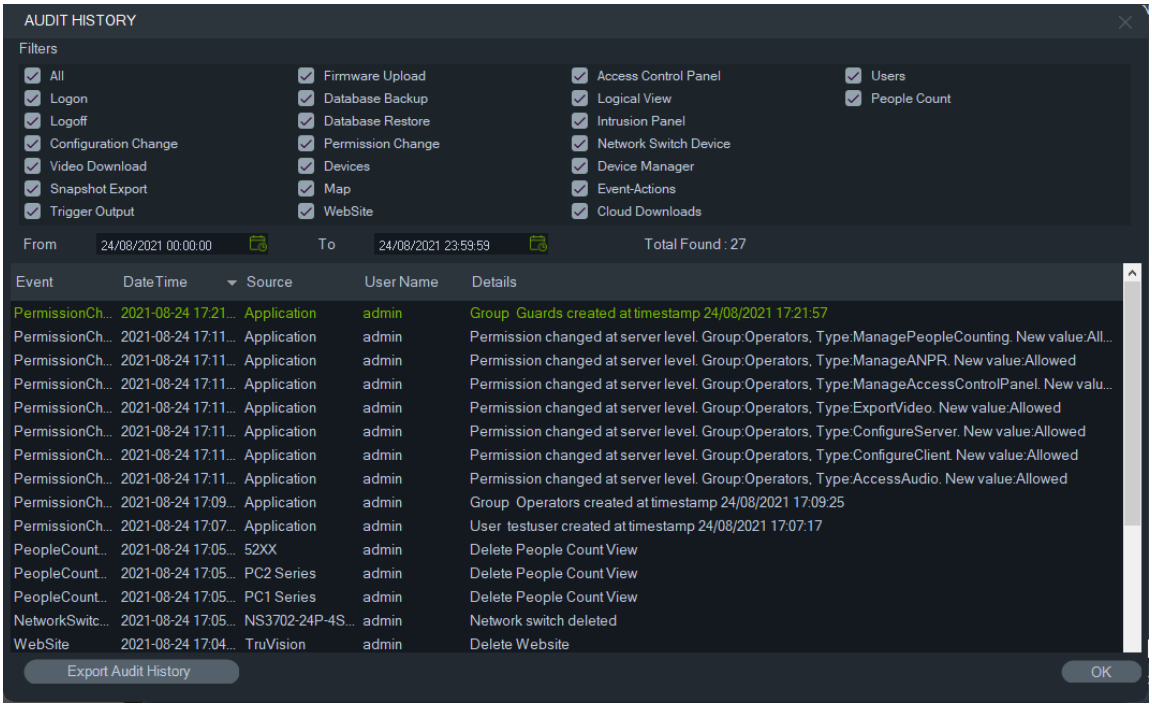
The system logs:

- User actions
- Configuration changes
- System events

Users can filter audit data by:

- Event type
- Time range

Audit logs support monitoring, troubleshooting, and compliance requirements.



The **Audit history** tab logs all user activity which can be searched using **Filters** selections. Click **OK** when finished making selections.

Click **Export Audit History** to save the list of configured events in the CSV file format.

Configuration summary

1. Enable audit logging
2. Apply filters
3. Select time range
4. Export logs if required

Notes / best practices

- Use audit logs for troubleshooting and compliance

Tasks and scheduling

The system provides task management features for monitoring automated and scheduled processes.

Tasks

The Tasks module tracks:

- Video exports

- Database backups and restores
- Scheduled operations

It provides real-time status and reporting for each task, including success or failure details.

Tasks are generated automatically when system operations are initiated, such as video exports, backups, or firmware updates. They provide real-time feedback on operation status and execution.

Configuration summary

1. Initiate operations (export, backup)
2. Monitor task status
3. Review results

Notes / best practices

- Tasks provide real-time system feedback

Recurring tasks

Recurring tasks allow automated execution of operations on a defined schedule.

Typical use cases include:

- Scheduled video exports
- Periodic data processing

Recurring tasks include scheduling information and execution status, allowing users to monitor ongoing automated processes.

Configuration summary

1. Define schedule
2. Configure recurring operations
3. Monitor execution

Notes / best practices

- Use recurring tasks to automate repetitive processes

Event-Actions

Event-actions define automated system behavior by linking events generated by devices to predefined actions within the system.

This feature enables the system to respond automatically to events such as alarms, motion detection, or device status changes.

Event-actions concept

An event-action consists of:

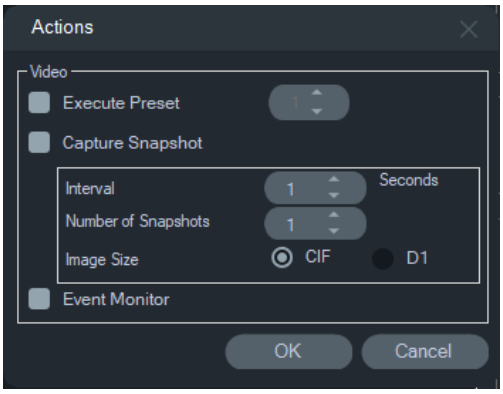
- **Events:** Conditions or triggers generated by devices
- **Actions:** Operations executed when the event occurs

Examples include:

- Displaying cameras in the Viewer
- Triggering outputs such as doors or relays
- Generating notifications
- Creating snapshots or recordings

Event-actions allow automation of workflows and improve response time to critical situations.

(1)**Name** and **Title**. Previously configured event-actions appear in the **Name** drop-down menu. Type a title name for a new event-action in the **Title** box.
(2)**Disable**. Disables the currently selected event-action in the **Name** drop-down menu.
(3)**Events**. Drag a device from the event-action panel into the **Events** box. An Events window appears with a list of options (see below). Click **OK** when finished selecting event options.
(4)**Actions**. Drag a device from the event-action panel into the Actions box. When a camera is added to the Actions table, a Video Actions window appears, with a list of options (see graphic below). Select to call up a preset of the camera (if applicable), generate multiple snapshots with configurable interval and image size, or show the camera on the Event Monitor viewer.

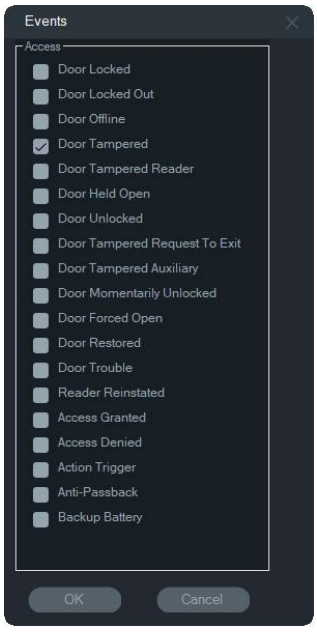


(5)**Date and Time Range**. Specify a **Date Range** and **Time Range** for the event-action to send notifications. Notifications will be sent 24 × 7 if no date and time ranges are specified.
(6)**Meet Any/Meet All**. Select **Meet Any** to trigger all event-action notifications. Select **Meet All** to trigger event-actions that occur within the duration specified in seconds.
(7)**Notification**: Select this option to have a custom notification generated when the configured event occurs.
(8)**Digital Output active timespan**. Enable **Digital Output active timespan** to configure time (in seconds) to deactivate the relay output after it has been activated by the Event-action.
(9)**Add/Save/Delete**. Click **Add** to add a new event-action, click **Save** to save a new event-action, and click **Delete** to delete an existing event-action.

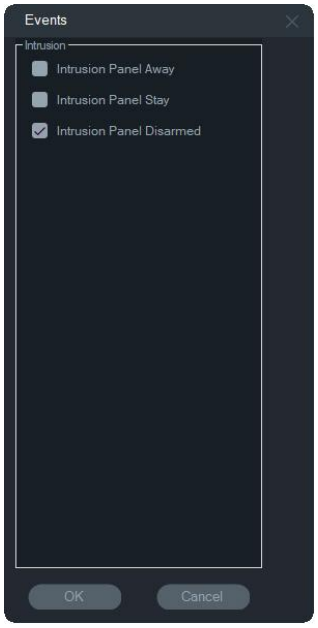
Note: TruVision Navigator 9.2 no longer supports Logical Events. If you are updating from an earlier version of the software that had Logical Events saved, you will be asked to migrate these Logical Events to Event Actions.

Video events

Access events

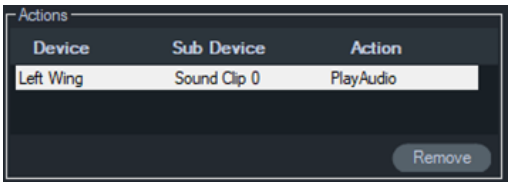


Intrusion events

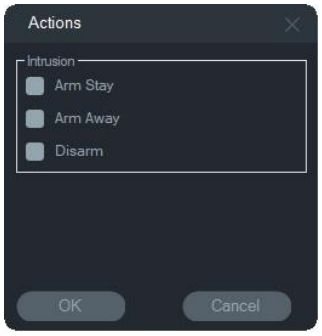


Access actions

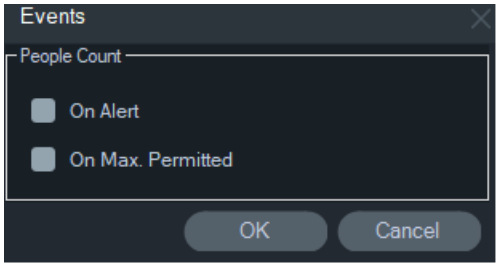
IP speaker actions



Intrusion actions



People counting events



Event sources and actions

Event-actions can be configured using multiple types of sources and targets:

Event sources may include:

- Video events (motion, video loss)
- Access control events
- Intrusion system events
- Device status notifications

Actions may include:

- Displaying video in Event Monitor
- Triggering outputs or relays
- Generating notifications
- Creating snapshots
- Activating presets (e.g., PTZ positions)

This flexibility allows integration across different subsystems.

Event and action logic

Event-actions support logic to control when actions are triggered:

- **Meet Any:** Triggered when any selected event occurs
- **Meet All:** Triggered when all selected conditions are met within a defined time

Additionally, actions can be limited by:

- Date ranges
- Time schedules
- Duration of activation (e.g., output relay timing)

These controls allow precise definition of system behavior.

Notifications and integration

Event-actions can generate notifications that appear in the system and may be linked to other configured features such as:

- Notifier panel
- Email notifications
- Event Monitor

They act as a bridge between **event detection (Chapter 7)** and **system response (Chapter 14)**.

To configure event-actions:

1. Define the triggering event(s) from one or more devices
2. Define the action(s) to execute when the event occurs
3. Configure logical conditions (Meet Any / Meet All)
4. Define time and date ranges if required
5. Enable notification generation (optional)

6. Configure output duration for triggered actions if applicable

Notes / best practices

- Use event-actions to automate repetitive responses and reduce operator workload
- Test event-actions thoroughly to ensure correct behavior before deployment
- Avoid overly complex logic that may be difficult to maintain
- Combine event-actions with notification filtering to prevent overload
- Use scheduling to limit actions to relevant operational periods
- Event-actions replace legacy logical event filtering functionality

Real-world event-action examples

The following examples illustrate how event-actions can be used in real operational environments to automate responses and improve system efficiency.

Example 1 — Motion detection triggers camera display

Scenario:
A camera detects motion outside business hours.

Event:

- Motion detection from a specific camera

Actions:

- Display the camera in the Event Monitor
- Generate a notification in the Notifier

Configuration summary

1. Select the camera motion event as trigger
2. Define action to display the camera in Event Monitor
3. Enable notification generation
4. Configure time schedule (e.g., after business hours)

Value

- Enables operators to immediately see relevant video
- Reduces time to assess potential incidents

Example 2 — Video loss triggers alert

Scenario:
A camera loses video signal.

Event:

- Video loss notification

Actions:

- Generate notification
- Send email alert (if SMTP configured)

Configuration summary

1. Select video loss event
2. Enable notification action
3. Configure email delivery (SMTP required)
4. Apply filtering to avoid repeated alerts

Value

- Ensures rapid detection of system failures
- Reduces camera downtime

Example 3 — Motion triggers snapshot capture

Scenario:
Motion is detected in a monitored zone.

Event:

- Motion detection

Actions:

- Capture snapshots at defined intervals
- Store snapshots for review

Configuration summary

1. Select motion event
2. Enable snapshot action
3. Configure snapshot frequency and duration
4. Define storage location

Value

- Provides quick visual evidence without video review
- Useful for reporting and analysis

Example 4 — Multi-condition event (Meet All logic)

Scenario:
An alarm should only trigger when both motion and a sensor event occur.

