Manual

Qognify VMS 7.5

© 2024 Qognify GmbH

Contents

Contents 2

List of figures 11

Legal notice 12

Support 13

Functional overview 15

Usability 15

Interfaces and integrations 16

Clients and access options 18

Configuration and administration 20

Core Services and branches 22

Protection of privacy and data in accordance with legal regulations 23

Concept 24

Administrative rights and user rights 24

Hierarchical administration 24

Profiles 25

Qognify VMS encryption 25

Time zone handling 26

The QogniFinder 27

Installation 29

System requirements 31

General recommendations 32

Standard installation 35

Client installation 38

Installation of a distributed server 38

Custom installation 41

Modify and remove 45

Updating the system with the AutoUpdater ... 46
Upgrading / Migrating from Seetec 5.4.x to Qognify VMS ... 49
Recommended steps before migration ... 50
Migrating procedure ... 51
After the upgrade ... 52

Login ... 55

The user interface ... 61

The function bar ... 63
The menu items ... 63
File menu ... 64
View ... 85
Tools ... 96
Info ... 116
Help ... 125
Changing the user ... 126
The mode bar ... 126
The control bar ... 127
Search ... 128

Surveillance mode ... 131

Work area ... 132
Sequential alarm window ... 135
Click-2-Track ... 135
Custom layers ... 137
Camera image controller ... 140
Camera image control icons ... 141
Mini archive player ... 143
Manual alarm recording ... 144
Swiveling the camera in the image ... 144
Camera image statistics ... 145
Maps ... 145

Web pages ... 147
Overview ... 148
Camera control ... 149
Alarm list and system messages ... 158
Alarm messages ... 158
System messages ... 161
Searching in surveillance mode ... 161
Archive mode ... 163
Archive player ... 164
Using the jog dial ... 165
Timeline / time stream ... 166
Editing an area ... 166
Click-2-Track ... 167
Using the QogniFinder ... 168
Exporting recordings ... 171
Exporting the Click-2-Track history with the Export Designer ... 172
Evaluating exported video data ... 173
Write protection ... 173
Searching for alarms ... 175
Working with bookmarks ... 177
Edge storage import ... 180
iSearch ... 180
Report mode ... 185
Configuration mode ... 189
Functions ... 190
The configuration shortcuts ... 192
Find devices ... 192
Filtering the search results ... 193
Adding individual devices ... 194

Adding multiple devices ... 194
Camera import via CSV or XML files ... 195
Searching in configuration mode ... 198
Company and branches ... 199
Relationship between the main branch and its sub-branches ... 200
Working with branches ... 207
Working with the site map ... 208
Editing menu on the administration control ... 210
Cameras ... 211
Creating a camera manually ... 212
Creating a camera with the wizard ... 215
The AXIS body-worn camera controller ... 220
Configuring a camera ... 223
Configuring an Archive camera ... 267
Configuring multiple cameras ... 268
Selecting and deselecting multiple cameras at once ... 268
Moving cameras ... 269
Duplicating a camera ... 270
Deleting a camera ... 271
Converting a camera ... 271
Other hardware ... 272
Creating new hardware ... 272
Configuring hardware ... 273
Deleting hardware ... 274
Third-party interfaces ... 274
Qognify ... 285
Qognify Video Analytics ... 290
Advantech ... 314
AXIS ... 316
W&T ... 318
Wago ... 320
Event Interfaces ... 322

Creating an event interface ... 323
Creating a generic access control ... 324
Configuring event interfaces ... 325
Creating multiple-state icons ... 328
Deleting event interfaces ... 329
Users ... 329
Creating a user ... 330
Configuring a user ... 330
Deleting a user ... 337
Duplicating a user ... 338
Groups ... 338
Creating a new group ... 338
Configuring a group ... 339
Deleting a group ... 345
Duplicating a group ... 345
Profiles ... 345
General ... 346
Image settings ... 348
Video wall module mapping ... 350
Time management ... 351
Company calendars ... 354
Editing a company calendar ... 355
Alarms ... 356
Creating an alarm scenario ... 357
Creating an alarm scenario with the wizard ... 357
Configuring an alarm ... 361
Deleting an alarm ... 373
Duplicating an alarm ... 373
Layers ... 374
Maps and "Advanced Maps" ... 377
Creating a new map ... 377
Configuring a standard map ... 378

Configuring an advanced map ... 382
Deleting a map ... 385
Duplicating a map ... 385
Buttons ... 386
Creating a new button ... 386
Configuring a button ... 386
Deleting a button ... 388
Duplicating a button ... 389
Web pages ... 389
Creating a new web page ... 389
Configuring a web page ... 390
Deleting a web page ... 390
Duplicating a web page ... 391
Patrols ... 391
Creating a new patrol ... 391
Configuring a patrol ... 391
Deleting a patrol ... 394
Duplicating a patrol ... 394
Sequences ... 394
Creating a new sequence ... 395
Configuring a sequence ... 395
Deleting a sequence ... 397
Duplicating a sequence ... 398
Video walls ... 398
Creating a new video wall ... 398
Configuring a video wall ... 399
Deleting a video wall ... 399
Duplicating a video wall ... 399
License plate groups ... 400
Creating a new license plate group ... 400
Configuring a license plate group ... 401
Deleting a license plate group ... 401

Duplicating a license plate group 402
Server 402
Configuring the Core Service 403
Configuring the DeviceManager (DM) 404
Configuring the global OCR settings 412
Configuring the LPR module 413
Configuring the Qognify Analytics Server 3D module 417
Configuring the Analytics Interface module 417
Configuring the Gateway-Service (SGS) module 419
Configuring the transcoding module 420
Configuring the Motion Detection module 421
Configuring the QMM server module 422
Configuring the generic DVR module 423
Configuring a generic access control module 424
Configuring a Qognify event interface (QEI) module 424
Configuring a body-worn camera connector module 425
System 428
Configuring the video classification 429
Configuring the alarm classifications 431
Configuring the backup 432
Configuring the Event Manager 433
Configuring the SMTP server 441
Configuring the Email Manager 442
Configuring the SNMP server 442
Configuring the NAT list 443
Configuring the entity numbering 444
Configuring the AlarmWatchDog 446
Managing sound and icon files with custom media 447
Configuring the user security settings 448
Creating entity labels 449

LPR mode **451**

Admintools **455**

UpdateService Configuration Tool 456

Configuring the UpdateService 457

Configuring a group 459

Global repository 461

Editing the server configuration 463

Import of updates and patches at the UpdateAgent 465

Qognify Administration Tool 465

General settings 466

Management database (MaxDB) 467

Multimedia database 469

OPC Service 472

Security 473

Qognify ServiceManager 474

Switching the display language 474

Editing the settings 475

Starting and stopping the services 475

Qognify VMS VA Administration Tool 476

Switching the display language 477

Creating a new configuration file 477

Adding an LPR module 478

Adding an Analytics Server module 479

Adding a Transcoding engine module 481

Adding a Gateway Service module (SGS) 482

Adding an Analytics Interface module 483

Adding a server-based motion detection module 485

Adding a generic Access Control module 487

Configuring the AV export module 488

Adding a Qognify Event Interface module 490

Adding a body-worn camera connector module 492

Exporting the configuration settings 494

Command line parameters **497**

Shortcut keys **501**

Anywhere Viewer **503**

Switching the interface language 504

Import and play recording 504

Export a recording 507

Qognify VMS web client **509**

Installing the web client services on the Qognify server 510

Connecting with the Qognify web client 510

Remarks, limitations and known issues 511

Harden IIS 512

The Qognify VMS mobile client **515**

Installing the mobile client services on the Qognify server 516

Installing the mobile client on a mobile device 516

Configuring the Qognify mobile client on the mobile device 516

Remarks, limitations and known issues 517

Connecting with the Qognify mobile client 517

Installing the Qognify Metadata Manager (QMM) **518**

Installation and upgrade 519

Camera settings 531

Troubleshooting 533

The AlarmWatchDog **535**

List of figures

Maps - Camera icon settings 379
Maps - Button icon settings 380
Maps - Alarm icon settings 381
Maps - Camera icon settings 383
Maps - Button icon settings 384
Maps - Alarm icon settings 385

Legal notice

This document is an integral part of the software shipped by Qognify (referred to hereinafter as the vendor) and describes how to use and configure the software and the associated components.
The English version of the document is the original version. All translations are based on the English original.

Copyright

This document is protected by copyright. It is not permissible to pass on the information it contains to third parties without the vendor's expression permission. Any infringements will result in claims for damages.

Patent and copy protection

In the event of protection being provided by a patent, utility model or registered design, all rights are reserved. Brand names and product names are trade names or registered trademarks of their companies or organizations.

Address

Qognify GmbH
Werner-von-Siemens-Str. 2 - 6
D-76646 Bruchsal
Tel: +49 (0)7251/9290-0
Fax: +49 (0)7251/9290-815
Email: info.emea@qognify.com
Internet: https://www.qognify.com

Disclaimer

Subject to alterations without further notice. Suggestions regarding the improvement of this documentation are welcome. For suggestions, refer to "Support" on the facing page.

Version

This manual corresponds to Qognify VMS 7.5 (Version 7.5.x).

Support

Reporting a software problem

If you discover a software problem, please report it using the helpdesk portal at: https://www.qognify.com.

For assistance related to this manual, provide the version number of the manual as well, as it is updated on a regular basis and the installed version may be outdated (see "Version" on the previous page).

> **If the AutoUpdater is installed and configured correctly (see "Updating the system with the AutoUpdater" on page 46), the UpdateClient will automatically check for new versions of the software and the help system.**

3

Functional overview

This section provides an overview of the function of the various parts of the Qognify VMS “ecosystem” and how they are integrated.

Usability

Qognify VMS can be used intuitively and without a long familiarization phase - this means that you can focus on what is important. This begins with the modern user interface: uncluttered and clearly structured. Qognify VMS combines the benefits of modern operating concepts with tried and trusted functionality and ergonomics - such as in glare-free night mode.

As a result, you maintain an overview and are able to respond quickly to events - whether you are currently working in Surveillance mode, in Archive mode, or in Configuration mode. This is a benefit that becomes more important the greater the number of image sources and locations in a company that need to be kept in view simultaneously.

Efficient alarm management

- With alarm counter and toast messages, all current alarms remain "on the screen" even in Archive mode
- Clear layout via classification of the alarms: alarm types can be differentiated in Archive mode at a glance by differently colored alarm tracks
- Easy understanding of events due to the alarm view, which shows on one screen what happened before the alarm, what triggered the alarm and what is happening at present

Time-saving functions

- Multi-configuration for simultaneous editing of multiple cameras in one working step - including across several locations
- Camera selection via lasso directly in the map - for rapid interpretation of situations
- Interconnection of views on video walls via drag & drop

Interfaces and integrations

Qognify VMS integrates seamlessly into existing and new system environments via interfaces. This is an important prerequisite, especially in large projects with multiple applications communicating with one another or with multiple locations. Qognify VMS fulfills all possible requirements: in addition to direct integration of a variety of hardware and software solutions, a range of standards and protocols is supported - exceeding the scope of traditional security applications.

This also offers economic advantages: the outlay is low for new installations because Qognify VMS can be easily integrated into existing system environments. Due to the broad scope of integration, older devices and systems can still continue to be used - for sustainable solutions.

Hardware integration

- Qognify VMS is not dependent on a specific manufacturer, over 1000 camera models from around 40 manufacturers are supported. We follow a principle of maximum possible integration depth and support functions such as multi-streaming, virtual cameras or movement detection on the terminal.
- Many additional camera models can also be integrated via the ONVIF standard.
- Analogue cameras and systems are integrated via video servers and can therefore still be used.
- I/O modules can be used to send and receive control signals - this means that doors can be opened by clicking on the Qognify interface, for example.

System integration

- Sector-specific IT systems such as cash register and merchandise management solutions are integrated quickly and easily via a driver-based concept.
- Security systems such as building management and PSIM systems, access control systems, intruder and fire alarm systems as well as alarm centers and control room solutions are integrated via interfaces.
- Other third-party systems can be integrated via network I/Os and TCP triggers - this means, for example, that an event in access control can trigger an alarm in Qognify VMS.
- VoIP-compatible devices are included due to the support of various SIP servers - this permits bidirectional voice communication between clients and voice stations directly in Qognify VMS.
- Qognify VMS uses a server interface to support the leading system-wide standard in automation and security technology: OPC UA. This means for example, that link-ups to access control or building management systems can be implemented.

Analytics integration

Server-based or camera-based analysis applications from other manufacturers can be integrated flexibly via the standardized Qognify Analytics Interface. Plug-ins from the following providers are currently certified:

- Agent VI
- CogVis
- Securiton IPS (ACAP-based analysis)
- Axis Perimeter Defender
- Digital Barriers SafeZone Edge

Additional plug-ins are also available. For further information, see "Generic VCA channel" on page 291.

SDK - Software Development Kit

Qognify VMS can be integrated into third party systems as well - using a Software Development Kit with detailed documentation.

Clients and access options

Qognify VMS offers access options and transmission solutions that allow you to monitor your company at all times and from anywhere. Your data is secure at all times - protected by our comprehensive functions for data protection and encryption.

Windows client

Windows-based client that permits the complete system operation and management - in Surveillance mode, in Archive mode, and in Configuration mode. The client is only available for 64-bit systems.

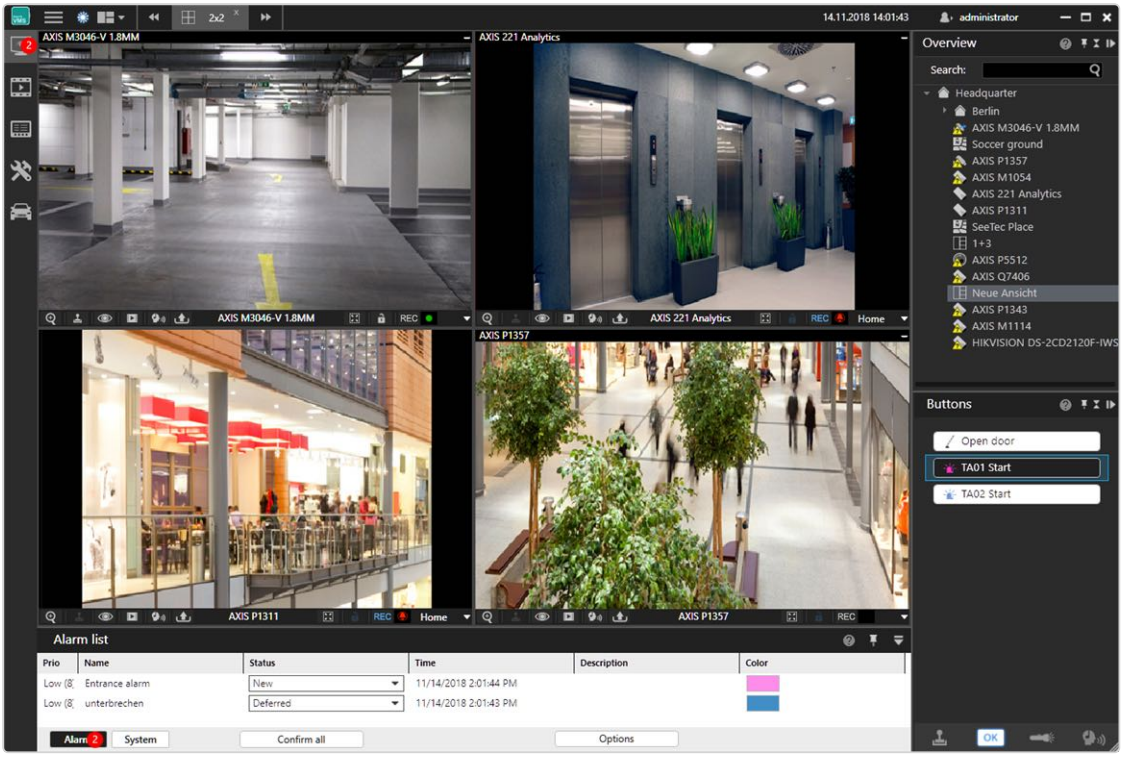


Fig. 1: Windows client

Web client

The Web client permits platform-independent access to installations with Qognify VMS from a PC connected to the internet - in surveillance mode and in Archive mode. It can be operated under Microsoft Windows, Mac OS X and Linux and only requires a current web browser. Additional plug-ins are not required as all input formats (e.g. Motion JPEG, MPEG-4, H.264) are converted into a standardized format via the Qognify transcoding service.

Mobile client

The Mobile client offers rapid system access on the move via tablets and smartphones (iOS and Android). In addition to the live view from camera images, it permits archive research as well as the editing of alarms. This means that security personnel can respond to events even during a patrol, for example.

DisplayAgent / Virtual matrix

Large-screen systems and video walls from different manufacturers can be linked in either via manufacturer-specific split computers or using the Qognify DisplayAgent. The video walls can be controlled via a standard Qognify client, views and cameras can be linked in simply via drag & drop.

Multi installation login

A Qognify client can be connected to 50 independent Qognify installations with an overall maximum of 5000 devices - with access to all cameras, views and alarms. This is the ideal solution for small alarm centers or for business parks with centralized security services.

Qognify VMS Anywhere client

The Qognify VMS Anywhere client can be started on any Windows-based computer without previously installing the software. The Qognify VMS Anywhere client offers all the functions of an installed client such as live views and archive views as well as administration and system configuration - taking account of individual user rights.

Configuration and administration

Qognify VMS adapts to the structure of your company - and therefore supports from one up to several thousand cameras. Via the distributed installation of the software across multiple servers, the overall system can be optimally dimensioned and expanded at any time. This means that the servers can also be available at different locations if required.

The architecture of Qognify VMS is based on a strict physical separation of clients and servers. Saving of image data and communication with the cameras are integrated as system services. Therefore, no separate program needs to be started on the server and no local login is required.

Hierarchical administration

Detailed rights to cameras, control elements (e.g. PTZ control) and additional Qognify VMS components such as buttons or layout plans can be individually allocated to every user. The user rights matrix forms the organigram of your company: This means that even systems distributed worldwide with several thousand cameras and numerous locations can be managed and controlled centrally using Qognify VMS.

Alarm scenarios - as individual as your company

Even though many work-flows within a sector are the same - every company has its own processes. Qognify VMS therefore allows you to define complex alarm routines individually. In a type of matrix, any start events (e.g. motion detection, events from video analysis, I/O contact, network I/O, button) can trigger a variety of different actions. These include alarm recording and visualization, sending triggers to third party

systems via physical I/O contacts or network I/Os, sending video sequences via email and FTP as well as launching external programs. This means that a customized workflow can be set up for each alarm situation, offering optimal support for the security personnel and facilitating a rapid response.

To make creating an alarm scenario as simple as possible, Qognify VMS provides an alarm wizard that guides the user step by step to the goal. Naturally the alarm scenarios are based on the detailed rights concept of Qognify VMS and can be assigned to individual users or user groups.

Fail-safe security via failover concept

In Qognify VMS , in the event of a failure two functions ensure that the video system continues to run and remains accessible at all times:

- In case of failure of one or more recording servers, a hot standby server immediately takes over the image recording. The image data does not have to be transferred back later (available for Qognify VMS Infinity X).
- If the central management server is no longer accessible, a proxy server is engaged that provides temporary storage for all relevant configuration data and access rights. The system continues to work in "island mode" and can be operated without faults.

Microsoft cluster and virtualization are also supported.

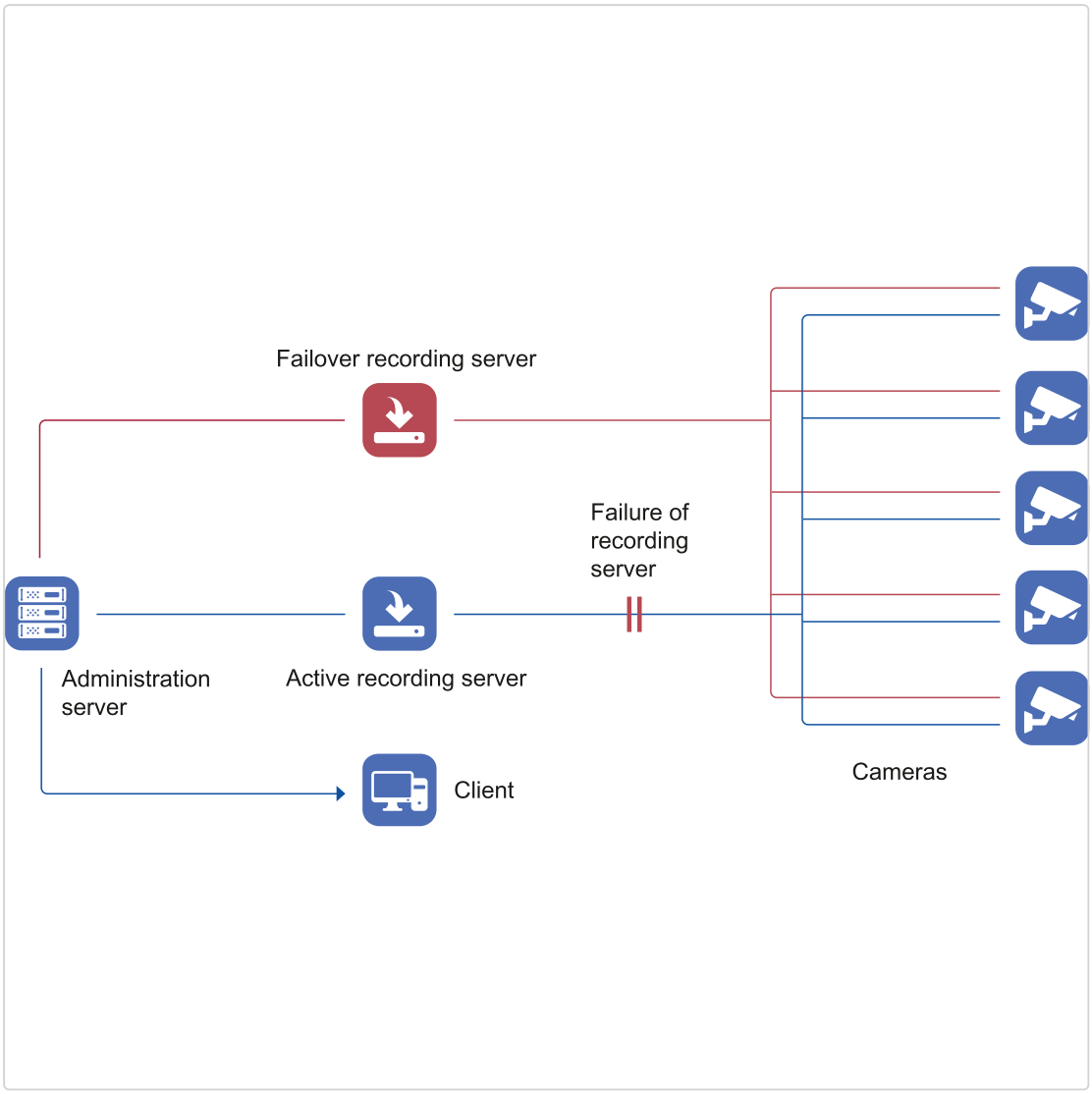


Fig. 2: Fail-safe security via failover concept

Core Services and branches

The Core Service server of the company is installed, configured and managed as "Core Service Main" (CSM) in the main branch. The Core Services of the branches cannot manage or configure the CSM or a Core Service within another sub-branch. The Core Services of the sub-branches are regarded as "Core Service Sub" services, CSS. All CSS are configured by the CSM (for configuration, see "Configuring the Core Service" on page 403).

If the CSM fails, the CSS switch automatically to an "insular mode", thereby providing the required services for the respective sub-branch. In "insular mode", the CSS cannot be configured. Hence, configuration mode and report mode are not available.

Once the CSM returns to normal operating mode, the CSS can be managed again by the CSM.

Protection of privacy and data in accordance with legal regulations

Qognify VMS offers various mechanisms to protect the privacy of employees, customers and visitors. This means that sensitive areas of the image or moving objects can be anonymized. System access can also be secured via the four-eye principle (input of a second password).

Qognify VMS is also well protected on the system level: data between the server and client is sent encrypted - one reason why Qognify VMS is certified, e.g. for use within the financial sector (see certificates).

Privacy masking

Sensitive image areas are masked by a freely definable area and hidden in the live and archive images, depending on rights. This means that social areas, public areas or keyboards to enter PIN numbers can be removed from the video monitoring, for example (for details, see "Privacy masking" on page 262).

Motion scrambling

Moving objects or objects that differ from a reference image defined in advance are displayed pixelated in the live image and thus anonymized (for details, see "Privacy masking" on page 262).

Encryption

Data transmission between the services in a Qognify VMS environment is encrypted (for details see "Qognify VMS encryption" on page 25).

Certificates

For use in the financial sector in particular, Qognify VMS has the relevant certifications - such as the "BGV / UVV Kassen" certificate that defines the requirements for video surveillance in financial institutions in Germany. Fiducia IT AG, the largest IT service provider for credit unions, has also approved Qognify VMS for use on their IT systems.

Concept

Administrative rights and user rights

In Qognify VMS, two types of users can be configured:

- **Administrator**. An administrator and an administrator group are installed by default. Both can neither be deleted nor deactivated. The administrator is a user with configuration rights and belongs to the administrator group. An administrator inherits the administrator group's rights. For the administration of branches, restricted administrative rights can be assigned to users that may manage only the objects (e.g. cameras) within the branch without "seeing" other branches.
- **Users**. The user has restricted rights and can be member of one or more user groups. A user inherits the rights of his group or groups. The user group's rights are defined in the Group control (see "Groups" on page 338). Additionally, the user may have specific rights that are not included in his groups' rights. These additional rights are defined in the User control (see "Users" on page 329). Group rights take priority over single user rights. In other words, a user in a group cannot receive any exceptions (i.e. further restrictions or "negative rights"), only additional restrictions. A user's membership of particular groups is revealed by the colored fields (see "Groups" on page 338 for information on how to configure the colors of groups).

Hierarchical administration

Qognify VMS has a multi-level administration that allows a user to be assigned administration rights to only a part of the installation or some of the functions.

- For a general description of administrative and user rights, see "Administrative rights and user rights" above.
- For defining user group rights and specific user rights, see "Manage user rights" on page 333.

The system allows subdivision of the administrative rights levels and division into a main branch and as many sub-branches as required. The sub-branches are defined as logical units with their own configuration context and cannot be nested.

- Users or other entities such as user groups, maps, DeviceManagers or cameras **that belong to a sub-branch** are restricted to their associations only, so that users only receive access to video data and the configuration of the associated branches.
- Users or other entities such as user groups, maps, DeviceManagers or cameras **that belong to the main branch** are also able to interact with sub-branches. Administration rights for the applicable sub-branches can be explicitly assigned to users or user groups belonging to the main branch.

The system avoids simultaneous configuration of a branch by two or more users, but it does allow simultaneous configuration of different branches by different users.

Profiles

Each user group automatically is assigned to a profile which is defined in the software configuration (see "Profiles" on page 345). Users within a group inherit the group's profile, but may have additional profiles depending on the groups they belong to or profiles that have been assigned to the individual user. When a user logs in, he is asked to select a profile (if multiple profiles are available and activated). The administrator can enable or disable profiles for users and user groups.

Qognify VMS encryption

Qognify confirms that the communication between the Qognify VMS clients and the Qognify VMS server is encrypted in all versions of the Qognify video management series.

> **Qognify VMS uses the AES encryption with a key length of 128 bits.**

The following features regarding the encrypted communication between Qognify VMS clients and Qognify VMS server (and vice versa) are available:

- **Encrypted transmission**

  Encrypted transmission is enabled by default using the above-mentioned AES encryption. The encryption is always activated.

- **Password**
  The password is always transmitted from the Qognify VMS client to the Qognify VMS server as "salted SHA-512 hash".
- **Camera audio and video streaming**
  Securing the transmission using encryption depends on the used camera model. The streaming method "RTSP over RTP over HTTPS" has to be supported. TLS 1.2 will be used if supported by the camera.
- **Storing audio and video streams**
  Incoming streams sent to the Qognify VMS DeviceManager (DM) are forwarded to the local Qognify VMS MultimediaDatabase (MDB). The transmission from the DM to the MDB proceeds within the same server (local TCP STACK). Therefore no encryption is required. Qognify VMS stores the streams in one or several file systems in parallel. The file systems are configurable by the administrator. The data storage in the Qognify MDB is encrypted in a proprietary format. We assume that the physical and logical access to the storage server is restricted by administrative actions. The export from the MDB is encrypted, thereby ensuring that access to the stream is impossible without password, as any alteration of the data exported will result in the password not working and confirms the validity of the exported data. The protection of the raw data prevents a manipulation and ensures the authenticity of the data.
- **Audio and video streaming to the Qognify VMS clients**
  Streams are only sent to the Qognify VMS clients if needed (e.g. if a camera image is displayed in Surveillance mode or Archive mode).
  The streams are sent over TCP or UDP to the Qognify VMS clients and are transmitted using our own proprietary transmission protocol.

Time zone handling

Time zone information (date and time) is stored as time zone information in the UTC[1] format. When a Qognify VMS client displays a date and time, it usually uses the local time zone of the machine, which can be different from the server time zone that stores the information such as recording date and time.
When loading and viewing images or files in Archive mode, the timestamp of the loaded information is always displayed in the local time zone of the client.

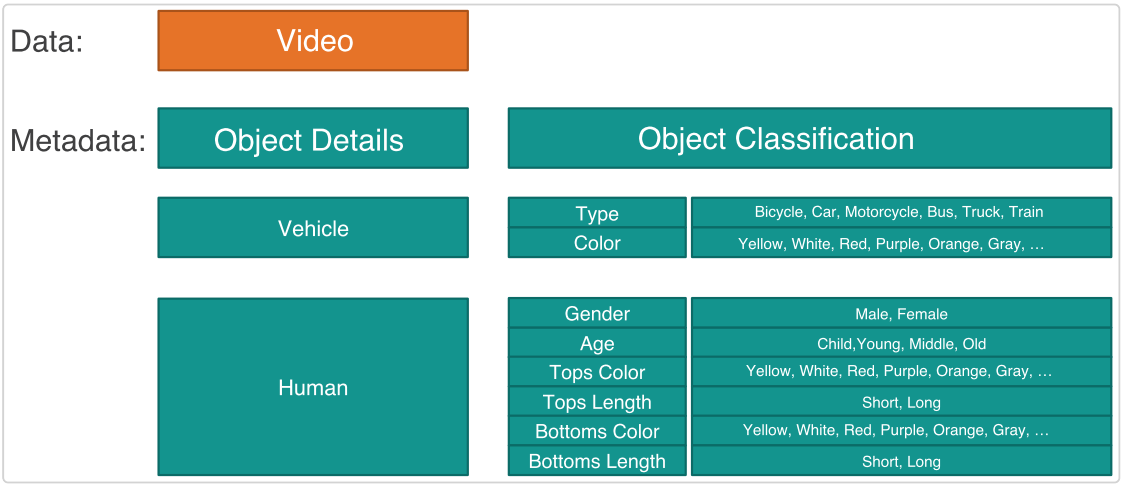
[1] Coordinated universal time

Example

The server is located in Europe and saves a video at 22:00 h local time that is also displayed in the timestamp within the video. If a client in California (USA) watches this video in archive mode, the client displays 2 pm, i.e. the local time of the client. Hence the time line in archive mode displays 2 pm and the clock in the video displays 22:00 h.

The QogniFinder

The QogniFinder enhances the search function for objects in images through an increased use of metadata. Metadata provide information about other data like "red" or "blue" (adjectives) describe a shirt (noun). The diagram below describes this metadata construct for objects in a video stream.



Qognify VMS manages the metadata that are applied to the objects in images. The software discovers the objects in an image and applies the existing metadata to the objects found. Thereby, searching for objects in images according to their metadata is significantly enhanced.

4

Installation

> **When migrating from SeeTec 5 to Qognify VMS 7.5, the Core Service Main has to be defined. This cannot be changed at a later state (e.g. changing to Core Service Sub), as it will result in data loss.**

- Qognify VMS must not be installed on a compressed drive, since this can result in problems with the database. A drive on which Qognify VMS is already installed must not be compressed subsequently.
- Microsoft .NET Framework 4.6.2 is installed during installation, which may require a restart in the case of a first-time installation.

> **From Qognify VMS 7.5 onwards, DirectX 9 is not longer installed since DirectX is already installed with recent windows operating systems by default.**

- The Qognify AutoUpdater is installed in a separate folder.

Information on rollbacks

Rolling back to a previously installed version of Qognify VMS may be necessary to assure system operation with a minimum of interruption. The deinstallation of the previous version and the subsequent installation of the new version is carried out "under the hood". In case of an installation error all steps will be reverted.

To use the rollback feature, a new version of Qognify VMS must be installed WITHOUT removing the previous version. Rollback is available for Qognify VMS version 16 and newer.

Virus scanning

> **Web guard and internet security features must not be installed on Qognify VMS systems.**

- To run Qognify VMS software properly, exclude specific locations, processes and network traffic, since virus scanning could use a high amount of system resources.
- The scanning process could temporarily lock files. This may lead to a disruption in the recording process or even database corruption.
- Do not perform a real time and system scan of Qognify VMS directories containing recording databases (by default C:\Program Files\Qognify, as well as all subfolders).
- Avoid a real time and system scan on archived storage directories.
- Create the following additional exclusions:
  - C:\Program Files\Qognify and all subdirectories.
  - Path to Multimedia Database Zone(s)
- Exclude real time network scanning on TCP ports
- Exclude network scanning of the processes starting with VMS_* (e.g. VMS_Client.exe)

Firewalls

By default, multiple ports on the server computer must be available to allow the Qognify VMS software to function correctly in a network environment with a firewall.

Setup types

- **Client & Server**. This installation type installs the client and server modules on the computer (see "Standard installation" on page 35).
- **Client**. This installation type installs only the client modules (see "Client installation" on page 38).
- **Distributed server**. This installation type installs only the client and the server services for the cameras (DM/MDB) on the selected computer (see "Installation of a distributed server" on page 38).
- **User-defined**. In a user-defined installation, it is possible to install only specific components on a computer (see "Custom installation" on page 41).

System requirements

> **Overview of the software and hardware requirements can be found on our support pages: https://www.qognify.com/support-training/**

Known limitations

- The performance requirements of the Qognify server services depend, above all, on the video volume transferred and the storage hardware.
- **The server software can only be installed on computers with the NTFS file system.**
- For the server, an additional 25 MB of RAM should be available for each camera.
- The hardware requirements depend on the configuration. Qognify VMS is based on an advanced software architecture in response to technological progress. Qognify recommends

  a 64-bit operating system for data-intensive clients in order to enable the use of the Qognify

  64-bit client.

> **If in doubt contact Qognify support (see "Support" on page 13).**

Requirements for the Help system

- Current internet browser with JavaScript activated
- For the PDF-based help file Adobe Reader or a comparable application is recommended

General recommendations

Virtual environments

> **The latest updated system requirements and parameters are published on https://www.qognify.com/support-training/hardware-recommendations/.**

- Qognify recommends not to use clients in virtual environments, because the rendering performance is severely decreased.
- Qognify recommends dedicated network interfaces.
- Virtualization could need more CPU power than its physical counterpart
- Qognify recommends directly attached storage or iSCSI.
- Because virtualization decreases performance, Qognify recommends testing the planned server environment.
- Qognify VMS is compatible with Citrix XEN, VMware vSphere and Microsoft Hyper-V.

Thin clients

Thin client environments are not supported.

CPU recommendations

- Video processing needs a lot CPU power. Qognify recommends to always use the latest powerful CPU models.
- You can find a comparison at https://www.cpubenchmark.net/high_end_cpus.html.
- It is recommended to use a single socket server with up to 10 physical cores.

Windows clustering and operating system

- Always installing the latest system updates is recommended.
- 64 Bit versions are recommended.

Network layout

- Depending on the number of cameras in your system and the resulting required network bandwidth, the use of multiple separate networks for the cameras, the clients, and the storage must be considered to prevent overload on your network.
- Since the Qognify client does not need a direct connection to the cameras, only the Qognify server needs access to both networks.

Do not use teaming or binding of network interfaces.

Usage of cameras

- Cameras should be referenced only once. Configuring a camera multiple times per installation or in different installations will cause problems with some camera types.
- Contact Qognify project engineering for further information.

Benchmark results

The following benchmark results for a QognifyQognify VMS client with recommended hardware setup and 4 displays:

H.264

- 48 cameras, 320 x 240 @ 512 kbps CBR and 25 fps
- 40 cameras, 640 x 480 @ 1024 kbps CBR and 25 fps
- 30 cameras, 704 x 480/704 x 576 @ 2048 kbps CBR and 25 fps
- 18 cameras, 720p @ 4096 kbps CBR and 25 fps
- 12 cameras, 1080p @ 4096 kbps CBR and 25 fps
- 12 cameras, 3 Megapixel @ 4096 kbps CBR and 25 fps

H.265

- 48 cameras, 320 x 240 @ 200 kbps ~VBR and 25 fps
- 32 cameras, 640 x 480 @ 400 kbps ~VBR and 25 fps
- 16 cameras, 720p @ 600 kbps ~VBR and 25 fps
- 8 cameras, 1080p @ 2000 kbps ~VBR and 25 fps

Standard installation

The standard installation installs the system with the client and server on a single system.

Preparation

1. Copy the ZIP archive with the installation files to the computer on which the software will be installed and unpack the archive.
2. Double-click **setup.exe** to start the installation.
3. Select the installation language. You can configure the language of the user interface after installation (see "Changing the language" on page 79).
4. Select **OK** to start installation, and select **Next**.
5. Read the software license agreement, and select **Next**.

   The program can only be installed if the End User License Agreement (EULA) is accepted.
6. Select the destination folder, and select **Next**.