Events:

- Motion detection
- Sensor input

Logic:

- Meet All

Actions:

- Trigger alarm output
- Send notification

Configuration summary

1. Select multiple event conditions
2. Configure “Meet All” logic
3. Define action (output + notification)

Value

- Reduces false alarms
- Improves reliability of alerts

General best practices for event-actions

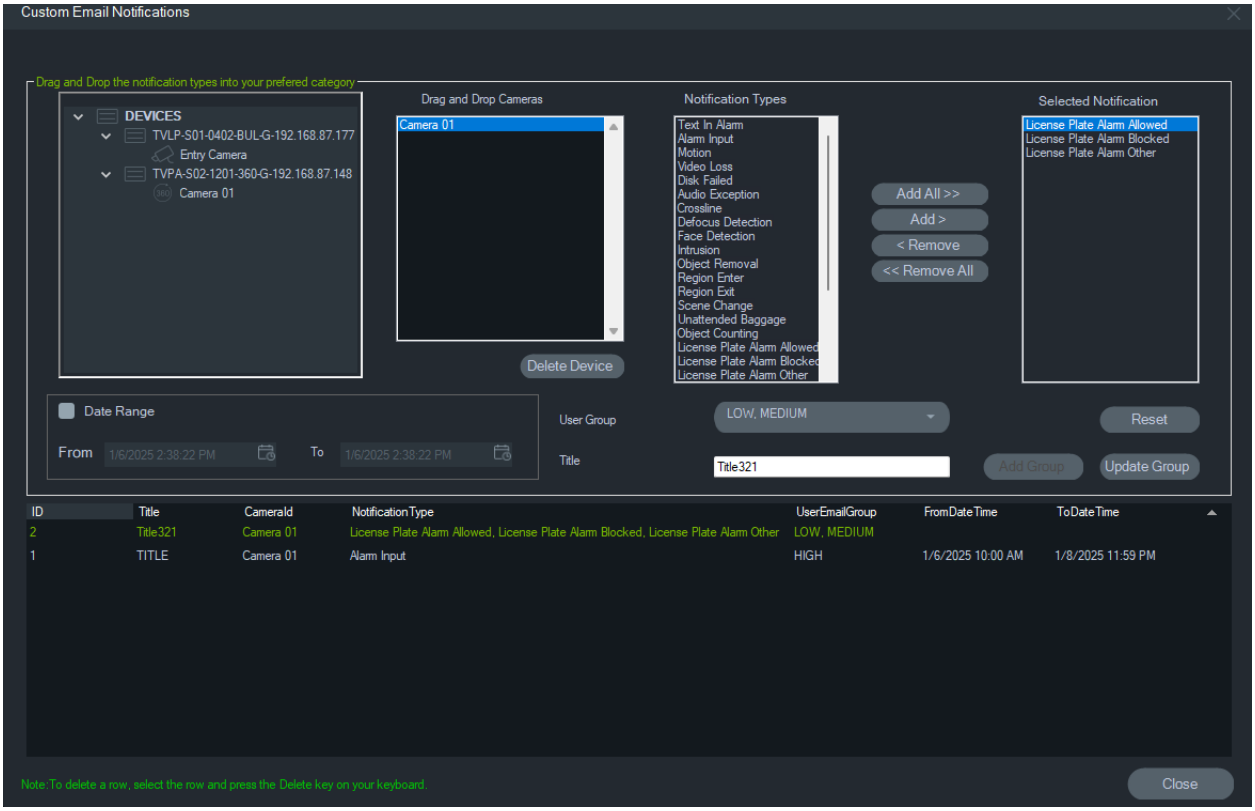
- Keep configurations simple and easy to understand
- Use naming conventions for event-actions (e.g., “Motion_AfterHours_Display”)
- Test each event-action scenario before deployment
- Avoid excessive overlapping rules that may create conflicts
- Use scheduling and filtering to reduce unnecessary triggers
- Combine event-actions with notification settings for optimal results

Custom email notifications

The emails sending by the software can be customized, so that recipients only receive emails with relevant information.

Custom email notification setup

In the main menu, select Custom Email Notifications. A pop-up form will be shown.



The following operations are possible:

- Create
- Update
- Delete

Creation of a Custom Email Notification

1. Drag and Drop Cameras from the Devices into the **Drag and Drop Camera** list.
2. Select the notifications from the **Notification Types** and add those Notifications into the **Selected Notification** list.
3. You can also add and remove all the notifications by clicking on **Add All >>** and **<< Remove ALL** buttons.
4. Check **Data Range** checkbox if you want to select a time duration to receive the notifications at the particular time range. Once selected the

date range, click on the calendar and select the date and time in the **From** and **To** calendars.

5. Select a User Group from the drop down list. You can select multiple groups if needed.
6. Add a unique **Title** to the Group.
7. Using the Reset button, you can reset all the entries (like Drag and Drop Camera, Select Notification, Date Range, User Group, Title).
8. Now click **Add Group** to create a custom group for sending emails on the notifications.

The added group will be populated in the below table.

Updating of Custom Email Notification

1. The table shows all the custom email notification groups. If you want to make any changes select a particular group from the table.
2. All the selected options for that group will be shown in the form.
3. You can reset all the values if you want to change all the selected values for the Group.
4. Now you will see that the **Update Group** button will be enabled when an item is clicked on in the table and the **Add Group** button will be disabled.
5. Change the required fields and click the **Update Group** button to update the group.

Once the group details are updated the **Update Group** button will be disabled, and **Add Group** button will be enabled.

Deletion of Custom Email Notification

Select any item that you want to delete, and press **Delete** button from the keyboard. You will get a confirmation prompt “Are you sure you want to delete this item?”. If OK, click on **Yes**, and the custom notification group will be deleted.

Appendix A
Minimum system requirements

Software requirements

The following operating systems and other software components are prerequisites for client and server installation:

Note: 32-bit operating systems are not compatible with TruVision Navigator 8.0+.

Table 5: Client software requirements

Component	Version	Notes
Operating System	Microsoft Windows 10 64-bit	
	Microsoft Windows 11 64-bit	
	Microsoft Windows Server 2012 R2 64-bit	
	Microsoft Windows Server 2016	
	Microsoft Windows Server 2019	
	Microsoft Windows Server 2022	
	Microsoft Windows Server 2025	
Other	Microsoft .NET Framework 4.8	Packaged with the installation

Table 6: Server software requirements

Component	Version	Notes
Operating System	Microsoft Windows 10 64-bit	
	Microsoft Windows 11 64-bit	
	Microsoft Windows Server 2012 R2 64-bit	
	Microsoft Windows Server 2016	
	Microsoft Windows Server 2019	
	Microsoft Windows Server 2022	
	Microsoft Windows Server 2025	

Component	Version	Notes
Database	SQL Server 2012/2014/2016/2019/2022 (use updated versions)	Go to www.microsoft.com for details on version compatibility with the operating systems listed above.
Other	Microsoft .NET Framework 4.8	Packaged with the installation
Other	Microsoft Visual C++ 2010 x64 Redistributable 10.0.40219	Packaged with the installation
Other	WinPCAP 4.1.3	Packaged with the installation

Server/client hardware guidelines

The following specifications are only meant to serve as a guideline as Navigator system performance varies according to the robustness of the machine.

Table 7: Server hardware specifications

Component	Recommended	Notes
CPU	Intel® Core™ i5-11600K processor (12 Mb cache, up to 4.90 GHz)	CPU power is directly related to the performance of the application when running and rendering video. The better the CPU, the more responsive the application will be.
Memory	16 GB RAM	RAM is related to the number of different applications that can run simultaneously as well as the number of different operations that TruVision Navigator can perform at once. The higher the RAM, the better the performance of the application.
Hard Drive	500 GB – 7200 RPM, SATA 3.0 Gb/s, 16 MB Cache	Optional - TruVision Navigator requires approximately 800 MB of storage to install. To store exported video from the devices on the local machine, an increase storage size may be required.
Graphics Card	Nvidia® GeForce RTX 2060	Video Card capability is directly related to the video rendering performance within TruVision Navigator. The better the video card, the better the video rendering performance.
Resolution	1920 x 1080	
Network	Gigabit Ethernet (10/100/1000 Mbps), 2.5 GbE or higher for better performance and higher bandwidth.	The network interface card can be a performance bottle neck depending upon the throughput of the card. If the card’s throughput is less than the amount of data streaming to the machine, performance issues may occur.

Performance factors and upgrade recommendations

The TruVision Navigator application recommends utilizing more sub-streams and fewer main streams to optimize the number of videos you can stream. This recommendation helps maintain better performance and resource management.

Performance factors

The performance of the application when streaming multiple videos varies based on several factors, including:

- System Configuration: Overall computer capabilities include CPU power and available RAM.
- Graphics Card: Quality and power are crucial for efficiently handling multiple video streams.
- Camera Performance: Resolution, frame rate, and bitrate significantly affect streaming performance. The encoding such as H.264, H.265 and H.265+ also impacts camera performance.
- Network Performance: Speed and stability of the network connection are vital for smooth video streaming.

Video stream limits

- **Recommended limit:** The application recommends streaming up to 64 video streams to maintain optimal performance. Exceeding this limit may result in a decline in application performance.

  Warning message: The application displays the following warning message upon exceeding 64 streams:

  “You have exceeded the recommended limit of 64 video streams. App performance may degrade with more streams. The maximum limit is 100.”

- **Maximum limit:** The application allows streaming up to 100 video streams. Reaching this limit will prevent additional streams from opening.

  Error message: The application displays the following error message upon exceeding 100 streams:

  “You have reached the maximum limit of 100 video streams. Please close some streams to continue.”

System upgrade recommendation

For systems with minimum configurations, the application is designed to handle a limited number of video streams effectively. If you need to open and stream more videos, it is essential to upgrade your system's configuration. This includes enhancing your CPU, adding more RAM, and upgrading your graphics card to ensure optimal performance and avoid potential issues.

By following these guidelines, you can ensure a smoother and more efficient video streaming experience on the TruVision Navigator.

Supported recording devices

Table 8 shows the supported recording devices.

Table 8: Supported recording devices

TruVision NVR 10 (TVN 10/10S/10C/10CS)*
TruVision NVR 21 (TVN 21)*
TruVision TVN 22*
TruVision TVN 23
TruVision TVR 12HD*
TruVision TVR 15HD*
TruVision TVR 44HD*
TruVision TVR 45HD*
TruVision TVR 16*
TruVision TVR 17
TruVision TVR 18
TruVision TVR 46*
TruVision NVR 71 (TVN 71)*
TruVision NVR 70 (TVN 70)*
TruVision NVR 11 (TVN 11)*
TruVision NVR 12 (TVN 12)
TruVision NVR 20 (TVN 20)*
TruVision NVR 50 (TVN 50)*
TruVision DVR 10 (TVR 10)*
TruVision DVR 11/11C (TVR 11/11C)*
TruVision DVR 12/12C (TVR12/12C)*
TruVision DVR 40 (TVR 40)*
TruVision DVR 41 (TVR 41)*
TruVision DVR 42 (TVR 42)*
TruVision DVR 60 (TVR 60)*
DVSR-xU*

* These models are in End-of-Life status and not actively supported.

Note: The latest firmware can be downloaded via the cloud connection.

Discoverable devices

IMPORTANT: A wired network connection is required for device discovery. Do not use a Wi-Fi network connection to discover devices.

Note: Unmanaged devices do not support the discovery feature.

Intrusion panels

Table 9 shows the discoverable intrusion panels and related firmware versions.

Table 9: Discoverable intrusion panels

Devices	Supported Firmware
UltraSync Self-Contained Hub	B0403001A58P002011-33 or later
UltraSync Modular Hub	B0403001A56P002005-01 or later
ZeroWire	B0403001A58P002010-31 or later
xGen	B0403001A56P002005-16 or later

Appendix B
Device details

Summary

This appendix contains important compatible device information.

TruVision Camera

Feature	Support	Notes
Supported Device(s)	TVB, TVC, TVD, TVE, TVF, TVGP, TVP, TVS, TVTH, TVW, UVP, RS, TVGP, TVFC, TVLP, TVTH, TVPA (TruVision Open Standard Cameras)	
H.265 Support	Depends on model (Series 4 or later)	
Default Ports	Video = 8000 (editable) Command and Control = 8000 (editable) Configuration = 80 (editable) RTSP = 554 (editable)	
Default Username / Password	N/A	Activation required
Default IP Address	192.168.1.70	
Network Discovery	Supported	
Compression	H.264, H.265, H.265+	
Connection Types	TCP, UDP	
Streaming Limits	Depends on the actual device capabilities.	
Stream Overlay	VCA Rules, Motion Rules, Camera Name, Date and Time	
High / Low Bandwidth	No	
Dual Streaming	Yes	Depends on the actual device capabilities.

Feature	Support	Notes
Stream Nomenclature	The Main stream is referred to as: TruVision Navigator = Main stream The Substream is referred to as: TruVision Navigator = Substream	
Third, Fourth, and Fifth Streams	Depends on the actual device capabilities.	
Playback Controls	Play Pause Frame Advance Fast Forward (1x, 2x,4x, 8x) Slow motion (1.0x, 0.5x, 0.25x, 0.125x, 0.0625x)	Video jumps back four seconds after resuming playback from Fast Forward and Frame Advance. When fast forwarding video and it catches up to present time (or Live video), the video in the viewing tile remains paused until the user clicks the **Live** button in the Controller. No other playback controls will work until the **Live** button is selected.
Digital Zoom	Live and Playback*	*For models that support SD cards.
Snapshot	Yes	
Local Record	Yes	
Instant Replay	Yes*	*For models that support SD cards.
Disk Analysis	No	
Time Line Disk Analysis	Yes	
Video Export	Yes*	*For models that support SD cards.
TruVision Navigator Player	Yes	.mp4 proprietary file format.
PTZ Control	Yes*	*For TVP and UVP models
Focus, Iris, Zoom	Yes*	*For TVP and UVP models
Presets	Yes*	*For TVP and UVP models
Tours	Yes*	*For TVP and UVP models
Camera Search	Alarm Event Motion VCA	
Smart Search	No	
People Density Search	Yes	
Point-of-Sale Text	No	
Motion	Yes	
Audio	Yes	
Bi-directional Audio	Yes	

Feature	Support	Notes
Notifications	No	
Health Diagnostics	Yes	
Firmware Upload	Yes	Via browser page.
Bulk Firmware Upload	No	
Device Configuration	Yes	Via browser page.
Bulk Configuration	No	
Remote Reboot	Yes	
Device log support	Yes	Via browser page.
Trigger Outputs	Yes	
Fisheye Dewarp	Yes	
Sync Playback	Yes	
Get Thumbnail	No	
Change IP	Yes	
Activate	Yes	
Reset Password	Yes	
Change Password	Yes	
Excel Configuration Push	No	
HTTPS	Yes	
Reset Factory Default	Yes	
Sync Time (NTP)	Yes	
Network Storage	No	
Backup & Restore System Config	Yes	
Dual NIC	No	
DDNS	Yes	
Mobile App	Yes (TVRMobile)	
RTSP Live	Yes	
RTSP Playback	Yes	
Thumbnail Search	No	

TruVision TVN 12 / TVN 71 / TVN 70 / TVN 21 / TVN 22 / TVN 23 / TVR12 HD / TVR 44HD / TVR 45HD / TVR 16 / TVR 17/TVR 18/ TVR 46 / TVR 15HD

Feature	Support	Notes
H.264 Support	Yes (TVN 12)	
H.265 Support	Yes (TVN 12, TVN 71, TVN 22, TVN 23, TVR15HD & TVR 45HD [for IP cameras only], TVR 46, TVR 16, TVR 17, TVR18) No (TVN 70, TVR 44HD, TVR 15HD, TVR 12HD, TVN 21)	
H.265+ Support	Yes (TVN 12, TVN 23, TVR 18)	
Default Ports	Video = 8000 (editable) Command and Control = 8000 (editable) Configuration = 80 (editable) Notifications = 5001 (editable) RTSP = 554 (editable)	
Default Username / Password	N/A	Activation required
Default IP address	192.168.1.82	
Network Discovery	Supported	
Connection Types	TCP, UDP	
Streaming Limits	256 Live streams and 128 Playback streams (TVN 71) 128 Live or Playback streams	
Stream Overlay	VCA Rules, Motion Rules, Camera Name, Date and Time	
POS Text	TVN 21 (via RS-232) TVN 22 (via RS-232 and IP) TVN 23 (via RS-232 and IP) TVR 45HD (only for analog cameras; via RS-232 and IP)	
High / Low Bandwidth	No	
Dual Streaming	Yes	
Smooth Stream	Yes	