Standard installation

1. For the standard installation, select "Client & server" as the setup type and select **Next**.

2. Select **IP addresses / hostnames found** as network address for server communication.

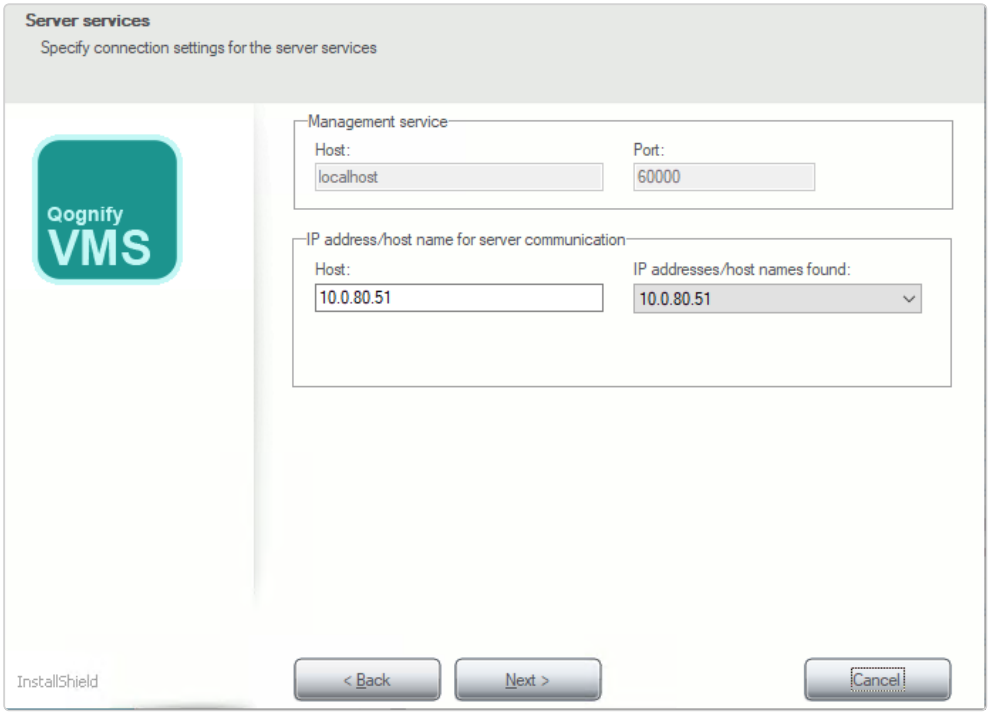


Fig. 3: Standard installation - 1

> **It is recommended to leave the port number of the management service unchanged at "60000". If the port number must be changed, contact the Qognify support before applying changes.**

> **The installation program shows you all of the existing network addresses and host names of the PC or server. Neither the IP 127.0.0.1 nor the host name "localhost" may be used for communication with the server.**

3. If the update server is installed on a different host than the Core Service Main host, enter the IP address for the host of the **UpdateService** (see "Configuring and updating the UpdateAgent" on page 47). The UpdateAgent can connect to the UpdateService at the specified IP address.

   > **By default, the UpdateService uses port 63000 and 63001 to communicate with the UpdateAgents.**

4. Select **Next**.

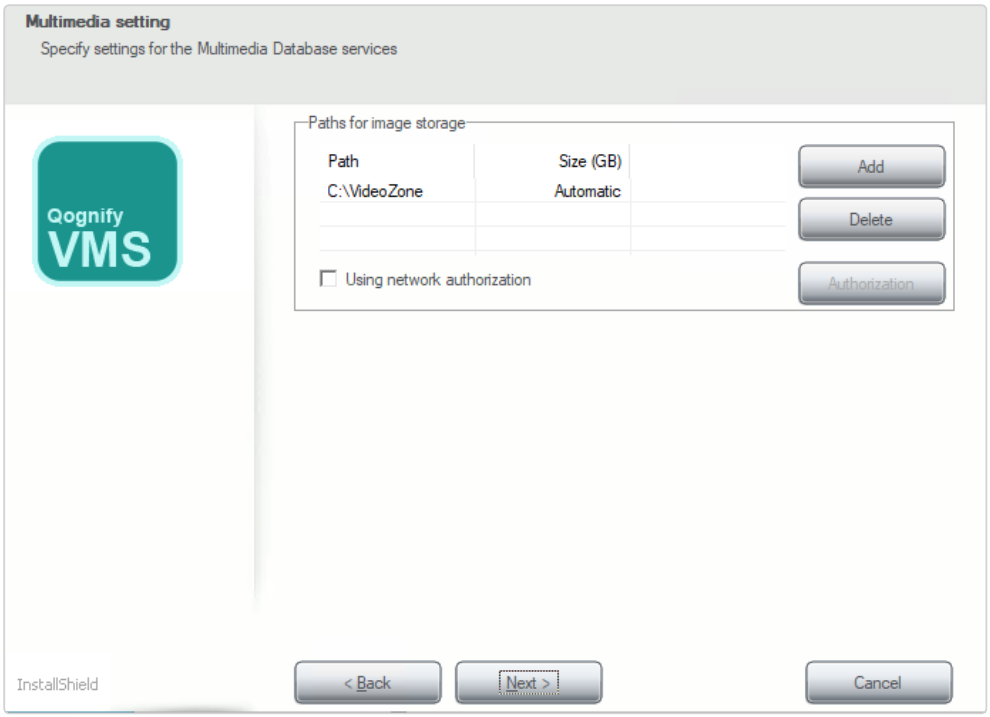


Fig. 4: Standard installation - 2

5. Alter the existing path for image storage, or delete or add further folder paths. If the folder is created on a network drive, enter the complete UNC path.

   > *Example* *"\\IP address\Release name\Path..."*

6. If the network drive is protected with a user name and password, select **Using network authorization** and click **Authorization**.
7. Enter the user name and password for accessing the network drive, and click **OK**. Ensure that the specified user is available locally and that the domain is included in the user name field (e.g. "Domain\\User name").
8. Select **Next**.
9. Select **Install**. Qognify VMS is now installed on your computer. If the UpdateService has been installed, the service will now connect to the Update server and download the newest patch files, if available. To find out how to start the program and modules, see "Login" on page 55.
10. Configure the system with the Qognify VMS client (see "Configuration mode" on page 189).

Client installation

In the client installation, only the client is installed on the computer.

Preparation

1. Copy the ZIP archive with the installation files to the computer on which the software will be installed and unpack the archive.
2. Double-click **setup.exe** to start the installation.
3. Select the installation language. You can configure the language of the user interface after installation (see "Changing the language" on page 79).
4. Select **OK** to start installation, and select **Next**.
5. Read the software license agreement, and select **Next**.

   The program can only be installed if the End User License Agreement (EULA) is accepted.

6. Select the destination folder, and select **Next**.

Installation

1. Select "Client" as the setup type (see "Installation" on page 29).
2. Select **Install**.

The client is installed on the computer. If the UpdateService has been installed, it will connect to the Update server and download the newest patch files, if available.
To find out how to start the program and modules, see "Login" on page 55.

Installation of a distributed server

In distributed server installation, only the database modules for the image database are installed together with the client on a different computer from the already installed client and core server. The distributed server reduces the utilization of the core server because the image database is located partially or entirely on the distributed server.

In order to configure the server, you need an installed and configured client and core server (see "Standard installation" on page 35).

The required ports 60000 - 60008 for communication between the distributed server and the main server must be open.

Preparation

1. Copy the ZIP archive with the installation files to the computer on which the software will be installed and unpack the archive.
2. Double-click **setup.exe** to start the installation.
3. Select the installation language. You can configure the language of the user interface after installation (see "Changing the language" on page 79).
4. Select **OK** to start installation, and select **Next**.
5. Read the software license agreement, and select **Next**.

   The program can only be installed if the End User License Agreement (EULA) is accepted.

6. Select the destination folder, and select **Next**.

Installation

1. Select "Distributed server" as the setup type (see "Installation" on page 29).

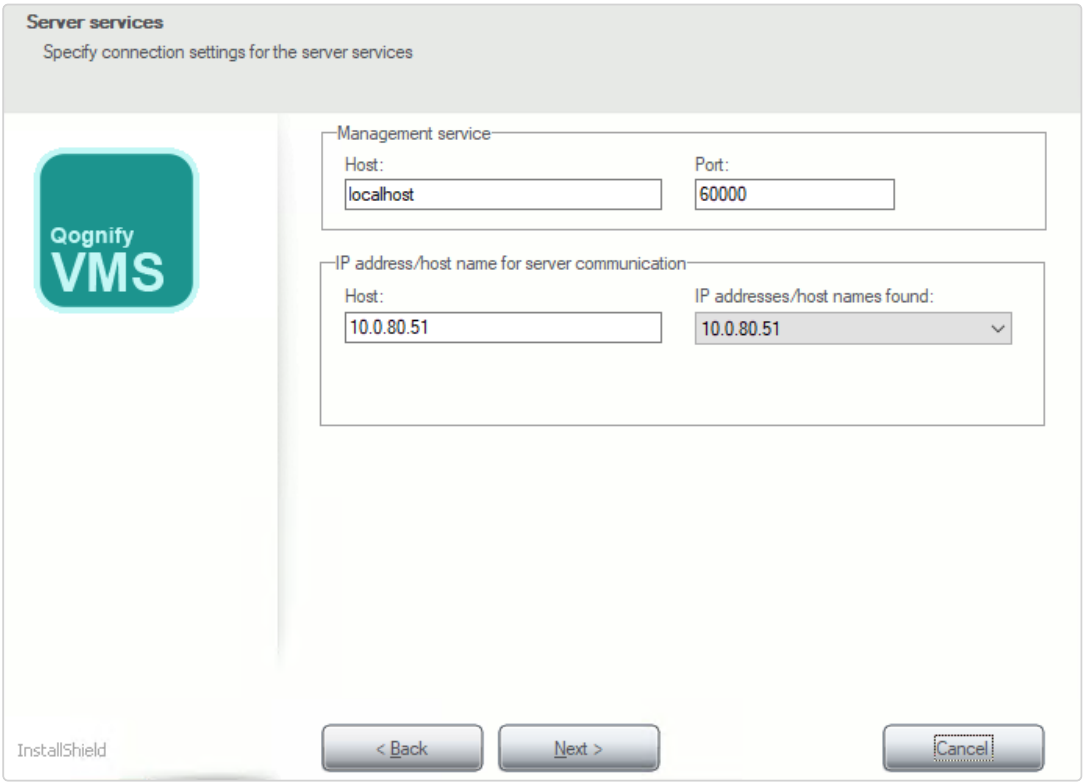


Fig. 5: Installation of a distributed server - server settings

1. Specify the IP address of the main Core Service Main Core (CSM) server as the **Host** in the "Management service" area.

   It is recommended to leave the port number of the management service unchanged at "60000". If the port number must be changed, contact the Qognify "Support" on page 13 before applying changes.

2. Select **IP address/host name for server communication** as the network address. The installation program shows you all of the existing network addresses and host names of the PC or server.

   Neither the IP 127.0.0.1 nor the host name "localhost" may be used for communication with the server.

3. If NAT (Network Address Translation) is used, enable Activate if NAT is to be used and enter the IP-address of the NAT-router.
4. Enter the IP address for the host of the **UpdateService** (see "Configuring and updating the UpdateAgent" on page 47).

   > **By default, the UpdateService uses port 63000 and 63001 to communicate with the UpdateAgents.**

5. Select **Next**.

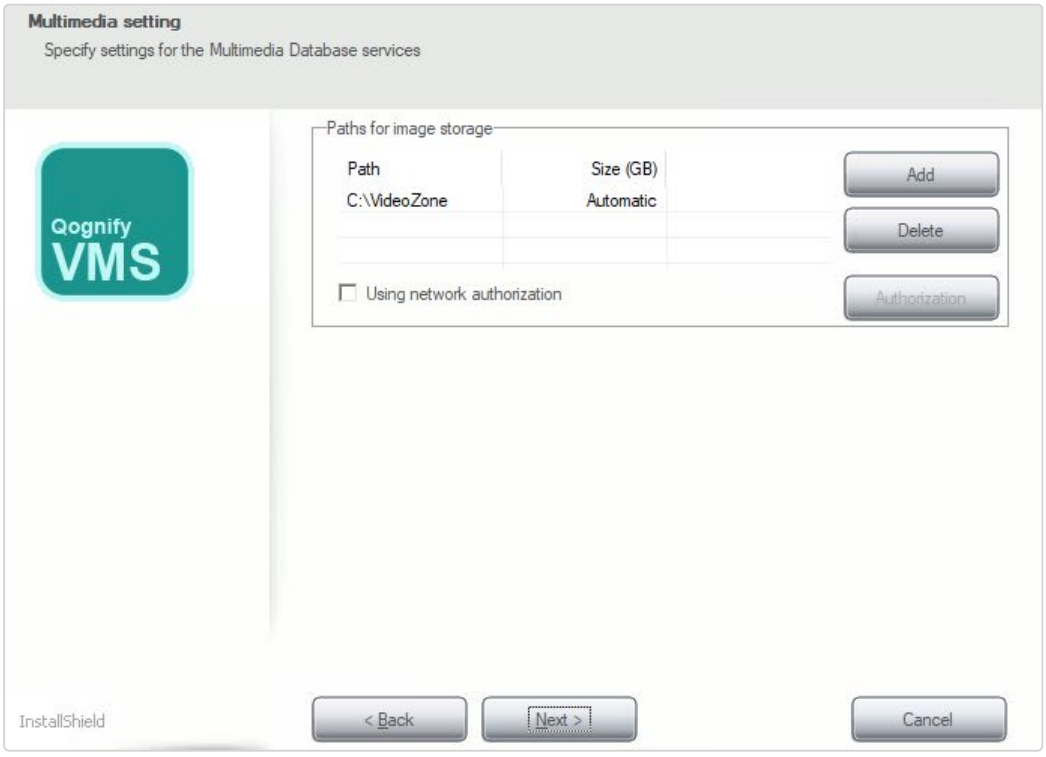


Fig. 6: Installation of a distributed server - multimedia settings

1. Alter the existing **path for image storage**, or delete or add further folder paths. If the folder is created on a network drive, enter the complete UNC path.

   > *Example "\\Server name\Release name\Path..." or "\\IP address\Release name\Path..."*

2. If the network drive is protected with a user name and password, select **Using network authorization** and click **Authorization**.
3. Enter the user name and password for accessing the network drive, and then click **OK**. Ensure that the specified user is available locally and that the domain is included in the user name field (e.g. "Domain\\User name").
4. Select **Next**.
5. Select **Install**. The server is then installed on your computer .If the UpdateService has been installed, the service will now connect to the Update server and download the newest patch files, if available.
6. Configure the system with the Qognify client (see "Configuration mode" on page 189).

Custom installation

In a user-defined installation you can install selected modules. It is also possible to install a further core server in Sub Core mode that serves as a redundant server and thus increases the reliability of the Main Core server.

Preparation

1. Copy the ZIP archive with the installation files to the computer on which the software will be installed and unpack the archive.
2. Double-click **setup.exe** to start the installation.
3. Select the installation language. You can configure the language of the user interface after installation (see "Changing the language" on page 79).
4. Select **OK** to start installation, and select **Next**.
5. Read the software license agreement, and select **Next**.

   The program can only be installed if the End User License Agreement (EULA) is accepted.

6. Select the destination folder, and select **Next**.

Custom installation

1. Select "Custom" as the setup type (see "Installation" on page 29).
2. Select the desired services and features. You can deselect services and features that are not required.

   > **If a previously installed service is deselected, it will be removed. For installation of the UpdateService on the server and the UpdateAgent on the client, see "Configuring and updating the UpdateAgent" on page 47.**

3. Select **Next**.
4. Select **Install**.

The services and features are installed.

Components for the custom installation

The following components are available for user-defined installation.

Client components

Fig. 7: Custom installation - Client components

- **Client (64-bit)**: The client only for 64-bit operating systems
- **Mobile client**: The server-side mobile client components (Transcoding module and Gateway Service) to connect with mobile apps on iOS and Android platforms (see "The Qognify VMS mobile client" on page 515)
- **Web client**: The server-side web client components (transcoding module, gateway service and Microsoft IIS web server with website) to connect with web-browsers (see "Qognify VMS web client" on page 509)
- **Viewer**: The offline viewer to see exported images (see "Anywhere Viewer" on page 503)

Server components

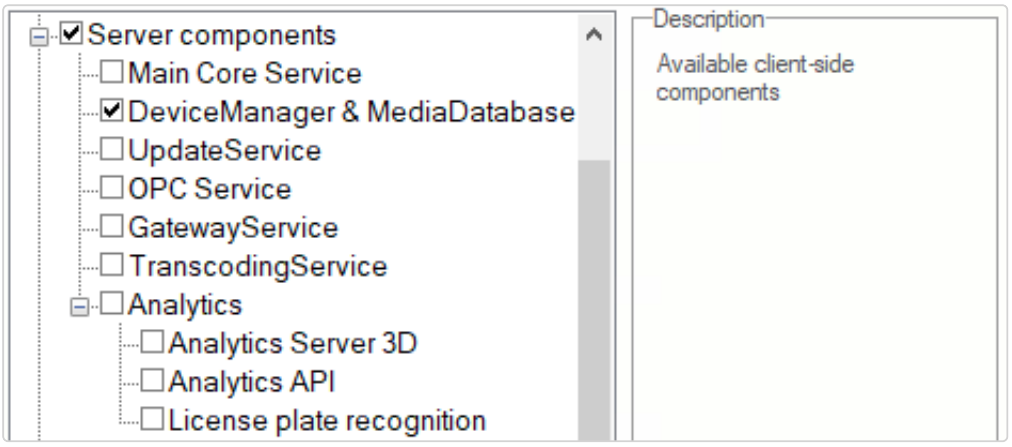


Fig. 8: Custom installation - Server components

- **Core Service Main**: The Main Core services and management database
- **Core Service Sub**: The Sub Core services and management database for redundant system management

  > **Sub Core and Main Core cannot be installed simultaneously on the same machine.**

- **DeviceManager & MediaDatabase**: The services for the DeviceManager and MediaDatabase. These services are mainly responsible for image handling processes
- **UpdateService**: The UpdateService is managing the automated update and patch processes on the Qognify system (see "UpdateService Configuration Tool" on page 456)
- **OPC Service**: The "Open Platform Communications" interface provides a standardized data exchange between applications and devices in real time (see Technical Guide on OPC Service for Qognify VMS R3 or later).
- **GatewayService**: The GatewayService is required to use mobile and Web clients (see "Installing the mobile client services on the Qognify server" on page 516)

- **TranscodingService**: The TranscodingService is required to use mobile and Web clients (see "Configuring the transcoding module" on page 420)
- **Analytics**: The server side components for Qognify VideoAnalytics features
  - **Analytics Server 3D**: The server-side Analytics Server 3D components for third-party video analysis software used on the computer (see "Configuring the Qognify Analytics Server 3D module" on page 417)
  - **Analytics** (legacy): The server-side analysis components installed on the computer (see "Qognify Analytics" on page 301)
  - **Analytics API**: The server-side Analytics API components for third party video analysis software installed on the computer
  - **License plate recognition**: The server-side license plate recognition installed on the computer (see "License plate recognition" on page 293)

Tools

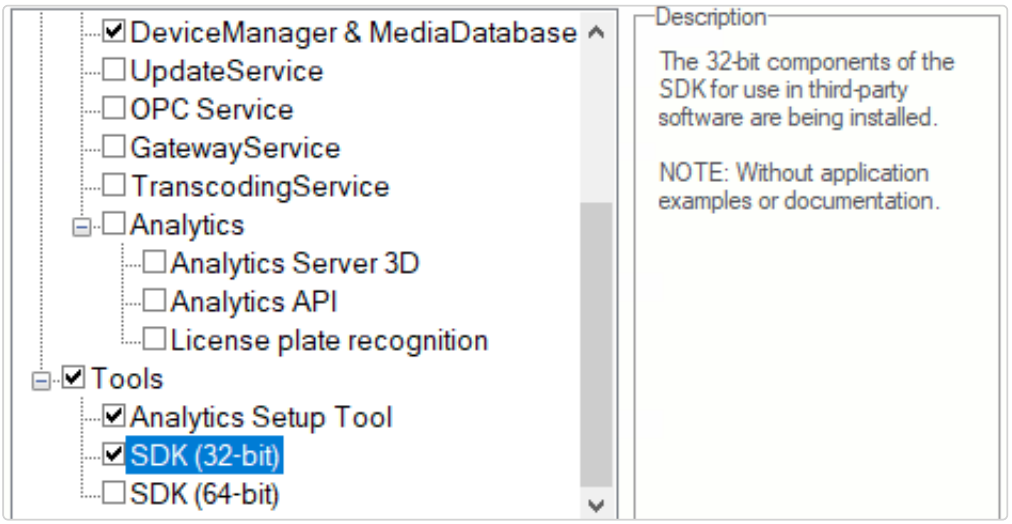


Fig. 9: Custom installation - Tools

- **Analytics Setup Tool**: The tool for configuring and calibrating scenarios for the Qognify Analytics Server 3D (see "Configuring a Qognify Analytics Server module" on page 312)
- **SDK (32-bit)**: The 32-bit components of the SDK for use in third-party software
- **SDK (64-bit)**: The 64-bit components of the SDK for use in third-party software

Modify and remove

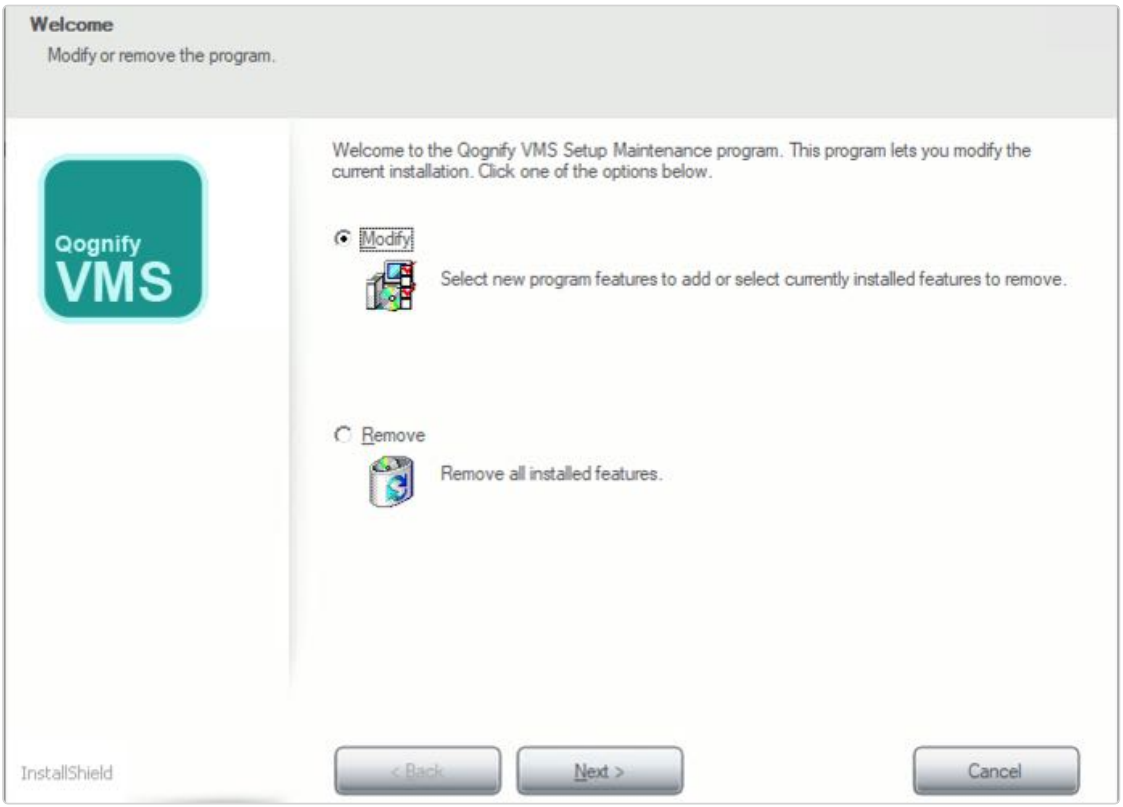


Fig. 10: Modify and remove

1. Open the settings of the operating system and select **Apps**.
2. Select **Apps and features**.
3. Select **Qognify VMS**.

4. Select **Modify** or **Uninstall**.
   - To install or uninstall additional Qognify VMS components select "Modify" and select **Next**. This allows you to carry out a user-defined installation to install and remove selected modules and services (see "Custom installation" on page 41).
   - To remove the program from the hard disk, select "Uninstall" and select **Next**. All components of the application except for the configuration settings are deleted from the hard disk and removed from the directory services.

     > **To completely remove all traces of the program after uninstallation, delete the remaining Qognify folder in "C:\Program Files" manually.**

Updating the system with the AutoUpdater

With the Qognify VMS AutoUpdater you can keep all system components up to date, if it is a single “All-in-one” installation on one PC or a distributed installation with multiple servers and clients.
The Qognify VMS AutoUpdater system consists of two components, the UpdateService and the UpdateAgent(s):

- The UpdateService: Immediately after the installation and thereafter the UpdateService frequently checks for new patches or updates and distributes them to the connected UpdateAgents. In a standard installation the UpdateService is installed on the Core Service Main server. Optionally the UpdateService can be installed on another server (see "Custom installation" on page 41).

  > **The UpdateService requires a regular license with a valid Service Maintenance Agreement (SMA) or a demo license not yet expired.**

- The UpdateAgent(s): An UpdateAgent is automatically installed with any Qognify VMS component (services, clients, tools etc.). Dependent on the configuration of the UpdateService an UpdateAgent receives updates or patches from the update server automatically or by a manual trigger. This enables automatic or user defined installation of updates and patches for multiple clients.

Installing the Qognify VMS UpdateService

The UpdateService is installed on the Core Service Main by default. If you need to install the UpdateService on a different hardware than the core server follow the steps below.

- By default, the UpdateService uses port 63000 and 63001 to communicate with the UpdateAgents.
- Check that ports 63000 and 63001 are not blocked by a firewall.
- Only one server should be the UpdateService server. Having multiple UpdateService servers is not recommended.
- To install and run the UpdateService on a different server than the Core Service Main server, it is recommended to remove it from the main server before installation (see "Updating the system with the AutoUpdater" on the previous page).

Before installing updates with the UpdateService (e.g. from Qognify VMS R3 to Qognify VMS7.5), update all UpdateAgents with the current UpdateService (i.e. Qognify VMS7.5).

1. Select the server that runs the Qognify VMS UpdateService.
2. Provide the IP address of the server for the UpdateService. All UpdateAgents have to connect to the UpdateService by the specified IP address
3. Start a user-defined installation and select "UpdateService" in the server components (see "Custom installation" on page 41)

Configuring the Qognify VMS UpdateService

The UpdateService and the update behavior of the UpdateAgents can be managed with the Qognify VMS UpdateServer Configuration tool. The UpdateServer Configuration tool will be installed automatically with the UpdateService on the server.

> **For configuration settings, see "UpdateService Configuration Tool" on page 456.**

Configuring and updating the UpdateAgent

The UpdateAgent is installed automatically on each computer where a Qognify VMS component (e. g. Core Service, Client, DeviceManager, VA-Service etc.) is

installed. During the installation process the IP address of the UpdateService has to be provided (see "Standard installation" on page 35). After installation, the UpdateAgent is enabled and configured by the installer by default.

> **If the IP address of the UpdateServer has changed, the UpdateAgent has to be configured manually in the configuration file of the UpdateAgent.**

Manually changing the IP settings for the UpdateAgent

1. Stop the UpdateAgent with the Qognify ServiceManager (see "Starting and stopping the services" on page 475).
2. Open the configuration file "/conf/updateclient.conf.xml" in the installation directory with a text editor.
3. Set the new IP address of the UpdateService. The IP address is identical to the network address of the client with the UpdateService installed.
4. Save the settings.
5. Start the UpdateAgent with the Qognify ServiceManger (see "Starting and stopping the services" on page 475).

Example

updateclient.conf.xml

```
<?xml version="1.0"?>
<ServerInformation xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns:xsd-d="http://www.w3.org/2001/XMLSchema">
<ip>10.0.8.131</ip> <port>63000</port>
</ServerInformation>
```

Manual updating

The Qognify VMS system can be patched or updated automatically by the AutoUpdater. If the AutoUpdater is configured correctly, uninstalling the previous version of Qognify VMS is not required before updating to a newer version.
Any version prior to SeeTec 5.4 must be removed before upgrading (see "Upgrading / Migrating from Seetec 5.4.x to Qognify VMS" on the facing page).

> **Before updating the system manually, make sure that your system meets the hardware and software requirements (see "System requirements" on page 31).**

1. Manually backup the CONF directory (C:\Program Files\Qognify\Conf).
2. Manually backup the administration database MaxDB (C:\Program Files\Qognify\SAPDB\backup).
3. Uninstall the current Qognify version with the Windows® control panel. The folder structure of the installation directory and the database remain intact.
4. Install the new Qognify VMS7.5 software.
5. Import the new license file (see Import license file).

It is also possible to import the new license file before updating.

Upgrading / Migrating from Seetec 5.4.x to Qognify VMS

This section is intended for the preparation and implementation of a migration from Seetec 5.4.x to Qognify VMS 7.5. It describes the necessary steps of the analysis and the basic process.
Note that the preparation, depending on the technical specification of the existing system, should start well before the actual migration, since delivery times may have to be considered for hardware components.

The Qognify support team can be contacted before migrating complex installations (e.g. logistics, CIT, BVI, etc.) (see "Support" on page 13).

Documents to be considered

- Qognify VMS 7.5 readme file
- System requirements for Qognify VMS 7.5 (see "System requirements" on page 31)
- Supported third-party interfaces

Recommended steps before migration

Migrating to Qognify VMS is only possible from Qognify 5.4.0 or higher. Older versions must be updated to Qognify 5.4.x before migration. Migration may require replacement of hardware components.

1. Backup the existing management database MaxDB and the configuration directory (see "Manual updating" on page 48).
2. Analyze the existing system well before the actual date of migration to make sure that hardware and / or operating system requirements are met (see "System requirements" on page 31). For Qognify VMS 7.5, a 64-bit operating system is required.
3. Make sure that any device of the configuration is listed in the "Supported third-party interfaces" (PDF) and check the supported functionality.
4. Make sure that you have a valid license for Qognify VMS 7.5.
5. Capture the specification of the existing server and client hardware and compare it with the requirements as described in the section on "System requirements" on page 31.

Minimum requirements for graphic cards

Some graphics cards which are used in Qognify 5.4.x, are not suitable for use with Qognify VMS because they do not or only partially support DirectX, e.g. Matrox graphic boards, Nvidia Quadro NVS 290 or 420.

- Dedicated graphics adapter without shared memory, 16 mio. colors, supporting DirectX 9.0 or higher
- Memory size: 2 GB
- Memory bandwidth with 100 GB/s
- Minimum display resolution:
  - 1280 x 768 (with text size 100%)
  - 1600 x 960 (with text size 125%)
  - 1920 x 1152 (with text size 150%)

For Microsoft Windows Server 2012 only

1. Check if the Windows feature "Desktop Experience" is installed (for Microsoft Windows Server 2008, this is done automatically).
2. If not, install the feature by following the steps: Server Manager = > Manage => Add Roles and Features => Features => User Interfaces and Infra-structure (Installed) = > Desktop Experience => Add Features => Next = > Install.

Migrating procedure

Hardware and operating system already meet the requirements

1. Perform a backup of the MaxDB database and the configuration directory.
   - In Qognify Administration (Start Menu > Programs > SeeTec5) change to Management database (MaxDB) and create a backup via **Backup**. The backup will be stored in C:\Program Files\SeeTec\SAPDB\backup.
   - The configuration directory is located in: C:\Program Files\SeeTec\conf
2. Uninstall Seetec 5.x via the Windows Control Panel.
   - The folder structure remains
   - The database remains.
3. Install Qognify VMS7.5.
4. Install and activate a new license (see "Info" on page 116).

Migrating to new hardware and / or new operating system

1. Make sure that the existing Qognify VMS version is at least 5.4.0. If not, upgrade to the latest version 5.4.8.
2. Perform a backup of the MaxDB database.
   - In Qognify Administration (Start Menu > Programs > Qognify 5) change to Management database (MaxDB) and create a backup via **Backup**. The backup will be stored in C:\Program Files\Qognify\SAPDB\backup.

3. Install Qognify VMS7.5.
4. Start the Qognify Administration Tool (Start Menu > Programs > Qognify) on the newly installed system and restore the backup of the existing system under Management database (MaxDB).

   > **Note that the backup must be available locally and must not be unpacked!**

5. Install and activate a new license (see "Info" on page 116).

After the upgrade

Changes

- All users except the administrator are disabled.
- The administrator's password is reset to "pass". (The passwords of all other users must be reassigned during activation.)
- The services SeeTec5_ENT, SeeTec5_EVT, SeeTec5_AUTH, SeeTec5_ALARM, and SeeTec5_EXT will be migrated to a single service called VMS_CORE. Hence, there is only one log file "core.log" and only one configuration file "core.conf.xml".
- The names of all services now start with "VMS_".
- Indication of the storage volume is no longer possible at camera configuration / image storage. It can only be configured for time limit. Cameras, for which a storage volume was configured, will have a time limit set to 9999 days.
- The division between ExpansionPackage and CorePackage no longer exists.
- The installer moves all application components into the single target directory C:\Program Files\Qognify.
- Monitor wall is replaced by DisplayAgent.
- Encrypted server communication is standard without the need of further configuration.

- Fly-out windows are not available anymore.
- Dockable GUI elements are not available anymore.
- Suppressing alarms is not available anymore.
- Qognify Gateway Services (SGS/SAG) is HTTPS only.
- Blackberry Mobile not available anymore.

Checks

1. Check the configuration of the services AvExport and Gateway service after the migration in the SeeTec VA Administration Tool, as the configuration of SeeTec 5 is not migrated.
2. Recalibrate the Qognify Analytics Channel and set up all Qognify Analytics rules.
3. Check server side motion detection and reconfigured if required.
4. Check the configuration of video classifications.

5

Login

Once the system is installed, you have to log in on the client to use the installed services.

To automate the startup of the client, command line parameters can be defined, e.g. to start the client with a different language or with predefined passwords (see "Command line parameters" on page 497).

KEEP THE ADMINISTRATOR'S PASSWORD IN A SECURE PLACE!
If you forget the administrator's password and no additional users have been added to the administrator group, it is no longer possible to access the system configuration settings. The administrator password cannot be restored.

1. Start the **Qognify VMS client** in the **Qognify** folder in the Start menu or on the desktop.

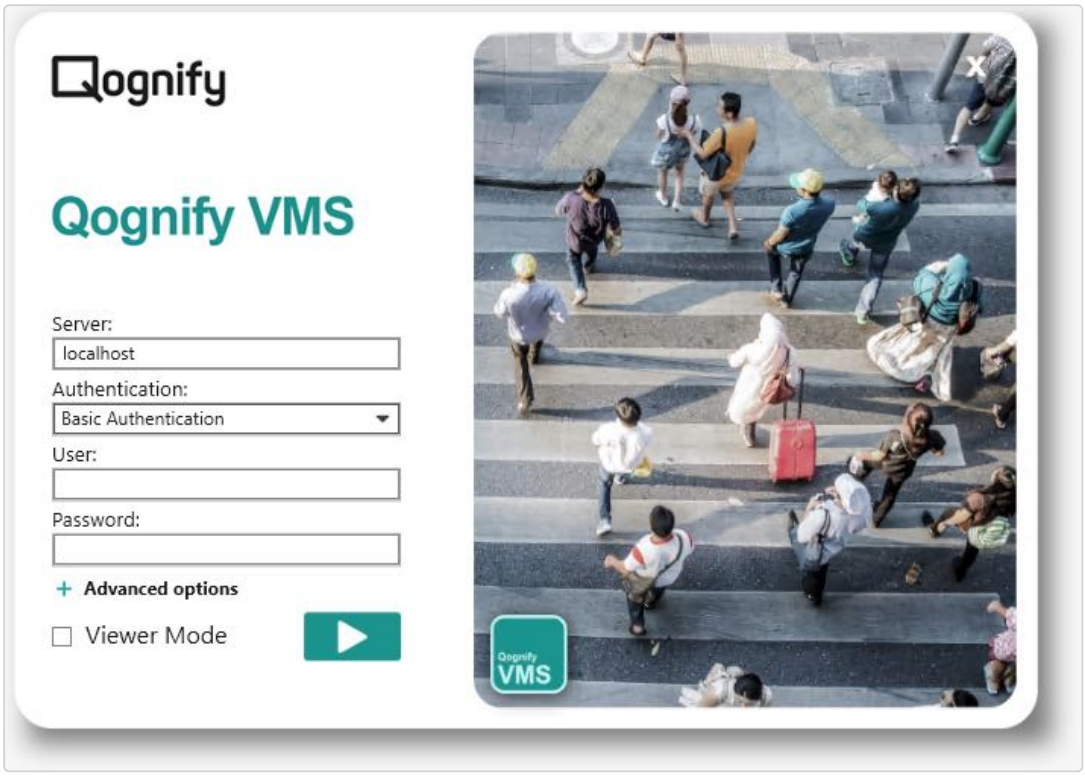


Fig. 11: Login

2. Select the **Authentication** method. The following authentication methods are available:
   - Basic authentication with user name and password as defined in the configuration within Qognify VMS.
   - Windows authentication with the current user credentials of the Windows operating system, i.e. the same login as required for logging into the system. The user will have the rights of the groups he is in (see "Groups" on page 338).
   - Windows authentication with the user's Active Directory (AD) credentials. The user will have the rights of the groups he is in (see "Groups" on page 338).

   > **This feature can only be used if the use of Active Directory (AD) is part of the Qognify VMS license.**

3. If **Basic Authentication** is selected, enter the **user** name and the **password**.

   > **Make sure the user name and password are entered correctly, as the system distinguishes between upper and lower case (case-sensitive).**

4. Apply by clicking the arrow. The client is started in surveillance mode (see "Surveillance mode" on page 131).

> **In Viewer mode, Qognify VMS is used for the display of exported data in Archive mode (see "Anywhere Viewer" on page 503).**

All login attempts (successful and failed) are logged in the report view of the report mode together with the IP or name of the computer used.

The number of failed login attempts is defined in configuration mode by the administrator. Also, a failed login attempt can trigger an notification, which is also defined in configuration mode (see "Configuring the user security settings" on page 448).

Changing the password

When logging in for the first time, you are required to modify the default user password.

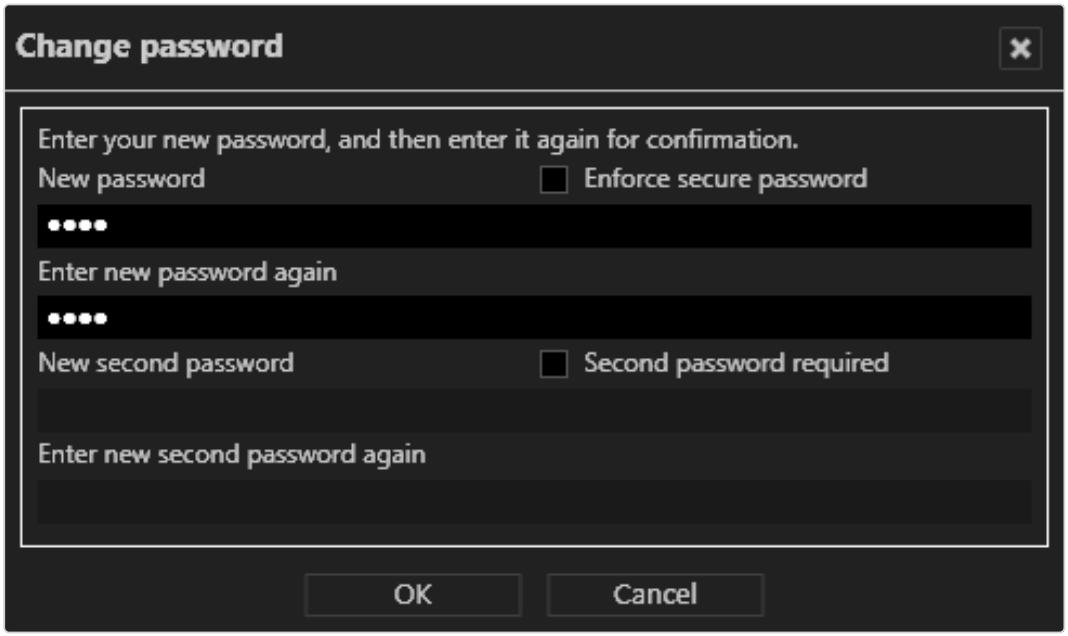


Fig. 12: Change password

1. Enter the **User** name ("administrator") and default **Password** ("pass").
2. Enter your new password.
3. Disable **Enforce secure password** if you do not require increased password security (see "Configuring a user" on page 330).
4. If necessary, enter a second password (see "Configuring a user" on page 330).
5. Click **OK**.

Changing the database backup password

Database backups are encrypted and require a password. When logging in for the first time, you are required to modify the default database backup password.

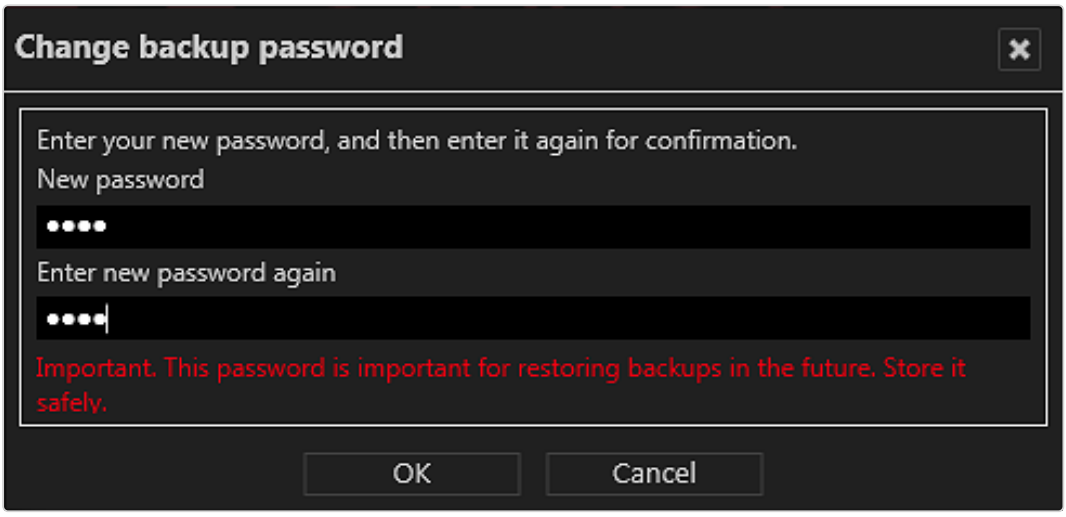


Fig. 13: Change the database backup password

1. Enter the database backup password.
2. Repeat the new database backup password.
3. Click **OK**.

Advanced login options

In the advanced options of the login screen, additional user management functions or log in as a user with two passwords is configured.

1. Click **Advanced options** in the login window.

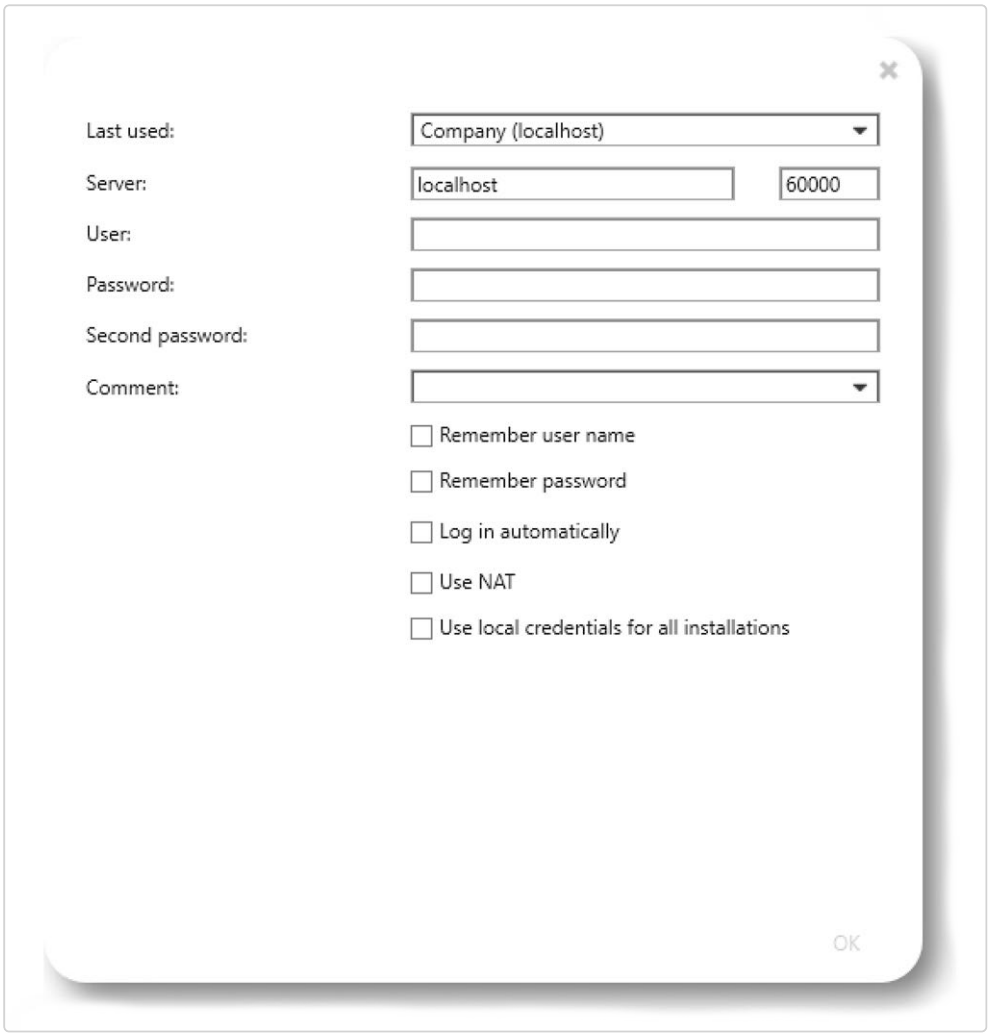


Fig. 14: Advanced login options

The following options are available:

- **Last used**: list of previously connected servers
- **Server**: name and port of a different server
- **Second password** if required for login
- **Comment**: additional information for the selected login.

- **Remember user name** and **Remember password**: avoids having to enter the user data for log in. The system enters the specified user name and password in the login window.

  > **Due to legal regulations, in France the user name and password may not be saved for installations.**

- **Log in automatically**: displays the user interface when the program starts up (without log in).
- **Use NAT**: enables the client to access a different server over the internet. Deselect this option if no internet connection is required. This option requires NAT-settings in configuration mode (see "Configuring the NAT list" on page 443).
- To login to all installations with the same user name and password, select **Use local credentials for all installations**. Optionally this option can be activated in the installation manager (see "Disconnect and reconnect a Qognify installation" on page 84).

  > **Make sure that the remote user credentials are the same as the local credentials.**

KEEP THE ADMINISTRATOR'S PASSWORD IN A SECURE PLACE!
If you forget the administrator's password and no additional users have been added to the administrator group, it is no longer possible to access the system configuration settings. The administrator password cannot be restored.

Logging in Viewer Mode

The viewer mode provides a way of accessing a reduced set of features in Qognify VMS without connection to the database and the user directories for viewing exported data in offline mode.

1. Restart Qognify VMS and select **Viewer Mode**.
2. Apply by clicking the arrow on the login screen. The client starts in Viewer Mode.

6

The user interface

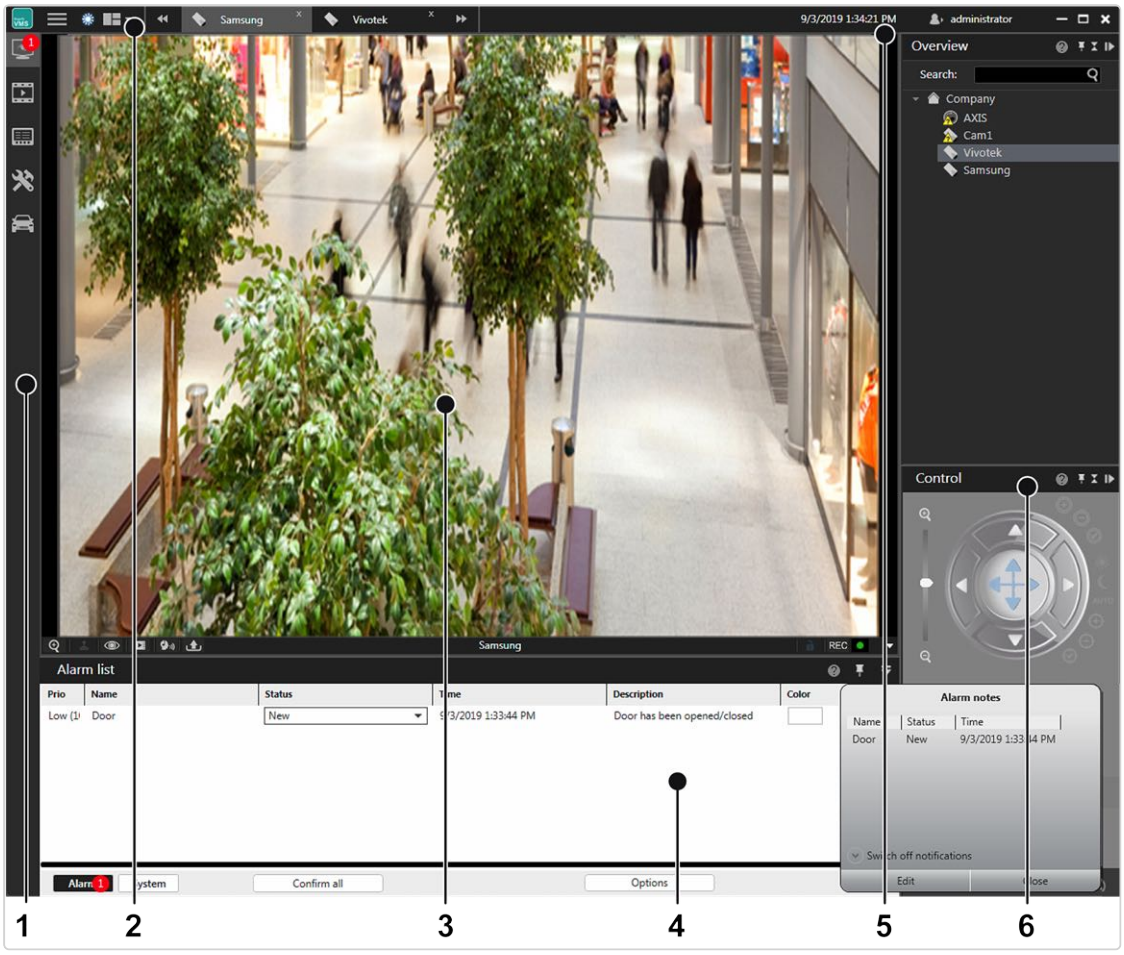


Fig. 15: The user interface

The user interface is divided into different sections:

- **The mode bar** (1) allows you to switch between surveillance mode, archive mode, report mode, configuration mode and LPR mode (see "The mode bar" on page 126).
- **The function bar** (2) provides basic operating functions that can vary depending on the mode used. (see "The function bar" on the facing page). The function bar also contains the menu (see "The menu items" on the facing page).
- **The Work area** (3) is the main window for displaying the selected mode functions. The work area can be divided in multiple tabs containing different contents like cameras, layers, LPR functions etc. (see "Work area" on page 132).
- **Information** control (4) is displayed in the lower part of the work area. The information control is used for the alarm list and system messages (see "Alarm list and system messages" on page 158) in surveillance mode, and for displaying search results in configuration mode (see "Searching in configuration mode" on page 198).

- **Login information** (5) displays which user currently logged in and provides user switching and easy logout (see "Changing the user" on page 126).
- **The control bar** (6) contains the tabs for controlling the contents of the work area (see "The control bar" on page 127).

The function bar

Fig. 16: The function bar

The function bar provides basic operating functions that can vary slightly depending on the selected mode:

- **Logo toggle** ( ): Triggers an action when clicked. The logo action can be configured from the tools menu (see "Configuring a logo action" on page 112).
- **Navigation** ( ): Opens or closes the navigation menu for the menus File, View, Tools, Info, Help (see "The menu items" below).
- **Day- / night mode toggle** (/): Switches the background of the user interface darker (night mode) or lighter (day mode). This function is available in all modes except the configuration mode.
- **Layer menu** ( ): This function allows the user to create and arrange custom layers in surveillance mode (see "Custom layers" on page 137).
- **User information** ( ): Displays the current user and provides functions to log off or change the user (see "Changing the user" on page 126).
- **Current time**: Displays the current client time and date.
- **Tab selector**: Displays all opened layers in tabs for quick access (see "Creating layers and adding objects" on page 133).

The menu items

The menu items are available in all modes. The display of some menu items depends on user rights:

- **File**. Options for changing the settings of the client, the language, password, profile, installation, installation manager, and switches the user (see "File menu" below).
- **View**. Manages the settings of the connected monitors and the video wall as well as the LPR master data (see "View" on page 85).
- **Tools**. Displays and removes the write protection of recordings, configures the multiple export of image data and defines the logo action (see "Tools" on page 96).
- **Info** Displays information on the system and license (see "Info" on page 116).
- **Help**. Calls the Help system and provides options for solving problems (see "Help" on page 125).

File menu

The menu "File" displays the following options:

- Client configuration
- Change language
- Change password
- Change profile
- Change user
- Switch installation
- Installation manager
- Exit

Client configuration

You can specify settings for visualization options, behaviors on user input, network load etc. with the client configuration.
Modification options for the following categories are available:

> **The settings of the client are stored locally in the Windows user profile. They can only be changed by a user with administrator rights.**

1. After changing the client configuration, restart the client for the changes to take effect.

Client

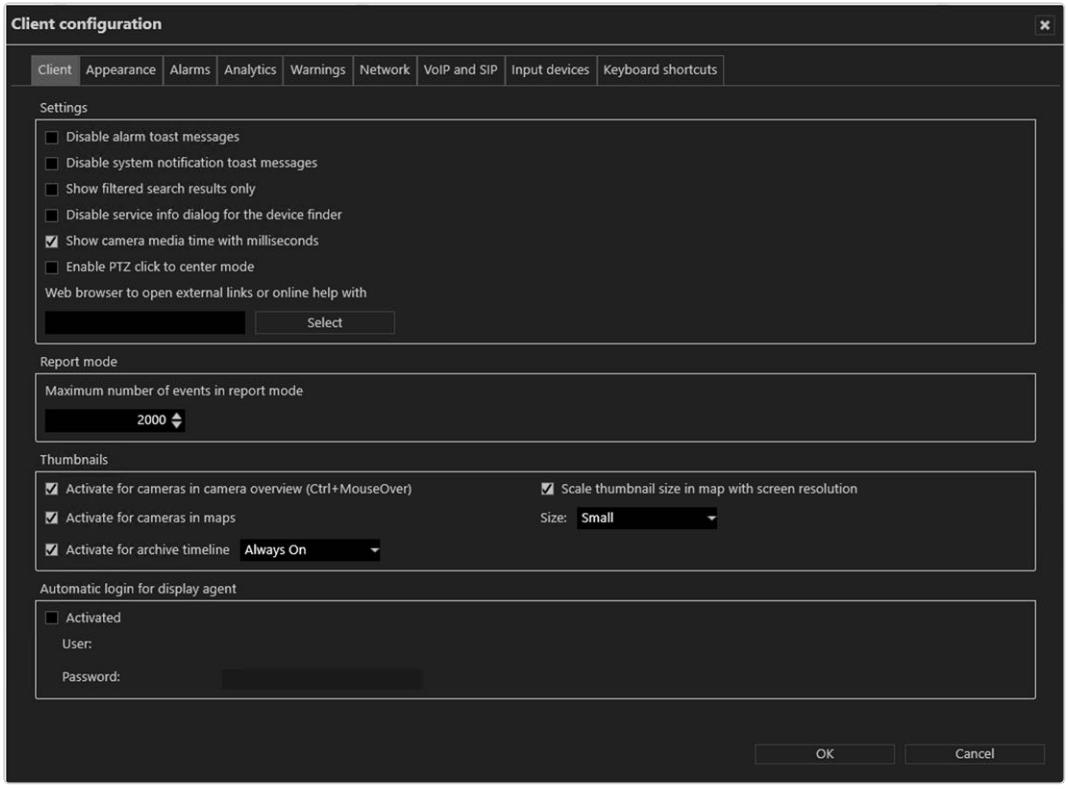


Fig. 17: Client configuration - Client

Settings

- **Disable alarm toast messages** to suppress alarm notification for toast messages (see "Alarm notification" on page 160).
- **Disable system notification toast messages** to suppress system notifications for toast messages (see "System messages" on page 161).
- **Show filtered search results only** to display only the relevant search results in the search results list. (If deactivated, the search results will be highlighted in the control bar, but all items are displayed.)

- **Disable service info dialog for the device finder** to suppress the status information about the "SSDP Discovery" service (SSDPSRV), which may not be installed on the operating system. This service provides UPnP (Universal plug and play) support for the DeviceFinder. If the check box is activated, the user will be asked to install the service if not already available.
- **Show camera media time with milliseconds** to display the time in the archive player with more detail (see "Archive player" on page 164).
- **Enable PTZ click to center mode** to enable clicking into the live image of a camera to shift the selected point into the image center using physical pan/tilt.
- **Merge alarm list and system messages** to display alarms and system messages in a single list (see "Alarm list and system messages" on page 158).
- **Web browser** to open external links or the online help system.

Report mode

- **Maximum number of events in report mode** to limit the amount of events displayed in report mode.

Thumbnails

- **Activate for cameras in camera overview** to activate the thumbnail view of the camera image in the camera overview. You can open thumbnails by rolling the mouse cursor over the names of the cameras in the overview while holding down the CTRL key.
- **Activate for cameras in maps** to activate the thumbnail view of the camera image in the maps. You can open the thumbnail by using the mouse pointer to hover over the name of the camera in the map.

- **Scale thumbnail size in map with screen resolution**. The scaling adapts the thumbnail size to the screen resolution. The higher the resolution of the screen is, the higher will be the resolution of the thumbnails.
- **Activate for archive timeline** displays a small preview image of the selected time segment when moving the mouse over the timeline in archive mode. The options are "Off", "Always on" and "Control Key pressed", with "Always on" as the default setting.

Automatic login for DisplayAgent

- When **Activated**, the **user** name and **password** must be entered to start the DisplayAgent automatically when the client is started.

Appearance

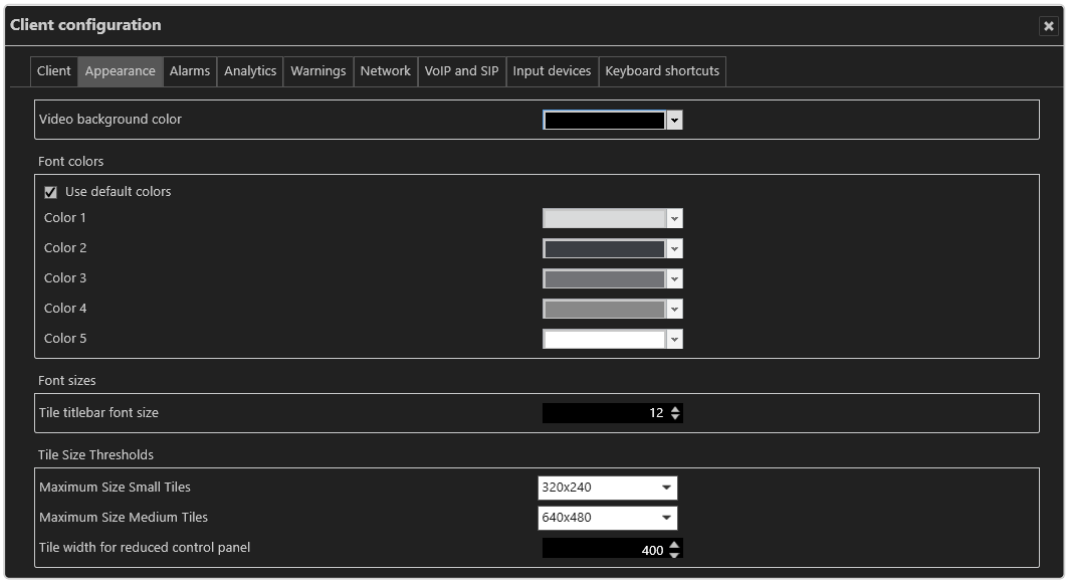


Fig. 18: Client configuration - Appearance

- **Video background color** is displayed around a video image if its aspect ratio is not the equal to the aspect ratio of a view or tile.

- **Font colors**. The default font colors can be changed
  - **Color 1** on a dark background
  - **Color 2** on a light background
  - **Color 3** on a mixed background like the main menu
  - **Color 4** on a mixed background like table headings
  - **Color 5** on a video player border (black background)
- **Use default colors** reverts to the default settings.
- **Tile titlebar font size**: The font size in the title of layers or tiles can be changed.
- **Tile Size Thresholds**: Sets the thresholds for streaming different resolutions based on tile size.
  - **Maximum Size Small Tiles** displays the maximum tile size for low streaming resolution.
  - **Maximum Size Medium Tiles** displays the maximum tile size for average streaming resolution.
  - **Tile width for reduced control panel** sets the tile width for a minimized tile when only the audio controls should be displayed.

Alarms

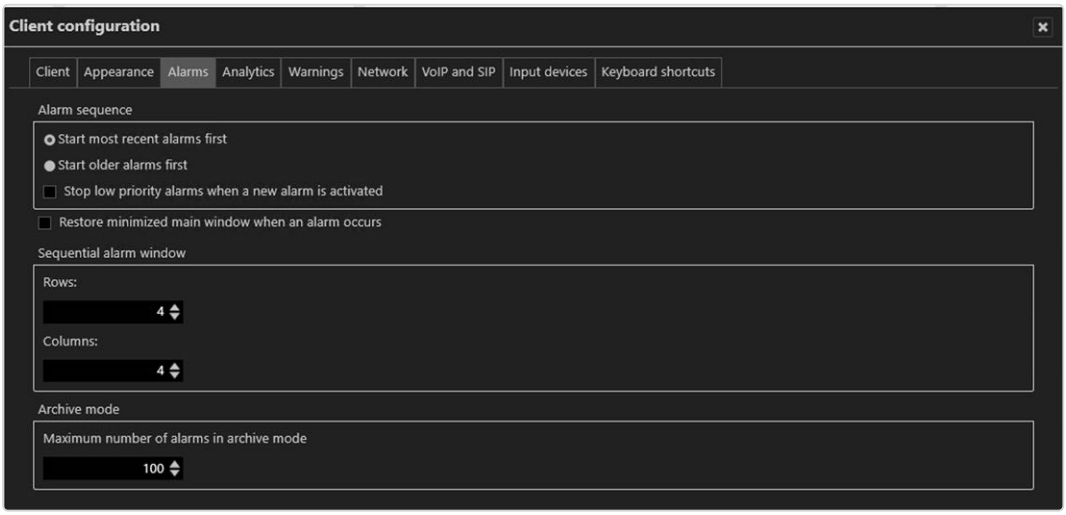


Fig. 19: Client configuration - Alarms

- **Alarm sequence** to specify starting with more recent or older alarms when processing the alarm list.

- **Stop low priority alarms when a new alarm is activated** to stop low-priority alarms (priority 1-4) before the end of the predefined alarm interval is reached (see "Configuring an alarm" on page 361).

  > **High priority alarms cannot be stopped.**

- **Restore minimized main window when an alarm occurs** to restore the main window in case of an alarm. If this option is not activated, the main window will not be restored in case of an alarm.
- **Sequential alarm window** to specify the desired number of rows and columns to be displayed (see "Adding a sequential alarm window" on page 86).
- **Maximum number of alarms in archive mode** to specify the maximum number of alarms displayed in archive mode (see "Archive mode" on page 163).

Analytics

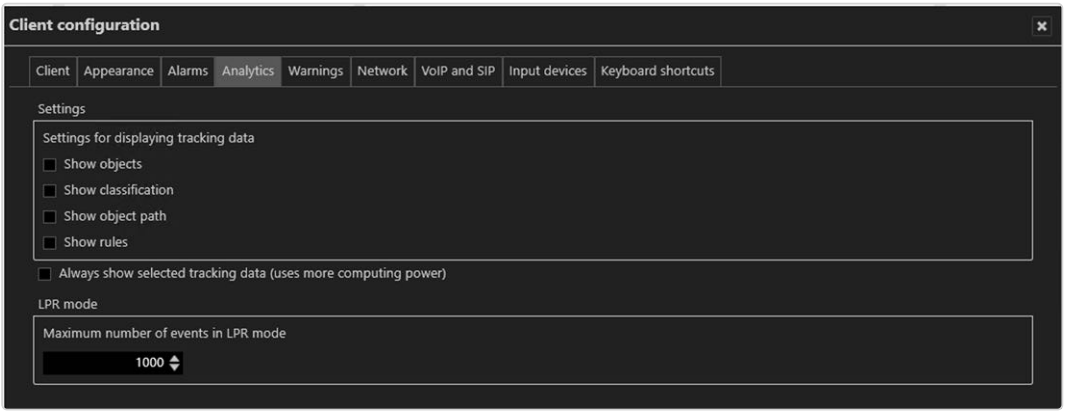


Fig. 20: Client configuration - Analytics

The tracking data settings are defined as global settings in configuration mode (see "Qognify Analytics" on page 301). They can be activated separately.

1. Select which tracking data should always be displayed in selected camera images:

- Objects
- Classification
- Counts

- Object path
- Rules

2. Select **Always show selected tracking data** to display tracking data also in not selected camera images. This options needs more performance on the client.
3. Configure the **Maximum number of events in LPR mode** when searching for license plates. When the maximum is reached, a warning is displayed.

> **Increasing the number may lead to sluggish performance and longer loading times.**

Warnings

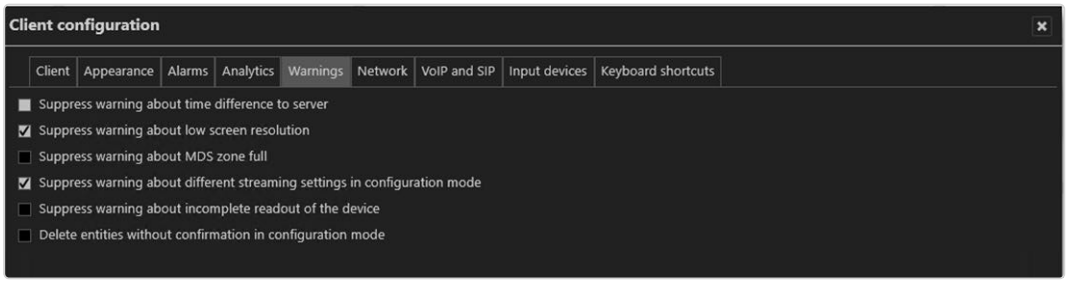


Fig. 21: Client configuration - Warnings

- **Suppress warning about time difference to server** to suppress a warning if there are more than ten seconds of time difference between client and server.
- **Suppress warning about low screen resolution** to suppress a warning if the screen used does not have a high enough resolution (see "System requirements" on page 31).
- **Suppress warning about MDS zone full** to prevent a warning when the storage depth limit of the multimedia database is reached (see "Qognify Administration Tool" on page 465).
- **Suppress warning about different streaming settings in configuration mode** to suppress the warning that recording losses can occur if there are discrepancies between the settings for standard and alarm recording if not using a second stream for alarm recording (see "Video streams" on page 242).

- **Delete entities without confirmation in configuration mode** to delete the entity (camera, time template, alarm, button, etc.) without receiving a request for confirmation when you select **Delete** in configuration mode.

Network

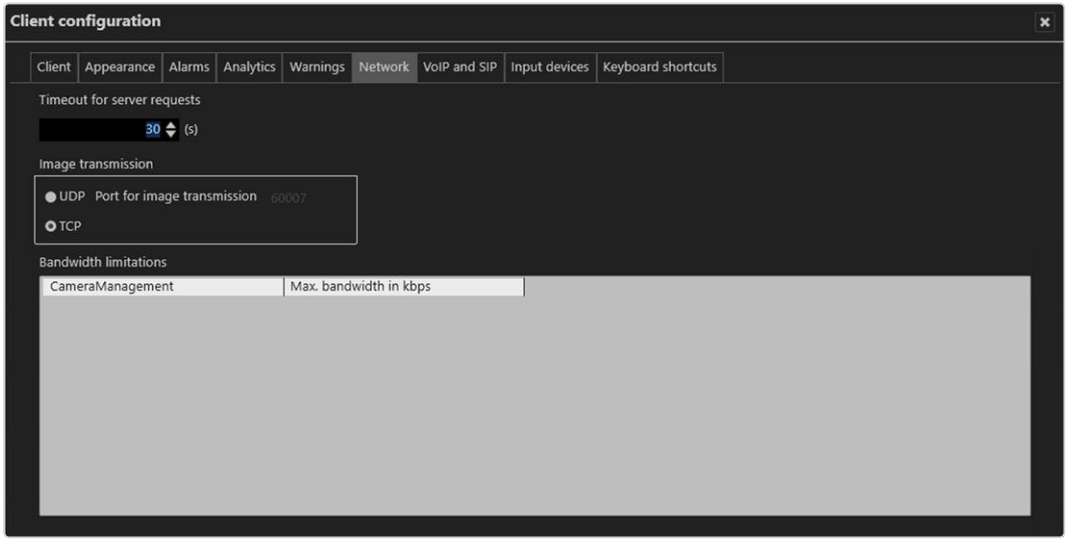


Fig. 22: Client configuration - Network

The following options are available:

- **Timeout for server request** to increase the time limit in seconds if the server does not respond quickly enough.
- **Image transmission** via the UDP or default TCP port. The UDP port is freely selectable.

  > **Select UDP only on 100% reliable network connections.**

- **Bandwidth limitations** to limit the bandwidth when accessing DeviceManager servers with a low-bandwidth connection to avoid overloading the network.

  > **It is not recommended to limit the bandwidth between a client and the server. Frames will be dropped on a limited bandwidth.**

VoIP and SIP

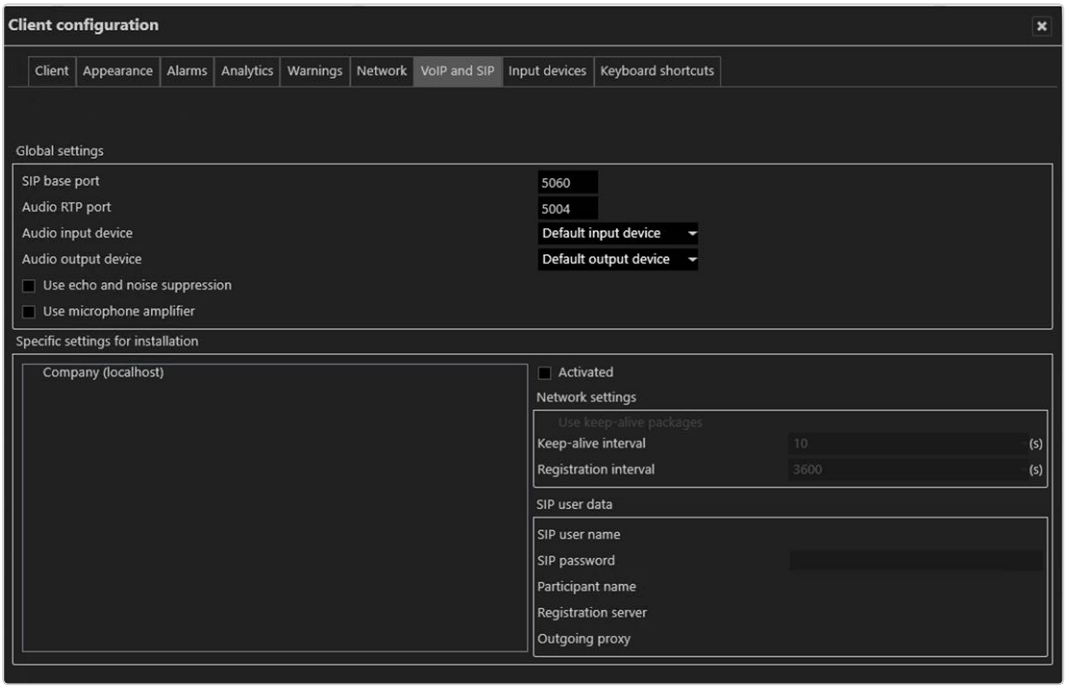


Fig. 23: Client configuration - VoIP and SIP

The Qognify VMS client can act as SIP client to communicate with other clients or voice units that support the SIP standard.

- **SIP base port** number (the default is "5060").
- **Audio RTP port** (the default is "7000").
- **Audio input device** and **audio output device**. Regardless of this, incoming calls go via the operating system's default audio output device.
- **Use echo and noise suppression** to improve the sound quality.
- **Use microphone amplifier** to increase the volume of the input device.
- **Specific settings for installation** displays all existing Qognify installations.
- **Use keep-alive packages** to adjust the intervals at which the client is to log in to the SIP or VoIP server. The default value for **Keep-alive interval** is 10 (s), and for **Registration interval** it is 3600 (s).
- **SIP user name** and **SIP password** for the SIP server.
- **Participant name**. The participant name is displayed as the called participant in archive mode.
- **Registration server** and **Outgoing proxy**: IP address of the SIP server.

> **A SIP server is required (see VoIP).**

Input devices

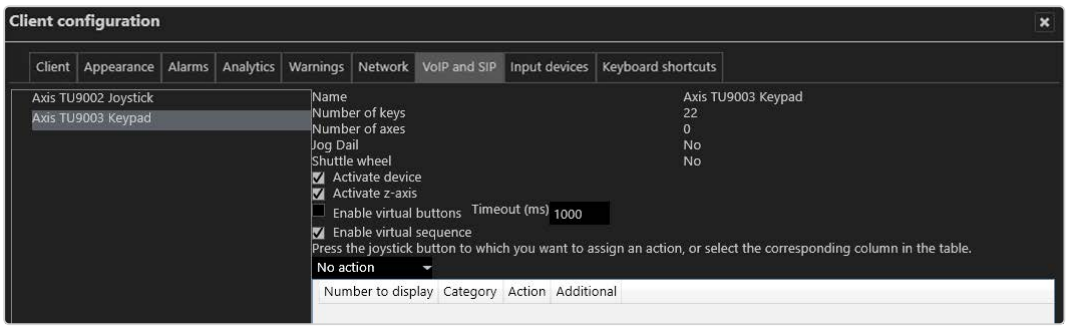


Fig. 24: Client configuration - Input devices

In this section of the client configuration, input devices like jog dials, joysticks, or key pads are configured.

> **The input device or the corresponding device drivers must be installed on the Windows system before it can be configured.**

> **The input device must be connected to the client computer before the client starts. Otherwise it will not appear in the client configuration.**

Select and display entities with buttons of a input device

1. Connect the device to the USB port of the client computer.
2. Select the device. The device functions are listed on the right-hand side of the dialog box.
3. Enable **Activate the device**.
4. Enable the functions, e.g. virtual buttons or virtual sequences.
5. If necessary, activate the z-axis (depending on the hardware, usually available on joysticks).
6. Press the input device button to which you want to assign an action or select the buttons number from the list.
7. Select the desired action (for example, when a certain button of the joystick is pressed, a camera or a map is to be displayed in a certain window of the Qognify configuration).

> **After confirming the changes, restart the client for the changes to take effect.**

Configuring virtual buttons or sequences of the Axis TU9003 keypad

Using the Axis TU9003 keypad, a camera can be displayed on a local Qognify window or on a Qognify GmbH DisplayAgent (see "DisplayAgent" on page 87). To reduce the number of buttons that must be configured, each camera is numbered.
Only one of the following options can be assigned:

- With the option **virtual buttons**, up to 1000 virtual buttons can be configured for the Axis TU9003 keypad to invoke up to 1011 actions.
- The use of **virtual sequences** requires a correctly configured entity numbering (see "Configuring the entity numbering" on page 444). In surveillance or archive mode virtual sequences can be started on the keypad (see examples below).

> **For a detailed description of the Axis TU9003 keypad functions refer to the manufacturer's documentation.**

1. Select **Enable virtual buttons** or **virtual sequences**.
2. With virtual buttons enabled, enter a value for the timeout (ms). Within this period, the user must press the buttons to execute the configured action.
3. For buttons or virtual buttons, select any button on the keyboard to display the assigned button in the list in the column “Number to display” and define the action from the drop-down menu.

> **After confirming the changes, restart the client for the changes to take effect.**

Key assignments for keypad TU9003

The keys of the Axis TU9003 keypad are assigned as follows:

F1	Target: Local monitor / window

F2	Target: Display Agent
F5	Show web page
F8	Target: Tile
F9	Show temporary layer
F10	Show map
	Show layer
	Show camera

Examples

- 0-F1-1- : Show camera 1 in main window.
- 0-F1-1- : Show layer 1 in main window.
- 0-F1-1-F10: Show map 1 in main window.
- 0-F1-5-F9: Show an empty 2x2 temporary layer window in main window.
- 1-F8-1- : Show camera 1 in first tile of the current layer.