Feature	Support	Notes
Stream Nomenclature	The Main stream is referred to as: TruVision Navigator = Main stream The Substream is referred to as: TruVision Navigator = Substream	
Playback Controls	Play Pause Frame Advance Fast Forward (1x, 2x, 4x, 8x) Slow motion (1.0x, 0.5x, 0.25x, 0.125x, 0.0625x)	Frame reverse and rewind speeds directly depend on the actual device capabilities. Video jumps back four seconds after resume playback from Fast Forward and Frame Advance. When fast forwarding video and it catches up to present time (or Live video), the video in the viewing tile will automatically switch to live view.
Digital Zoom	Live and Playback	
Snapshot	Yes	
Local Record	Yes	
Instant Replay	Yes	There is a two-to-five-minute video buffer in the device. While video is in the buffer, it cannot be viewed. After the buffer fills, the video is written to the hard drive and is available for playback. This affects Instant Replay and the Playback button in TruVision Navigator. Those two features get their time increment from the user-defined Instant Replay configuration in the TruVision Navigator Settings window, **Server** tab. As a result, this time should be set to an increment to greater than five minutes. If a search is executed for video still in the buffer, Live video appears.
Disk Analysis	Alarm Motion Recorded VCA Text (except TVR 45HD, TVR 15HD)	Video Loss is not supported in disk analysis. Disk analysis takes approximately 15-45 seconds depending on the amount of recorded data on the device. Video Loss is only supported for Analog Channels for TVR 44HD, TVR 12HD, TVR 45HD, TVR 15HD.
Time Line Disk Analysis	Yes	
Video Export	Yes	
TruVision Navigator Player	Yes	.mp4 proprietary file format.
PTZ Control	Yes	
Focus, Iris, Zoom	Yes	

Feature	Support	Notes
Presets	Yes	
Tours	Yes	Dependent on camera and device.
Camera Search	Alarm Event Motion Text VCA	
Smart Search	Yes	
Point-of-Sale Text	Yes	
Motion	Yes	
Audio	Yes	
Bi-directional Audio	Yes	
Notifications	Alarm Video Loss (TVR 12HD, 15HD, TVR 16, TVR 17, TVR 18, TVR 44HD, TVR 45HD, TVR 46,) Motion VCA Disk Full Disk Failure	To set up the device to send TCP notifications for cameras, right-click the device in the Navigator and select **Configure Device**. On the Camera tab's Event Section, select the events and set the schedules as appropriate. On the Camera tab's Rules Section, for each event type, ensure that "notify me" is selected. Repeat for each event type. On the Notifications tab, the Notify IP Address should be the IP address of where the TruVision Navigator Server services are located (Notification Writer and Notification Processor). The Notify Port is defaulted to 5001 and is editable. Ensure this port matches the one listed in the TruVision Navigator Settings window, **Notifications** tab. To set up the device to send TCP notifications for the device itself (e.g., Disk Full and Disk Failure), right-click the device in the Navigator and select **Configure Device**. For each notification type on the **Notification** tab, ensure that "notify me" is selected. Repeat for each notification type and click **Save**. Ensure the notification port on the device matches that of TruVision Navigator Server as described above. Restart both the Notification Writer and Notification Processor for TruVision Navigator to process the notifications. Email notification is not supported at the device-level.

Feature	Support	Notes
Health Diagnostics	IP Address MAC Address Model Name Serial Number Firmware Version Device Date/Time Total Device Health HDD Status HDD Capacity Cameras in Video Loss Cameras in Alarm Current Client Connections Record Status	
Firmware Upload	Yes	Via browser page.
Bulk Firmware Upload	No	
Device Configuration	Yes	Via browser page.
Bulk Configuration	No	
Remote Reboot	Yes	
IP Camera Support	Yes (TruVision) ONVIF	
Device Log Support	Yes	
Trigger Outputs	Yes	
Fisheye Dewarp	Yes	
Sync Playback	Yes	
Get Thumbnail	Yes (TVN 12, TVN 71, TVN 22, TVN 23, TVR 15HD, TVR 16, TVR 17, TVR 18, TVR 45HD, TVR 46)	
Change IP	Yes	
Activate	Yes	
Reset Password	Yes	
Change Password	Yes	
Excel Configuration Push	Yes	Newer NVRs
HTTPS	Yes	
Reset Factory Default	Yes	

Feature	Support	Notes
Sync Time (NTP)	Yes	
Network Storage	Yes	
Backup & Restore System Config	Yes	
Dual NIC	Yes	Depends on model
DDNS	Yes	
Mobile App	Yes (TVRMobile)	
RTSP Live	Yes	
RTSP Playback	Yes	
Thumbnail Search	Yes (TVN 12, TVN 71, TVN 22, TVN 23, TVR 15HD, TVR 16, TVR 17, TVR 18, TVR 45HD, TVR 46,)	

TruVision TVN 11

Feature	Support	Notes
Supported Firmware Versions	1.0e	
H.265 Support	Yes	
Default Ports	Video = 554 (editable) Command and Control = 8000 (editable) Configuration = 8000 (editable) Notifications = 5001 (editable) RTSP = 554 (editable)	
Default Username / Password	N/A	Activation required
Default IP address	192.168.1.82	
Network Discovery	Supported	
Compression	H.264, H.265	
Connection Types	TCP, UDP	
Streaming Limits	128 Live streams or Playback streams	

Feature	Support	Notes
Stream Overlay	VCA Rules Motion Rules Camera Name Date and Time	
High / Low Bandwidth	No	
Dual Streaming	Yes	
Stream Nomenclature	The Main stream is referred to as: On-Screen-Display = Time Lapse Web Browser = Time Lapse TruVision Navigator = Main stream The Sub stream is referred to as: On-Screen-Display = Alarm Web Browser = Alarm TruVision Navigator = Sub stream The Event stream is referred to as: On-Screen-Display = N/A Web Browser = Event TruVision Navigator = Event The Schedule stream is referred to as: On-Screen-Display = Schedule Web Browser = Schedule TruVision Navigator = Schedule	
Playback Controls	Play Pause Frame Advance Fast Forward (1x, 2x, 4x, 8x) Slow motion (1.0x, 0.5x, 0.25x, 0.125x, 0.0625x)	Frame reverse and rewind speeds not supported. Video jumps back four seconds after resume playback from Fast Forward and Frame Advance. When fast forwarding video and it catches up to present time (or Live video), the video in the viewing tile will automatically switch to live view.
Digital Zoom	Live and Playback	
Snapshot	Yes	

Feature	Support	Notes
Local Record	Yes	
Instant Replay	Yes	
Disk Analysis	Alarm Motion Recorded VCA Text	Video Loss is not supported in disk analysis. Disk analysis takes approximately 15-45 seconds depending on the amount of recorded data on the device.
Time Line Disk Analysis	Yes	
Video Export	Yes	
TruVision Navigator Player	Yes	.mp4 proprietary file format.
PTZ Control	Yes	
Focus, Iris, Zoom	Yes	
Presets	Yes	
Tours	Yes	Dependent on camera and device.
Camera Search	Alarm Event Motion Text VCA	
Smart Search	Yes	
Point-of-Sale Text	No	
Motion	Yes	
Audio	Yes	
Bi-directional Audio	Yes	

Feature	Support	Notes
Notifications	Alarm Motion VCA Disk Full Disk Failure	To set up the device to send TCP notifications for cameras, right-click the device in the Navigator and select **Configure Device**. On the Camera tab's Event Section, select the events and set the schedules as appropriate. On the Camera tab's Rules Section, for each event type, ensure that "notify me" is selected. Repeat for each event type. On the Notifications tab, the Notify IP Address should be the IP address of where the TruVision Navigator Server services are located (Notification Writer and Notification Processor). The Notify Port is defaulted to 5001 and is editable. Ensure this port matches the one listed in the TruVision Navigator Settings window, **Notifications** tab. To set up the device to send TCP notifications for the device itself (e.g., Disk Full and Disk Failure), right-click the device in the Navigator and select **Configure Device**. For each notification type on the **Notification** tab, ensure that "notify me" is selected. Repeat for each notification type and click **Save**. Ensure the notification port on the device matches that of TruVision Navigator Server as described above. Restart the Notification Processor for TruVision Navigator to process the notifications. Email notification is not supported at the device-level.
Health Diagnostics	IP Address MAC Address Model Name Serial Number Firmware Version Device Date/Time Total Device Health HDD Status HDD Capacity Cameras in Video Loss Cameras in Alarm Current Client Connections Record Status	
Firmware Upload	Yes	Via browser page.
Bulk Firmware Upload	No	
Device Configuration	Yes	Via browser page.
Bulk Configuration	No	
Remote Reboot	Yes	

Feature	Support	Notes
IP Camera Support	Yes (TruVision) Onvif	
Device Log Support	Yes	
Trigger Outputs	Yes	
Fisheye Dewarp	Yes	
Sync Playback	Yes	
Get Thumbnail	Yes	
Change IP	Yes	
Activate	Yes	
Reset Password	Yes	
Change Password	Yes	
Excel Configuration Push	Yes	
HTTPS	Yes	
Reset Factory Default	Yes	
Sync Time (NTP)	Yes	
Network Storage	Yes	
Backup & Restore System Config	Yes	
Dual NIC	Yes	
DDNS	Yes	
Mobile App	Yes (TVRMobile)	
RTSP Live	Yes	
RTSP Playback	Yes	
Thumbnail Search	Yes	

TruVision TVN 10/20/50 (NVR)

Feature	Support	Notes
Supported Firmware Versions	2.1n (TVN 10, 10S, 10CS) 3.2a (TVN 20) 2.2i (TVN 50)	
Support H.265	No	
Default Ports	Video = 8000 (editable)	

Feature	Support	Notes
	Command and Control = 8000 (editable) Configuration = 8000 (editable) Notifications = 5001 (editable) Firmware Upload = 8000 (editable)	
Default Username / Password	admin / 1234 or no default Activation required (TVN 10)	We recommend changing this default password at time of installation.
Default IP Address	192.168.1.82	
Network Discovery	Supported	
Compression	H.264	
Connection Types	TCP UDP	
Streaming Limits	TVN 10: 64 Live or Playback streams including those used by the web page. TVN 20: 48 Live or Playback streams simultaneously with a maximum of six streams per channel. TVN 50: 128 Live or Playback streams including those used by the web page.	If users try to open more streams than a recorder supports, they will get a black video tile containing an error message.
Stream Overlay	Camera Name Date and Time	
High / Low Bandwidth	No	
Dual Streaming	Yes	
Stream Nomenclature	The Main stream is referred to as: On-Screen-Display = Time Lapse Web Browser = Time Lapse TruVision Navigator = Main stream The Substream is referred to as: On-Screen-Display = Alarm Web Browser = Alarm TruVision Navigator = Substream The Event stream is referred to as:	

Feature	Support	Notes
	On-Screen-Display = N/A Web Browser = Event TruVision Navigator = Event The Schedule stream is referred to as: On-Screen-Display = Schedule Web Browser = Schedule TruVision Navigator = Schedule	
Playback Controls	Play Pause Frame Advance Fast Forward (2x,4x,8x,16x) Slow motion (1.0x, 0.5x, 0.25x, 0.125x, 0.0625x) Rewind (1x, 2x 4x)	Frame Reverse and Rewind Speeds are not supported in TVN 10 and TVN 20. Video jumps back four seconds after resume playback from Fast Forward and Frame Advance. When fast forwarding video and it catches up to present time (or Live video), the video in the viewing tile will automatically switch to Live view.
Digital Zoom	Live & Playback	
Snapshot	Yes	
Local Record	Yes	Pause during local record is not supported.
Instant Replay	Yes	There is a two-to-five-minute video buffer in the device. While video is in the buffer, it cannot be viewed. After the buffer fills, the video is written to the hard drive and is available for playback. This affects Instant Replay and the Playback button in TruVision Navigator. Those two features get their time increment from the user-defined Instant Replay configuration in the TruVision Navigator Settings window, **Server** tab. As a result, set this time increment to greater than five minutes. If a search is executed for video still in the buffer, Live video appears.
Disk Analysis	Alarm Motion Recorded Untagged (TVN 10/TVN 20 only)	Video Loss is not supported in disk analysis. Disk analysis takes approximately 45 to 90 seconds depending on the amount of recorded data on the device.
Timeline Disk Analysis	Yes	
Video Export	Yes	There will be approximately four seconds of additional video exported prior to the specified start time.
TruVision Navigator Player	Yes	.mp4 proprietary file format.
PTZ Control	Yes	

Feature	Support	Notes
Focus, Iris, Zoom	Yes	PTZ protocol GE RS-485 does not support Focus and Iris commands in this release.
Presets	Yes	
Tours	Go To Record	Only one tour is supported (which is hard coded to Tour 1 on the PTZ camera).
Camera Search	Alarm Event Motion	
Smart Search	Yes (TVN 50 only)	
Point-of-Sale Text	Yes (TVN 50 only)	
Motion	Yes	Get the configuration for this device via TruVision Navigator and set the active zones on a per camera basis via the Motion Configuration option associated with each camera.
Audio	Yes	There are 16 audio inputs per device (one per channel). Enabling audio on the device is a per channel setting. Access the settings by going to the device configuration and enabling the audio option on the Recording tab for each camera. If enabled, as soon as any camera from the device is added in the TruVision Navigator Viewer and selected, the audio will play.
Bi-directional Audio	Yes	
Notifications	Alarm Video Loss Motion Disk Full Disk Failure	To setup the device to send TCP notifications for cameras, right-click the device in the Navigator and select **Configure Device**. On the Camera tab's Event Section, select the events and set the schedules as appropriate. On the Camera tab's Rules Section, for each event type, ensure that "notify me" is selected. Repeat for each event type. On the Notifications tab, the Notify IP Address should be the IP address of where the TruVision Navigator Server services are located (Notification Writer and Notification Processor). The Notify Port is defaulted to 5001 and is editable. Ensure this port matches the one listed in the TruVision Navigator Settings window, **Notifications** tab.

Feature	Support	Notes
		To setup the device to send TCP notifications for the device itself (e.g., Disk Full and Disk Failure), right-click the device in the Navigator and select **Configure Device**. On the Notification tab, for each notification type, ensure that “notify me” is selected. Repeat for each notification type and click **Save**. Ensure the notification port on the device matches that of TruVision Navigator Server as described above. Restart both the Notification Writer and Notification Processor for TruVision Navigator to process the notifications.
Health Diagnostics	IP Address MAC Address Model Name Serial Number Firmware Version Device Date/Time Total Device Health HDD Status HDD Capacity Cameras in Video Loss Cameras in Alarm Current Client Connections Record Status	
Firmware Upload	Yes	
Bulk Firmware Upload	Yes	
Device Configuration	Yes	
Bulk Configuration	Yes	
Remote Reboot	Yes	
IP Camera Support	Yes	
Device Log Support	Yes	
Trigger Outputs	Yes (TVN 10 / TVN50 only)	
Fisheye Dewarp	Yes (TVN 10 / TVN50 only)	
Get Thumbnail	No	
Change IP	Yes	
Activate	No	
Reset Password	Yes	
Change Password	Yes	
Excel Configuration Push	No	

Feature	Support	Notes
HTTPS	Yes (TVN 10 only)	
Reset Factory Default	Yes	
Sync Time (NTP)	Yes	

TruVision TVR 10 (DVR)

Feature	Support	Notes
Supported Firmware Versions	2.7	
H.265 Support	No	
Default Ports	Video = 8000 (editable) Command and Control = 8000 (editable) Configuration = 8000 (editable) Notifications = 5001 (editable) Firmware Upload = 8000 (editable)	
Default Username / Password	admin / 1234	We recommend changing this default password at the time of installation.
Default IP address	192.168.1.82	
Network Discovery	Supported	
Compression	H.264	
Connection Types	TCP UDP	
Streaming Limits	24 Live or Playback streams simultaneously with a maximum of six streams per channel.	If users try to open more streams than a recorder supports, they will get a black video tile containing an error message.
Stream Overlay	Camera Name Date and Time	
High / Low Bandwidth	No	
Dual Streaming	Yes	
Stream Nomenclature	The Main stream is referred to as: On-Screen-Display = Time Lapse	Event Stream is not supported on the device.

Feature	Support	Notes
	Web Browser = Main stream TruVision Navigator = Main stream The Substream is referred to as: On-Screen-Display = N/A Web Browser = Substream TruVision Navigator = Substream	
Playback Controls	Play Pause Frame Advance Fast Forward (1x, 2x,4x, 8x 16x) Slow motion (1.0x, 0.5x, 0.25x, 0.125x, 0.0625x)	Frame reverse and rewind speeds are not supported. Video jumps back four seconds after resuming playback from Fast Forward and Frame Advance. When fast forwarding video and it catches up to present time (or Live video), the video in the viewing tile remains paused until the user clicks the **Live** button in the Controller. No other playback controls will work until the **Live** button is selected.
Digital Zoom	Live and Playback	
Snapshot	Yes	
Local Record	Yes	Pause during local record is not supported.
Instant Replay	Yes	There is a two to five minute video buffer in the device. While video is in the buffer, it cannot be viewed. Once the buffer fills, the video is written to the hard drive and is available for playback. This affects Instant Replay and the Playback button in TruVision Navigator. Those two features get their time increment from the user-defined Instant Replay configuration in the TruVision Navigator Settings window, **Server** tab. As a result, set this time increment to greater than five minutes. If a search is executed for video still in the buffer, Live video appears.
Disk Analysis	Alarm Motion Recorded	Video Loss is not supported in disk analysis. Disk analysis takes approximately 15-45 seconds depending on the amount of recorded data on the device.
Time Line Disk Analysis	Yes	
Video Export	Yes	There will be approximately four seconds of additional video exported prior to the specified start time.
TruVision Navigator Player	Yes	.mp4 proprietary file format.
PTZ Control	Yes	

Feature	Support	Notes
Focus, Iris Control	Yes	
Presets	Yes	
Tours	Go To Record	Only one tour is supported (which is hard coded to Tour 1 on the PTZ camera).
Camera Search	Alarm Event Motion	
Smart Search	No	
Point-of-Sale Text	No	
Motion	Yes	Get the configuration for this device via TruVision Navigator and set the active zones on a per camera basis via the Motion Configuration option associated with each camera.
Audio	Yes	There is one audio input per device. That input can be mapped to any camera on the device simply by enabling audio on that camera. Access the setting by going to the device configuration and enabling the audio option for each camera. If enabled, as soon as any camera from the device is added in the TruVision Navigator Viewer and selected, the audio plays.
Bi-directional Audio	No	
Notifications	Alarm Video Loss Motion Disk Full Disk Failure	To set up the device to send TCP notifications for cameras, right-click the device in the Navigator and select **Configure Device**. On the Camera tab's Event Section, select the events and set the schedules as appropriate. On the Camera tab's Rules Section, for each event type, ensure that "notify me" is selected. Repeat for each event type. On the Notifications tab, the Notify IP Address should be the IP address of where the TruVision Navigator Server services are located (Notification Writer and Notification Processor). The Notify Port is defaulted to 5001 and is editable. Ensure this port matches the one listed in the TruVision Navigator Settings window, **Notifications** tab.

Feature	Support	Notes
		To set up the device to send TCP notifications for the device itself (e.g., Disk Full and Disk Failure), right-click the device in the Navigator and select **Configure Device**. For each notification type on the **Notifications** tab, ensure that “notify me” is selected. Repeat for each notification type and click **Save**. Ensure the notification port on the device matches that of TruVision Navigator Server as described above.
Health Diagnostics	IP Address MAC Address Model Name Serial Number Firmware Version Device Date/Time Total Device Health HDD Status HDD Capacity Cameras in Video Loss Cameras in Alarm Current Client Connections Record Status	
Firmware Upload	Yes	
Bulk Firmware Upload	Yes	
Device Configuration	Yes	
Bulk Configuration	Yes	
Remote Reboot	Yes	
IP Camera Support	N/A	
Device log support	Yes	
Trigger Outputs	Yes	
Fisheye Dewarp	N/A	
Sync Playback	No	
Get Thumbnail	No	
Change IP	Yes	
Activate	No	
Reset Password	Yes	
Change Password	Yes	

Feature	Support	Notes
Excel Configuration Push	No	
HTTPS	No	
Reset Factory Default	Yes	
Sync Time (NTP)	Yes	
Network Storage	Yes	
Backup & Restore System Config	Yes	
Dual NIC	No	
DDNS	No	
Mobile App	Yes	
RTSP Live	No	
RTSP Playback	No	
Thumbnail Search	No	

TruVision TVR 11 / TVR 12 (DVR)

Feature	Support	Notes
Firmware Versions	3.1.b (TVR 11/11C) 1.2.d (TVR 12/12C)	
H.265 Support	No	
Default Ports	Video = 8000 (editable) Command and Control = 8000 (editable) Configuration = 8000 (editable) Notifications = 5001 (editable) Firmware Upload = 8000 (editable)	
Default Username / Password	admin / 1234	We recommend changing this default password at time of installation.
Default IP Address	192.168.1.82	
Network Discovery	Supported	
Compression	H.264	

Feature	Support	Notes
Connection Types	TCP UDP	
Streaming Limits	64 Live or Playback streams including those used by the web page.	
Stream Overlay	Camera Name Date and Time	
High / Low Bandwidth	No	
Dual Streaming	Main streams and substreams are available on live view mode only.	
Stream Nomenclature	The Main stream is referred to as: On-Screen-Display = Time Lapse Web Browser = Time Lapse TruVision Navigator = Main stream The Substream is referred to as: On-Screen-Display = Alarm Web Browser = Alarm TruVision Navigator = Substream The Event stream is referred to as: On-Screen-Display = N/A Web Browser = Event TruVision Navigator = Event The Schedule stream is referred to as: On-Screen-Display = Schedule Web Browser = Schedule TruVision Navigator = Schedule	
Playback Controls	Play Pause Frame Advance Fast Forward (1x, 2x, 4x, 8x) Slow motion (1.0x, 0.5x, 0.25x, 0.125x, 0.0625x)	Video jumps back four seconds after resuming playback from Fast Forward and Frame Advance. When fast forwarding video and it catches up to present time (or live video), the video automatically switches to live view.

Feature	Support	Notes
	Rewind (1x, 2x, 4x) - Eight videos simultaneously	
Digital Zoom	Live and Playback	
Snapshot	Yes	
Local Record	Yes	
Instant Replay	Yes	There is a two to five minute video buffer in the device. While video is in the buffer, it cannot be viewed. Once the buffer fills, the video is written to the hard drive and is available for playback. This affects Instant Replay and the Playback button in TruVision Navigator. Those two features get their time increment from the user-defined Instant Replay configuration on the TruVision Navigator Server Properties tab. As a result, set this time increment to greater than five minutes. If a search is executed for video still in the buffer, Live video appears.
Disk Analysis	Alarm Motion Recorded	Video Loss is not supported in disk analysis. Disk analysis takes approximately 15-45 seconds depending on the amount of recorded data on the device.
Time Line Disk Analysis	Yes	
Video Export	Yes	There will be approximately four seconds of additional video exported prior to the specified start time.
TruVision Navigator Player	Yes	.mp4 proprietary file format.
PTZ Control	Yes	
Focus, Iris, Zoom	Yes	
Presets	Yes	
Tours	Go To Record	Only one tour is supported (which is hard coded to Tour 1 on the PTZ camera).
Camera Search	Alarm Event Motion Text	
Smart Search	Yes	
POS Text	Yes	
Motion	Yes	Get the configuration for this device via TruVision Navigator and set the active zones on a per camera basis via the Motion Configuration option associated with each camera.

Feature	Support	Notes
Audio	Yes	There are four audio inputs per device. That input can be mapped to any camera on the device simply by enabling audio on that camera. Access the setting by going to the device configuration and enabling the audio option for each camera. If enabled, as soon as any camera from the device is added in the TruVision Navigator Viewer and selected, the audio plays.
Bi-directional Audio	Yes	
Notifications	Alarm Video Loss Motion Disk Full Disk Failure	To set up the device to send TCP notifications for cameras, right-click the device in the Navigator and select **Configure Device**. On the Camera tab's Event Section, select the events and set the schedules as appropriate. On the Camera tab's Rules Section, for each event type, ensure that "notify me" is selected. Repeat for each event type. On the Notifications tab, the Notify IP Address should be the IP address of where the TruVision Navigator Server services are located (Notification Writer and Notification Processor). The Notify Port is defaulted to 5001 and is editable. Ensure this port matches the one listed in the TruVision Navigator Settings window, **Notifications** tab. To set up the device to send TCP notifications for the device itself (e.g., Disk Full and Disk Failure), right-click the device in the Navigator and select **Configure Device**. On the **Notifications** tab, for each notification type, ensure that "notify me" is selected. Repeat for each notification type and click Save. Ensure the notification port on the device matches that of TruVision Navigator Server as described above. Restart the Notification Processor service for TruVision Navigator to process the notifications. Email notification is not supported at the device-level.
Health Diagnostics	IP Address MAC Address Model Name Serial Number Firmware Version Device Date/Time Total Device Health HDD Status HDD Capacity Cameras in Video Loss	

Feature	Support	Notes
	Cameras in Alarm Current Client Connections Record Status	
Bulk Firmware Upload	Yes	
Device Configuration	Yes	
Bulk Configuration	Yes	
Remote Reboot	Yes	
IP Camera Support	N/A	
Device Log Support	Yes	
Trigger Outputs	Yes	
Fisheye Dewarp	N/A	
Get Thumbnail	No	
Change IP	Yes	
Activate	Yes	
Reset Password	Yes	
Change Password	Yes	
Excel Configuration Push	No	
HTTPS	No	
Reset Factory Default	Yes	
Sync Time (NTP)	Yes	
Thumbnail Search	No	

TruVision TVR 40 (DVR)

Feature	Support	Notes
Supported Firmware Versions	3.2.d	
H.265 Support	No	
Default Ports	Video = 8000 (editable) Command and Control = 8000 (editable)	

Feature	Support	Notes
	Configuration = 8000 (editable) Notifications = 5001 (editable) Firmware Upload = 8000 (editable)	
Default Username / Password	Administrator / 3477	We recommend changing this default password at time of installation.
Default IP Address	192.168.1.82	
Network Discovery	Supported	
Compression	H.264	
Connection Types	TCP UDP	
Streaming Limits	24 Live or Playback streams simultaneously with a maximum of six streams per channel.	If users try to open more streams than a recorder supports, they will get a black video tile containing an error message.
Stream Overlay	Camera Name Date and Time	
High / Low Bandwidth	No	
Dual Streaming	Yes	
Stream Nomenclature	The Main stream is referred to as: On-Screen-Display = Schedule Web Browser = Main stream TruVision Navigator = Main stream The Substream is referred to as: On-Screen-Display = N/A Web Browser = Substream TruVision Navigator = Substream The Event stream is referred to as: On-Screen-Display = Event Web Browser = Event TruVision Navigator = Event	The Substream, Event, and Time Lapse streams are derivative configurations of the Main stream. Typically, the Main stream is recorded on a schedule, the Event stream is recorded on Event, the Time Lapse stream is recorded continuously, and the Substream can be viewed Live.