Configuring virtual buttons or sequences of the Axis T8312 keypad

Using the Axis T8312 keypad, a camera can be displayed on a local Qognify window or on a Qognify GmbH DisplayAgent (see "DisplayAgent" on page 87). To reduce the number of buttons that must be configured, each camera is numbered. Refer to the manufacturer's documentation of the keyboard. Only one of the following options can be assigned:

- With the option **virtual buttons**, up to 1000 virtual buttons can be configured for the Axis T8312 keypad to invoke up to 1011 actions.

- The use of **virtual sequences** requires a correctly configured entity numbering (see "Configuring the entity numbering" on page 444). In surveillance or archive mode virtual sequences can be started on the keypad (see examples below).

For a detailed description of the Axis T8312 keypad functions refer to the manufacturer's documentation.

1. Select **Enable virtual buttons** or **virtual sequences**.
2. With virtual buttons enabled, enter a value for the timeout (ms). Within this period, the user must press the buttons to execute the configured action.
3. For buttons or virtual buttons, select any button on the keyboard to display the assigned button in the list in the column “Number to display” and define the action from the drop-down menu.

After confirming the changes, restart the client for the changes to take effect.

The keys of the Axis T8312 keypad are assigned as follows:

- **First row:**
  - F1: Local display
  - F2: Display agent
  - F5: Web page
- **Second row:**
  - : Predefined layer
  - : Camera
  - : Tile
  - : Temporary layer
  - : Maps
- **Keypad:**

- 0 - 9: Predefined sequences, buttons or virtual buttons 0...999
- : Toggle between buttons 0...999 and virtual buttons 1000...1011:
  - Alt: 1001
  - : 1002
  - : 1003
  - : 1004
  - : 1005
  - : 1006
  - F1: 1007
  - F2: 1008
  - F3: 1009
  - F4: 1010
  - F5: 1011

Key assignments for keypad T8312

1. Press the key combinations on the keypad. The first key selects the entity or number, the second number specifies the entity type or device type, e.g.:
   - Pressing the keys 0 - F1 - 5 - displays camera number 5 on display (F1) number 0, the local main display.
   - Pressing the keys 3 - F2 - 1 - displays the predefined layer number 1 on the display agent (F2) number 3.
   - Pressing the keys 1 - F1 - 5 - displays the layer number 5 (a 2x2 layer) on display (F1) number 1 (the local secondary display).
   - Pressing the keys 0 - F1 - 5 - - 45 - displays the camera number 45 on display (F1) number 0 (the local main display) in tile number 5.

For improved efficiency when assigning the virtual buttons or sequences, the software “remembers” the previously assigned location, e.g. windows or tiles.

Example

- The keys 0 - F1 - 5 - ▢ have been assigned to display camera 5 on display 0 (see above). Entering next 6 - ▢ will display camera 6 on the same display.

Restrictions and special cases

- The jog dial and shuttle wheel are supported in archive mode for the Axis T8313 jog dial controller. The Axis TU9001 does not have a jog dial available.
- If multiple joysticks of the same type are used, the joystick settings can become mixed up after the update to version VMS 7.5. If this happens, change the physical connection accordingly.
- It must be made sure that no other application has access to the joystick to prevent erratic behavior.
- The Videotec DCZ control unit is also supported with the following restrictions:
  - Only 32 of 38 buttons can be used.
  - Only the outer jog dial can be used in archive mode.

Keyboard shortcuts

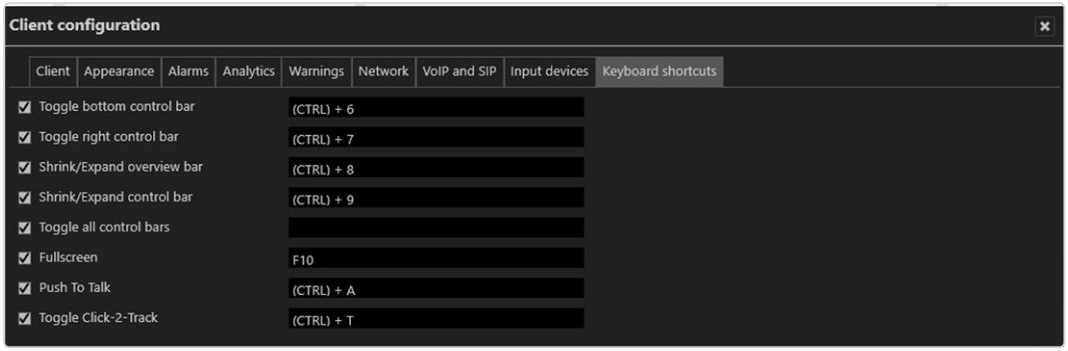


Fig. 25: Client configuration - Keyboard shortcuts

Custom keyboard shortcuts can be defined for rearranging the client surface.
The following functions can be configured:

- Toggle bottom control bar (default: (CTRL) + 6)
- Toggle right control bar (default: (CTRL) + 7)
- Shrink/Expand overview bar (default: (CTRL) + 8)
- Shrink/Expand control bar (default: (CTRL) + 9)
- Toggle all control bars (default: ESC)
- Full screen (default: F10)
- Push To Talk (default: (CTRL) + A)

For more shortcuts, see "Shortcut keys" on page 501.

Changing the language

The following languages are available for the user interface and the help system:

- English
- Czech
- Danish (only user interface)
- Dutch
- French
- German
- Greek (only user interface)
- Hebrew
- Italian
- Japanese (only user interface)

- Norwegian (only user interface)
- Polish
- Portuguese (only user interface)
- Russian
- Romanian
- Spanish
- Swedish (only user interface)
- Thai (only user interface)
- Turkish

Additionally, you can define the user interface with a user defined language (see "Technical_Guides_Qognify_Qognify VMS_7.5_EN.pdf").

1. Select **Change language** from the **File** menu.
2. Select the desired language. If you select **Windows default**, the operating system language is used.
3. Click **OK** to apply the selection, and restart the client.

Changing the password

You can change the user's password at any time, depending on the user rights.

1. Choose **Change password** from the **File** menu.

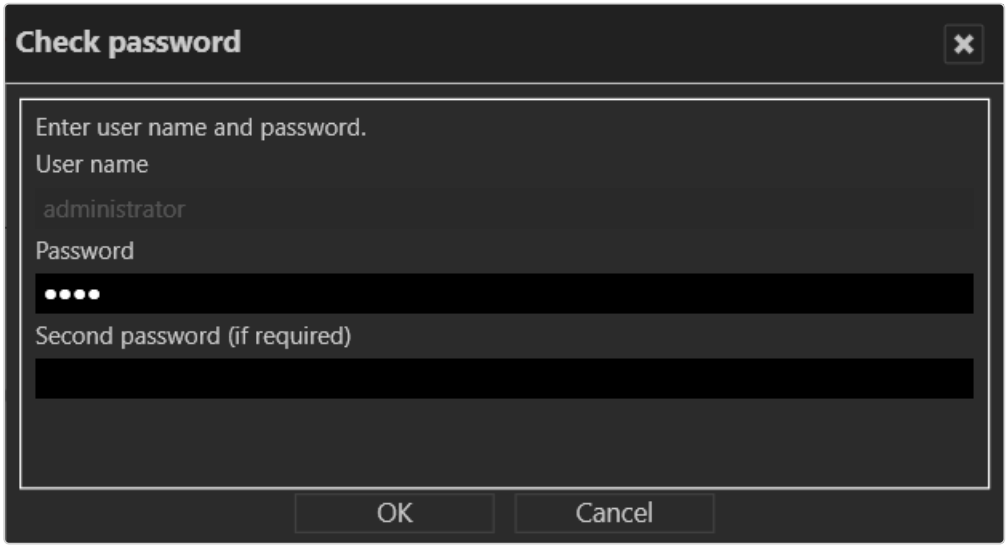


Fig. 26: Changing the password - 1

2. Enter the password for the current user and click **OK**.

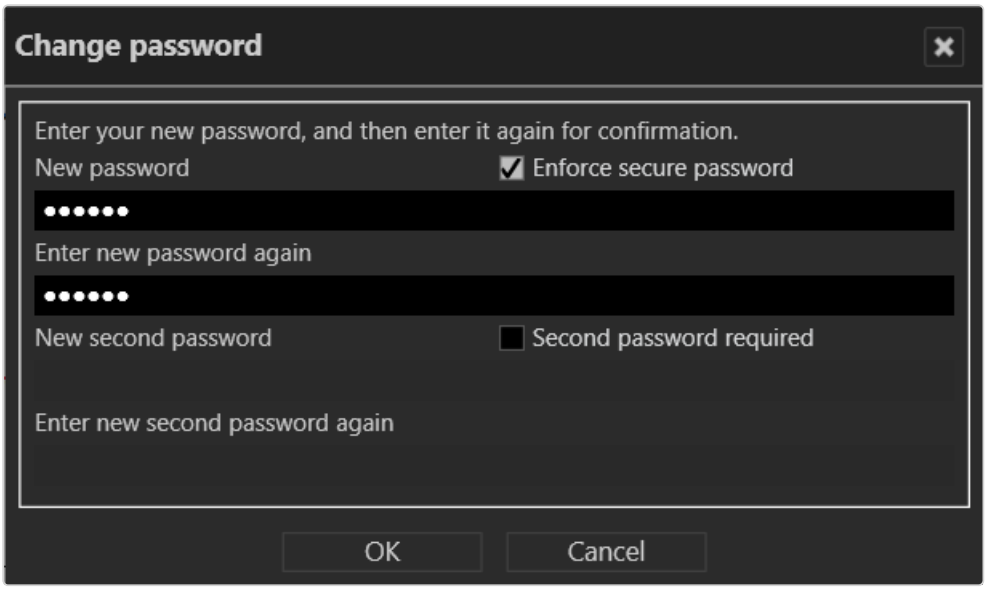


Fig. 27: Changing the password - 2

3. Enter the new password.
4. Click **OK** to apply the password.

Changing the profile

If multiple profiles are used (user profile, group profile, etc.), you can change to a different profile. The profiles can be managed in configuration mode (see "Profiles" on page 345).

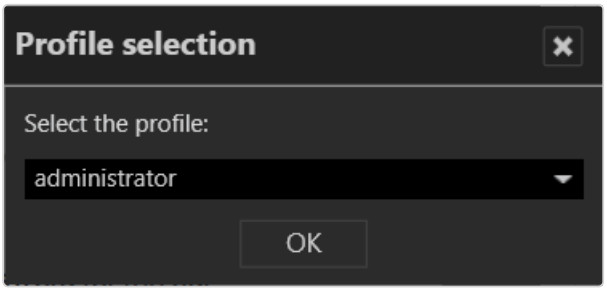


Fig. 28: Changing the profile

1. Select **Change profile** and the desired profile.
2. Click **OK** to confirm. The current profile is logged off, and the selected profile is activated.

Changing the user

A different user can log on without closing the Qognify VMS client.

1. Select **Change user** from the **File** menu, and select the user.
2. Click **OK** to confirm your selection. The current user is logged out, and the new user has to log in with a user name and password (see "Login" on page 55).

Alternatively, the user can also be changed via the user icon in the function bar (see "Changing the user" on page 126).

Switching Qognify VMS installation

If you have installed multiple independent Qognify servers, you can connect to a different Qognify server.

1. Choose **Switch installation** from the **File** menu. The login screen is displayed (see "Login" on page 55).
2. Enter the server name or IP address and the user name and password. The current installation is terminated, and the selected installation is started.

Installation manager

The installation manager manages and defines connections to multiple installations (CoreServers). The current connection status is displayed.

Connecting to multiple installations can result in huge client and network load.

When using bandwidth optimized archive playback from multiple installations, make sure all installations are appropriately configured (see "Bandwidth optimization" on page 430).

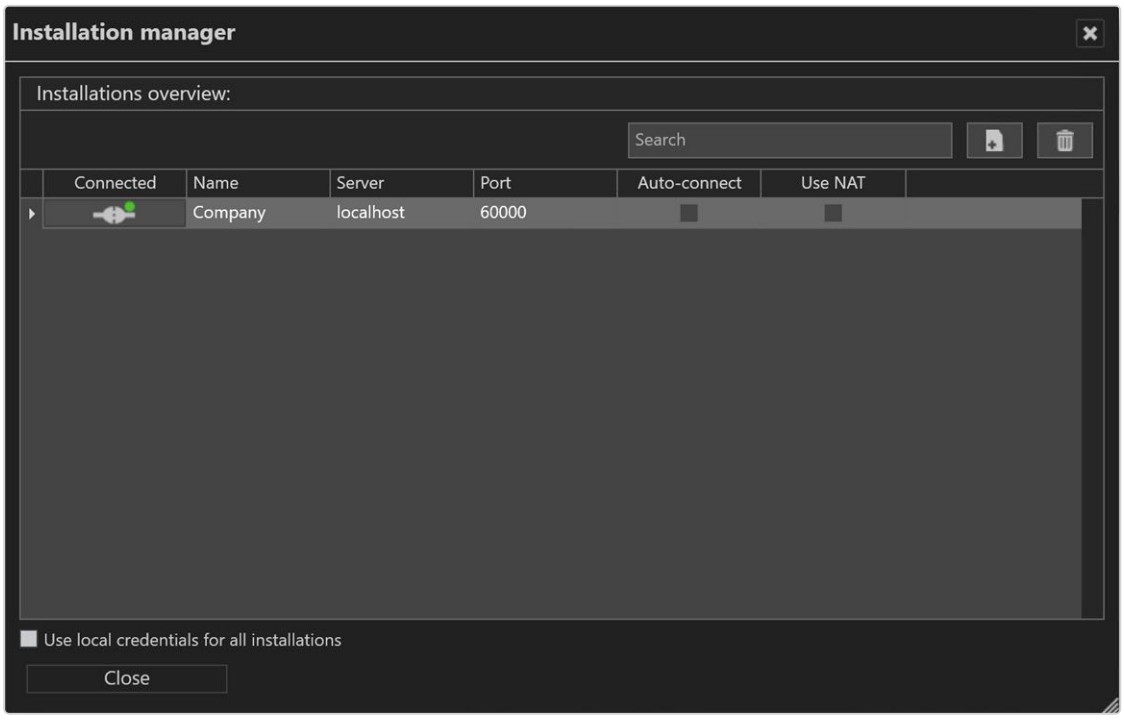


Fig. 29: Installation manager

- **Autoconnect**: Activates or deactivates the client to connect to the selected installation automatically.
- **Search**: Searches for available installations
- **New** ( ): Adding a new installation
- **Delete** ( ): Removes the installation from the list

1. To edit a connection, click on the respective installation name.
2. To add an installation, select **New** ( ) and edit the connection. The new installation is not connected automatically.
3. To connect an available installation, enable **Autoconnect**.

Requirements

- The server version on all servers to which a connection will be established cannot be higher (newer) than the client.
- All servers must support multi-installation login. A license must be available for Qognify multi-installation login.

Add an installation

1. Select **Installation manager** from the **File** menu, and select the desired servers.
2. If the server is not displayed, add the installation by entering the installation name, the IP address or host name, and the port number of the server.
3. Click **Add**.

Reorder installations

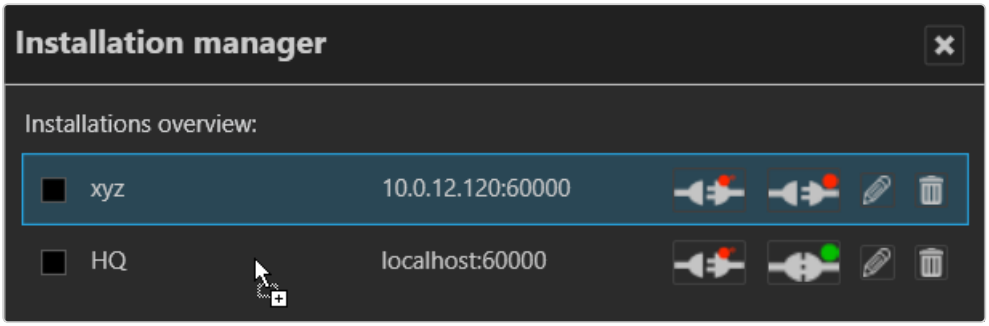


Fig. 30: Reorder installations

1. Reorder the list of installations by selecting one object and dragging it to the designated place in the list.

Disconnect and reconnect a Qognify installation

The color marker in the symbol indicates the connection state: a green dot indicates a connected system and red dot stands for disconnected.

1. Click **Autoconnect** to connect the client to the selected server automatically when starting the client.
2. For manual connecting or disconnecting, click **Connect** or **Disconnect**.
3. To login to all installations with the same user name and password, select **Use local credentials for all installations**. Optionally this option can be activated on the login window (see "Advanced login options" on page 59).

> **In this case make sure that the remote users are the same as the local credentials.**

Edit Qognify installations

Changes the IP address, host name and the port number of the selected server.

1. Click **Edit** at the Qognify installation that you want to change. The selected server is displayed at the bottom of the window.
2. Edit the installation name, the IP address or host name, and the port number of the server.
3. Click **Apply**.

Delete saved Qognify installations

Tidies up the list of Qognify installations most recently called by the client (see "Login" on page 55).

1. Click **Delete**  at the Qognify installation that you no longer want to be available for selection.
2. To delete multiple installations at once, select the installations you want to delete and click **Delete selected objects**.

View

The menu view displays the following options:

- Adding a window
- Adding sequential alarm window
- Keep the aspect ratio
- Borderless display
- DisplayAgent
- Video wall dispatcher
- LPR master data editor
- Count analysis
- Access control data editor

> **The settings made in the View menu are stored locally and have to be made on each client and for each Windows® login profile individually.**

Exceptions are:

- Settings for the "LPR master data editor" on page 87
- Count analysis data

These data are saved on the server(s) by their corresponding services.

Adding a window

This function allows you to distribute the display of the work area to multiple connected monitors.

1. Choose **Add window** from the **View** menu. A second window opens.
2. Move the window to the connected monitor. The client saves the setting and makes it available when you log in again.
3. To use multiple connected monitors, repeat these steps.

Adding a sequential alarm window

In case of an alarm scenario, cameras that are defined as alarm cameras in an active alarm scenario are displayed in a separate alarm window (see "Alarms" on page 356). The name of the camera is displayed and the color of the image frame in the window corresponds to the color of the alarm scenario.

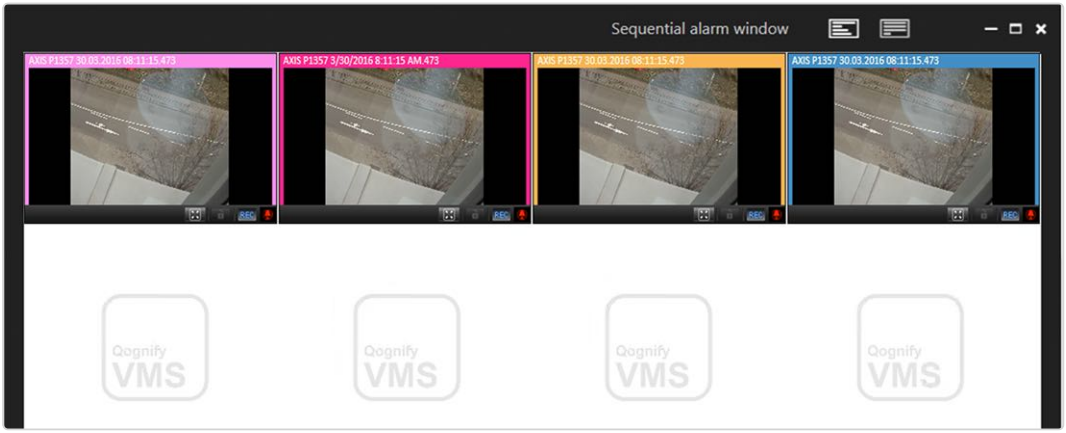


Fig. 31: Adding a sequential alarm window

1. Select **Add sequential alarm window** to display all alarm related cameras in a new dedicated window.
2. Select one of the following options:

- **Row mode** to display images with one alarm per row
- **Continuous mode** to display multiple alarms per row

Keeping the aspect ratio

1. Select **Keep aspect ratio** to adapt the camera image to the layer window. The camera image may appear distorted.
2. Deselect **Keep aspect ratio** to display the camera image with the original aspect ratio.

Borderless display

1. Select **Borderless display** to hide the controls and the bars between the camera images in layers with multiple cameras. If a camera is selected, the border will be displayed.
2. Deselect **Borderless display** to hide the controls and the bars between the camera images in layers with multiple cameras.

DisplayAgent

The Qognify DisplayAgent allows you to use standard PCs and monitors to create a full-fledged remote-controlled video wall controlled by the video wall dispatcher (see "Video walls" on page 398).

> **A video wall dispatcher is required to control a DisplayAgent.**

Video wall dispatcher

The video wall dispatcher can control associated monitors dynamically. You can drag and drop camera images, layers, maps and web pages to display them on video walls, e. g. Qognify Display Agents or eyevis video walls.

LPR master data editor

In the LPR (license plate recognition) master data editor you can add and delete license plates, as well as edit related data like driver's name, tickets, history and notifications.

> **The license plate recognition must be configured in the Qognify VA Administration Tool prior to usage (see "Qognify VMS VA Administration Tool" on page 476) and in configuration mode (see "Configuring the global OCR settings" on page 412 and "Configuring the LPR module" on page 413).**

The LPR master data editor is only available when at least one LPR group with the appropriate rights has been configured (see "License plate groups" on page 400).

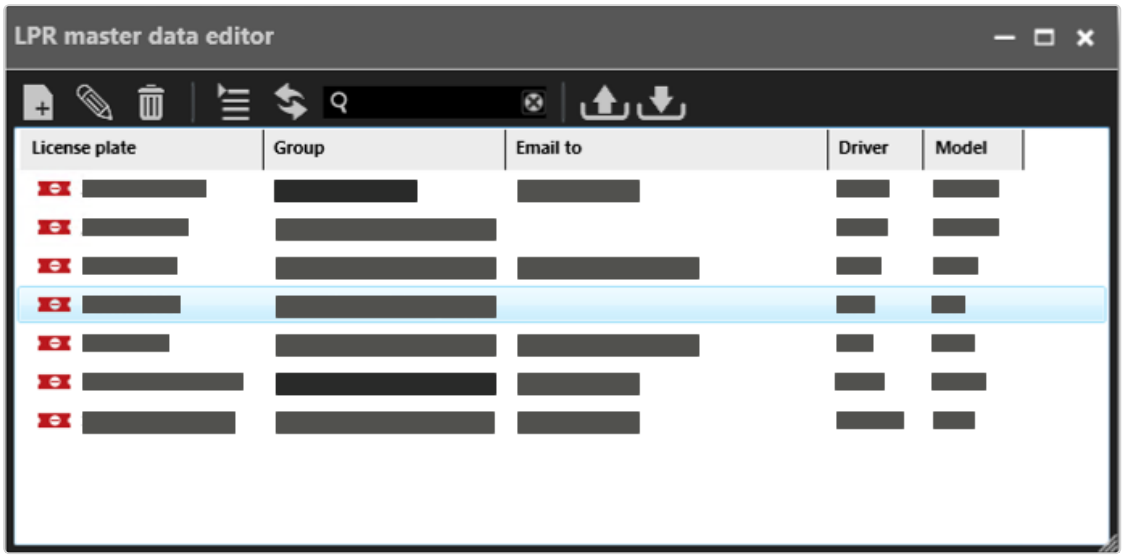


Fig. 32: LPR master data editor

To manage license plates, the following options are available:

Creating a new license plate

Depending on the configuration, the window for entering new data is opened automatically as soon as a license plate is recognized by the camera (see "Configuring the global OCR settings" on page 412).

You can start the LPR master data editor from the "View" menu.

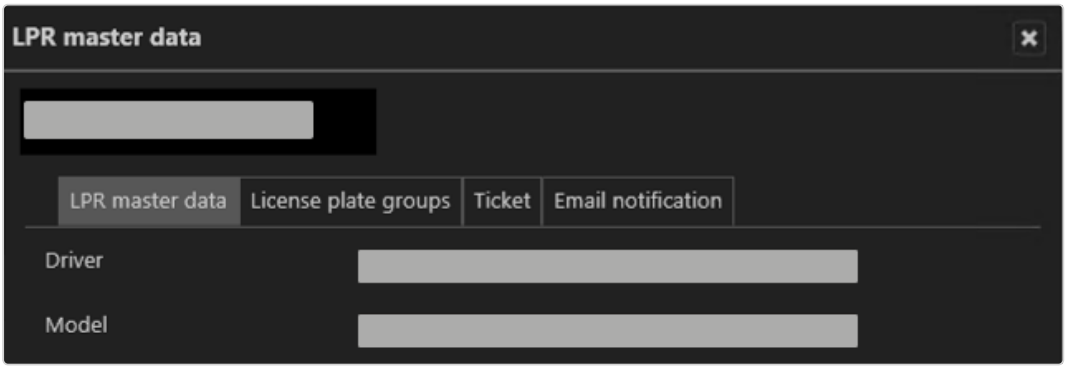


Fig. 33: Creating a new license plate

1. Select **New** in the master data editor.
2. Enter the new license plate in the text box in the upper left if it is not yet displayed.
3. Select the tab **License plate groups** and assign the license plate to one or more license plate groups. License plate groups are created in configuration mode in the license plate groups area (see "License plate groups" on page 400).

4. Optionally, add descriptions for the license plate. The names and number of text fields are defined in the server area in configuration mode (see "Configuring the global OCR settings" on page 412).
5. Select **OK** to apply the settings.

Editing a license plate

1. Select a license plate in the list of the master data editor.
2. Select **Edit** to change the details for the license plate.

LPR master data

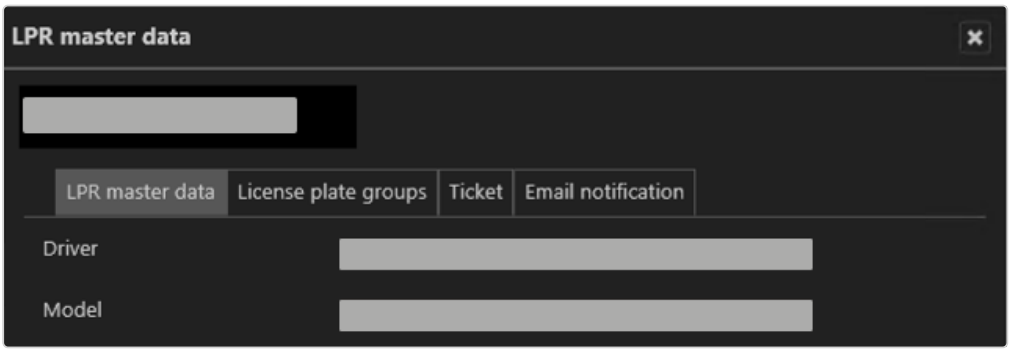


Fig. 34: LPR master data

1. Edit the license plate, the driver's name and the vehicle model.
2. Select **OK** to apply the settings.

License plate groups

License plate groups define the affiliation of a license plate to one or more groups.

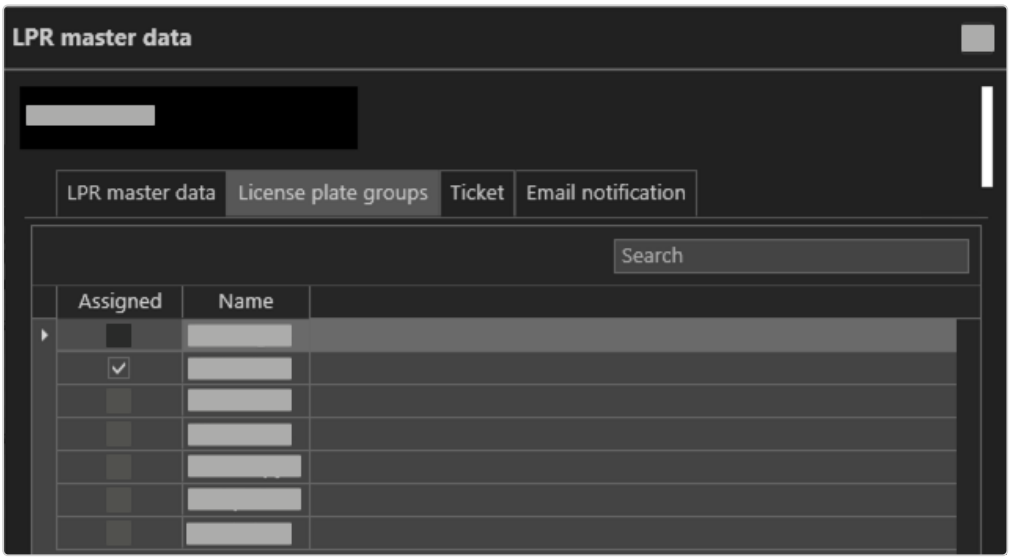


Fig. 35: Ticket

1. Assign the group or groups to which the selected license plate belongs.
2. Select **OK** to apply the settings.

Ticket

Tickets define the validity time periods for certain licenses, e. g. a license plate is allowed to pass a barrier at office time only.

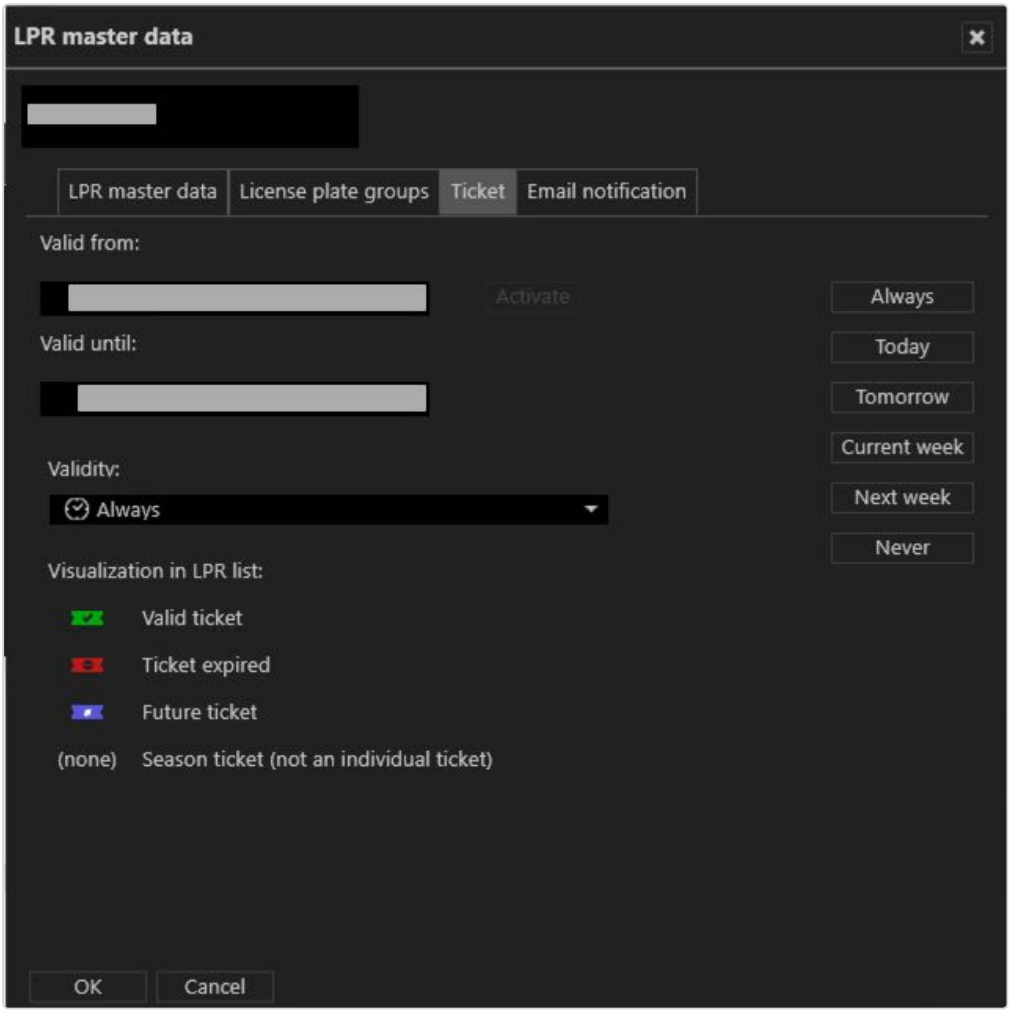


Fig. 36: Ticket

1. Select a predefined **Validity** period for the license plate. The predefined validity periods are displayed on the left.
2. To enter a specific time period, click **Activate** and enter the desired time period. The status of the ticket is indicated in the LPR list by a different font color and an icon. If a period is already defined, activation is no longer enabled.
3. Select **OK** to apply the settings.

Email notification

You can send email notifications to certain recipients as soon as the vehicle with the specific license number is recognized.

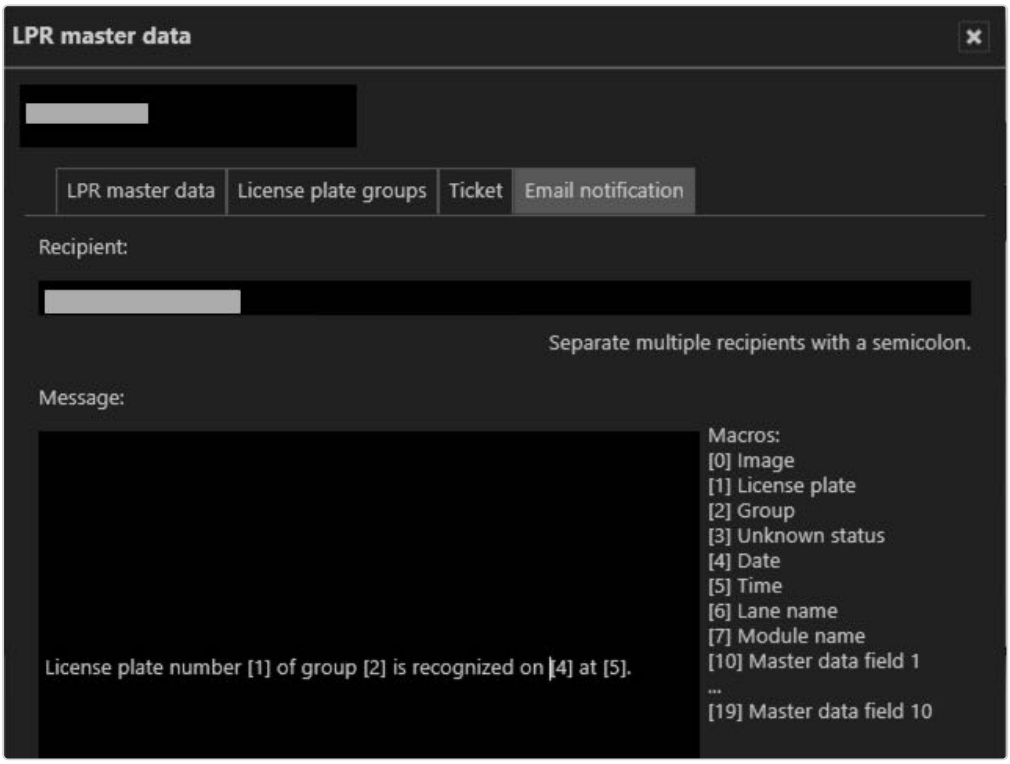


Fig. 37: Email notification

1. Enter the email addresses of the recipients separated by semicolons.
2. Enter the text for the email body. The numbers on the right are placeholders for variables (i.e. license plate details) that are sent automatically.
3. Select **OK** to apply the settings.

Example: The text in the message "License plate [1] was recognized [4] at [5]." is sent as "License plate LU CY 8000 was recognized 15.04.2010 at 4:25 pm." in the email.

Deleting a license plate

1. Select a license plate from the list.
2. Select **Delete** to remove the selected license plate from the list.
3. Acknowledge the deletion. The license plate is removed from the database.

Displaying only license plates of a selected group

1. Select **Change view** and select the license plate group.
2. To see all license plates, select **Change view** and select **All**.

Displaying license plate groups

License plates in the list can be sorted and displayed by license plate groups.

1. Select **Change view** to display only the license plates belonging to the selected group.
2. Click the arrow beside the name of the license plate group to close it.
3. Click the arrow again to open the license plate group again.

Refreshing the view

1. Select **Refresh view** to refresh the data by updating the data from the server.

Searching for a license plate

1. To search for a license plate in the list, enter part of the master data set of the license plate into the **Search** . The search is started automatically, and the result is displayed in the list.
2. Click the **X** in the search to clear the search.
3. When the configured maximum number of search results is exceeded, the result can be exported as a CSV file.

Exporting license plate master data

You can export the master data of selected license plates as a *.CSV file (a text file with values separated by semicolons) in order to analyze or prepare it for further import into databases.

1. Select the license plate whose master data you wish to export. To export multiple license plates, select the license plates while pressing and holding the CTRL key.
2. Select **Export** to export the master data as a CSV file (see "Data fields for export and import" below).

Importing license plate master data

You can import the master data of license plates from a *.CSV file (a text file with values separated by semicolons) .

1. Select **Import** and select a CSV file with the license plate master data to be imported (see "Data fields for export and import" below).