Feature	Support	Notes
	The Time Lapse stream is referred to as: On-Screen-Display = Time Lapse Web Browser = Time Lapse TruVision Navigator = Time Lapse	
Playback Controls	Play Pause Frame Advance Fast Forward (1x, 2x,4x, 8x 16x) Slow motion (1.0x, 0.5x, 0.25x, 0.125x, 0.0625x)	Frame Reverse and Rewind Speeds are not supported. Video jumps back four seconds after resume playback from Fast Forward and Frame Advance. When fast forwarding video and it catches up to present time (or Live video), the video in the viewing tile remains paused until the user clicks the **Live** button in the Controller. No other playback controls will work until the **Live** button is selected.
Digital Zoom	Live and playback	
Snapshot	Yes	
Local Record	Yes	Pause during local record is not supported.
Instant Replay	Yes	There is a two to five-minute video buffer in the device. While video is in the buffer, it cannot be viewed. After the buffer fills, the video is written to the hard drive and is available for playback. This affects Instant Replay and the Playback button in TruVision Navigator. Those two features get their time increment from the user-defined Instant Replay configuration on the TruVision Navigator Settings window, **Server** tab. As a result, this time should be set to an increment to greater than five minutes. If a search is executed for video still in the buffer, Live video appears.
Disk Analysis	Alarm Motion Recorded Untagged	Video Loss is not supported in disk analysis. Disk analysis takes approximately 45 to 90 seconds depending on the amount of recorded data on the device.
Timeline Disk Analysis	Yes	
Video Export	Yes	There will be approximately four seconds of additional video exported prior to the specified start time.
TruVision Navigator Player	Yes	.mp4 proprietary file format.
PTZ Control	Yes	
Focus, Iris, Zoom	Yes	PTZ protocol GE RS-485 does not support Focus and Iris commands in this release.
Presets	Yes	

Feature	Support	Notes
Tours	Go To Record	Only one tour is supported (which is hard coded to Tour 1 on the PTZ camera).
Camera Search	Alarm Event Motion Text	
Smart Search	No	
Point-of-Sale Text	Yes	Overlay on video only. To display POS data on top of the camera view, right-click the POS-configured camera's video tile and select **POS Mode** > **In Band**.
Motion	Yes	Get the configuration for this device via TruVision Navigator and set the active zones on a per camera basis via the Motion Configuration option associated with each camera.
Audio	Yes	There are 16 audio inputs per device (one per channel). Enabling audio on the device is a per channel setting. Access the settings by going to the device configuration and enabling the audio option on the Recording tab for each camera. If enabled, as soon as any camera from the device is added in the TruVision Navigator Viewer and selected, the audio will play.
Bi-directional Audio	Yes	
Notifications	Alarm Video Loss Motion Disk Full Disk Failure	To set up the device to send TCP notifications for cameras, right-click the device in the Navigator and select **Configure Device**. On the Camera tab's Event Section, select the events and set the schedules as appropriate. On the Camera tab's Rules Section, for each event type, ensure that "notify me" is selected. Repeat for each event type. On the **Notifications** tab, the Notify IP Address should be the IP address of where the TruVision Navigator Server services are located (Notification Writer and Notification Processor). The Notify Port is defaulted to 5001 and is editable. Ensure this port matches the one listed in the TruVision Navigator Settings window, **Notifications** tab.

Feature	Support	Notes
		To set up the device to send TCP notifications for the device itself (e.g., Disk Full and Disk Failure), right-click the device in the Navigator and select **Configure Device**. On the **Notification** tab, for each notification type, ensure that “notify me” is selected. Repeat for each notification type and click **Save**. Ensure the notification port on the device matches that of TruVision Navigator Server as described above. Restart the Notification Processor service for TruVision Navigator to process the notifications.
Health Diagnostics	IP Address MAC Address Model Name Serial Number Firmware Version Device Date/Time Total Device Health HDD Status HDD Capacity Cameras in Video Loss Cameras in Alarm Current Client Connections Record Status	
Firmware Upload	Yes	
Bulk Firmware Upload	Yes	
Device Configuration	Yes	
Bulk Configuration	Yes	
Remote Reboot	Yes	
IP Camera Support	N/A	
Device Log Support	Yes	
Trigger Outputs	Yes	
Fisheye Dewarp	N/A	
Get Thumbnail	No	
Change IP	Yes	
Activate	No	
Reset Password	Yes	
Change Password	Yes	

Feature	Support	Notes
Excel Configuration Push	No	
HTTPS	No	
Reset Factory Default	Yes	
Sync Time (NTP)	Yes	

TruVision TVR 41 / TVR42 (DVR)

Feature	Support	Notes
Supported Firmware Versions	3.0c (TVR 41) 1.2d (TVR 42)	
Support H.265	No	
Default Ports	Video = 8000 (editable) Command and Control = 8000 (editable) Configuration = 8000 (editable) Notifications = 5001 (editable) Firmware Upload = 8000 (editable)	
Default Username / Password	admin / 1234	We recommend changing this default password at time of installation.
Default IP Address	192.168.1.82	
Network Discovery	Supported	
Compression	H.264	
Connection Types	TCP UDP	
Streaming Limits	64 Live or Playback streams simultaneously including those used by the web alarm.	
Stream Overlay	Camera Name Date and Time	
High / Low Bandwidth	No	
Dual Streaming	Yes	

Feature	Support	Notes
Stream Nomenclature	The Main stream is referred to as: On-Screen-Display = Time Lapse Web Browser = Time Lapse TruVision Navigator = Main stream The Substream is referred to as: On-Screen-Display = Alarm Web Browser = Alarm TruVision Navigator = Substream The Event stream is referred to as: On-Screen-Display = N/A Web Browser = Event TruVision Navigator = Event The Schedule stream is referred to as: On-Screen-Display = Schedule Web Browser = Schedule TruVision Navigator = Schedule	
Playback Controls	Play Pause Frame Advance Fast Forward (1x, 2x, 4x, 8x) Slow motion (1.0x, 0.5x, 0.25x, 0.125x, 0.0625x) Rewind (1x, 2x, 4x) -8 simultaneously	Video jumps back four seconds after resume playback from Fast Forward and Frame Advance. When fast forwarding video and it catches up to present time (or Live video), the video in the viewing tile remains paused until the user clicks the **Live** button in the Controller. No other playback controls will work until the **Live** button is selected.
Digital Zoom	Live & Playback	
Snapshot	Yes	
Local Record	Yes	
Instant Replay	Yes	
Disk Analysis	Alarm Motion Recorded	Video Loss is not supported in disk analysis. Disk analysis takes approximately 15-45 seconds depending on the amount of recorded data on the device.

Feature	Support	Notes
	Untagged	
Timeline Disk Analysis	Yes	
Video Export	Yes	There will be approximately four seconds of additional video exported prior to the specified start time.
TruVision Navigator Player	Yes	.mp4 proprietary file format.
PTZ Control	Yes	
Focus, Iris, Zoom	Yes	
Presets	Yes	
Tours	Go To Record	Only one tour is supported (which is hard coded to Tour 1 on the PTZ camera).
Camera Search	Alarm Event Motion Text	
Smart Search	Yes	Browser only
Point-of-Sale Text	Yes	
Motion	Yes	Get the configuration for this device via TruVision Navigator and set the active zones on a per camera basis via the Motion Configuration option associated with each camera.
Audio	Yes	There are four audio inputs per device. That input can be mapped to any camera on the device simply by enabling audio on that camera. Access the setting by going to the device configuration, and enabling the audio option on the Recording tab for each camera. If enabled, as soon as any camera from the device is added in the TruVision Navigator Viewer and selected, the audio will play.
Bi-directional Audio	Yes	

Feature	Support	Notes
Notifications	Alarm Video Loss Motion Disk Full Disk Failure	To set up the device to send TCP notifications for cameras, right-click the device in the Navigator and select **Configure Device**. On the Camera tab's Event Section, select the events and set the schedules as appropriate. On the Camera tab's Rules Section, for each event type, ensure that "notify me" is selected. Repeat for each event type. On the Notifications tab, the Notify IP Address should be the IP address of where the TruVision Navigator Server services are located (Notification Writer and Notification Processor). The Notify Port is defaulted to 5001 and is editable. Ensure this port matches the one listed in the TruVision Navigator Settings window, **Notifications** tab. To set up the device to send TCP notifications for the device itself (e.g., Disk Full and Disk Failure), right-click the device in the Navigator and select **Configure Device**. On the **Notification** tab, for each notification type, ensure that "notify me" is selected. Repeat for each notification type and click **Save**. Ensure the notification port on the device matches that of TruVision Navigator Server as described above. Restart the Notification Processor service for TruVision Navigator to process the notifications. Email notification is not supported at the device-level.
Health Diagnostics	IP Address MAC Address Model Name Serial Number Firmware Version Device Date/Time Total Device Health HDD Status HDD Capacity Cameras in Video Loss Cameras in Alarm Current Client Connections Record Status	
Firmware Upload	Yes	
Bulk Firmware Upload	Yes	
Device Configuration	Yes	
Bulk Configuration	Yes	
Remote Reboot	Yes	

Feature	Support	Notes
IP Camera Support	N/A	
Device Log Support	Yes	
Trigger Outputs	Yes	
Fisheye Dewarp	N/A	
Get Thumbnail	No	
Change IP	Yes	
Activate	No	
Reset Password	Yes	
Change Password	Yes	
Excel Configuration Push	No	
HTTPS	No	
Reset Factory Default	Yes	
Sync Time (NTP)	Yes	

TruVision TVR 60 (Hybrid DVR)

Feature	Support	Notes
Supported Firmware Versions	4.7a	
Support H.265	No	
Default Ports	Video = 8000 (editable) Command and Control = 8000 (editable) Configuration = 8000 (editable) Notifications = 5001 (editable) Firmware Upload = 8000 (editable)	
Default Username / Password	admin / 1234	We recommend changing this default password at time of installation.
Default IP Address	192.168.1.82	
Network Discovery	Supported	
Compression	H.264	
Connection Types	TCP UDP	

Feature	Support	Notes
Streaming Limits	48 Live or Playback streams simultaneously with a maximum of six streams per channel.	If users try to open more streams than a recorder supports, they will get a black video tile containing an error message.
Stream Overlay	Camera Name Date and Time	
High / Low Bandwidth	No	
Dual Streaming	Yes	
Stream Nomenclature	The Main stream is referred to as: On-Screen-Display = Time Lapse Web Browser = Time Lapse TruVision Navigator = Main stream The Substream is referred to as: On-Screen-Display = Alarm Web Browser = Alarm TruVision Navigator = Substream The Event stream is referred to as: On-Screen-Display = N/A Web Browser = Event TruVision Navigator = Event The Schedule stream is referred to as: On-Screen-Display = Schedule Web Browser = Schedule TruVision Navigator = Schedule	
Playback Controls	Play Pause Frame Advance Fast Forward (1x, 2x,4x, 8x,16x) Slow motion (1.0x, 0.5x, 0.25x, 0.125x, 0.0625x)	Frame Reverse, Rewind, and Playback Speeds are not supported. Video jumps back four seconds after resume playback from Fast Forward and Frame Advance.

Feature	Support	Notes
		When fast forwarding video and it catches up to present time (or Live video), the video in the viewing tile will remain paused until the user clicks the **Live** button in the Controller. No other playback controls will work until the **Live** button is selected.
Digital Zoom	Live & Playback	
Snapshot	Yes	
Local Record	Yes	Pause during local record is not supported.
Instant Replay	Yes	There is a two to five minute video buffer in the device. While video is in the buffer, it cannot be viewed. Once the buffer fills, the video is written to the hard drive and is available for playback. This affects Instant Replay and the Playback button in TruVision Navigator. Those two features get their time increment from the user-defined Instant Replay configuration in the TruVision Navigator Settings window, **Server** tab. As a result, set this time increment to greater than five minutes. If a search is executed for video still in the buffer, Live video appears.
Disk Analysis	Alarm Motion Recorded Untagged	Video Loss is not supported in disk analysis. Disk analysis takes approximately 45 to 90 seconds depending on the amount of recorded data on the device.
Timeline Disk Analysis	Yes	
Video Export	Yes	There will be approximately four seconds of additional video exported prior to the specified start time.
TruVision Navigator Player	Yes	.mp4 proprietary file format.
PTZ Control	Yes	
Focus, Iris, Zoom	Yes	PTZ protocol GE RS-485 does not support Focus and Iris commands in this release.
Presets	Yes	
Tours	Go To Record	Only one tour is supported (which is hard coded to Tour 1 on the PTZ camera).
Camera Search	Alarm Event Motion	
Smart Search	No	
Point-of-Sale Text	No	
Motion	Yes	Get the configuration for this device via TruVision Navigator and set the active zones on a per camera basis via the Motion Configuration option associated with each camera.

Feature	Support	Notes
Audio	Yes	There are 16 audio inputs per device (one per channel). Enabling audio on the device is a per channel setting. Access the settings by going to the device configuration and enabling the audio option on the Recording tab for each camera. If enabled, as soon as any camera from the device is added in the TruVision Navigator Viewer and selected, the audio will play.
Notifications	Alarm Video Loss Motion Disk Full Disk Failure	To setup the device to send TCP notifications for cameras, right-click the device in the Navigator and select **Configure Device**. On the Camera tab's Event Section, select the events and set the schedules as appropriate. On the Camera tab's Rules Section, for each event type, ensure that "notify me" is selected. Repeat for each event type. On the Notification tab, the Notify IP Address should be the IP address of where the TruVision Navigator Server services are located (Notification Writer and Notification Processor). The Notify Port is defaulted to 5001 and is editable. Ensure this port matches the one listed in the TruVision Navigator Settings window, **Notifications** tab. To setup the device to send TCP notifications for the device itself (e.g., Disk Full and Disk Failure), right-click the device in the Navigator and select **Configure Device**. On the Notification tab, for each notification type, ensure that "notify me" is selected. Repeat for each notification type and click **Save**. Ensure the notification port on the device matches that of TruVision Navigator Server as described above. Restart both the Notification Writer and Notification Processor for TruVision Navigator to process the notifications.
Health Diagnostics	IP Address MAC Address Model Name Serial Number Firmware Version Device Date/Time Total Device Health HDD Status HDD Capacity Cameras in Video Loss Cameras in Alarm Current Client Connections Record Status	
Firmware Upload	Yes	

Feature	Support	Notes
Bulk Firmware Upload	Yes	
Device Configuration	Yes	
Bulk Configuration	Yes	
Remote Reboot	Yes	
IP Camera Support	Yes	
Device Log Support	Yes	
Trigger Outputs	Yes	
Fisheye Dewarp	N/A	
Get Thumbnail	No	
Change IP	Yes	
Activate	No	
Reset Password	Yes	
Change Password	Yes	
Excel Configuration Push	No	
HTTPS	No	
Reset Factory Default	Yes	
Sync Time (NTP)	Yes	

DVSRxU

Feature	Support	Notes
Supported Firmware Versions	2.31s	
H.265 Support	No	
Default Ports	Video = 8000 (editable) Command and Control = 8000 (editable) Configuration = 8000 (editable) Notifications = 5001 (editable) Firmware Upload = 8000 (editable)	
Default Username / Password	Administrator / 3477	We recommend changing this default password at time of installation.

Feature	Support	Notes
Default IP address	192.168.1.10	
Network Discovery	Supported	
Compression	H.264	
Connection Types	TCP UDP	
Streaming Limits	24 Live or Playback streams simultaneously with a maximum of six streams per channel.	If users try to open more streams than a recorder supports, they will get a black video tile containing an error message.
Stream Overlay	Camera Name Date and Time	
High / Low Bandwidth	No	
Dual Streaming	Yes	
Stream Nomenclature	The Main stream is referred to as: On-Screen-Display = Schedule Web Browser = Main stream TruVision Navigator = Main stream The Substream is referred to as: On-Screen-Display = N/A Web Browser = Substream TruVision Navigator = Substream The Event stream is referred to as: On-Screen-Display = Event Web Browser = Event TruVision Navigator = Event The Time Lapse stream is referred to as: On-Screen-Display = Time Lapse Web Browser = Time Lapse TruVision Navigator = Time Lapse	The Substream, Event, and Time Lapse streams are derivative configurations of the Main stream. Typically, the Main stream is recorded on a schedule, the Event stream is recorded on Event, the Time Lapse stream is recorded continuously, and the Substream can be viewed Live.

Feature	Support	Notes
Playback Controls	Play Pause Frame Advance Fast Forward (2x, 4x)	Frame reverse, rewind, and playback speeds are not supported. Video jumps back four seconds after resume playback from Fast Forward and Frame Advance. When fast forwarding video and it catches up to present time (or Live video), the video in the viewing tile will remain paused until the user clicks the **Live** button in the Controller. No other playback controls will work until the **Live** button is selected.
Digital Zoom	Live and Playback	
Snapshot	Yes	
Local Record	Yes	Pause during local record is not supported.
Instant Replay	Yes	There is a two to five minute video buffer in the device. While video is in the buffer, it cannot be viewed. Once the buffer fills, the video is written to the hard drive and is available for playback. This affects Instant Replay and the Playback button in TruVision Navigator. Those features get their time increment from the user-defined Instant Replay configuration in the TruVision Navigator Settings window, **Server** tab. As a result, set this time increment to greater than five minutes. If a search is executed for video still in the buffer, Live video appears.
Disk Analysis	Alarm Motion Recorded	Video Loss is not supported in disk analysis. Disk analysis takes approximately 45-90 seconds depending on the amount of recorded data on the device.
Time Line Disk Analysis	Yes	
Video Export	Yes	There will be approximately four seconds of additional video exported prior to the specified start time.
TruVision Navigator Player	Yes	.mp4 proprietary file format.
PTZ Control	Yes	
Focus, Iris, Zoom	Yes	PTZ protocol GE RS-485 does not support Focus and Iris commands in this release.
Presets	Yes	
Tours	Go To Record	Only one tour is supported (which is hard coded to Tour 1 on the PTZ camera)
Camera Search	Alarm Event Motion Text	

Feature	Support	Notes
Smart Search	No	
Point-of-Sale Text	Yes	Overlay on video only. To display POS data on top of the camera view, right-click the POS-configured camera's video tile and select **POS Mode** > **In Band**.
Motion	Yes	Get the configuration for this device via TruVision Navigator and set the active zones on a per camera basis via the Motion Configuration option associated with each camera.
Audio	Yes	There are 16 audio inputs per device (one per channel). Enabling audio on the device is a per channel setting. Access the settings by going to the device configuration and enabling the audio option on the Recording tab for each camera. If enabled, as soon as any camera from the device is added in the TruVision Navigator Viewer and selected, the audio will play.
Bi-directional Audio	Yes	
Notifications	Alarm Video Loss Motion Disk Full Disk Failure	To set up the device to send TCP notifications for cameras, right-click the device in the Navigator and select **Configure Device**. On the Camera tab's Event Section, select the events and set the schedules as appropriate. On the Camera tab's Rules Section, for each event type, ensure that "notify me" is selected. Repeat for each event type. On the Notifications tab, the Notify IP Address should be the IP address of where the TruVision Navigator Server services are located (Notification Writer and Notification Processor). The Notify Port is defaulted to 5001 and is editable. Ensure this port matches the one listed in the TruVision Navigator Settings window, **Notifications** tab. To set up the device to send TCP notifications for the device itself (e.g., Disk Full and Disk Failure), right-click the device in the Navigator and select **Configure Device**. For each notification type on the **Notification** tab, ensure that "notify me" is selected. Repeat for each notification type and click **Save**. Ensure the notification port on the device matches that of TruVision Navigator Server as described above. Restart both the Notification Writer and Notification Processor for TruVision Navigator to process the notifications. Email notification is not supported at the device-level.
Health Diagnostics	IP Address MAC Address Model Name Serial Number	

Feature	Support	Notes
	Firmware Version	
	Device Date/Time	
	Total Device Health	
	HDD Status	
	HDD Capacity	
	Cameras in Video Loss	
	Cameras in Alarm	
	Current Client Connections	
	Record Status	
Firmware Upload	Yes	
Bulk Firmware Upload	Yes	
Device Configuration	Yes	
Bulk Configuration	Yes	
Remote Reboot	Yes	
IP Camera Support	N/A	
Device Log Support	Yes	
Trigger Outputs	Yes	
Fisheye Dewarp	No	
Get Thumbnail	No	
Change IP	Yes	
Activate	No	
Reset Password	Yes	
Change Password	Yes	
Excel Configuration Push	No	
HTTPS	No	
Reset Factory Default	No	

Capabilities (Properties dialog)

Right-click a first-generation recorder in the Navigator panel and select **Properties** to display the Properties window.

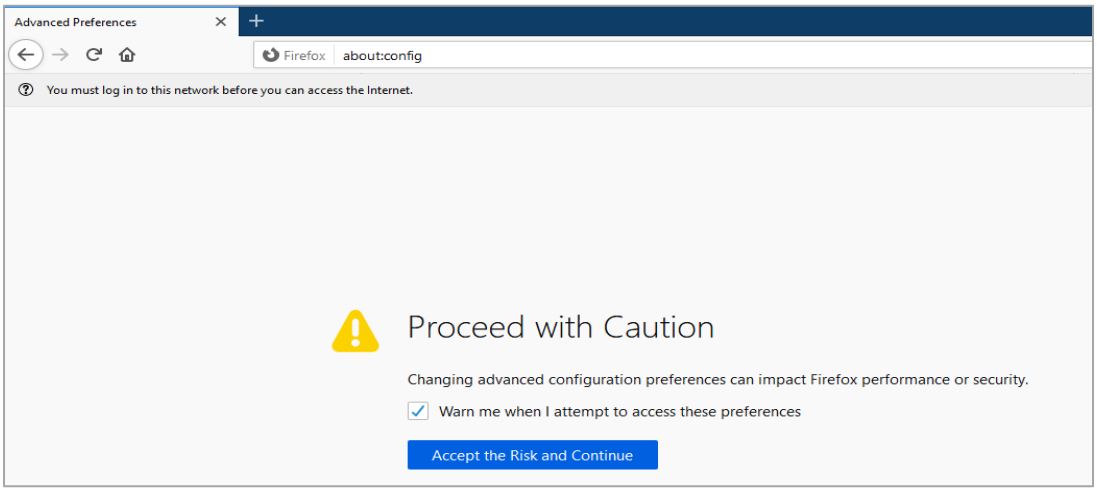
The **Capabilities** tab contains a read-only list that indicates which video, camera, and device controls as well which connection types are supported.

Appendix C
Web browser settings for self-signed certificates

Mozilla Firefox

See also: https://support.mozilla.org/en-US/questions/1232718

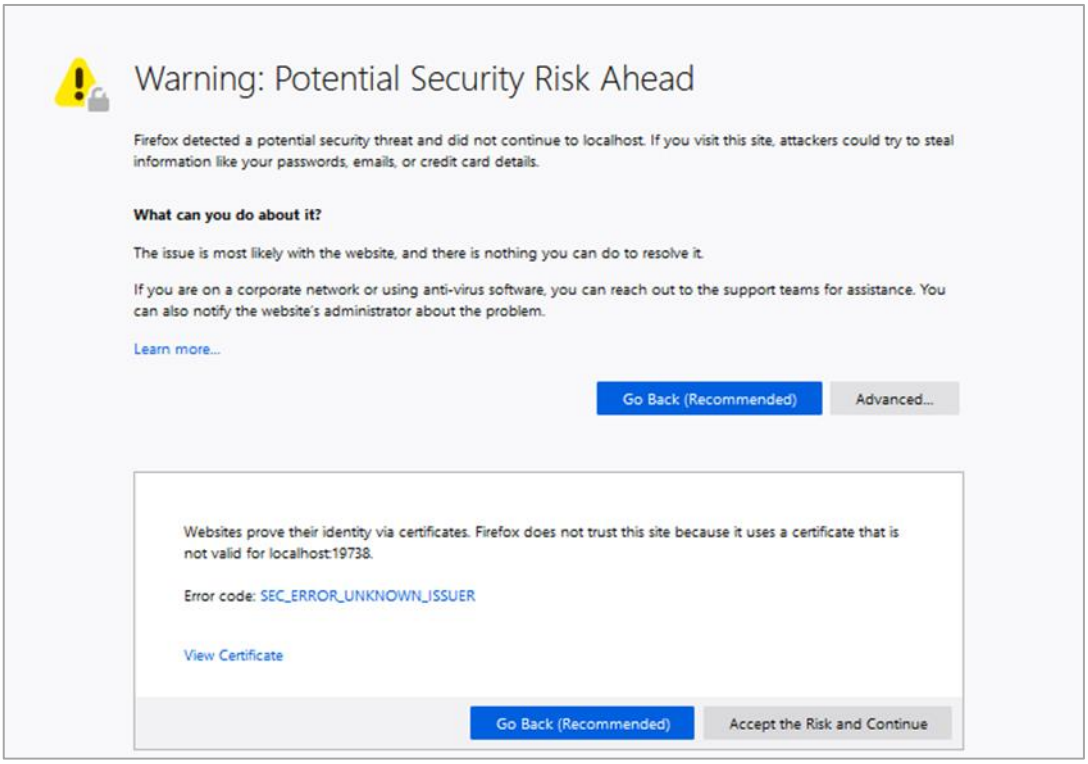
1. Open a new tab in the Firefox web browser. Type “about:config” (without quote marks) into the address bar and press enter on the keyboard.
2. Click the **Accept the Risk and Continue** button (see graphic below).



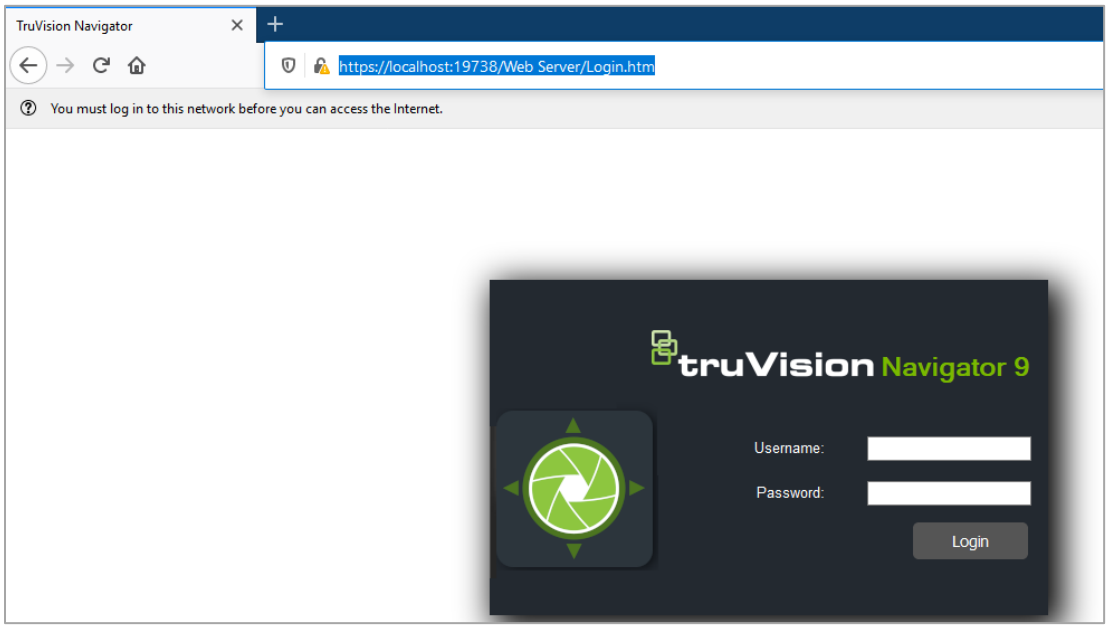
3. In the web browser search bar type “security.enterprise_roots.enabled” (without quote marks) and press enter on the keyboard (see graphic below).

4. Double-click **True** and it will change to **False** (see graphic below). Make sure that “security.enterprise_roots.enabled” is set to False.

5. Open a new tab and paste the web page URL in the address bar. Click **Advanced**. You will get a warning (see graphic below).