Data fields for export and import

The export and import file must contain the following data fields:

```
LicencePlate;reserved;Group;;;;;;;;;;AlwaysValid;ValidFrom;
ValidTill;Email;EmailText;TimePattern;modify
```

Field name	Value	Note
LicensePlate		The license plate
reserved		
Group	Text	Name of license plate group as configured (see "License plate groups" on page 400) If there is no entry the group will be defined as "unknown"
;	Text	Placeholders for user-defined master data fields (see "Configuring the global OCR settings" on page 412)
ValidFrom	Date-time value	Datetime in the format yyyy-MM-dd HH:mm:ss (for example 2021-01-15 23:59:59)

Field name	Value	Note
ValidTill	Date-time value	Datetime in the format yyyy-MM-dd HH:mm:ss (for example 2021-01-15 23:59:59)
AlwaysValid	1	"always valid" (same values in fields **ValidFrom** and **ValidTill**
	0	different values in fields **ValidFrom** and **ValidTill**
ValidityName	negative value, e.g. -1	Always
	positive value	**ID of related time template**
Modify	■ "0": Modify existing license plate information like group, custom fields etc. ■ "1": Add a new license plate into the database. ■ "-1": Removes the selected license plate information from the editor but does not delete the item in the data-base. ■ "2": Import or export the membership of an additional group of a license plate. For more groups to import or export, add as many lines as needed.	Value change is possible (see "Importing license plate master data" on the previous page). **All fields except for "modify", "LicencePlate", and "Group" are ignored if "modify" is set to "2".**

Example:
LicencePlate;reserved;Group;;;;;;;;;;AlwaysValid;ValidFrom;ValidTill;Email;EmailText;TimePattern;modify
QV MS 8285;;unknown;;;;;;;;;;1;2024-12-01 02:55:30;2024-12-01 02:55:30;;;-1;0
QV MS 8286;;test;;;;;;;;;;1;2024-11-30 02:55:30;2024-11-01 12:55:30;;;-1;1
QV MS 8287;;test;;;;;;;;;;1;2024-10-31 09:29:59;2024-10-01 23:55:00;;;-1;-1

Tools

This menu displays the following options:

- Multiple export of image data (see "Multiple export of image data" on page 104)
- Write protection of recordings (see "Removing write protection from recordings of multiple cameras" on page 111)
- Configure logo action (see "Configuring a logo action" on page 112)
- Status report for automatic image export (see "Status report for automatic image export" on page 113)
- Manual reference image comparison (see "Manual reference image comparison" on page 114)

The Export Designer

The Export Designer in Qognify VMS configures the image export, i.e. adding shapes to hide specific areas of the exported images to increase privacy or defining a time range.

Creating a new export

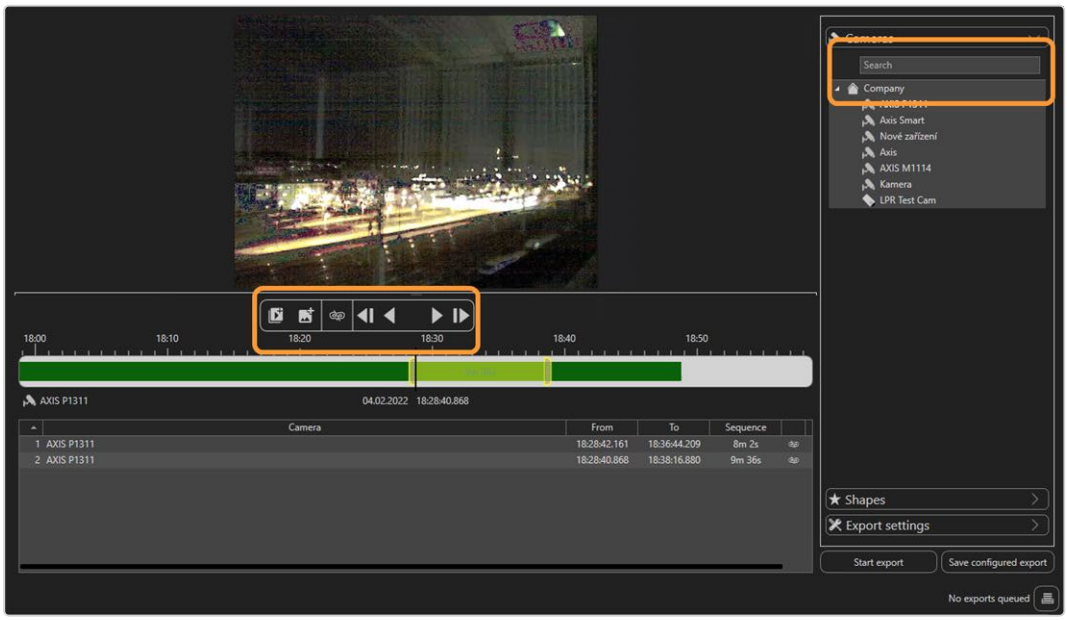


Fig. 38: The Export designer

Defining the image or image sequence

1. In the **Tools** menu, select **Create New** in the Export Designer.
2. Select a camera from the list or search for a camera in the search box above the list.
3. Move the timeline to the desired position. The corresponding frame is displayed. Zoom in or out of the timeline using the scroll wheel of the mouse for more detail.
4. Select **Add sequence** to set the time range of an image sequence export.
5. Drag the handle of the sequence delimiter to the right. This defines the time range for the export. Images within that range can be exported.
6. To mark only a single image for the export, select **Add single image** and drag the marker to the position on the timeline.

Viewing privacy masks

To determine if privacy masks are used in an image, a privacy mask can be highlighted in the preview window before exporting.

> **Without permission to hide privacy masks (or in offline mode), the button is deactivated and privacy masks are always shown and exported.**

1. To highlight a privacy mask in the image, select **Mask** in the **Tools** menu. All privacy masks of the current image in the preview window are displayed.
2. Before exporting a file with privacy mask disabled or enabled, toggle the **Mask** for a selected camera in the list on or off (for exporting, refer to "Defining the export settings" on page 99).

Adding shapes

Areas of the image or image sequence can be hidden in the export to prevent information from being displayed in the export result, e.g. license plates or privacy sensitive objects.

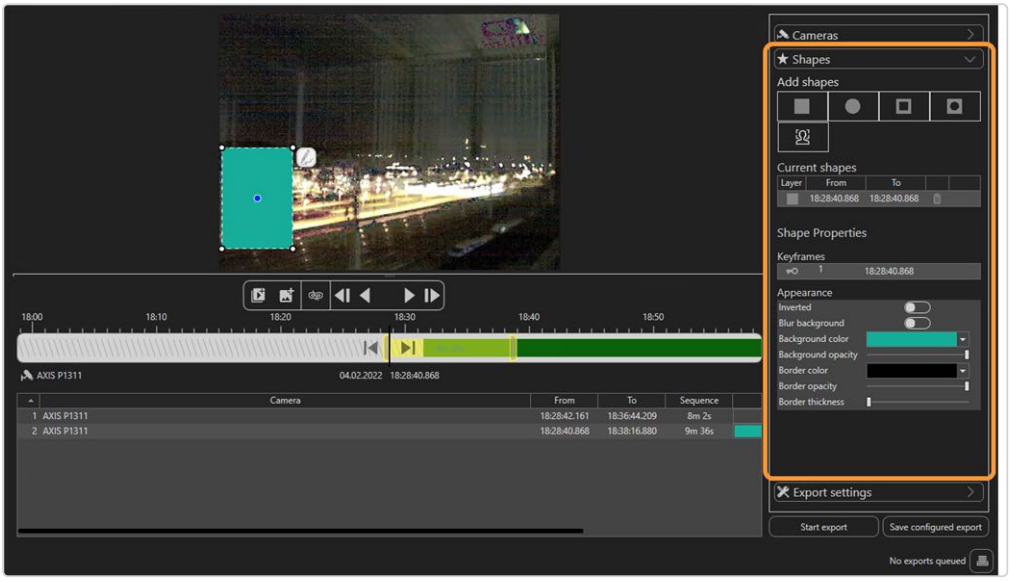


Fig. 39: Adding shapes in the Export designer

1. To add a shape, open **Shapes** in the toolbar on the right and select a shape. The selected shape is placed in the top left corner.
2. Drag the shape onto the image or sequence and resize.
3. Define the background color and transparency as well as the border color and transparency.
4. Move the shape icon on the timeline to define the object to be masked within the time range.
5. To delete a shape from the image, select **Delete** next to the shape in the list of “Current shapes”.
6. To delete a keyframe, select **Delete keyframe** next to the keyframe in the list of “Keyframes”.

Adding a mask with "Click2Mask"

To confirm with privacy protection, persons in a scene can be masked automatically before exporting. This feature is called “Click2Mask”.

To use "Click2Mask", the BVI server module must be installed. This feature requires 64bit mode and cannot be used with the package Qognify VMS S50.

1. To add a mask, select a camera and add an image sequence.
2. Open **Shapes** in the toolbar on the right and select **Analyze** .

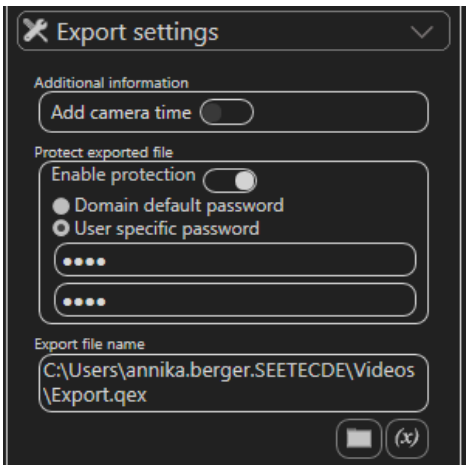
   Qognify VMS analyzes the sequence for a person. The resulting sequence is displayed in the section "Keyframes".
3. If necessary, adjust the shape.

Defining the export settings

For security reasons, not all users are permitted to directly export image data. For users with limited export permissions, the selected export files are collected in virtual "basket" as export preparation.

1. To enable the export preparation, move the slider to the right.

   - When disabled, the files can be directly exported by the user.
   - When enabled, the files are saved on the server as "prepared exports" and can only be exported by a user with sufficient user rights.
2. To define the export settings such as a password protection, open **Export settings** in the toolbar on the right.



3. Enable the display of the camera time as additional information in the image.

4. Enable password protection if required, and set either a domain default password or a user specific password.

   If password protection is enabled for the profile by default, it can only be disabled by the administrator (see "General" on page 346).

5. Click the folder icon and select the export location of the file.
6. To add a variable to the export file name, click **(x)** and select the variable. You can insert variables that will be included in the file name at the time of export, such as:
   - Insert a variable for camera name: The name of the selected camera is included in the exported file name.
   - Insert a variable for export time: The time of the export is automatically included in the file name and can be defined by a timestamp, the date, day, time, etc.
   - GUID: The global unique identifier of the file is included in the file name.
7. Save the export settings.
8. Select **Start export** or select **Save prepared export**, if export preparation has been enabled.

   - When **Start export** has been selected, the exporting progress is displayed.
   - When Save prepared export has been selected, the files are stored on the server in the export preparation queue

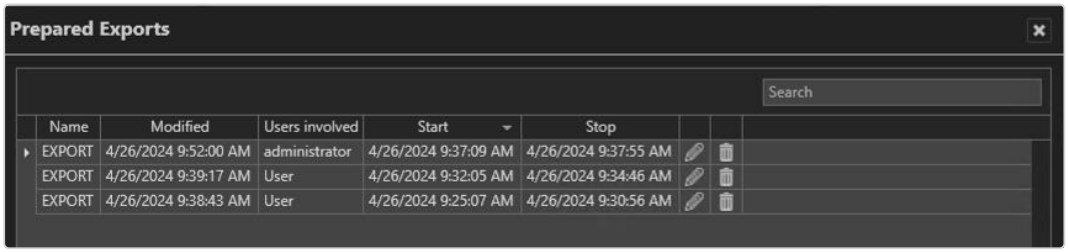
9. Open the Export Manager to open the exported file.

Resuming the export

Exports are queued in the Export Designer. The export settings can be restored in case of failure. The settings file that has previously been configured in the export designer is reloaded into the export queue.

1. In the **Tools** menu, select **Resume** in the Export Designer.
2. Optionally, delete or open and reconfigure the export settings.
3. Start the export.

Opening the prepared exports



Prepared exports that have been configured and saved can be loaded into the Export Designer without the need to reconfigure. The setting will replace the current configuration in the queue.

1. In the **Tools** menu, select **Load** in the Export Designer. Only prepared exports are displayed that the current user has access to.
2. Optionally, delete or open and reconfigure the export settings.
3. Start the export.

Sharing a camera

Apart from a user with administrative rights, any user can share a camera if the user rights are set (see "Manage user rights" on page 333).

If a sharing or receiving party is deleted or deactivated, or loses the sharing or live view rights while sharing cameras, the sharing is stopped.

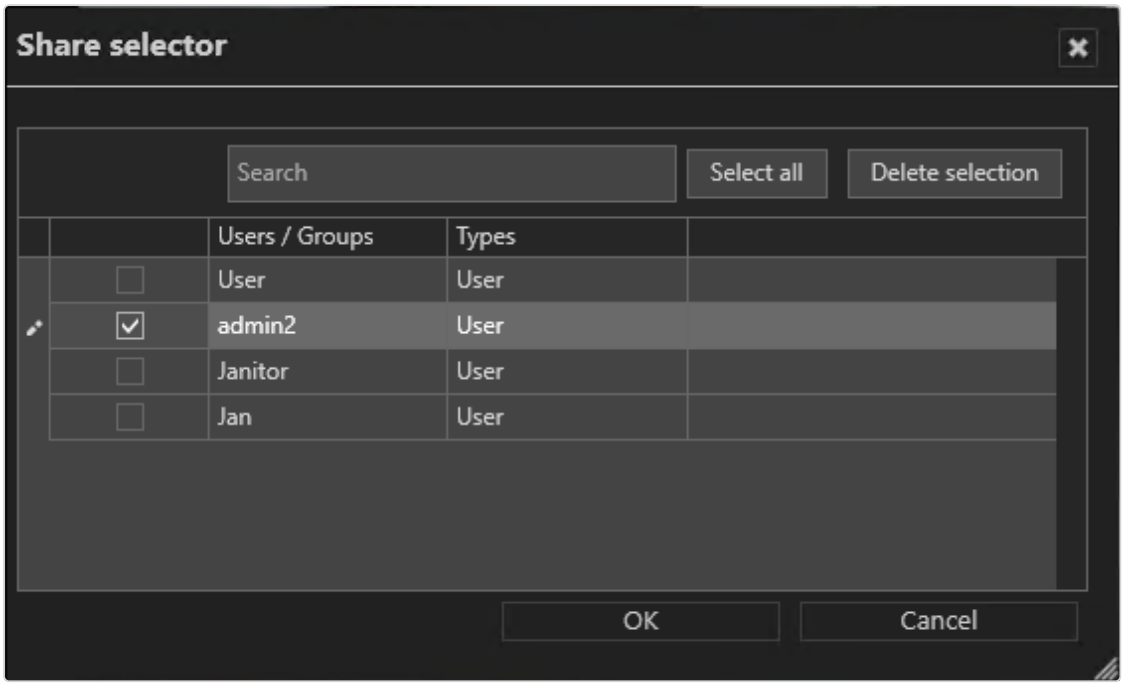


Fig. 40: Sharing a camera

Start sharing a camera

1. In Surveillance mode, open the camera in the work area.
2. Select **Share manager** > **Start sharing** from the **Tools** menu.
3. Select the user or group.
4. Click **OK** to confirm.

Stop sharing a camera

1. In Surveillance mode, open the camera in the work area.
2. Select **Share manager** > **Stop sharing** from the **Tools** menu.

Restriction manager

A user or group can temporarily be restricted from accessing cameras with the "Restriction manager". This can be required to limit access for users or groups that are normally allowed to view images by restricting access to image data exposing sensitive private data (e.g. accidents) for a certain period.

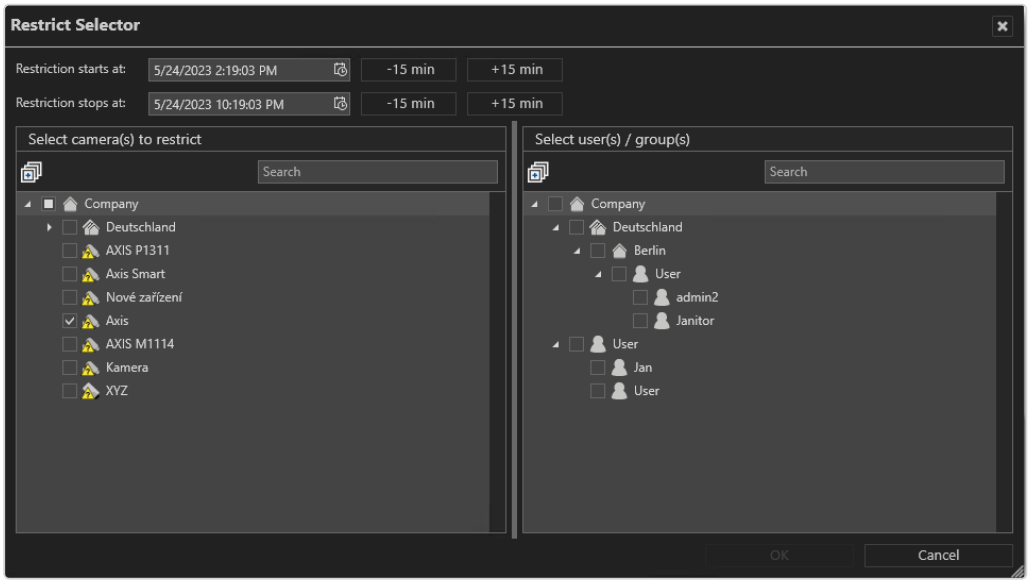
> **Restricting the view of image data to other users requires the appropriate permissions (see "Manage user rights" on page 333).**

Known limitations

- If a user or group restricting other users or groups is deleted the restrictions remain.
- If a user or group restricting other users or groups is deactivated the restrictions remain.
- If a user has permissions from multiple groups and one group is restricted, the user will be restricted as well.
- An administrator can be restricted, but may undo his restrictions.
- Restriction takes precedence over sharing, i.e. a restricted image cannot be seen when restricted for the user or group.
- A user or group can restrict itself.
- If a user is allowed to configure a camera, but is restricted, the user is still able to configure the camera but cannot see a video.

Restricting a camera

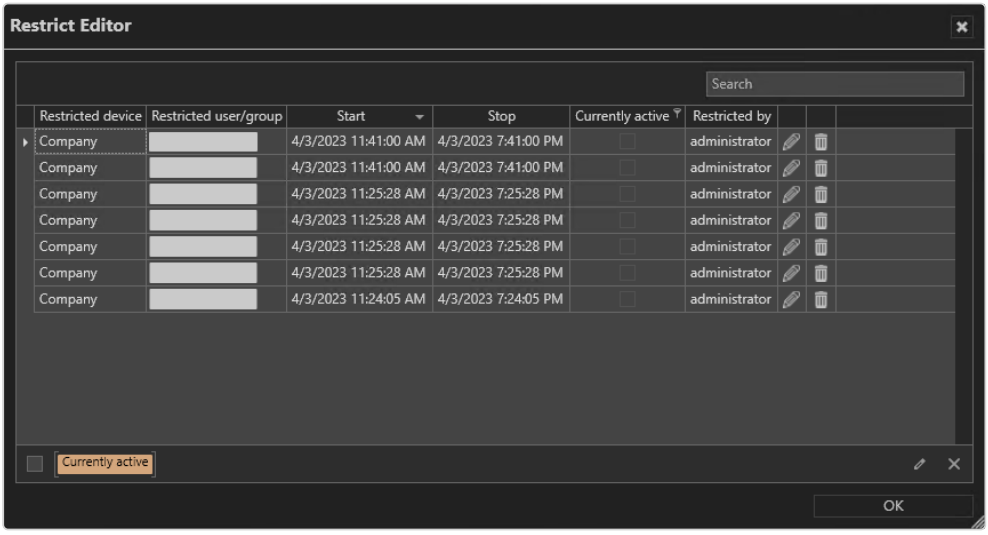
1. In Surveillance mode, select **Restrict manager > Start restricting** from the **Tools** menu. All cameras in the active layer are pre-selected.



2. Define the restriction starting and stopping time.
   - If the time interval is set in the past, the user still can access the image in Surveillance mode, but will not be able to see it in Archive mode.
   - If the time interval is set in the future, the user will neither see the image in Surveillance mode nor in Archive mode.
3. If required, set the restriction interval before and after the restriction period.
4. Select the camera(s) to be restricted.
5. Select the users that should be banned from access.
6. Select **OK**.

Editing restrictions

1. Select **Restrict manager > Edit restrictions** from the **Tools** menu.



2. Select **Currently active** to display only the currently active restrictions.
3. Select the restriction and select **Edit** .
4. Define the start and end times of the restriction and click **OK**.

Multiple export of image data

Image data can be exported with two different processes:

- Using “Multiple export of image data” in surveillance mode.
- Exporting video from the opened tiles in archive mode (see "Exporting recordings" on page 171).

When exporting video recordings, the exported data are saved in encrypted form and can then be played back on a computer without a Qognify installation with the Qognify viewer. The **Qognify viewer** is found in the export directory.
The setup files for the **Qognify Viewer** and the burning tool for burning the exported video material onto a storage medium can also be found in the folder "Tools" of the Qognify installation (see "Anywhere Viewer" on page 503).

> **During the export process, the Qognify viewer installation file is copied to the export folder as well. This allows the files to be run on a computer without a Qognify VMS installation with only the Qognify viewer installed. The Qognify viewer will import the files and display them as separate time intervals.**

1. Select **Multiple export of image data** from the **Tools** menu.
2. Select one of the following options.

AVI export to the client

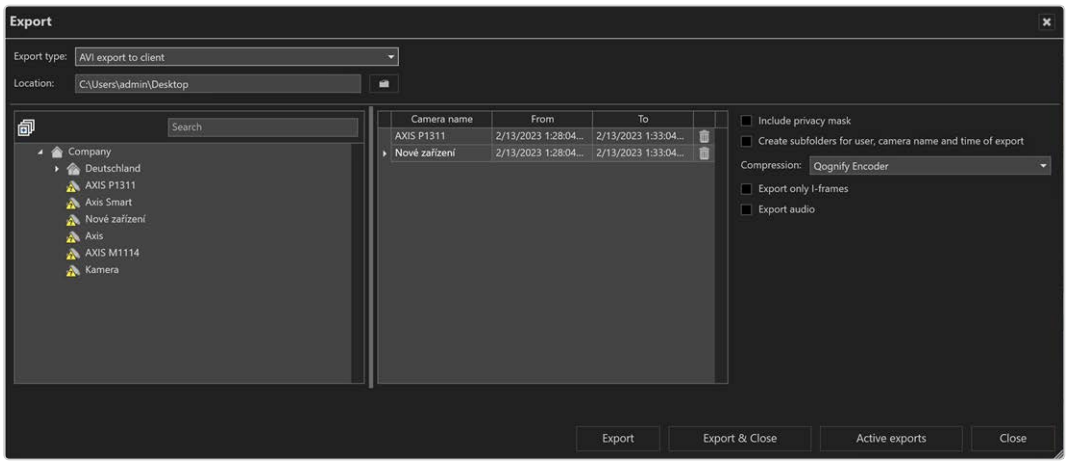


Fig. 41: AVI export of image data

1. Make sure that a temporary folder for image data export to the client is configured and available (see "Video backup" on page 409).
2. To open or close the list, select **Expand/collapse all** .
3. Drag and drop the cameras for export into the right column. For each camera, all marked time spans are displayed.
4. To delete a time span, select **Delete selected items** in the corresponding row.
5. Specify if the image data is exported with or without **privacy masks**.

   Exporting without privacy masks can lead to a breach of privacy laws.

6. To store the exported image data in separate folders by user, camera name and time of export, select **Create subfolders for user, camera name and time of export**.
7. Select the video compression format:
   - Qognify Encoder
   - DV Video Encoder
   - MJPEG compressor
   - Source format
8. Specify if **only i-Frames** should be exported.
9. Enable **Audio** if the video source contains audio channels that should be included in the export.
10. To carry out the export immediately, click **Export**. The settings are saved after export or by closing the window.

The filename of the AVI file has following format:
<camera name>_<fromDate>-<fromTime>_<toDate>-<toTime>.avi
The name cannot be changed. If the name already exists, a sequential number is automatically appended.

JPEG export to the client

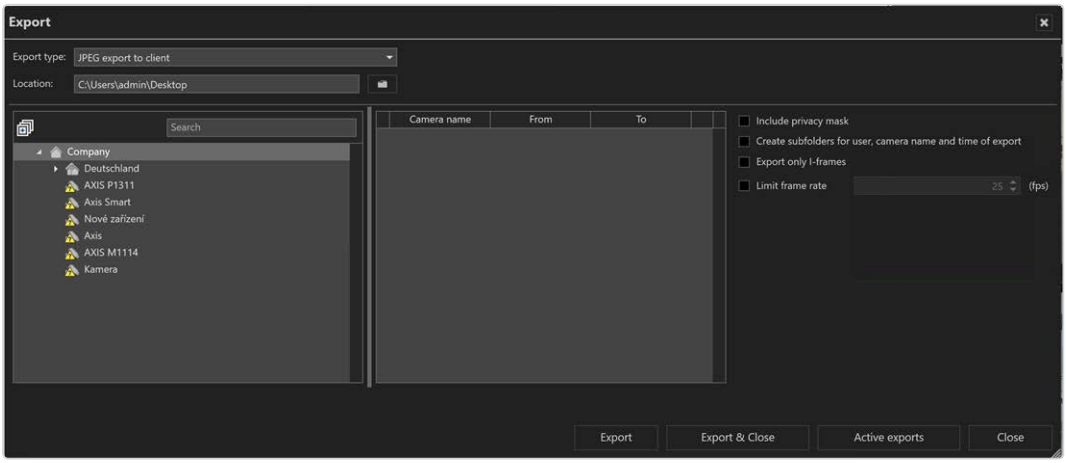


Fig. 42: JPEG export of image data

1. Make sure that a temporary folder for image data export to the client is configured and available (see "Video backup" on page 409).

2. To open or close the list, select **Expand/collapse all** .
3. Drag and drop the cameras for export into the right column. For each camera, all marked time spans are displayed.
4. To delete a time span, select **Delete selected items** in the corresponding row.
5. Specify if the image data is exported with or without **privacy masks**.

   Exporting without privacy masks can lead to a breach of privacy laws.

6. To store the exported image data in separate folders by user, camera name and time of export, select **Create subfolders for user, camera name and time of export**.
7. Specify if **only i-Frames** should be exported.
8. To specify the number of exported frames, enable **Limit frame rate** and specify the number of images per second of video stream (default is 25 fps).
9. To carry out the export immediately, click **Export**. The settings are saved after export or by closing the window.

Export of native data to the client

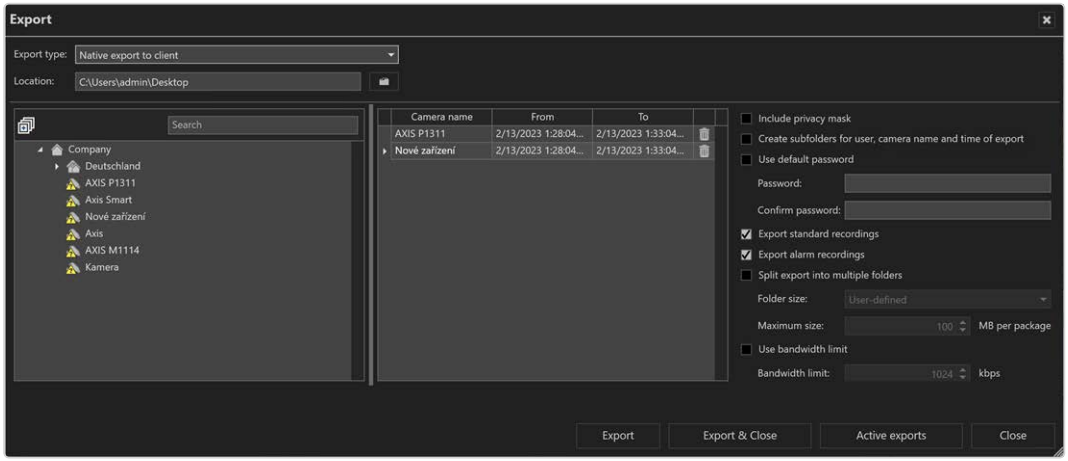


Fig. 43: Export of native image data to the client

1. Make sure that a temporary folder for image data export to the client is configured and available (see "Video backup" on page 409).

   During export, the exported image data from the failover server are transmitted to the production server. Make sure the production server provides enough storage space.

2. To open or close the list, select **Expand/collapse all** .
3. Drag and drop the cameras for export into the right column. For each camera, all marked time spans are displayed.
4. To delete a time span, select **Delete selected items** in the corresponding row.
5. Specify if the image data is exported with or without **privacy masks**.

   Exporting without privacy masks can lead to a breach of privacy laws.

6. To store the exported image data in separate folders by user, camera name and time of export, select **Create subfolders for user, camera name and time of export**.
7. To secure the exported image data using the default password, select **Use default password**.

   This option is disabled when the usage of the default password is enforced in the profile settings in configuration mode.

8. If you want to use your own **password** instead of the default password, enter this password and repeat it. The default password is set in configuration mode in the DeviceManager (DM) section (see "Video backup" on page 409).
9. Specify if only standard recordings should be exported or if **alarm recordings** should be exported as well.
10. To store the exported image data in folders of approximately the same size as the expected file size, select **Split export into multiple folders** and specify the **folder size** and **maximum size** of the image file. Image data that exceeds the specified size is split into multiple files so that they can be stored on data carriers such as CD-ROMs or DVDs.
11. If the image data is to be exported to a client that has only a low-bandwidth connection, select **Use bandwidth limit** and specify the bandwidth limit.

12. To carry out the export immediately, click **Export**. The settings are saved after export or by closing the window.

Exporting native image data to the server

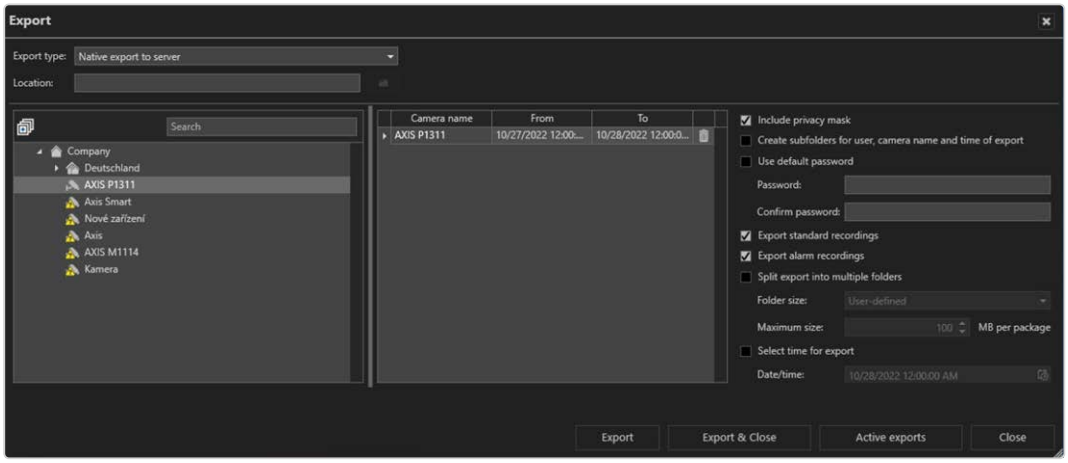


Fig. 44: Exporting native image data to the server

1. Make sure that a temporary folder for image data export to the server is configured and available (see "Video backup" on page 409).

   > **During export, the exported image data from the failover server are transmitted to the production server. Make sure the production server provides enough storage space.**

2. To open or close the list, select **Expand/collapse all** .
3. Drag and drop the cameras for export into the right column. For each camera, all marked time spans are displayed.
4. To delete a time span, select **Delete selected items** in the corresponding row.
5. Specify if the image data is exported with or without **privacy masks**.

   Exporting without privacy masks can lead to a breach of privacy laws.

6. To store the exported image data in separate folders by user, camera name and time of export, select **Create subfolders for user, camera name and time of export**.
7. To secure the exported image data using the default password, select **Use default password.**

8. If you want to use your own **password** instead of the default password, enter this password and repeat it. Optionally, use the default password. The default password is set in configuration mode in the DeviceManager (DM) section (see "Video backup" on page 409).
9. Specify whether only **standard recordings** are to be exported or whether **alarm recordings** are to be exported as well.
10. To split the exported files for storage on multiple data carriers such as CD-ROMs or DVDs, select **Split export into multiple folders**.

    > **The minimum size of the file is 100 MB.**

11. Select the desired **folder size** according to the export medium (e.g. CD, DVD, Blue-ray disc).
12. Specify the **maximum size** of the image file.
13. To carry out the export at a specific time, select **Select time for export**, and then specify a date and time for the export.
14. Specify the **date/time** period for the image data to be exported.
15. Click **Select** and specify the **location** of the exported image data.

    > **During export, the exported image data from the failover server are transmitted to the production server. Make sure the production server provides enough storage space.**

16. To carry out the export immediately, click **Export**. The settings are saved after export or by closing the window.

Viewing exported files

- For viewing the exported files, use the “VMS_PortableViewer”. The Viewer allows opening an viewing the exported files without modification and without installation of Qognify VMS.
- Optionally, use the offline mode of the Qognify VMS client.

Removing write protection from recordings of multiple cameras

The write protection of recorded image data can be deleted (see "Write protection" on page 173).

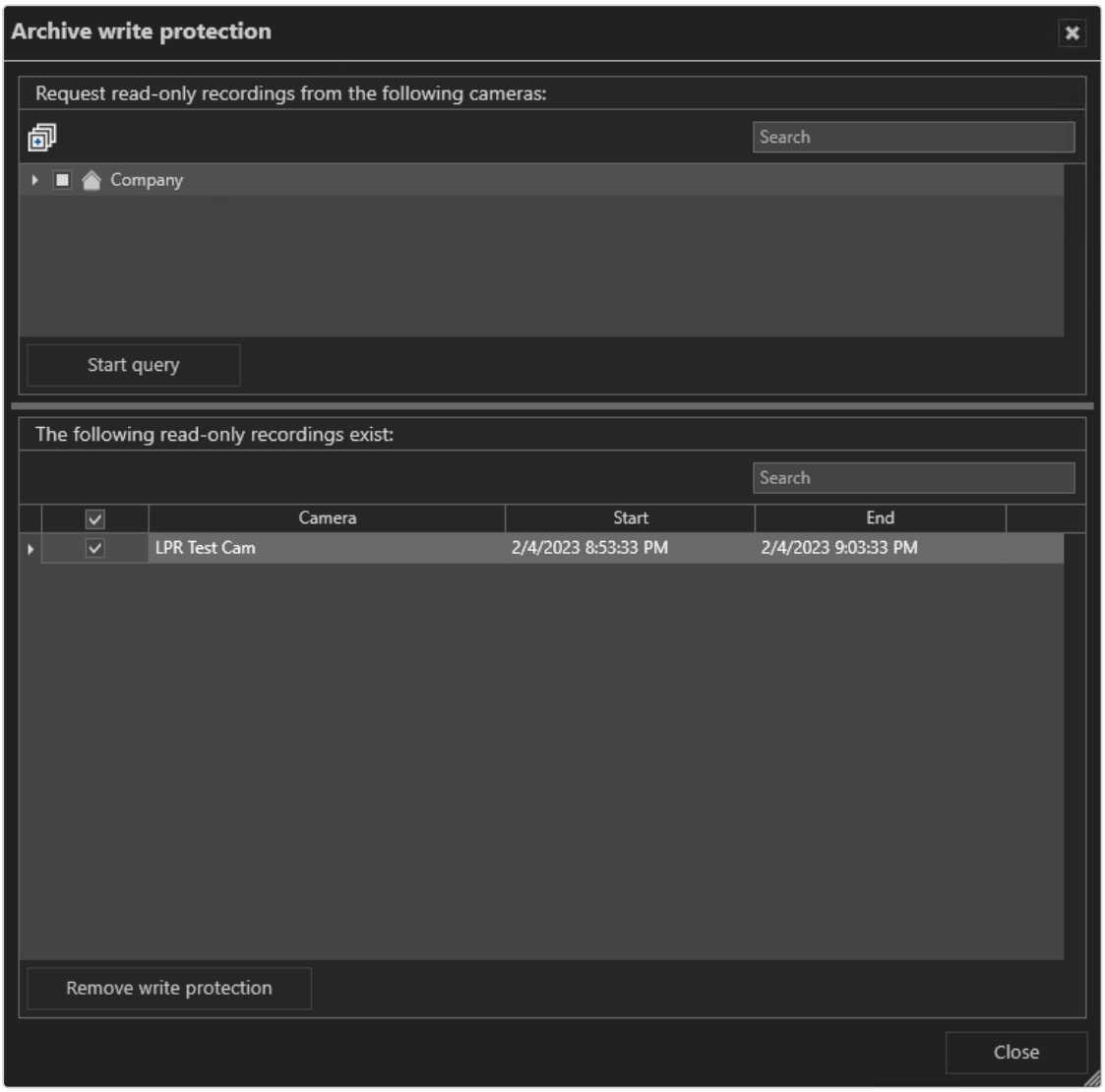


Fig. 45: Removing write protection from recordings of multiple cameras

1. Choose **Write protection of recordings** from the **Tools** menu.
2. Select the cameras to be checked to make sure whether there is a write-protected recording area.
3. Click **Start query** to display any write-protected recordings of the selected cameras.
4. Select the areas in which write protection is to be removed from recordings.
5. Select **Remove write protection**.
6. **Close** the window.

Configuring a logo action

Logo action allows you to specify which layer is to be displayed when you click the Qognify logo at the top of the screen.

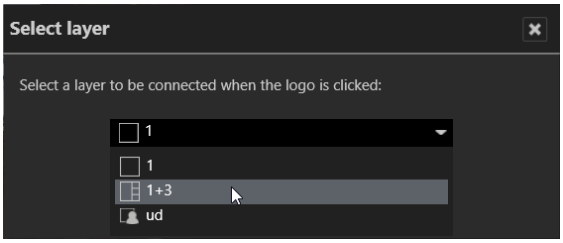


Fig. 46: Configuring a logo action

1. Select **Configure logo action** from the **Tools** menu.
2. Select the defined layers from the drop-down list. The layers are saved in the configuration menu (see "Layers" on page 374).
3. Click **OK** to confirm.

Status report for automatic image export

> **This menu item is only available after entering "Configuration mode" on page 189.**

The status report for automatic image export displays problems that have occurred during automatic image data export.

If any problems have occurred during the export of image data, the failed exports can be restarted or deleted from list.

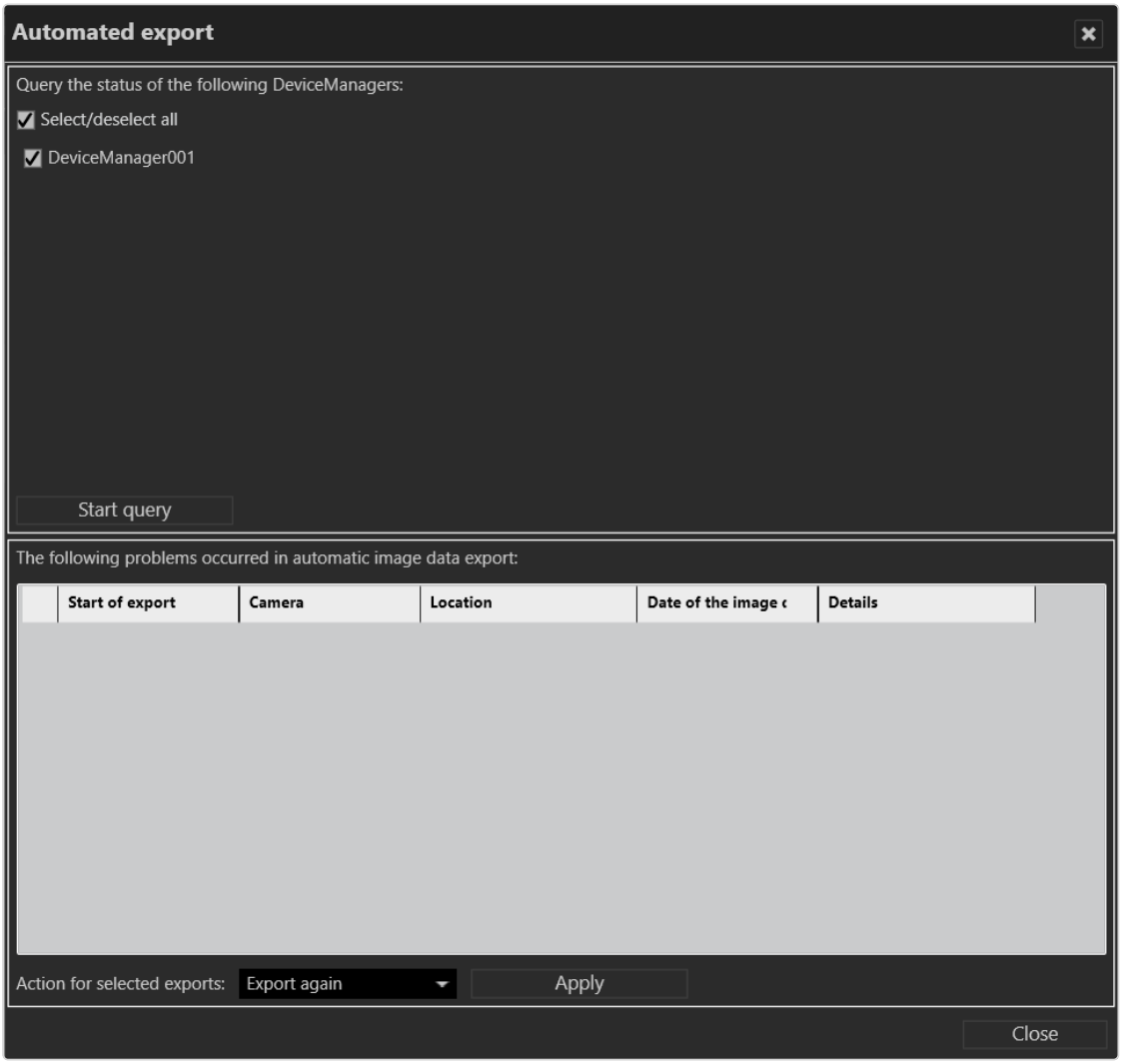


Fig. 47: Status report for automatic image export

The status report for automatic image export displays the list of failed automatic exports.

1. Select the DeviceManagers to be included in the query for failed automatic exports.
2. Click **Start query**. The errors and problems that have occurred on the selected DeviceManager are displayed.

3. Select one or more items in the list and select an **action for the selected exports**.
4. **Export again**. The selected image data export will be exported again.
5. **Remove from list**. The selected items will be removed from the result list.
6. Click **Apply** to perform the selected action.
7. Click **Close**.

Manual reference image comparison

To create reference camera images and compare camera images, the user must have the rights to see live images in surveillance mode (see "Administrative rights and user rights" on page 24).

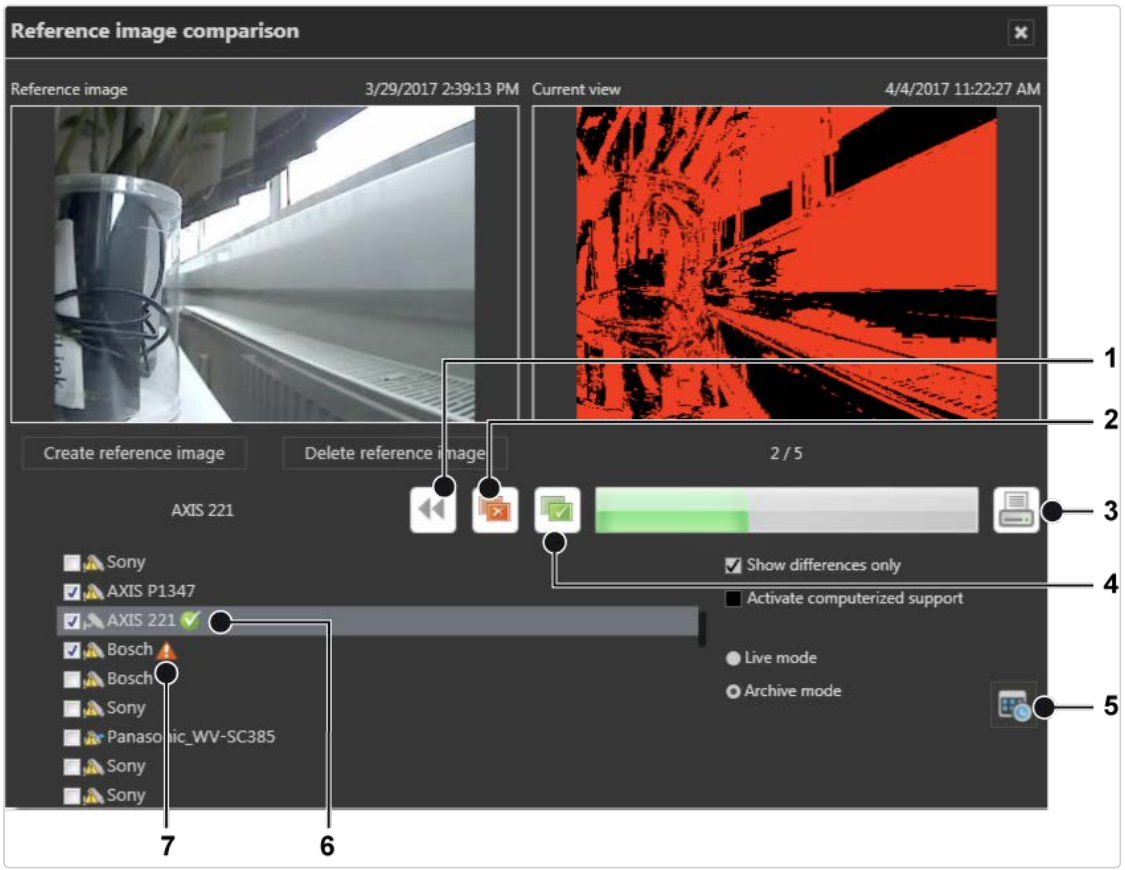


Fig. 48: Manual reference image comparison

The manual reference image comparison helps detect changes in the static object.

Mobotix cameras are only supported for Motion JPEG. Reference Image comparison does not work on images from fish-eye cameras.

1. Select a camera from the list and click **Create reference image**. The current camera image will be used as reference image. The current view displays the actual live image of the camera or an archived image.

2. To delete a reference image, select the camera from the list and click **Delete reference image**.
3. Select the camera and check both images for changes.
4. Select **Deviations** (2) to reject and mark the images as not identical. The red icon (7) is displayed behind the camera name.
5. Select **Congruence** (4) to accept mark the images as identical. The green icon (6) is displayed behind the camera name.
6. If the changes are difficult to see, select **Show differences only**. The changes detected by the image processing software will be displayed as highlighted areas in the current view. If no changes are detected, the current view turns black.
7. Deselect **Show differences only** to return to the actual camera image.
8. Select **Activate computerized support** to display a threshold scale. Move the pointer on the scale to change the threshold values. This changes the threshold values of the current image and helps discern possible changes in the image.
9. Select **Live mode** or **Archive mode**. When Archive mode is selected, the reference image can be compared to a recorded image.
10. Select **Calendar** (5) and select a date and time of the archived image.
11. To print a report of the results, select **Print** (3).

Printing the reference image comparison report

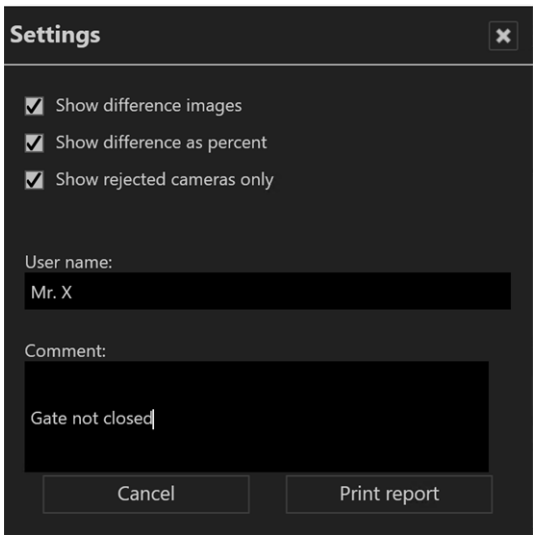


Fig. 49: Printing the reference image comparison report

1. In Settings, the print options can be specified:
   - Select **Show difference images** to print the current views with the differences highlighted.
   - Select **Show difference as percent** to print the percentage of the detected differences within each image.
   - Select **Show rejected cameras only** to print the report without the accepted cameras.
2. Enter the **User name** and add a **Comment**, if necessary.
3. Select **Print report**.

Info

The menu **Info** displays information about the system and both procedures to obtain a license for Qognify VMS 7.5. The installation must be activated within 30 days. This requires sending an automatically generated activation key, the product ID, to Qognify. This menu displays the following options:

- Activating the software
- Showing information about the software

Activate the Qognify VMS license online

The product is activated online to personalize a license or download a license file.

> **Online activation requires a connection to the internet.**

Personalize a license

Fig. 50: Personalize a license

1. In the **Info** menu, select **Activate product**.
2. Select **Online**.
3. Select **Personalize license** if you want to register it with your user data, and the license has not yet been registered.
4. Enter your installation number (**INR**) and user details.
5. Click **OK** to confirm your entries. The client connects to the Qognify registration server and transfers the license key to the computer.

Download a license

You can download a new license file if an update has been carried out and the license is required again.

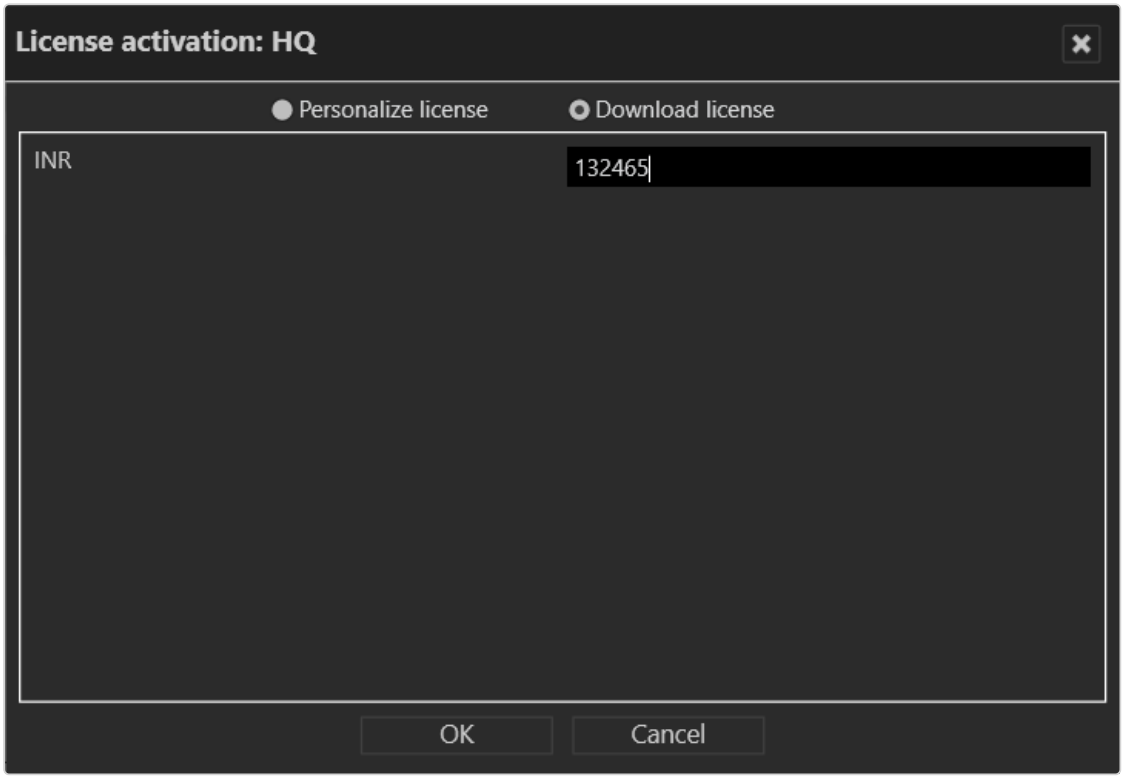


Fig. 51: Download a license

1. Select **Download license**.
2. Enter your installation number (**INR**).
3. Click **OK** to confirm your entries. The client connects to the Qognify registration server and transfers the license key to the computer.

> **If the product ID has changed (e.g. due to changes to the server hardware), contact the Qognify support (see "Support" on page 13).**

Activate the product offline

If the client has no internet access, activate the client by first applying for a license via email. After receiving the license file per email, it has to be imported.

Applying for a license

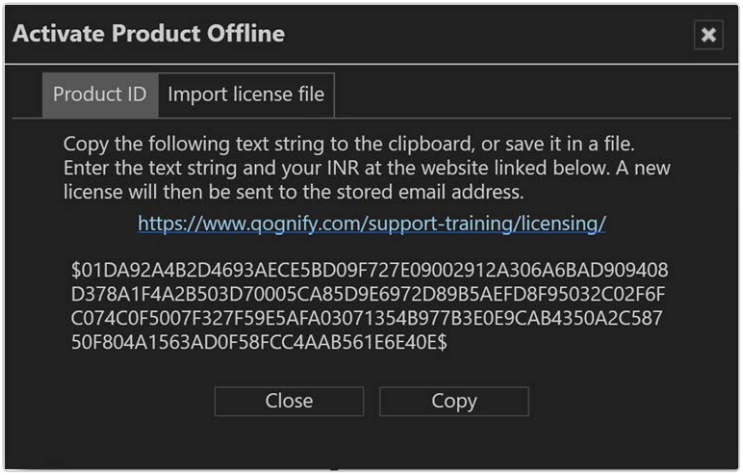


Fig. 52: Applying for a license

1. In the **Info** menu, select **Activate Product**.
2. Select **Offline**.
3. Select the tab **Product ID**. The software creates a unique product ID.
4. Click **Copy** to copy the displayed product ID to the clipboard.
5. Open the Qognify website and navigate to "Support" and "Licensing".
6. Select "New license code".
7. Enter your product ID and the other information requested there. You will receive the license file by email.

Importing a license file

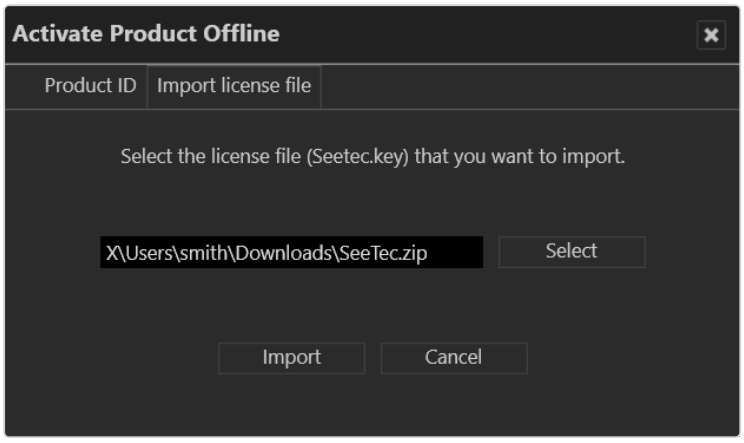


Fig. 53: Importing a license file

1. In the **Info** menu, select **Activate Product**.
2. Select **Offline**.
3. Select the tab **Import license file**.
4. Click **Select** and navigate to the storage location of the license file.
5. Select the license file. Upon import, the zipped file will be decompressed automatically.
6. Click **Import** to use the license key.

Show license

> **A test license will be installed during installation and is valid for 30 days. A demo license is valid until the displayed date. If no valid license is available, login is not possible. For further questions, contact the Qognify support (see "Support" on page 13).**

1. In the **Info** menu, select **Show information**.
2. Select **Show license**. Information on the license is displayed in three tabs.
3. Select tab **Overview** to see general information of the product, e.g. the INR (Installation Number), SMA (Software Maintenance Agreement), the validity period of the license (if it is a demo license).

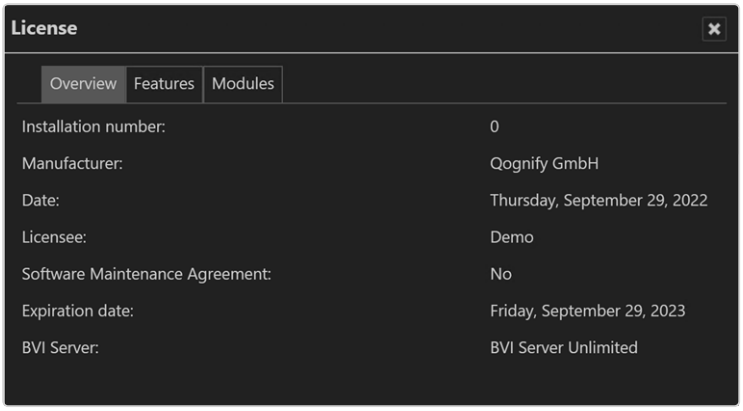


Fig. 54: Show license - overview

4. Select **Features** to see the features activated by the installed license file.

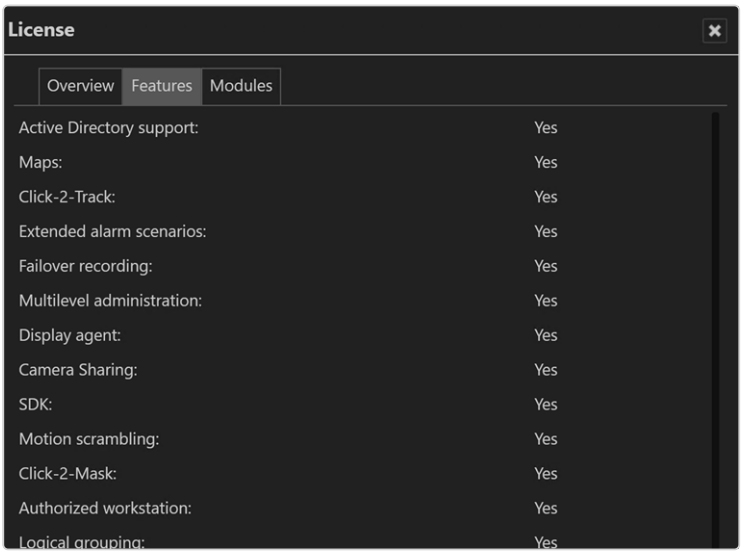


Fig. 55: Show license - features

5. Select **Modules** to see how many modules like cameras (devices), servers, analytics channels etc. are activated by the installed license file.

Fig. 56: Show license - modules

Show program information

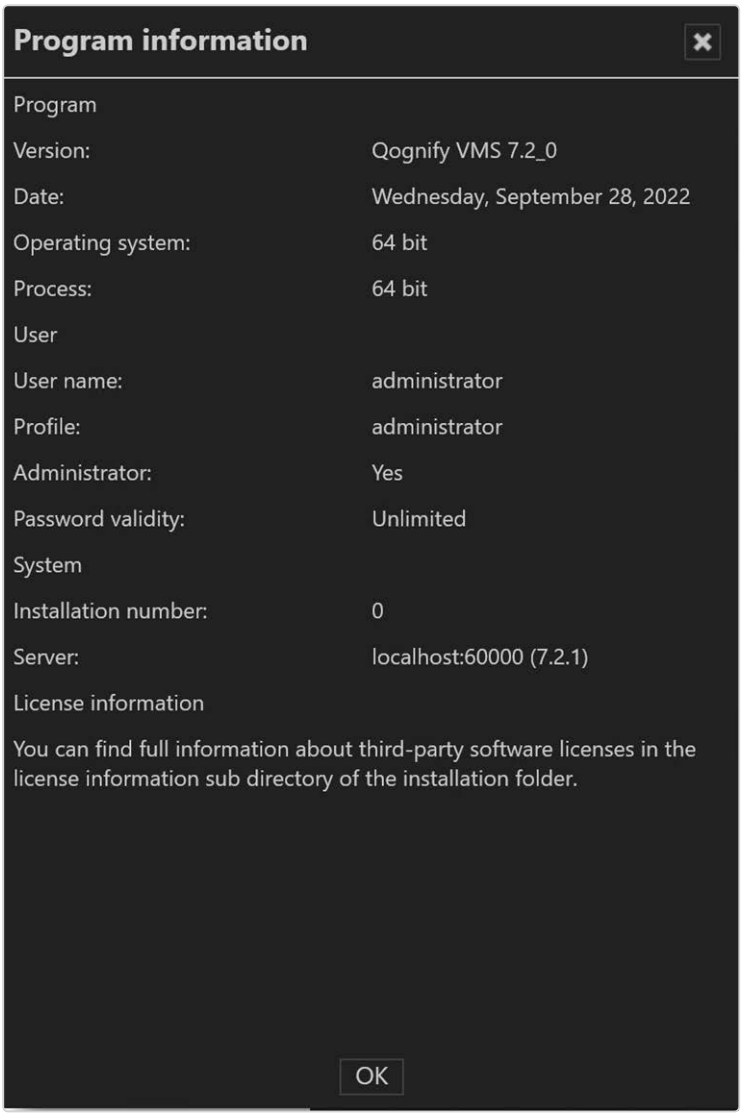


Fig. 57: Show program information

1. Select **Show program information** from the **Info** menu. The information on items such as the program version, current user and profile and also validity of password is displayed.

Show system information

Fig. 58: Show system information

1. Choose **Show system information** from the **Info** menu. The information on items such as the Core Service Main, the numbers of activated DeviceManagers, video sources (cameras) is shown.
2. Click **Copy** to copy the system information to the clipboard. You can paste the data from the clipboard to your email program to send it to support (see "Support" on page 13).

Help

The help menu displays the following options:

Online help

Starts the help system on the starting page. In addition, there are also links for accessing specific topics directly from the various controls and dialog boxes. The system automatically checks for current versions of the online help system. The user is notified if the installed version is not up-to-date.

> **When starting the help system for the first time, you may be prompted by the browser to activate ActiveX or allow JavaScript. The help system will not function properly, if those services are blocked.**

Start problem recording

If problems occur during operation, you can use the "Start problem recording" function to record, comment on and save them. The "Problem Steps Recorder" is part of the operating system.

1. Select **Start problem recording** from the **Help** menu.
2. Select **Start recording** and carry out the steps that led to the problem.
3. As soon as you have carried out these steps, stop recording.
4. If you want to add a comment to the recording, click **Add comment** (e.g. the time, behavior of the client and devices, etc.).
5. Specify where the file is stored.

Display help icons

1. The help icons are small gray circles with question marks in the program components that lead directly to the applicable section of the Online help system.
2. Enable or disable **Display Help icons** from the **Help** menu.

Changing the user

The user interface displays the current user in the function bar.

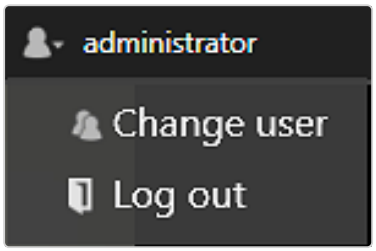


Fig. 59: Changing the user

1. Click the user icon in the function bar.
2. Click **Change user** to log on to the server as another user. Alternatively, change the user via the "File" menu (see "Changing the user" on page 81).
3. Click **Log out** to log out the current user from the server.

The mode bar

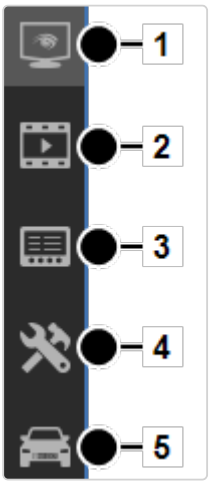


Fig. 60: The mode bar

The mode bar allows you to switch between display modes.

- **Surveillance mode** (1). After login, the system starts up in surveillance mode (see "Surveillance mode" on page 131). The number of alarms and system events that have occurred are indicated by a number in the icon. Additionally, the number of alarms and system events are indicated by a number in their respective tab in the alarm list (see "Alarm list and system messages" on page 158).
- **Archive mode** (2): Archive mode manages and displays recorded image data and search for alarm events (see "Archive mode" on page 163). The number of export operations that have occurred is indicated by a number in the **Archive** icon.
- **Report mode** (3). Report mode displays a list of the events that have occurred (see "Report mode" on page 185).
- **Configuration mode** (4). Configuration mode manages and configures the video sources, users and locations (see "Configuration mode" on page 189).

- **LPR mode** (5). LPR mode is used for license plate recognition in the image data of the corresponding cameras (see "LPR mode" on page 451).

The control bar

The control bar contains the tabs required, depending on the mode, for controlling the display or for configuration. You will find descriptions of the tabs in the sections describing each mode. Tabs cannot be moved. They remain anchored in position on the control bar.

Displaying items in tree view

1. Click ▼ on the left side of the upper item in the tab to display or hide the items beneath.

Opening the context sensitive help

1. Click **Help** to open the online help in the default web browser. The web browser can be selected in the client configuration (see "Client configuration" on page 64). The online help can also be started from the help menu (see "Help" on page 125).

Pinning the control bar

By default the control bar is always visible (pinned). An auto hide option is available.

- Select the pin to activate the auto hide function. In this state the control bar minimizes automatically to the right when the cursor moves away from the control bar. As soon as the cursor moves over the minimized control bar it appears automatically.

- Select the pin again to deactivate the auto hide function. In this state the control bar is always visible (default).

Minimizing and maximizing a control

- Click the double triangle to minimize a control to the top of the control bar.
- Click the double triangle to maximize a control.

Minimizing and maximizing the control bar

- Click the gray triangle in the upper-right corner of a control to minimize the control bar to the right. The size of the main window increases.
- Click a gray triangle on the minimized control bar to maximize the control bar.

Search

Qognify VMS provides mode-specific search and query functions:

- Searching in surveillance mode (see "Searching in surveillance mode" on page 161)

  > **Searching for items in the control bar is also available in Archive mode and LPR mode.**

- Searching for alarms in archive mode (see "Searching for alarms" on page 175)
- Searching (query) in report mode (see "Filtering the query" on page 186)
- Searching in configuration mode (see "Searching in configuration mode" on page 198)
- Searching (query) in LPR mode (see "LPR mode" on page 451)

7

Surveillance mode

Surveillance mode allows live images, web sites, maps, layers, alarms and patrols to be displayed and PTZ cameras and other peripherals, such as door openers, that are to be controlled (see "The user interface" on page 61).

1. To change to Surveillance mode, click **Surveillance mode** on the mode bar.

Camera operation

You can handle the functions of the camera using the control bar (see "Camera image controller" on page 140) or using the **Control** (see "Camera control" on page 149).

To operate a camera, select the camera in the work area.

You can recognize a standard recording by a green dot below the lower right edge of the camera image in surveillance mode. You can recognize an alarm recording by a red dot below the lower right edge of the camera image.

If there is no recording, a black square instead a red or green dot is displayed.

Tabs

The tabs allow you to open and close the layers (see "Work area" below).

Control bar

The control bar allows you to perform the following actions:

- Move the selected PTZ cameras and change the image detail (see "PTZ control" on page 149)
- Perform actions using buttons (see "Buttons" on page 153)
- Carry out patrols (see "Patrol" on page 153)
- Use the optionally installed communication options (camera and audio) (see "Audio" on page 154).
- Call dispatcher mode (if installed, see "Video wall dispatcher" on page 87). The dispatcher mode is switched on and off via the View menu.
- Select the cameras created for each location (see "Overview" on page 148)
- Search for specific installed cameras

Work area

The work area is the main window for displaying tiles with items such as camera images, patrols, or maps (see "The user interface" on page 61). The work area displays up to 100 tiles at the same time. The tiles can be arranged in different ways:

- Evenly as a grid
- With a main tile and smaller tiles

> **The name of the user of the camera is displayed in the top part of the image to all watchers, if configured (see "Configuring the user security settings" on page 448).**

Alarm notification ("Toast notification")

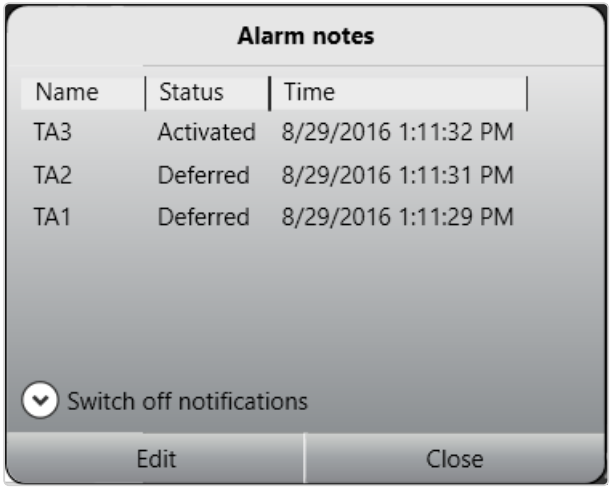


Fig. 61: Alarm notification ("Toast notification")

Depending on the setting, alarms and system messages are displayed as they occur in a separate message window (alarm notification) at the bottom of the screen. For further information, see the "Alarm messages" on page 158.

Creating layers and adding objects

Layers can be set in the layer area in configuration mode (see "Layers" on page 374). Temporary layers, which are only available for the user and are not saved, can optionally be combined.

In some layers, the available objects such as cameras or maps can be assigned to any tile in the work area.

1. Drag the desired layer from the **Overview** control to the work area. To configure the layers, see "Layers" on page 374.
2. Optionally, click **Layer menu** on the function bar (see "The function bar" on page 63) and select **Add layer**. You can select the desired number of tiles or create a user-defined layer. Or select **Load personal layer** to load a previous saved user defined layer. The selected layer is displayed right to the layer menu icon in the tab selector.
3. Drag the selected object from the overview panel to the desired empty tile in the work area. To move an object in the work area, drag it to the tile in which it is to be displayed. If there is an object there already, it is moved to the previous tile of the moved object.
4. Click the cross on the tab bar to close the layer.

5. Select **Open layer in secondary window** to display the new layer on a second screen (see "View" on page 85).
6. Select **automatic layer switching** and the desired **interval** to switch automatically between the opened layers after a certain interval.

> **Automatic layer switching is stopped in the event of an alarm scenario and automatically resumed after an alarm.**

Minimizing the display space for audio-only sources

A source may provide only audio input but requires the space of a whole tile. The required space can be reduced to a bar at the bottom of the layer view.

> **Up to four audio-only sources can be minimized.**

1. Select the audio-only source and drag it to an empty tile in the layer.
2. Select the audio mode icon and select "Audio only". The tile is reduced to a bar and displays only the following functions:

   - Layer options
   - Audio
   - Open tile in 1x1 layer
   - Start alarm recording
3. To expand the object, drag it to an empty tile.

Setting the viewing mode on multiple windows

The viewing mode feature is available when using multiple client window to keep the windows in different states. If multiple displays are connected to the client, client windows can be distributed to them. The viewing mode of each window can be set separately, so displays can remain in surveillance mode even if the main display is switched to another mode (e.g. archive mode or configuration mode).

Fig. 62: Viewing mode icon "Keep window in surveillance mode"

1. Switch to surveillance or archive mode and drag the required camera view onto the secondary window. The drag & drop feature works between surveillance and archive mode and vice versa.
2. On the secondary window, select **Keep window in surveillance mode** ( ). The camera view on the secondary window will remain in surveillance mode with live image even if the primary window is switched to another mode.
3. To remove the viewing mode on the secondary display, select the monitor icon again.
4. When clicking on the monitor icon on the secondary window **after** switching the viewing mode on the primary window, the last live image view will be restored on the secondary window.

Sequential alarm window

The settings for the sequential alarm window are defined in the View menu (see "Adding a sequential alarm window" on page 86).

Fig. 63: Sequential alarm window

1. To switch to the sequential mode, select **Row mode** ( ). The alarms will be displayed in a single row. If the number of alarm cameras exceeds the number of columns defined, the remaining alarm cameras will be ignored.
2. To switch to **Continuous mode**, select . If the number of alarm cameras exceeds the number of columns defined, the additional cameras will be added in the row below.

Click-2-Track

A person or object that moves across different camera views can be followed even without specifying the camera name of the following view. Instead, the person or object

path is defined in surveillance mode by activating the area covered by the adjacent camera.

This feature is configured in "Click-2-Track" on page 265. It is also available in archive mode (see "Click-2-Track" on page 167) and can be invoked with the mini archive player (see "Mini archive player" on page 143).

This feature requires an appropriate license and is not included in the standard package.

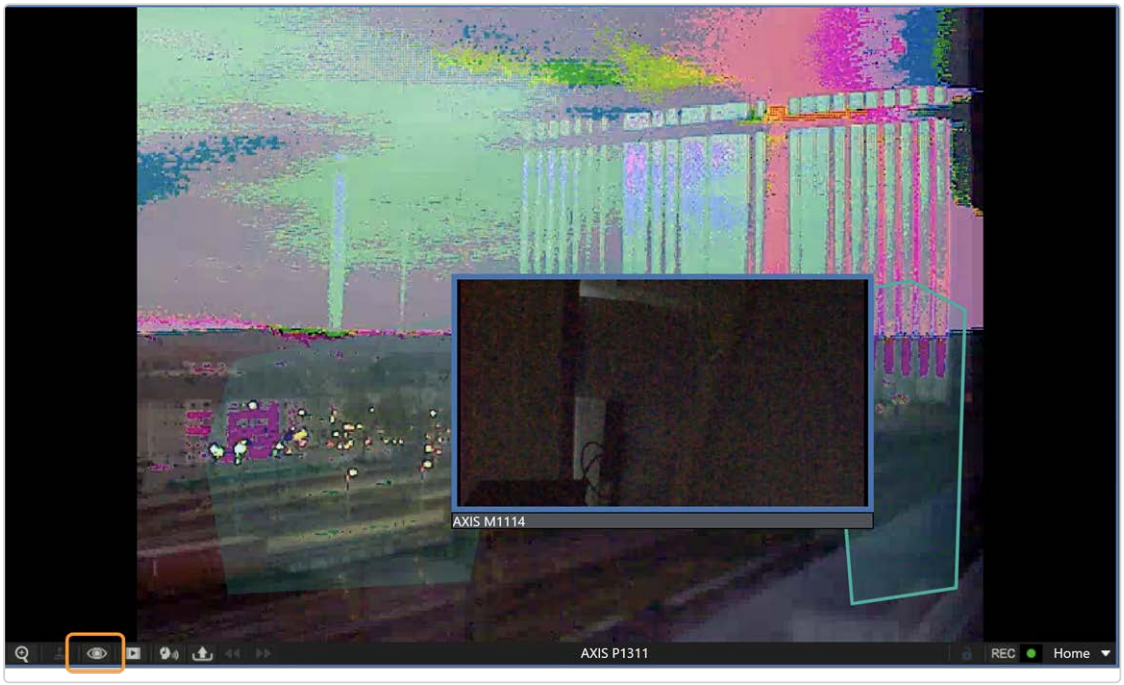
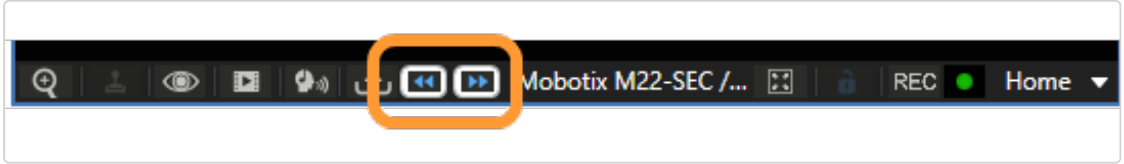


Fig. 64: Click-2-Track in surveillance mode

1. To start Click-2-Track, select the tile and click on the camera options.
2. Select **Activate**.
3. Select the region on the image where the person or object moves to. The linked camera image is displayed in the preview inset.
4. To bring the image in the inset into the tile, click on the preview. Click-2-Track remains activated.

History



Once multiple camera regions have been visited, the history buttons are active. They are used to navigate forward and backward through the history of this tile, since each tile has a separate history.

When using the Click-2-Track history in surveillance mode, the tile is switched to mini archive player.

> **Preview cameras shown while in mini archive mode display the same time as the mini archive player.**

Custom layers

When working in surveillance or archive mode, user-specific layers can be added and saved for each user separately. These custom layers can be defined and deleted by the user without any additional user right.