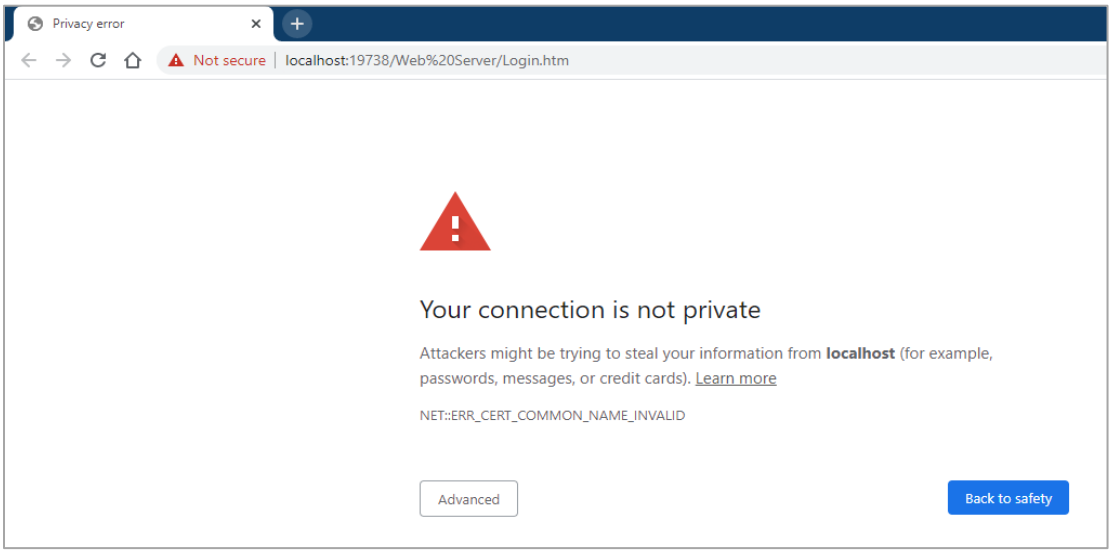


6. Click **Accept the Risk and Continue**. The TruVision Navigator login screen will be displayed (see graphic below).

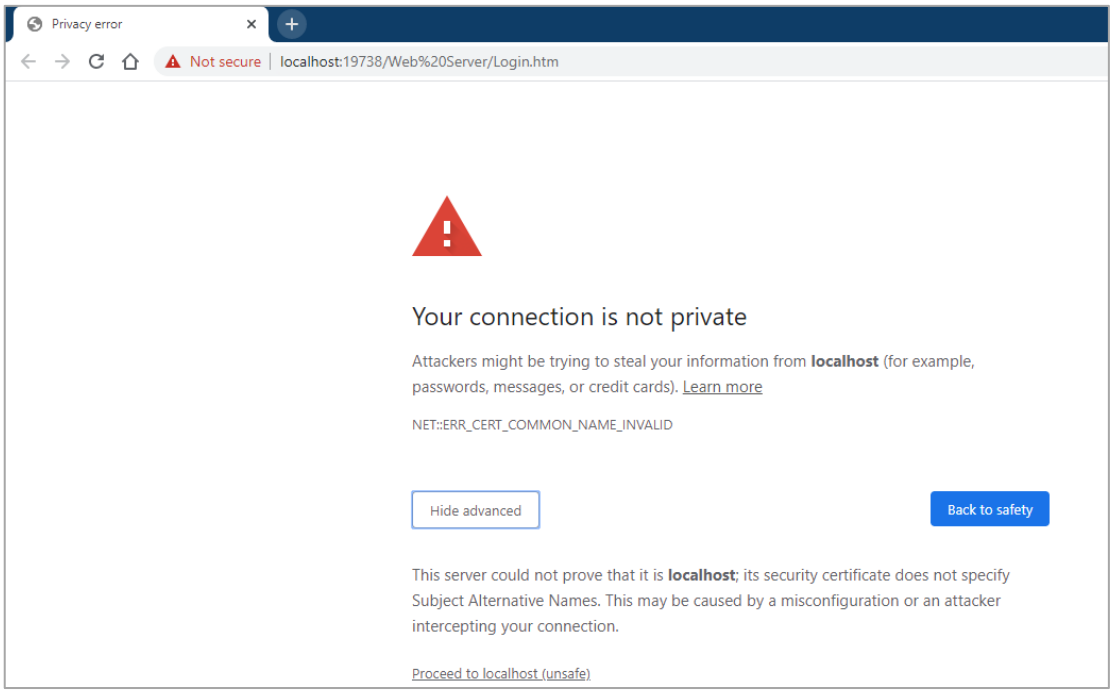


Google Chrome

1. Open a new tab in the Chrome web browser and paste the web page URL in the address bar. A warning will be displayed (see graphic below).



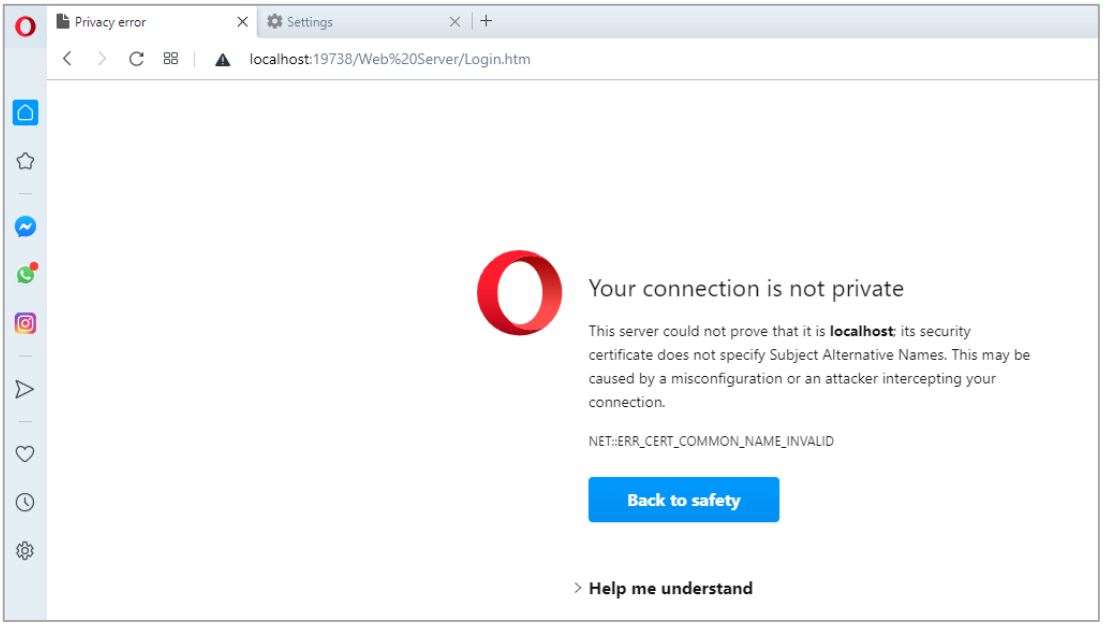
2. Click **Advanced**. A warning will be displayed (see graphic below). Click **Proceed to 'Name of the webpage'**.



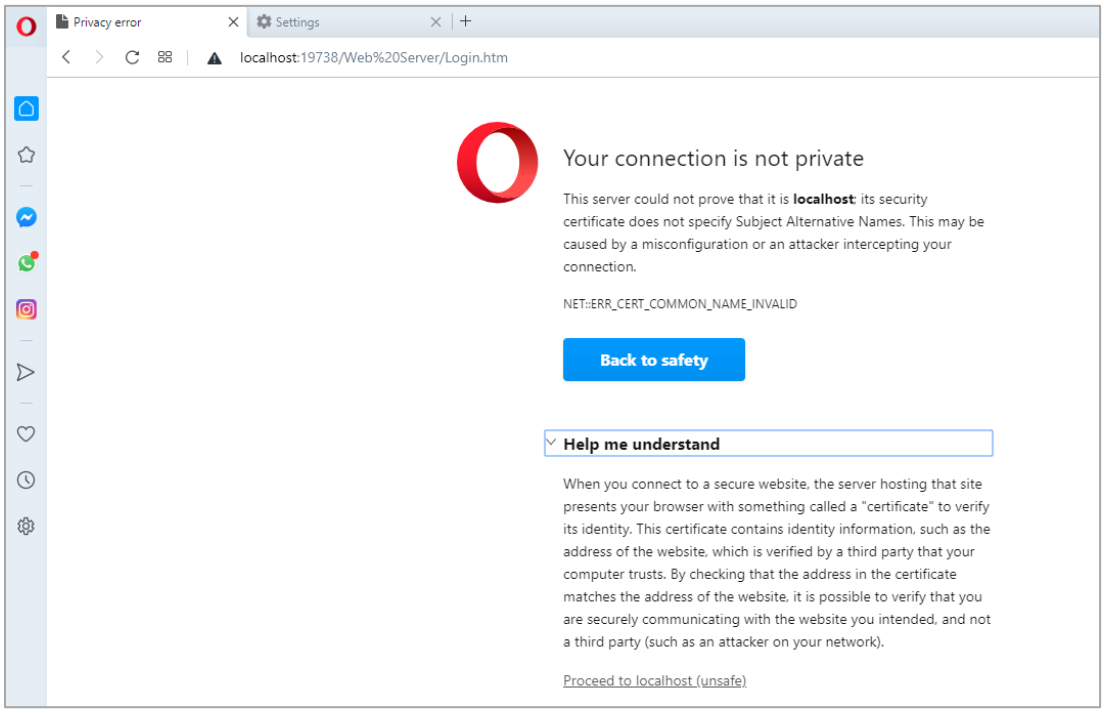
TruVision Navigator login screen will be displayed.

Opera

1. Open new tab and paste the web page URL in the address bar. A warning will be displayed (see graphic below).



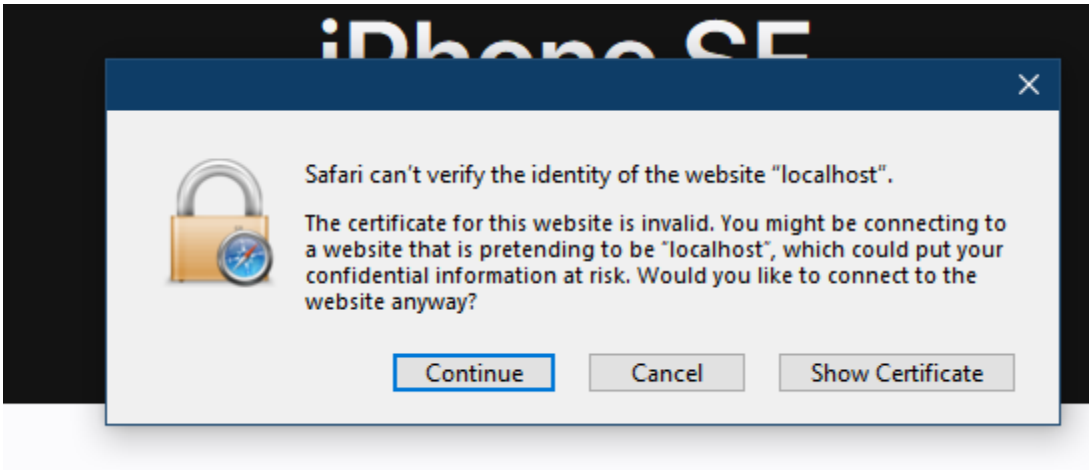
2. Click **Help me understand**. A warning will be displayed (see graphic below). Click **Proceed to 'Name of the webpage'**.



TruVision Navigator login screen will be displayed.

Apple Safari

1.Open new tab and paste the web page URL in the address bar. A warning will be displayed (see graphic below).



2.Click **Continue**. TruVision Navigator login screen will be displayed.

Appendix D
Configure Zenitel IP speakers

Introduction

Users can upload a wide range of announcement and warning audio clips. These clips can be played by users while they are viewing live video from cameras. This functionality allows relevant audio cues or messages to be added with conjunction with the visual feed or specific actions.

This appendix describes how to configure Zenitel IP speakers, so they can be used with TruVision Navigator.

The following Zenitel IP speakers can be used:

SKU	Description
STENTO-1023300011	IP Ceiling Speaker w/Mic (ELSIR-10CM)
STENTO-1023301311	IP Horn Speaker w/Mic (ELSII-10HM)
STENTO-1023301321	IP Long Horn Speaker w/Mic (ELSII-10LHM)
STENTO-1023302330	IP Cabinet Speaker w/Mic (ELSII-10WM)
STENTO-1023302340	IP Projector Speaker w/Mic (ELSII-10PM)

Note: The speakers integrate into TruVision Navigator via the ONVIF protocol.

Supported features in TruVision Navigator:

•Discovery of the speakers on the network

•Add the speakers to a specific speaker group

•Play manually sound clips that are stored in the internal memory of the speaker

•Use the speakers as Actions in the Event-Actions feature

•Show the speakers on a map

Note: To configure IP speakers please follow the procedures below.

IP Speaker initial setup

The Zenitel IP speakers are equipped with an embedded web interface that makes it possible to manage the speakers through a standard web browser login.

To access the IP speaker, your PC and the device must be connected to a PoE switch using network cables:

1. Connect the PC to a port on the network switch.
2. Connect the IP speaker to a PoE port on the network switch.
3. When the IP speaker is connected to the network, the IP address of the device is automatically assigned in one of two ways:

   - An IP address is automatically obtained from a DHCP server if a DHCP server is present on the network.

   - If no DHCP server exists, a random IP address (in the range 169.254.x.x) will be assigned.
4. To determine the IP address of the Zenitel speaker:

   - Connect a button to input 1 of the speaker's module.

   - During start-up (connecting a PoE cable) press the button.

   - You will hear the speaker's IP address.
5. Open a web browser and add the speaker's IP address.
6. Log in with the following credentials:

   - Username: admin

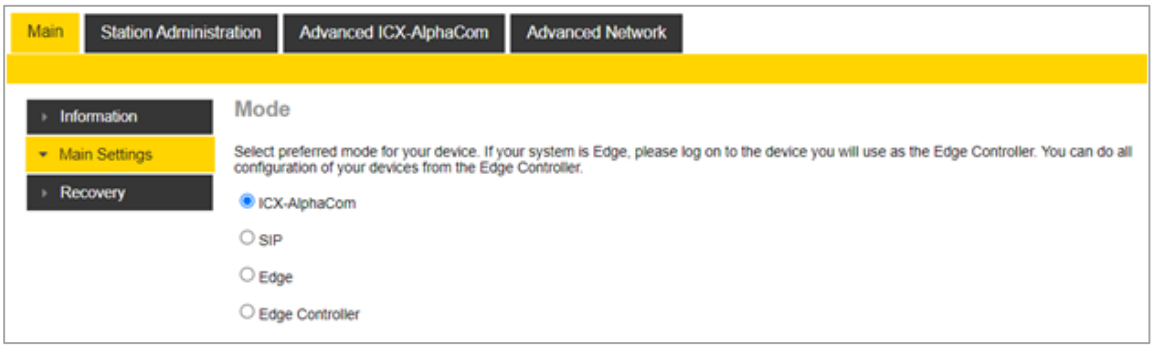
   - Password: alphaadmin

Configure working mode

By default, the IP speaker will have four working modes. To configure the I/O settings of the IP speaker, the working mode ICX-AlphaCom must be selected.

To set the correct working mode:

1. Login to the web page of the IP speaker.
2. Go to the **Main Tab** and click **Main Settings**.
3. In the **Main Settings**, you will find all the available modes.
4. Choose **ICX-AlphaCom** mode from the list.
5. Click the **Save** button to save the changes.



Then you need to configure the I/O settings. You need to change the I/O pins to act as outputs.

Configure I/O settings

To configure the I/O settings:

1.Go to the **Advanced ICX-AlphaCom** Tab.