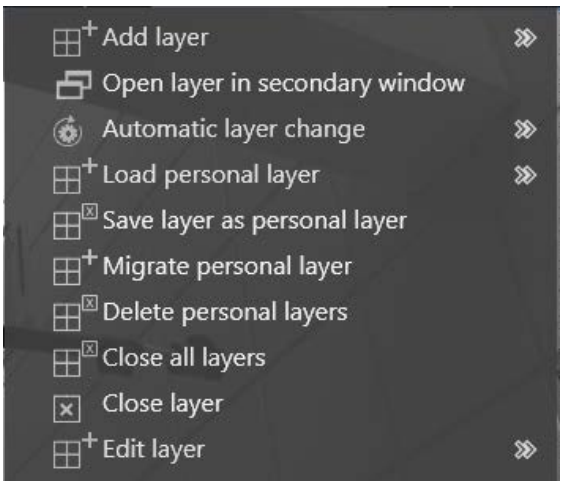
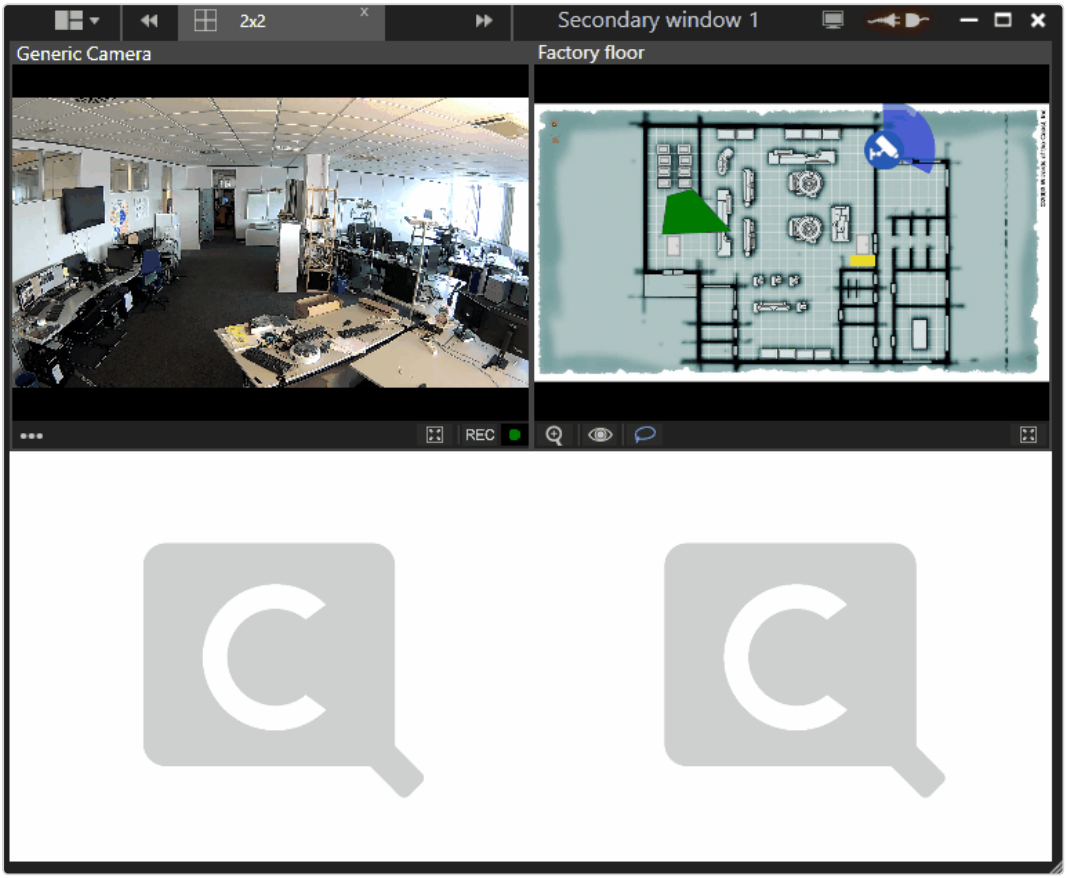


Fig. 65: Custom layers

1. To open a layer, select the **Layer** in the top bar.

Opening and closing a layer directly in a custom layer



1. Double click on a window to enlarge the layer.
2. Double-click on an enlarged layer to reduce its size to the preset state.

Adding a layer

1. Select **Add layer** and select the required arrangement of the layer fields or select a user-defined arrangement of rows and columns. The new layer is displayed.
2. Drag the tile (e.g. camera views, webpages, or maps) from the control bar into the fields and click **Save layer as personal layer** to save the new layer view for the current user on the server.

Migrating local layers

> **Personal layers have previously been named "local layers". Personal layers are stored on the server for each user account, so they can be accessed from any client the user is logged in to.**

1. Select **Migrate personal layer** to convert all local layers located in `localappdata/qognify` (or `localappdata/seetec` if it is an older installation) to the new personal layers. The .xml files of the old layer settings will be REMOVED after the process is finished successfully.

Expanding a layer

1. Select **Add layer** and select the required arrangement of the layer fields or select a user-defined arrangement of rows and columns. The new layer is displayed.
2. Select **Edit layer** and select any optional layout that provides additional tiles (unavailable tiles are disabled). The current layer tab is set to the new layout.

Opening a layer in the secondary window

1. Click **Open layer in secondary window** to move the new layer to a secondary window.

Changing a layer automatically

1. Click **Automatic Layer change** and select a time interval after which the next open layer is displayed.

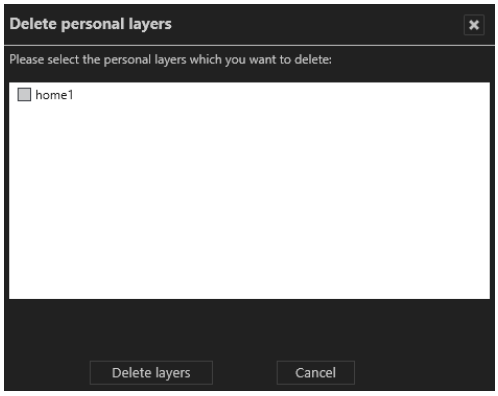
Loading a personal layer

1. To open an existing layer, click **Load personal layer** and select the layer.

Deleting personal layers

> **Local layers must be migrated to personal layers before they can be deleted (see "Migrating local layers" on the previous page).**

1. To delete a layer, click **Delete personal layers**.



2. Select the layer(s) to be deleted and click **Delete layers**.

Closing layers

1. To close a single layer, select **Close layer** or click the "x" layer tab.
2. To close all open layers, select **Close all layers**. Unsaved layers will close without further notice.

Camera image controller

You work with the images of the connected and configured cameras directly in the camera layer in the work area.

> **These functions refer only to the control options offered by Qognify VMS.**

Camera image control icons

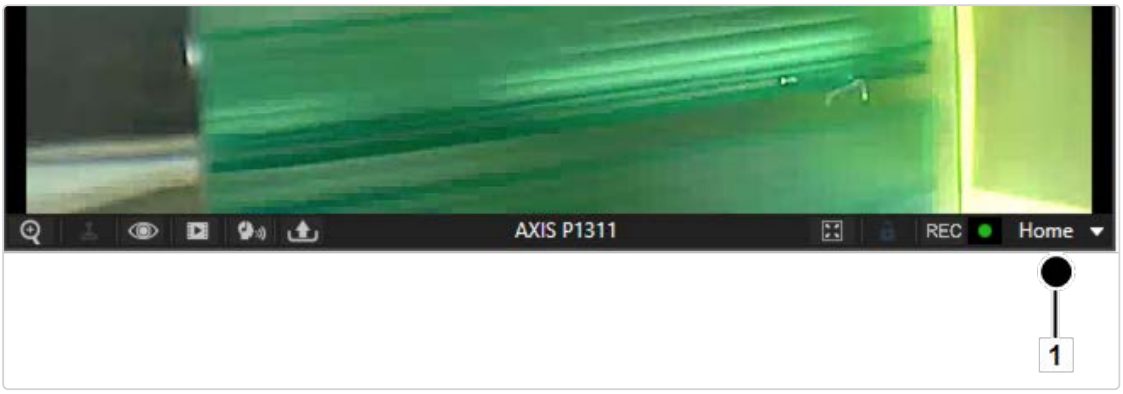


Fig. 66: Camera image control icons

- **Zoom** . Enlarges the image detail with the help of the digital or optical zoom function.
  - The image detail is enlarged or reduced in size using the scroll wheel on the mouse.
  - You can move the zoomed image by holding down the middle mouse button.
  - Optionally, when drawing a rectangle in the image while pressing the left mouse button, the enclosed area will be zoomed into.
  - PTZ cameras can be operated using the controller or a connected joystick. For some PTZ cameras, zooming into a defined rectangular area in an image by optical zoom is enabled.

> **Optical zoom is only possible if supported by the camera model.**

- **PTZ** . Moves the image detail in the layer. The image detail can be changed by clicking and moving the mouse pointer in the image (see "Camera image controller" on the previous page). PTZ cameras can be operated using the controller or a connected joystick (see "Swiveling the camera in the image" on page 144).

- **Layer options**  . Shows additional options:
  - **Tracking data**: Displays the specified rules and detected for this camera (e.g. tripwires) in the view. For configuration see "Qognify Analytics" on page 301
  - **Display statistics**: Displays statistical data on the image stream between the camera and the DeviceManager server and between the DeviceManager server and the client (see "Camera image statistics" on page 145).
  - **Activate privacy masking**: Activates or disables privacy masking. The settings for the camera are made in configuration mode in the Cameras area (see "Cameras" on page 211).
  - **Deselect**: Deselects the selected camera.
  - **Rotate Image (180°)**. Displays the camera image rotated by 180° rotation when the original camera image is displayed upside-down.
  - **Open in new tab**: Displays the camera in a separate layer.
  - **Open in side window**: Displays the camera in a separate layer in the first secondary window.
  - **Close**: Closes the active layer.
- **Mini Archive mode**  . Shows the recordings of the selected interval (see "Mini archive player" on the facing page).
  - The interval can be between 5 and 60 seconds and is displayed or selected by clicking the icon.
  - When selecting **Jump to time** you can easily jump to a certain time point of the recording.
- **Audio mode**  . Controls the cameras' audio feature (volume / mute / permanent on)
- **Export**  . Exports the current still image (video frame) as a JPEG file or prints the still image displayed.
- **Tile on 1x1 layer**  . Enlarges the tile so that it fills the full screen of the work area. This option is only available when the tile is not in full screen display.
- **Camera lock**  . Locks the camera for the user. Clicking the icon again releases the camera for other users. The camera lock function must be enabled in the Users settings in configuration mode (see "Users" on page 329).
- **REC**. Starts and stops manual recording. A red button on the right indicates if an alarm recording has started.

- **Recording status** : Indicates the recording behavior for the camera. A green dot stands for standard recording, a red dot stands for alarm recording (see "Multimedia database" on page 232). A blank black background stands for "no recording".
- **Positions** (1). Indicates the preset positions of the selected camera. The camera positions are set in configuration mode in the Cameras area (see "Camera positions / digital presets" on page 249). To control the set positions, see "Camera control" on page 149.

Mini archive player

The mini archive player allows control of the playback from a selected camera. More extensive archive functions are available in archive mode (see "Archive mode" on page 163).

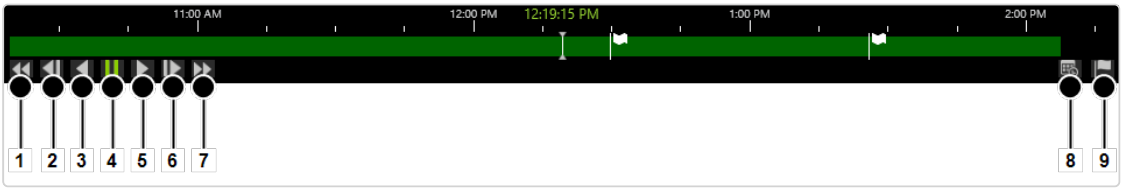


Fig. 67: Mini archive player

The mini archive player provides the following functions:

- **Fast rewind** (1): Click once to play the recording backwards at double speed. Click twice for four times the speed.
- **Previous frame** (2): Jumps to the event's previous frame or JPEG image.
- **Play backward** (3): Plays the archived video stream in reverse chronological order.
- **Pause** (4): Pauses the playback.
- **Play forward** (5): Plays the archived recording in the correct chronological order.
- **Next frame** (6): Jumps to the event's next i-frame or JPEG frame.
- **Fast forward** (7): Click once to play the recording forward at double speed. Click twice for four times the speed.
- **Calendar** (8): Opens a calendar window in order to jump to a specific point in time.
- **Add bookmark** (9): Adds a bookmark to the current frame (see "Working with bookmarks" on page 177).

Manual alarm recording

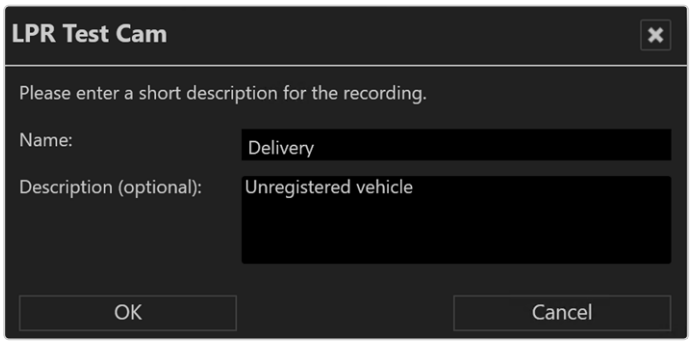
Alarm recordings can be started and stopped manually by the user who has started them. Additionally, bookmarks can be added to the recording. Bookmarks can be used for the search in archive mode (see "Searching for alarms" on page 175).

Starting manual alarm recording

1. Click the **REC** button (10, see above). A red bell on the right indicates whether alarm recording has started.

   > **To prevent unlimited recording, the maximum post-alarm duration must be specified in configuration mode in the camera settings (see "Multimedia database" on page 232).**

2. Optionally, click **Add bookmark**. A bookmark information window is displayed.



3. Enter the name and a short description of the bookmark.
4. Click **OK** to add the bookmark to the recording.

Stopping manual alarm recording

1. Click the **REC** button again. The recording is stopped.
2. Optionally, add an additional bookmark.

Swiveling the camera in the image

The camera can be moved in pan and tilt mode in the image. Swiveling the camera sideways is called "panning" (creating a panoramic effect), whereas swiveling the camera up and down is called "tilting".

1. Click **PTZ** . A red cross appears in the center of the image.
2. Click a point next to the cross. The distance of the point you click from the center of the cross determines the speed of the swivel operation in the relevant direction.
3. If you like, you can activate the zoom function of the PTZ camera. Using the mouse wheel, zoom in or out of the image.
4. Click **PTZ** again to deactivate the swivel function in the image.

When configured in the PTZ camera, the name of the user is displayed in the image during operation. During non-user interactions like alarm scenarios or sequences, "System" is displayed.

Camera image statistics

1. Select **Layer options** in the camera tool bar.
2. Select **Display statistics**. The statistics window remains open.
3. Close the statistics window by deselecting **Display statistics** in the **Layer options** .

The camera image statistics show information about the following details:

- The video images which are rendered by the client. The **Decoding (fps)** should be similar to the **Rendering (fps),**
- The video images which are recorded on the server,
- The quality of the audio stream,
- The network quality. The **Packet loss (%)** ratio as well as the **Max. Jitter (ms)** value should be as low as possible. High values indicate network problems, e. g. jitter may be caused by electromagnetic interference and crosstalk with carriers of other signals.

Maps

A map shows an area to be monitored. In configuration mode it is added to the software as a simple graphic (see "Maps and "Advanced Maps"" on page 377 in configuration mode). The various cameras and other functional icons are then integrated into this

graphic. The map can thus show a variety of different parts of the company: from the company site to fully automated production lines.

The map shows the cameras that the user can only.

> **If a camera has failed (due to power failure, no connection to the network, etc.), the camera icon is shown as a yellow warning sign.**

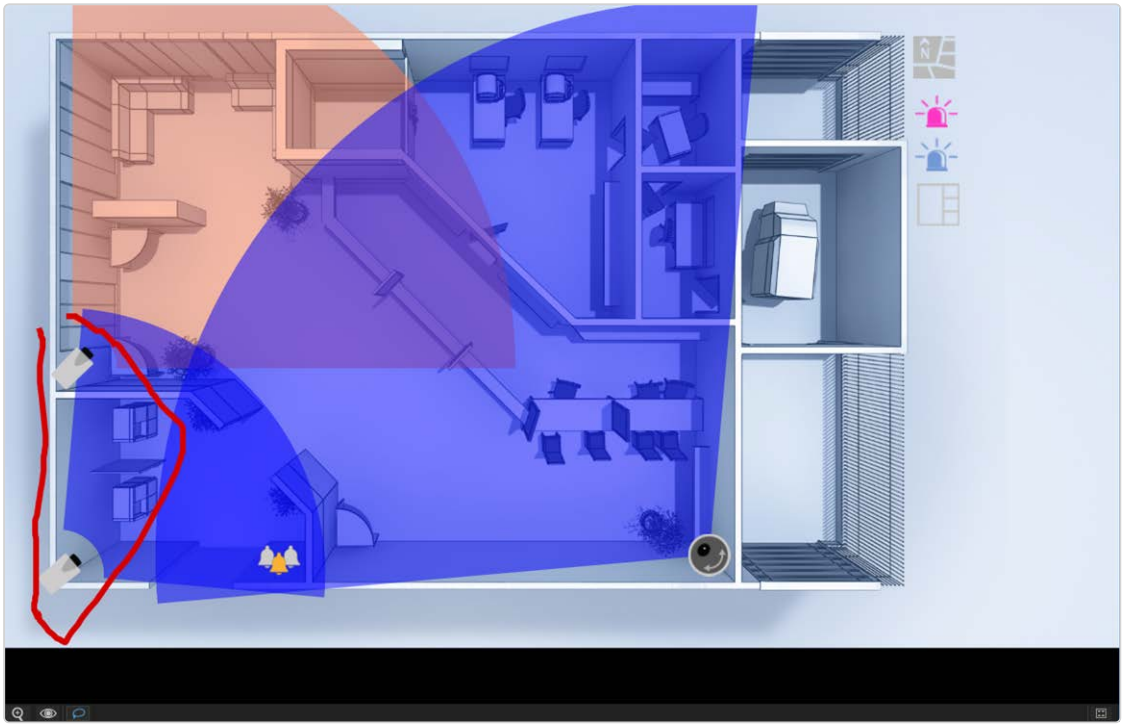


Fig. 68: Maps

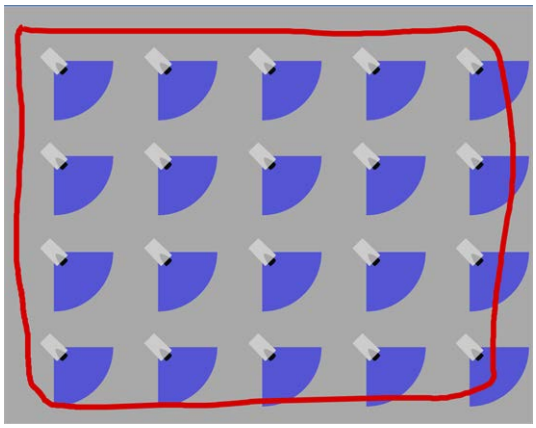
1. Select **Digital zoom** ( ) to activate the zooming function for the map.
2. Zoom the map detail by turning the mouse wheel while the mouse pointer is on the map area.
3. Select **Layer options** ( ) to open the map on a new tab or in a new window or to close the layer.
4. Select **Create lasso selection** ( ) to activate the lasso function. The lasso function is activated by default.
5. Draw a lasso around the cameras to be displayed in a layer (see "Using the lasso function" on the facing page).
6. Select **Window on 1x1 layer** ( ) to increase the size of the image to fill the whole work area.

Displaying a camera preview

1. Move the mouse pointer in the map to the desired camera. A preview of the camera image is displayed.
2. Click the camera symbol to open the camera image in a new layer.

Using the lasso function

> **Up to 16 cameras can be “caught” by the lasso function.**



1. Click **Create lasso selection** to activate the lasso function.
2. Hold the left mouse button pressed and move the mouse pointer around the cameras you want to select. The movement of the mouse pointer is highlighted by means of a red line.
3. Release the mouse button. The selected camera images are displayed in a new layer.

Web pages

In the web page layer, the user can call specific web pages in specified tiles in order to receive information on the company, for example. The (Internet or intranet) web pages displayed are specified in configuration mode (see "Web pages" on page 389).

1. Navigate in the web pages as in a browser. The navigation bar typically found in browsers is not displayed.

2. To display the page in its own layer, click **Full screen**. The following navigation controls are available:
   - **Back** : Returns to the previous page.
   - **Next** : Moves forward to the next page.
   - **Start page** : Returns to the start page. The start page is the page specified in configuration mode.
   - **Reload** or **Cancel loading** : Reloads the displayed page or stops loading the page. Reloading is only possible after the page is loaded. If the page loads too slowly, the loading can be canceled.

Overview

The **Overview** control displays all available cameras, maps, layers and web pages classified by the locations of the company.

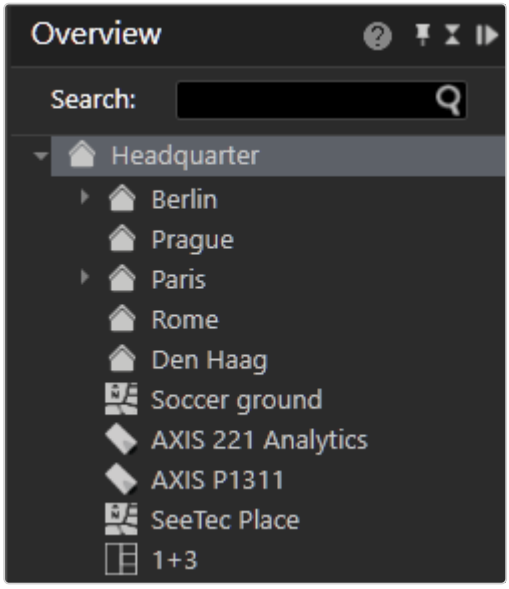


Fig. 69: Overview

1. Click the small triangle in front of the name of the site to display all of the objects assigned to this site.
2. Select an object from the list to display only this object.

Searching for an item

In the system's configuration settings, each item should have been given its own name.

Fig. 70: Searching for an object

1. To search for a specific item, enter the name of the item in the **Search** text box (see "Searching in surveillance mode" on page 161).

Camera control

Fig. 71: Camera control

The **Camera control** allows you to control the active cameras displayed in the work area.

- **PTZ** : starts the PTZ control function to operate with PTZ cameras
- **Buttons** : starts the button function for triggering preset processes
- **Patrol** : starts the patrol operation for starting a set of surveillance operations
- **Audio mode** : starts the audio mode for communication
- **Dispatcher** : starts the dispatcher mode for operating the video wall

PTZ control

Selected PTZ cameras are operated with the PTZ control. PTZ-related functions are available for PTZ cameras only. If no PTZ camera is selected or the PTZ function of the camera is deactivated, only digital zoom and digital preset selection is possible.

Using the PTZ control

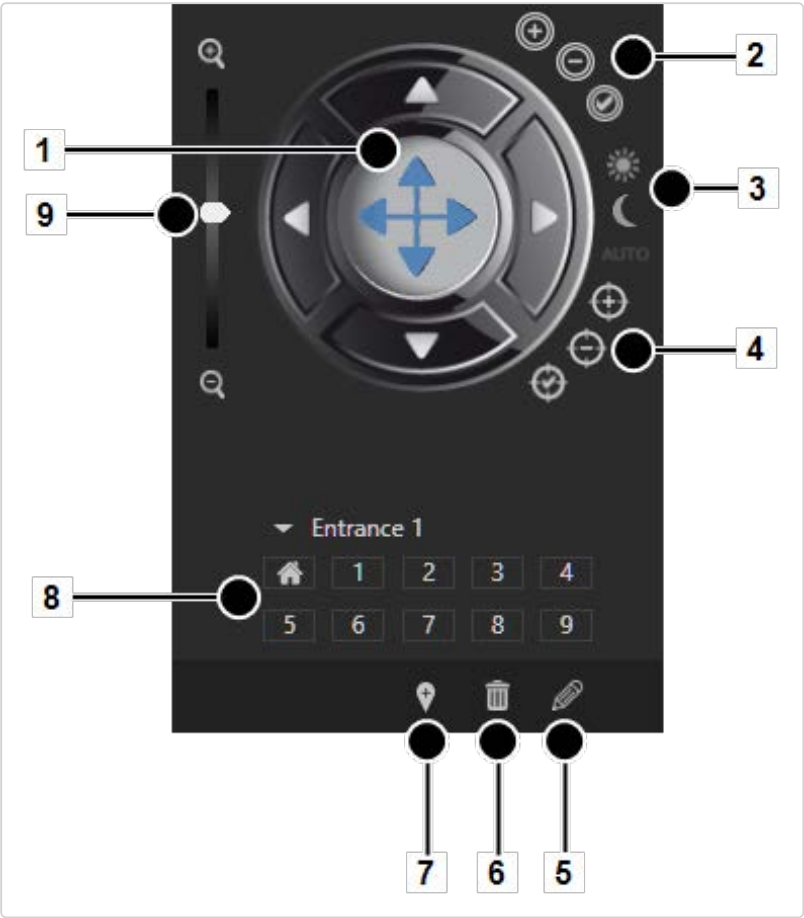


Fig. 72: Using the PTZ control

1. On the menu bar of the control, click **PTZ control** to switch to the operating mode of the cameras.
2. Select the camera image, and use **PTZ control** (1) to move the camera by moving the bright spot in the desired direction.
3. Drag the **Zoom** slider (9) up or down to make the camera zoom in or out of the image. Optionally, click the four direction arrows at the PTZ control to move the camera incrementally.

Using preset positions

Including the default position, ten preset positions are available by direct selection on the number field (8). More can be available in the drop down menu. The maximum number of presets depends on the camera. To edit preset positions in surveillance mode see "Editing camera preset positions" on page 152. In general, positions are set in the configuration mode (see "Configuration mode" on

page 189) by an administrator in the **Camera** area (see "Cameras" on page 211).

1. Click the required camera position on the number field (8) to pan the camera to the selected position.
2. Optionally, click the triangle beside the position name, and select the desired position from the drop-down list. The position is immediately approached.

Using multiple preset positions of a single camera in a single layer

Instead of using a fish-eye camera for a 360° view, multiple fixed camera images can be combined in a single layer (for layers in surveillance mode, see "Custom layers" on page 137).
Saving a layer remembers the camera position (digital preset, digital zoom, dewarping position) and when opening again will resume at the same position.
This applies to saved layers in configuration mode as well as for personal layers. Layers that are inserted into a video wall by drag & drop will retain the digital camera position on the video wall.

Exposure and focus setting

The following exposure and focus settings are available only if supported by the camera:

- **Iris settings** (2)
  - **Iris +**, **Iris -**: Opens or closes the iris of the camera to control the brightness.
  - **Auto Iris**: Automatically adjusts the iris opening to the optimum brightness of the environment.
  - **Autofocus**: automatically adjusts the image sharpness to the objects in the camera focus.
- **Day- and night mode settings** (3)
  - **Day mode**, **night mode**: The camera sets a filter when light conditions are poor.
  - **Auto**: The camera switches between daytime and nighttime vision automatically.

- **Focus settings** (4)
  - **Close-up focus**, **Close-up focus**: adjusts the image sharpness to the objects in the camera focus, depending on the distance of the object to the camera sensor chip.
  - **Autofocus**: automatically adjusts the image sharpness to the objects in the camera focus.

Editing camera preset positions

Camera (preset) positions can be defined (4), deleted (5) and edited (6) depending on user rights (see "Manage user rights" on page 333).

Creating a preset camera position

1. With the PTZ control (1) move the camera to the required position.
2. Click **Add new camera position** (7). The new camera position is added at the next free position number.
3. Enter a name for the position and click **OK**. The new camera position is added at the next free position number.

Deleting a preset camera position

1. Select the position from the number field or from the drop down menu.
2. Click **Delete** (6). The deleted camera position is released, and sub-sequent positions are shifted to compensate.

> *Example Position 3 is deleted. Position 4 is then shifted to position 3, position 5 to position 4 and so on.*

Editing a preset camera position

1. Select the position from the number field or from the drop down menu.
2. Click **Edit current preset** (5).

3. Edit the positions by means of changing the position name, PTZ-settings, focus settings etc.
4. Click **Save current changes**.

Buttons

Starting actions and processes with buttons

Actions or defined processes such as camera recordings or alarm scenarios are started with buttons.

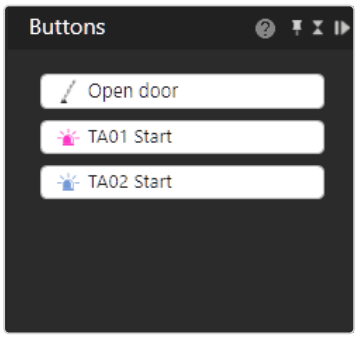


Fig. 73: Buttons

1. On the menu bar of the **Control** control, click **OK** to switch to the display of the buttons created. To configure buttons, see "Buttons" on page 386.
2. The buttons that the user is authorized to use are displayed.
3. Activate the desired action by clicking the button.

Patrol

Patrols can display cameras, set positions, maps and layers one after the other for a specific period. It is also possible to open or close digital outputs in a patrol and confirm checkpoints.

1. On the menu bar of the control, click **Patrol** to switch to the overview of the patrols configured. To configure the patrols, see "Patrols" on page 391.

Starting a patrol

1. Select the desired patrol, and select **Play** ▶. The defined cameras, preset positions, maps and layers are displayed one after the other for the specified period.

Stopping a patrol

1. Select **Stop** ■ to cancel the selected patrol.

Pausing a patrol

1. Select **Pause** ⏸ to interrupt the patrol. The patrol is paused.

Repeating a patrol

1. Select **Loop** 🔁. The patrol is repeated.
2. Select **Loop** 🔁 again. The repetition is canceled, and no more patrols are carried out once the current patrol is finished.

Navigating between points in the patrol

1. Click **Back** ⏮ or **Next** ⏭ to go to the previous or next item in the list.

Audio

1. On the menu bar of the **Control** control, click **Audio** to switch to audio mode.

For audio, the following options are available (if supported by the hardware).

VoIP

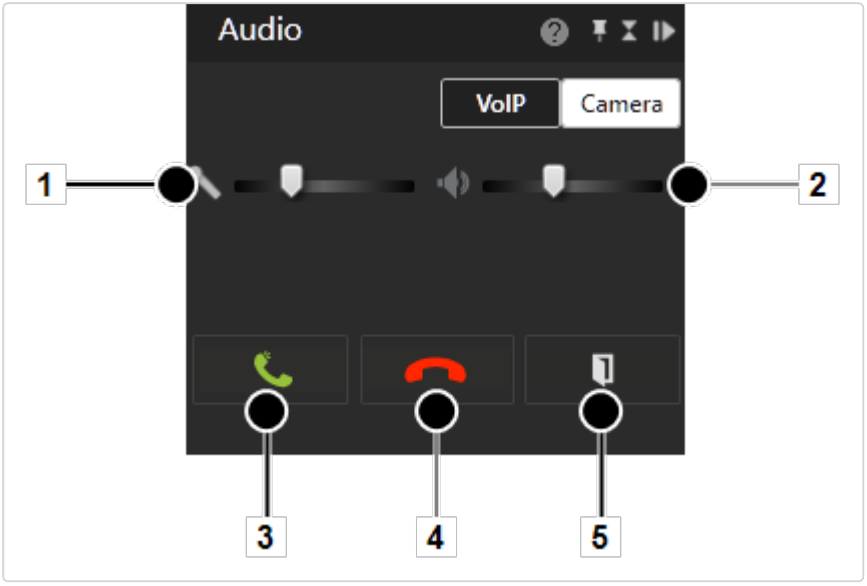


Fig. 74: VoIP

1. Select **VoIP** to select voice output over the network (Voice over IP).
2. Move the sliders for the **microphone** (1) and **loudspeakers** (2) to adjust the volume. The volume setting is saved locally for each client.
3. To speak to a person from the address book of the existing users, enter the name of the person in the text box, and click the magnifying glass icon or select a person from the list.
4. Click **green phone** (5) to start the call.
5. Click **red phone** (4) to finish the call. The name of the person you are talking to, the person's location and the duration of the call are displayed (2).
6. Click **DTMF** (3) to send a DTMF-sequence or call a button action. The sequence or button action is set by an administrator in the VOIP configuration (see VoIP).

Camera

If supported by the camera, audio transmission from the client to the camera is possible (for configuration of the push-to-talk function, see "Audio" on page 248).

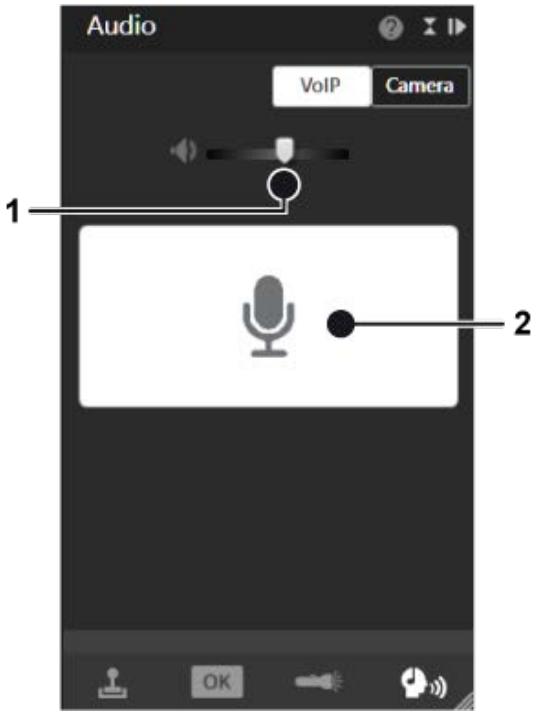


Fig. 75: Camera

1. Select **Camera** to select the direct audio system of the camera (if available).
2. Move the slider for the loudspeaker (1) to adjust the volume. The volume setting is saved locally for each camera.
3. To start audio communication to the camera press and hold the talk-button (2).
4. To stop audio communication to the camera release the talk-button (2).

Dispatcher mode

> **Dispatcher mode is displayed only if the video wall dispatcher is activated in the View menu (see "Video wall dispatcher" on page 87). In addition, at least one video wall must have been created in configuration mode (see "Video walls" on page 398).**

Using the Dispatcher mode

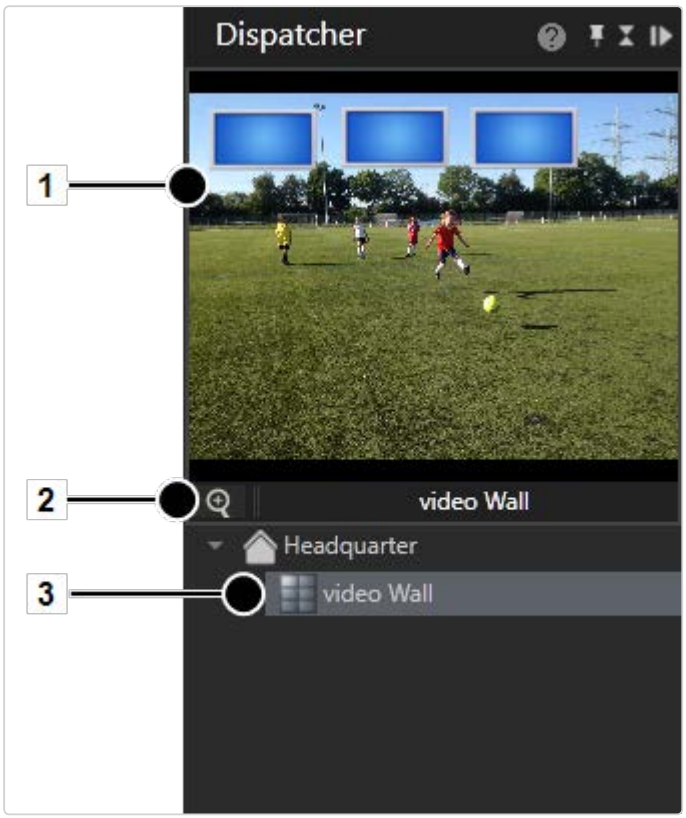


Fig. 76: Dispatcher mode

1. On the menu bar of the control, click **Dispatcher mode** to switch to video wall control.
2. Select the set video wall (3). The video wall is displayed , including the monitors (1) it contains.
3. Click **Digital zoom** (2) and scroll with the mouse wheel to zoom in or out.
4. Press the mouse button and drag the display icons left or right to see adjacent displays.
5. Drag the desired video sources, layers and maps to the monitor in the thumbnail (1).
6. If necessary, open the display of the monitor by-clicking it. The monitor with the active layers is displayed in the work area. You can drag the video sources, layers and maps directly into the work area if the video wall monitor is displayed.

Alarm list and system messages

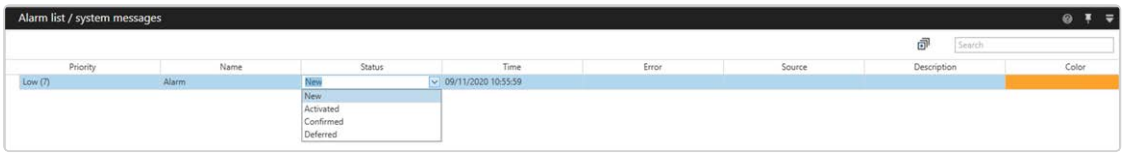


Fig. 77: Alarm list and system messages

The alarm list is at the bottom of the screen and can be opened or closed as required. It displays the combined list of alarm and system messages in the order of their occurrence. The most recent alarms are displayed first. In addition, the number of alarms that have occurred is shown in the surveillance mode icon on the mode bar.

1. To sort the alarm or system messages by the column category, click the column headings.
2. To change the status of an alarm, select the object in the column **Status** and select the status from the drop-down menu.
3. To collapse or expand the alarm list, click **Expand / collapse all** .

Alarm messages

All open alarms that have been assigned to the current logged-in profile are displayed in the alarm messages (see "Persons involved" on page 368). The type of alarm can be recognized by the color-code. The color in which the alarm is displayed can be set in configuration mode in the alarms control (see "Alarms" on page 356).

Changing the alarm status

An alarm has the following statuses:

- **Activated**: This alarm is currently active.
- **Confirmed**: These alarms have been viewed and will be removed from the alarm list. These alarms are removed from the alarm list for all users.
- **Deferred**: These alarms have been viewed and declared as important by the applicable user (e.g. security guard), because they will be required at a later time (e.g. for the patrol report). These alarms are retained in the alarm list. Deferred alarms are declared open at the next start.
- **Rejected**: These alarms are removed from the alarm list and considered unimportant or not applicable by the user.

1. Click the entry in the **Status** column of the alarm list to change the status of the alarm messages.
2. Optionally, click **Confirm all** to acknowledge the alarms and remove the red circle displaying the number of unconfirmed alarms.

Classifying an alarm

Every alarm on the alarm list can be classified according to the categories defined (refer to "Configuring the alarm classifications" on page 431).