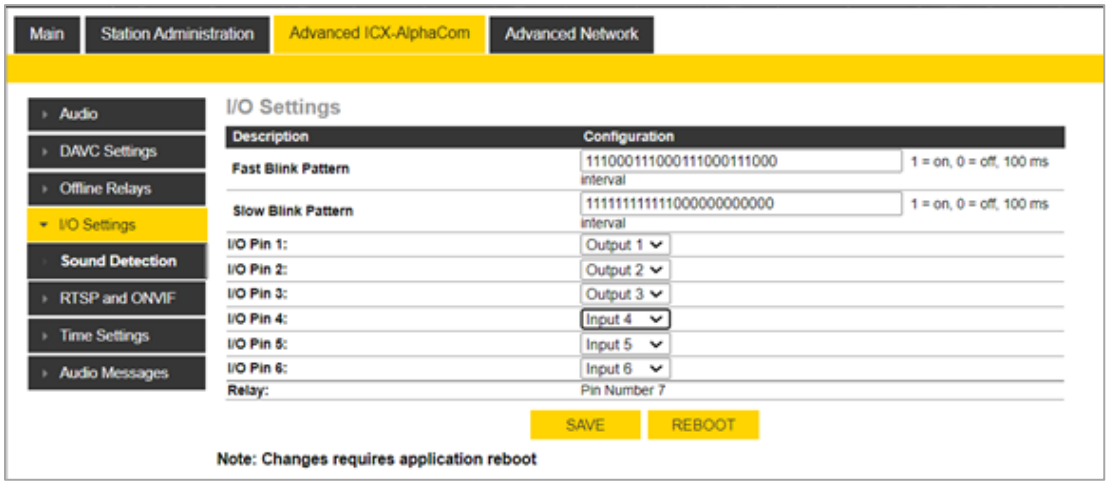
2.Click **I/O Settings**.

3.In the I/O Settings, change the configuration of the I/O pins to act as outputs.

4.After making the desired changes, click the **Save** button.

5.Click **Reboot** to reboot the IP speaker.

Note: These changes require speaker reboot for the settings to take effect.



Then you need to make sure that the IP speaker can be discovered as ONVIF device.

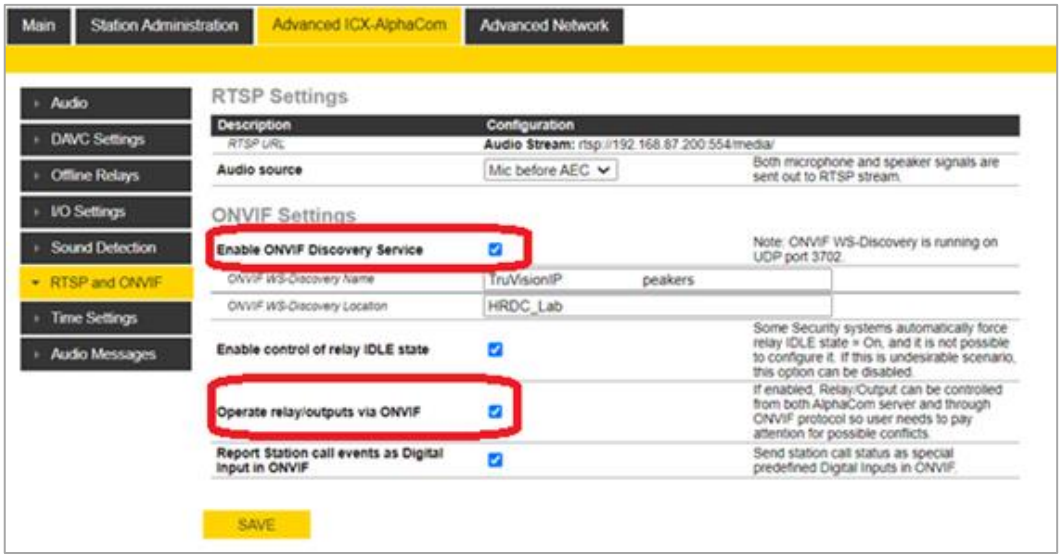
To enable the function to operate the relays/outputs via ONVIF:

1.Go to the **RTSP and ONVIF** menu.

2.Check the box **ONVIF Discovery Service**.

3.Check the box **Operate relay/outputs via ONVIF**.

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



Configure Edge mode

Note: Before the relays can be configured, you must set the working mode to Edge.

To set the Edge mode:

1.Login to the web page of the IP speaker.

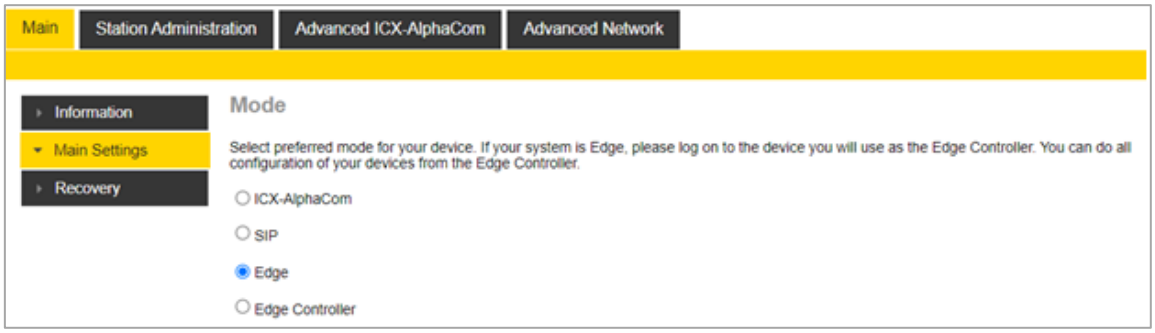
2.Navigate to **Main Settings** under the Main Tab.

3.Select the **Edge** mode.

4.Click **Save**.

5.After saving, click **Apply**.

The system will reboot to apply the new configuration.



Configure relays/outputs

Before configuring the relays, ensure that you have uploaded the audio clips.

To upload audio clips:

1.Go to the **Edge Configuration** tab.

2.Click **Audio Messages**.

3.Under the **Upload Media** section, click **Choose File** to select the audio file from your computer.

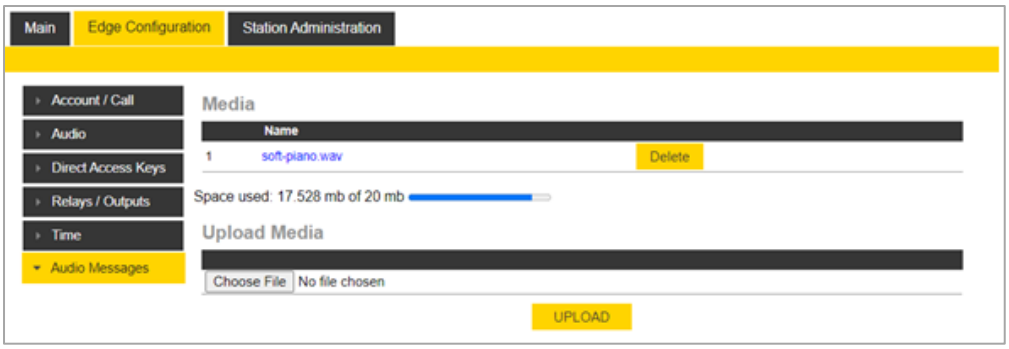
4.Once you have selected the file, click **Upload** to initiate the upload process.

5.After the upload is complete, you will be able to see the audio file listed under the Media section. If there were any issues with the upload, an error message will be displayed, indicating the reason for the failure.

Note:

•Audio message must be in the following format: WAV file, PCM 16-bit, 16000 sample rate and single channel (Mono).

•A maximum allowed file size to upload audio files is 20 MB.



Once audio messages are uploaded, you can assign them to a relay.

To assign an audio clip to a relay:

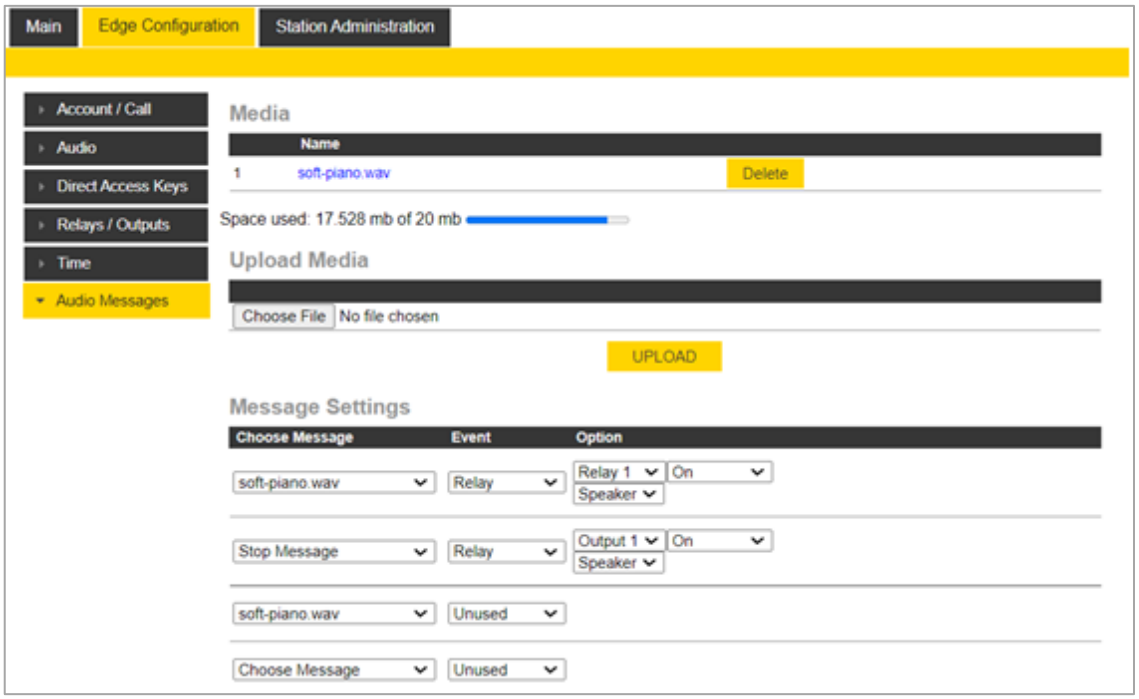
1.Under **Audio Messages**, go the **Message Settings** section.

2.Choose an audio message from the drop-down menu and select **Relay as Event**.

3.Select Relay 1 for the relay of the speaker. When more messages need to be assigned, select Output 1 to 6 as needed and assign the appropriate sound clip.

4.Click **Save**.

The speaker is now ready to be added in TruVision Navigator. For more information see “Adding IP speakers” on page 177**Error! Bookmark not defined.**.



Notes:

- Each relay/output should be configured with only one audio message. If multiple audio messages are configured for the same relay, the system will play the first audio clip in the list when the relay is activated.
- When selecting the event as relay, the option drop-down will display only the available outputs configured for the I/O pins in the ICX-AlphaCom mode. This ensures that the user can select from the list of outputs specifically configured for the ICX-AlphaCom mode.

Glossary

360° camera	360°cameras produce an ultra-wide field of view image.
Access control	Physical restriction to access or entry. Requiring a security badge to open a door is an example of access control.
Address book	A file containing the title, IP address, and credentials of recorders and cameras in the Navigator panel. This data can be imported or exported into Navigator as needed to save and restore these settings.
ANPR	Automatic Number Plate Recognition. A camera function that permits automatic reading of license plates of passing vehicles.
Bookmark	Denotes a date and time on the timeline that can be returned to quickly. Bookmarks contain editable information for describing an event. See also “timeline” and “bookmark manager.”
Bookmark manager	The Bookmark Manager window is a central location that contains all device-level bookmarks. See also “bookmark.”
Custom Notifications	Custom Notifications/Events provides a way to create customized, interdependent notifications from cameras connected to recorders as well as doors connected to TruPortal access control systems.
Dewarping	Fisheye cameras produce an ultra-wide field of view image which looks round and distorted. To make the image usable, the image needs to be flattened out (dewarped).
Digital output	Alarm output icons for recorders and cameras that appear in the Configure Map window, can be dragged onto maps, and triggered on or off.
DVR	Digital Video Recorder. A type of security footage recorder connected to analog or coaxial cameras.
Dwell time	A user-selectable amount of time that a PTZ camera remains at a preset before the camera moves to the next preset position.
Intrusion area	Icons that appear under the intrusion detection node in the Navigator panel that indicate if an intrusion area defined in an intrusion panel is disarmed, armed in stay mode, or armed in away mode.
Intrusion sensor	Intrusion sensors indicate the opened/closed state of a door or window. For motion sensors, they appear as “opened” when motion is being sensed.
IP camera	A digital video camera that connects directly to the network with its own IP address and has the ability to transmit images using a standard communications protocol such as TCP/IP.
LPR	License plate recognition. A camera function that permits automatic reading of license plates of passing vehicles.
Main stream	The video or audio stream that has priority. See also "substream".

NTP	Network Time Protocol. This synchronizes the time and date of a device with an NTP server.
NVR	Network Video Recorder. A type of security footage recorder connected to IP cameras.
Object counting	Refers to the number of people or objects detected passing either direction across a virtual line drawn by the user in the camera configuration UI.
POS	"Point-of-sale" as in a POS terminal. Examples: electronic cash register or an ATM.
Preset	A preconfigured action for a dome camera that will run automatically after a defined dwell time.
ProBridge	The ProBridge is a text translation device that captures an ATM’s transaction data and translates it to a format that can be interpreted by a DVR.
PTZ	Pan/Tilt/Zoom. A feature on cameras that can pan, tilt, and zoom via computer control. PTZ allows for a larger viewing area for a camera by allowing it to rotate in different directions.
Sequence	A series of camera streams that are programmed to switch, rotating one after another, in an individual video tile.
Server offline mode	Mode of operation in which the Navigator client can still operate in a client/server configuration when the server is offline. Some configuration options are not available in server offline mode.
SMTP	Simple Mail Transfer Protocol. A standard for e-mail transmission across the network.
Substream	A secondary video stream that is set at a lower quality setting to reduce the amount of bandwidth needed. See also "main stream".
Timeline	A graphical view of video over an interval of time that allows users to navigate through recorded videos.
Tour	A series of checkpoints assigned in a specific sequence with times assigned to reach each point.
Trigger alarm output	A method used to notify when an alarm or event has occurred. An external alarm output is triggered when an event occurs.
VCA	Video Content Analytics. The intelligent analysis of video to detect events of interest.
V-Stream	When available bandwidth is limited, V-stream encoding allows you to remotely view several channels in real time over the web browser.

Index

R

S

T

U

V

W

Z