1. Select the alarm in the alarm list.
2. Select the category from the drop-down list in the column **Classification**.

Message window (pop-up)

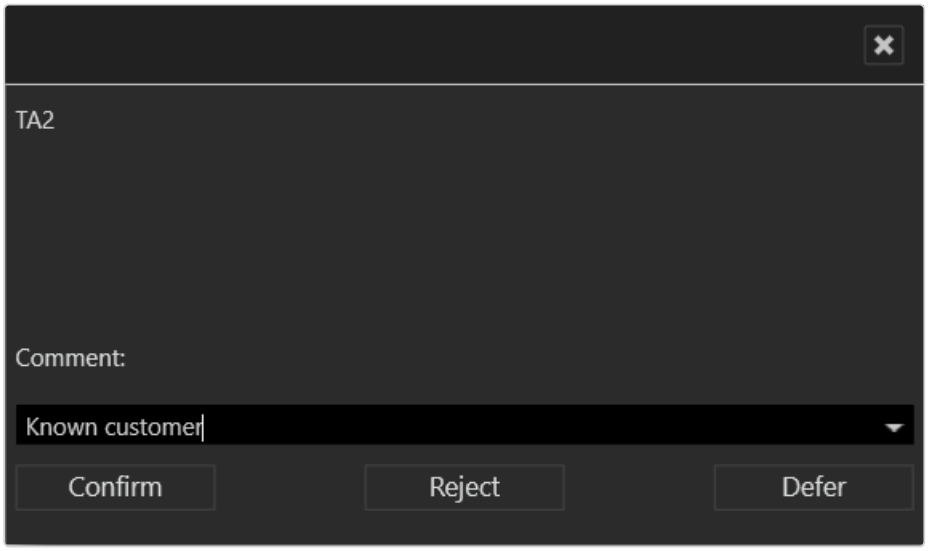


Fig. 78: Message window (pop-up)

As soon as an alarm occurs, a message window is displayed for high or medium priority alarms.

Low priority alarms are removed from the alarm list at the end of the alarm if they are acknowledged and another alarm occurs. Low priority alarms do not have an alarm status.

You can add a comment for this alarm. The comment is displayed in report mode and archive mode.

1. Click **Confirm** to acknowledge the alarm. The alarm is deleted from the alarm list and the next alarm is displayed.

2. **Reject** the alarm. The alarm is deleted from the alarm list and the next alarm is displayed.
3. **Reset** the alarm. The alarm is marked as deferred in the alarm list. No further alarm is displayed until an alarm is either called from the alarm list or acknowledged. This allows multiple alarms to be acknowledged simultaneously.

Alarm notification

A new alarm is displayed in a highlighted pop-up window that opens from the bottom of the screen (alarm notification).

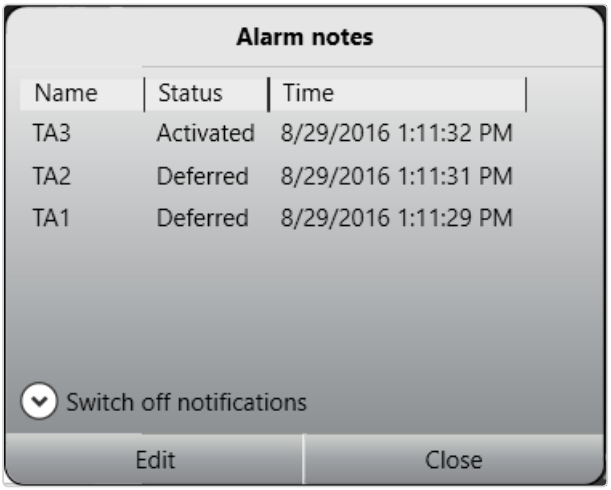


Fig. 79: Alarm notification

The notification window displays the alarm name, its status and the time of occurrence.

1. Click **Switch off notifications** to prevent the alarm notifications appear on the screen.
2. Select the time interval for the alarm message to be hidden ("snooze"). After the selected interval has elapsed, the alarm notification will be displayed again.
3. Select the alarm and click **Edit** to display the message window for editing.
4. Click **Close** to close the message window.

System messages

The system messages show the errors that have been reported by the system, such as failure of a server, database or camera and also losses of connection.
The errors are displayed in descending order by time of occurrence with a description, the internal error number, the message and the cause of the error.

1. Select one or more system messages and click **Remove selected** to remove the message from the list. The number in the red circle displaying the number of unconfirmed messages is reduced.
2. Optionally, click **Remove all** to remove all system messages from the list and to remove the red circle displaying the number of unconfirmed system messages.

Searching in surveillance mode

The search below the overview tab in the control bar helps you to find the contents of the active control bar more quickly.
If labels have been assigned to entities such as cameras, they can be used for searching, helping to narrow the search.

> **Searching for labels is not displayed if no labels are configured or no entities have been assigned to any label**

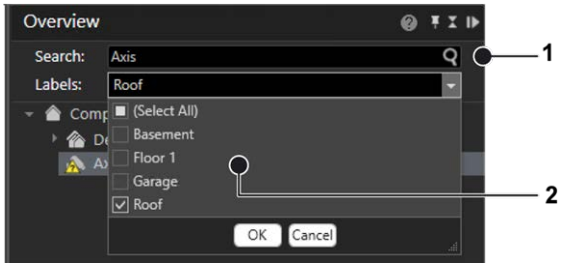


Fig. 80: Searching in surveillance mode

1. Enter the search term into the search field (1). The first term found in the overview is highlighted.
2. Click the magnifying glass on the right of the search field or click [Enter] on the keyboard to highlight the next term in the overview.

3. If configured, select one or more labels from the drop-down list “Labels” (2) and select **OK**. You can combine searching in the search field and filtering by labels to narrow down the results. Only results that contain both the search text and the labels are displayed (AND relationship).

- Filtering for an entity using a label displays the entities for that label even if they are also labeled with more than one label.
- Filtering for an entity using multiple labels displays the entities that have one or multiple labels assigned.
- Using the search term and labels at the same time displays the entities with the search term and the entities with the labels assigned.

> **You can only see labels for entities for which you have the appropriate user rights.**

Displaying search results in a temporary layer

1. Drag and drop the entity or its containing folder or branch onto the work area. The search result opens a new layer. When the results are within a folder or branch, you can drag & drop the whole branch or folder onto the work area. Only the filtered results are displayed, however.

> **When 4 layers are populated with up to 16 search results each, you are required to consent to adding more layers. Opening more than 64 results may take considerably longer.**

8

Archive mode

Archive mode is used for the retrospective evaluation of recordings. Only recorded data can be displayed in archive mode. To select the relevant image data, a camera must be selected in the camera overview or in the "Alarm list and system messages" on page 158.
The recording periods for the selected camera (green frame) are displayed in a time line in the "Archive player" on the next page. The icons for digital zoom and volume control are also displayed (only for cameras with audio recording activated).

1. To switch to archive mode, click **Archive mode** in "The mode bar" on page 126.
2. Select the camera or layer whose archived image data is to be displayed, or select an alarm from the alarm list.

Camera overview

The camera overview displays all installed cameras, maps and layers you are permitted to access. Cameras having integrated exported image data are displayed as "<camera name> [archive]".

1. Click the corresponding camera. The camera images are displayed in the main window.

Archive player

Fig. 81: Archive player

The archive player allows control of the playback from a selected camera. The player is divided into two sections. The actual archive player is shown on the left and timeline on the right.

The archive player has the following functions:

- **Bandwidth optimization options** ( ): Depending on the license and configuration an optimized video stream can be selected to reduce client and network load (see "Bandwidth optimization" on page 430).
- **Previous frame** ( ): Jumps to the recordings previous video frame.
- **Play backward** (3): Plays the archived video stream in reverse chronological order.
- **Pause** ( ): Pauses the playback.
- **Play** ( ): Plays the recorded video in the correct chronological order.
- **Next frame** ( ): Jumps to the recordings next video frame.
- **Real time** ( ): Plays the event in real time.
- **Next alarm recording** ( ): Jumps to the selected camera's next alarm recording.
- **Skip pause** ( ): Skips the pause between two recordings in playback mode.
- **Calendar** ( ): Opens a calendar window in order to navigate to a specific calendar time (date and time).
- **Zoom out from timeline** ( ) or **Zoom in to timeline** ( ): Enlarges or reduces the size of the display of the timeline. You can also zoom within the recording period by clicking the timeline and then turning the scroll wheel on the mouse.
- **Update timeline** ( ): Updates the camera's timeline. For manual synchronization with edge storage recordings (see "Full import" on page 238), hold down the CTRL key when clicking the icon.
- **Add bookmark** ( ): Adds a bookmark to the current frame (see).

- **Bookmark overview** ( ): Displays the overview of all bookmarks (see "Working with bookmarks" on page 177).
- **Multiselection mode** ( ): Sets a marker across multiple time streams.
- **Set marker** ( ): Sets the start and end markers for a selected area of the timeline (see "Editing an area" on the next page).

  Bookmarks are not supported in Viewer Mode / Qognify Viewer.
- **Delete marking** ( ): Deletes the selected marking.
- **QogniFinder** ( ): Starts the forensic search when the appropriate usage rights are provided (see "Using the QogniFinder" on page 168).
- **Synchronized mode** ( ): All visible cameras are synchronized to the time of the selected camera by default. If the synchronized mode is deactivated, each camera can show a different point in time.
- **Write protection** (/): Sets write protection for the marked area of the timeline. See "Write protection" on page 173
- **Delete area** ( ): Deletes the marked area from the timeline.
- **Export area** ( ): Starts the AVI export or the Qognify video data export (see "Exporting recordings" on page 171).

  Exporting in Qognify file format is not supported.
- **Jog dial**: Plays the sequence forward and backward. The further you turn the jog dial to the right or left, the faster the sequence is played forward or backward. The playback speed is displayed below the jog wheel.
- **Timeline / time stream**: See "Timeline / time stream" on the next page.

Using the jog dial

1. Turn the jog dial with the mouse to the left or right to play the sequence backwards and forward. When releasing the jog dial, it will return to the center position.
2. Click on a dot around the jog dial to position it there.
3. Click on the double bar above the dial to release.

Timeline / time stream

> **The time displayed in the timeline may differ from the time displayed in the video due to the way Qognify VMS stores the timestamp information (refer to "Time zone handling" on page 26).**

The timeline / time stream allows you to search across the entire recording period for relevant image material. The important color markings are:

- Green (standard recording)
- Red (alarm recording) - or any other color than green

1. Zoom into the recording period by clicking the timeline and turning the scroll wheel on the mouse. This improves the overview of the recording start of the camera.
2. Double-click any point in the timeline to move the selected point to the timeline center.

Preview

1. Move the mouse over the timeline or move the timeline to display the preview of the camera image at the selected time. The setting in the client configuration must be defined as “Always On” (see "Client configuration" on page 64).
2. Optionally, keep the control key pressed when moving the mouse over the timeline or moving the timeline. This will only display the preview with the control key pressed. For this, the setting in the client configuration must be defined as "Ctrl + MouseOver".

> **The preview feature is not available in the mini archive mode of a tile.**

Editing an area

1. Click the camera time stream next to the jog dial. If one camera is played or multiple cameras are played synchronously, the current time of the archive is displayed next to the playhead. If multiple cameras are played asynchronously, the current time of the archive is not displayed.
2. On the timeline, select **Set start marker** to mark the beginning of the section. When setting markers simultaneously across multiple timelines, select **Multiselection mode** first. When multiselection mode is active, the icon is green.
3. Move the time bar to the of the end of the section.

4. Select **Set end marker** to specify the end of the section.
5. Select **Delete area** to remove the section from the timeline.
6. Click **Export area** to export the section.
7. Select the required data format (**Type**), and select **OK**. The following export formats are available:
   - Qognify data format: The exported data are password-protected and can only be viewed with the viewer.
   - AVI: The exported data are not password-protected and can be viewed with any film software. This represents a high data protection risk.
8. Specify the required export settings (see "Multiple export of image data" on page 104).

Click-2-Track

The feature is used in archive mode to navigate from one camera to the next by clicking on the Click-2-Track regions in the image.
The preview of the Click-2-Track region shows the same point in time as the current archive timeline. If the archive is in playback mode, the preview inset plays at the same speed as the main image. The current speed and direction remains the same even when switching between Click-2-Track regions and changing the camera.

> **The feature works with playback forward and backward at different speeds as well as still images.**

The history feature

Click-2-Track stores a history of the camera according to the following criteria:

- Each camera stores the time when it was opened and the time when it was replaced by the next camera.
- When navigating to the next entry in history, the camera shows the opening time.
- When navigating to the previous entry in history, the camera shows the closing time.
- Only the Click-2-Track uses from the current tile are saved in the history feature. All tiles have their own history.

Example

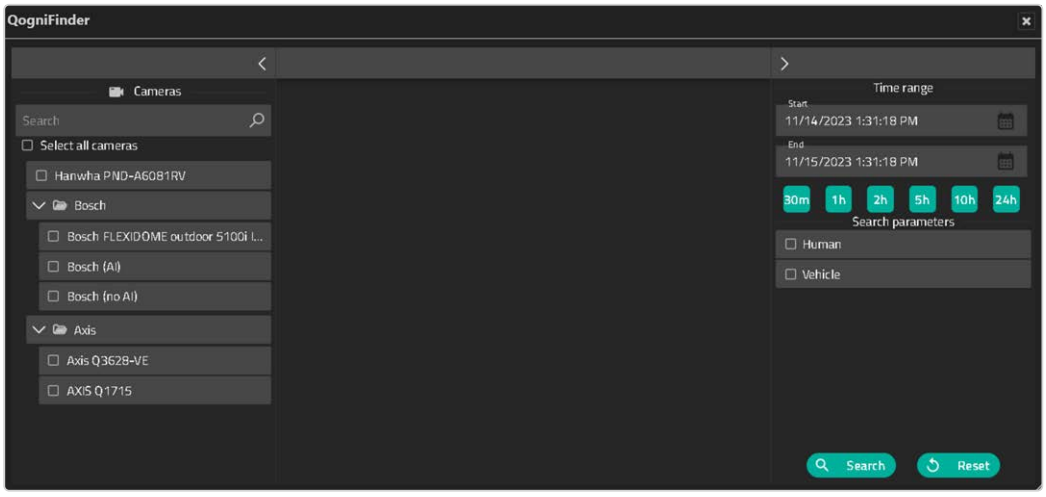
1. Camera A is viewed from 8:00 to 8:01, then the region for Camera B is selected.
2. Camera B is viewed from 8:01 to 8:02, then the region for Camera C is selected.
3. Camera C is viewed from 8:02 to 8:03, then the button **Back** in the history is used. The view jumps to Camera B at 8:02 with a still image, regardless of the previous speed.
4. When the button **Back** in history is used again, the view will jump to Camera A at 8:01 with a still image.
5. Using the button **Forward** in history, the view jumps to Camera B at 8:01, using it again jumps to Camera C at 8:02.

Using the QogniFinder

The QogniFinder interface uses the same language

> **QogniFinder must be enabled for the selected camera in configuration mode (see "Camera general" on page 226).**

1. In Archive mode, select the camera and select **QogniFinder** in the toolbar of the Archive player. When multiple cameras are configured, they are displayed as groups named according to the manufacturer's name.



2. Select the camera(s) used to search for objects.

> - If a camera does not support some search criteria, the corresponding search criteria are highlighted.
> - If a camera supports none of the search criteria, the camera is highlighted.

3. Define the **Time range** for the search by entering the start and end dates or selecting one of the predefined filters:

- 30 m: the last 30 minutes
- 1 h, 2 h, 5 h, 10 h, 24 h: the previous interval of one hour up to the last 24 hours

4. Enable the primary search parameters:

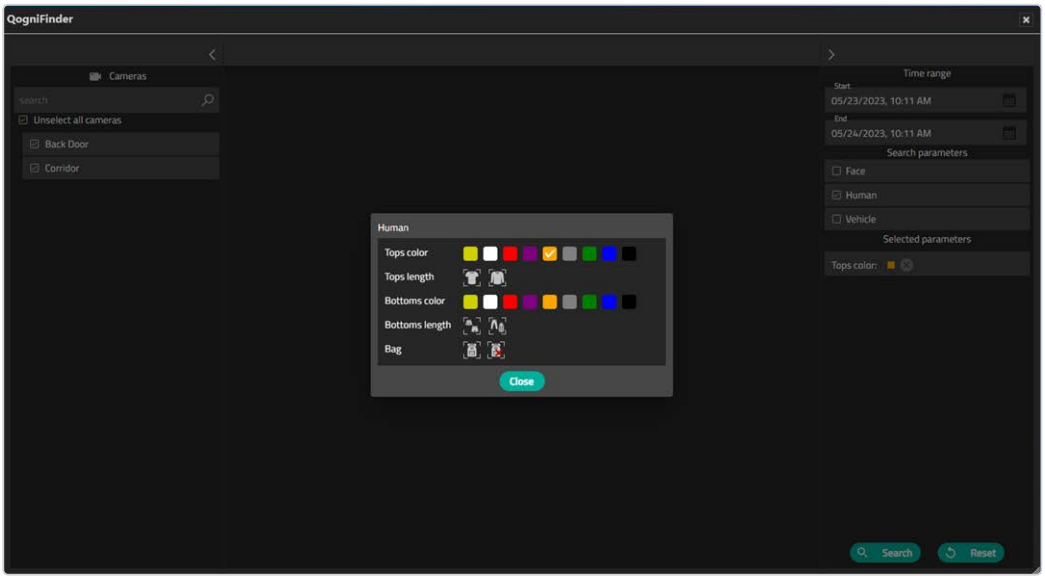
- Human (face and body combined)

> **For supported cameras from Hanwha, the search criterion "Human" also includes criteria such as "Hat", "Bag", etc.**

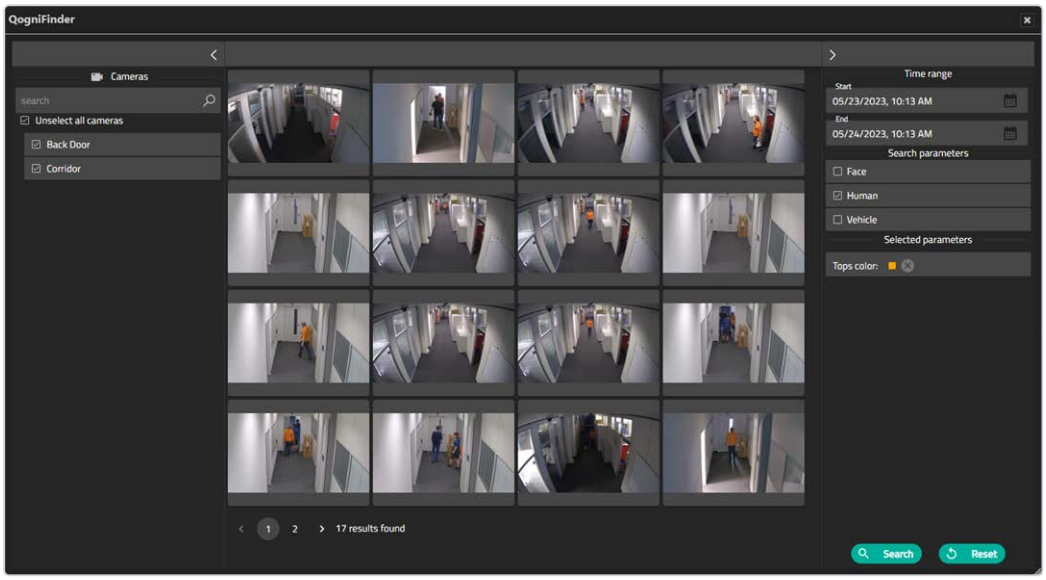
- Vehicle

> **For supported cameras such as specific cameras from Hanwha, Axis, or Bosch, the search for "Vehicle" also displays the vehicle type as criterion.**

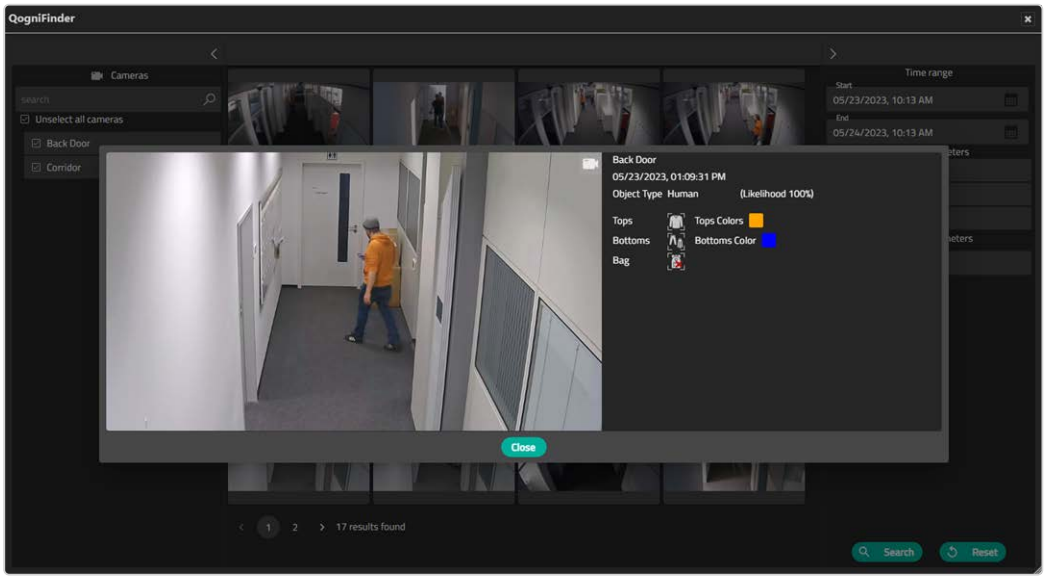
5. To define the search parameter, click on the enabled parameter(s) and specify further metadata such as clothing color or vehicle type.



6. Close the selection window and click **Search**. The objects within the specified time range and all images meeting the specified search criteria are displayed.



7. If more the 16 results are found, use the paging function at the bottom of the window to navigate to more objects or narrow the search by adding parameters or changing the time range.
8. To see the details of a result, move the mouse over the preview and click on the camera icon . The search parameters are displayed along with the selected scene.



9. If more than one result is found, navigate to the next or previous result using the buttons and .
10. To start a search with other parameters, select **Reset** and define the new search parameters.

Exporting recordings

Exporting a single frame

1. In the frame tile, select **Export** in the tile bottom.
2. Select the export format:
   - **Save video frame in file**. This saves the selected frame as a static image file (JPG).
   - **Print video frame**. This prints the selected frame as hardcopy with additional information such as camera and recording time.

Exporting a video file

1. Set the time range for the export by moving the recorded section and setting the marker at the start and end points.
2. Use the multiselect marker to select multiple timelines at once by placing it on the timeline of one camera. All camera timelines at the same vertical selection are marked.
3. To remove a time range, select **Delete marking** and select the time range(s) to be removed.
4. Select **Export** in the archive player controls.
5. Select the export type **Video data export** (password encrypted Qognify-specific format) or AVI export (unencrypted data format).

   > **If video data export is selected, the recordings are exported to the server or to the client (see "Multiple export of image data" on page 104).**

   > **If the export process is interrupted, e.g. due to a network error, it will automatically be resumed as soon as possible.**

6. Proceed according to the required targets (for the following procedures, refer to "Multiple export of image data" on page 104).

Exporting the Click-2-Track history with the Export Designer

When exporting an event with the Export Designer, the Click-2-track history can be exported as well.

> **For the cameras with Click-2-Track enabled, this handover feature also works in the "Anywhere Viewer" on page 503.**

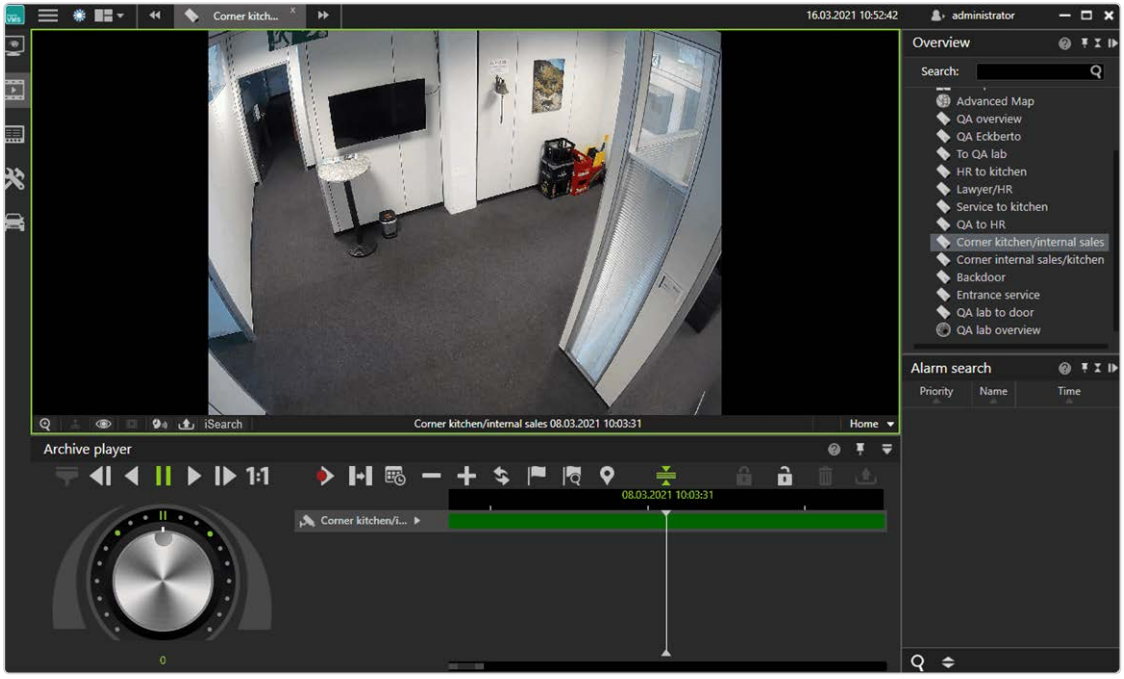
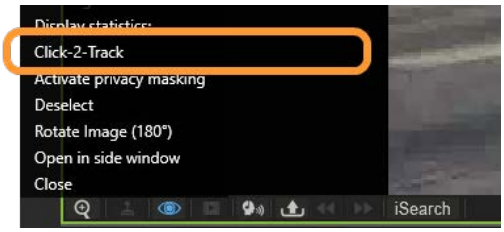


Fig. 82: Example of following a person in archive mode with Click2Track

1. Open the camera in the archive player.
2. Select **Click-2-Track** in the **Layer options** .



3. Select **Activate** and follow the shapes in the image sequence by clicking on the respective shape. This opens the camera sequence of the assigned camera.

4. Select **Click-2-Track > Open history in Export Designer** to start the Export Designer (see "The Export Designer" on page 96). The Click-2-Track history of the camera is displayed in a list as sequences.

5. Click on a privacy mask to include or exclude the privacy mask in the export.

> **Privacy masks cannot be hidden in offline mode.**

6. To delete a sequence from the export, select the sequence and click **Delete** . By default, all sequences are exported.

Evaluating exported video data

There are two options for evaluating the exported video data:

- On a system without a Qognify VMS installation, the video data can be evaluated using the Qognify VMS Viewer (see "Anywhere Viewer" on page 503).
- To integrate the video data within a Qognify VMS installation, an "archive camera" must be created in the configuration mode (see "Creating a camera manually" on page 212).

Write protection

> **Write protected recordings remain in the zone directory and will not be deleted. Make sure that sufficient disc space on the zone partition is available.**
> **Due to legal regulations, write protection may not be used for installations in France.**

Set write protection

The protected range in the timeline is at least as wide as the range selected by the user, as Qognify VMS may protect a wider range, for example to optimize the

performance of the Multimedia Database (mdb). The actual protected time range is displayed after setting the write protection.

1. On the timeline, select **Set markers** to mark the beginning of the section to be protected.
2. Move the time bar to the of the end of the section to be protected.
3. Select **Set markers** again to specify the section.
4. Select the closed **padlock** to protect recordings from being overwritten or deleted.

Remove write protection

1. Select **Open padlock** ( ) in the Archive player.

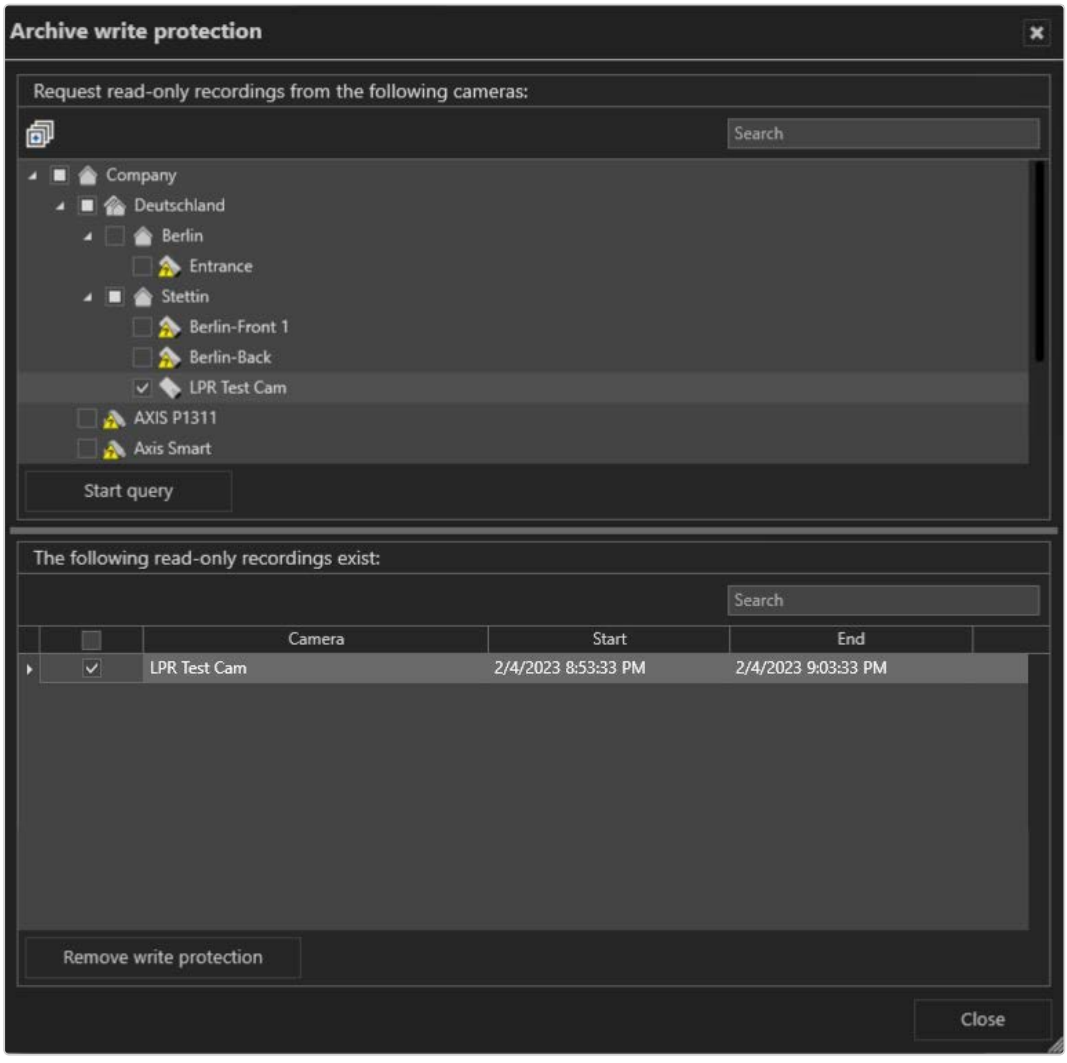


Fig. 83: Remove write protection

2. Select **Start query**.
3. Select the write protected sequences. Hold the CONTROL-key to select multiple sequences.
4. Select **Remove write protection**.

Searching for alarms

> **The time displayed in the timeline may differ from the time displayed in the video due to the way Qognify VMS stores the timestamp information (refer to "Time zone handling" on page 26).**

With the alarm search you can search for specific alarm depending on configurable conditions.

Creating an alarm query

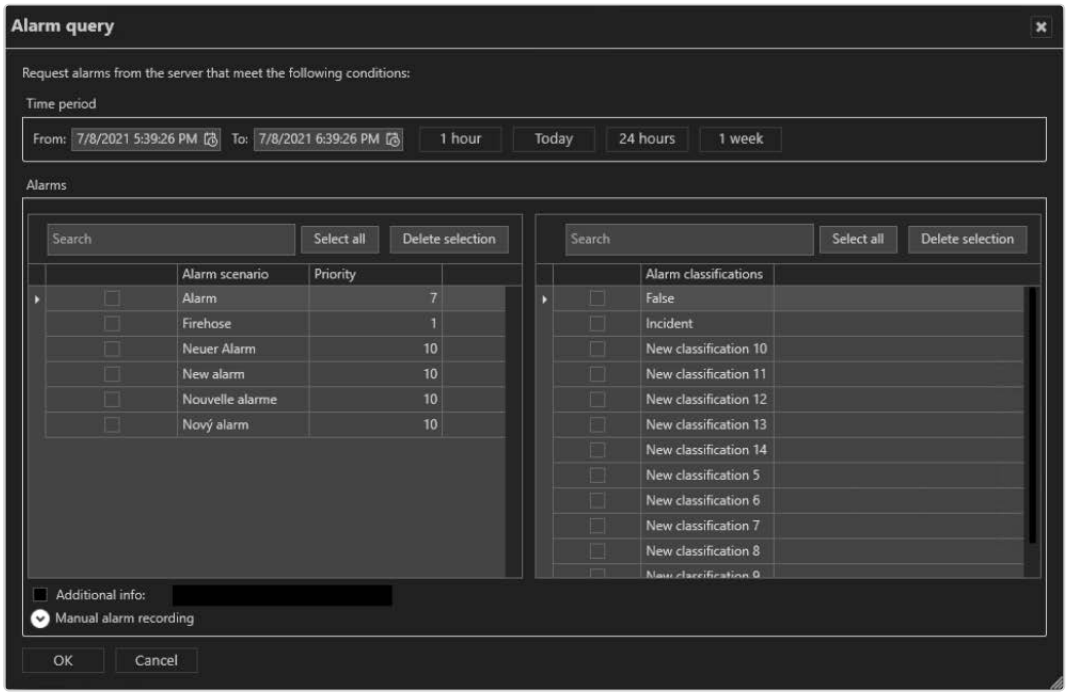


Fig. 84: Searching for alarms

1. Click **New request** in the Alarm search control. The Alarm query is displayed.
2. Specify the **Time period** for the alarm to be searched.

3. Optionally, select the recent time intervals of the last hour, the last 24 hours, the last week, or the current day.
4. Select the “Alarm scenario”, either by name or by priority.
   - To select all items, click **Select all**.
   - To deselect, click **Delete selection**.
5. Select the “Alarm classification” either by direct selection or by searching the classification term. The alarm categories are defined in the system configuration (see "Configuring the alarm classifications" on page 431).
6. If available, enter the additional information that is obtained by network triggers (e.g. Network IO) to be searched for.
7. Select **Manual alarm recording** to include manual recordings of the available video sources in the search.
8. Select the recordings of the camera or cameras to be searched.
9. Click **OK** to start the search.

Alarm search results

The results of your alarm query are displayed in the Alarm search control.

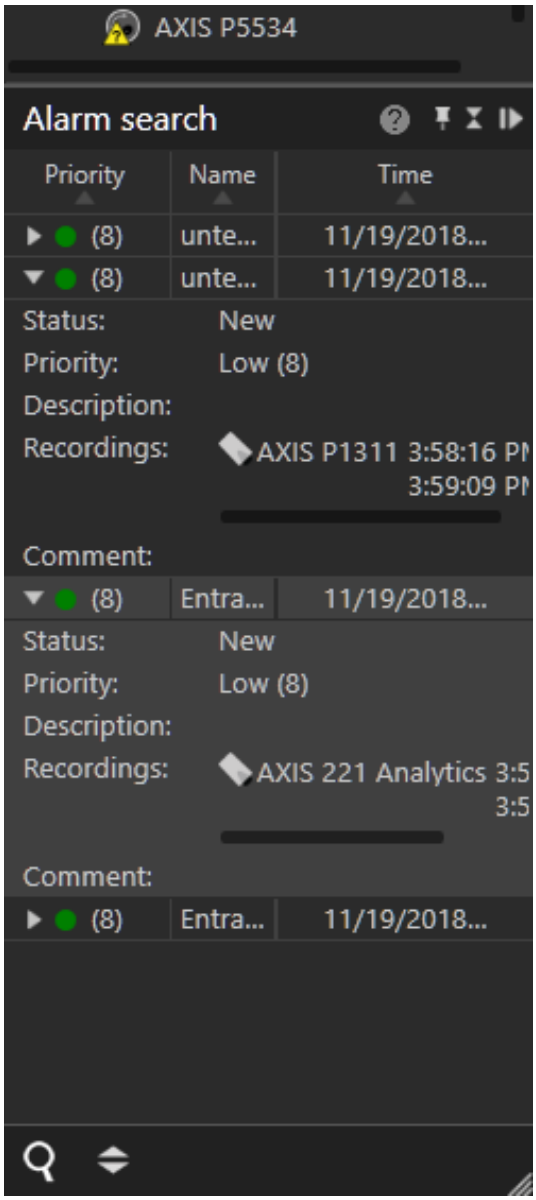


Fig. 85: Alarm search results

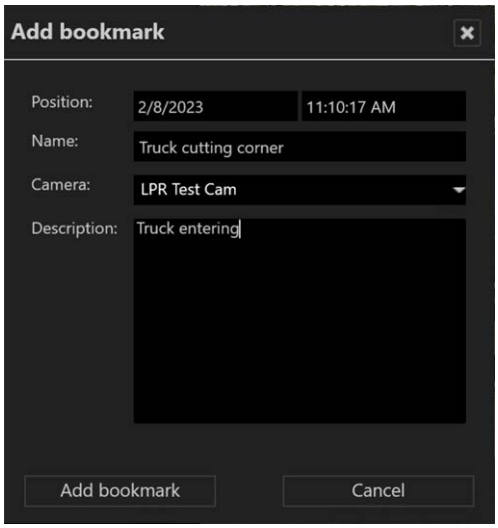
1. Click on one of the column headings **Priority**, **Name** or **Time** to sort the results accordingly.
2. Click on the on the arrow on the left of an alarm to display details.

Working with bookmarks

Bookmarks can be set in archive mode or when starting or ending a manual alarm recording (see "Manual alarm recording" on page 144).

Adding a bookmark

1. Move the timeline to the position where you want to set the bookmark.
2. Select **Add bookmark** ( ) in the Archive player.

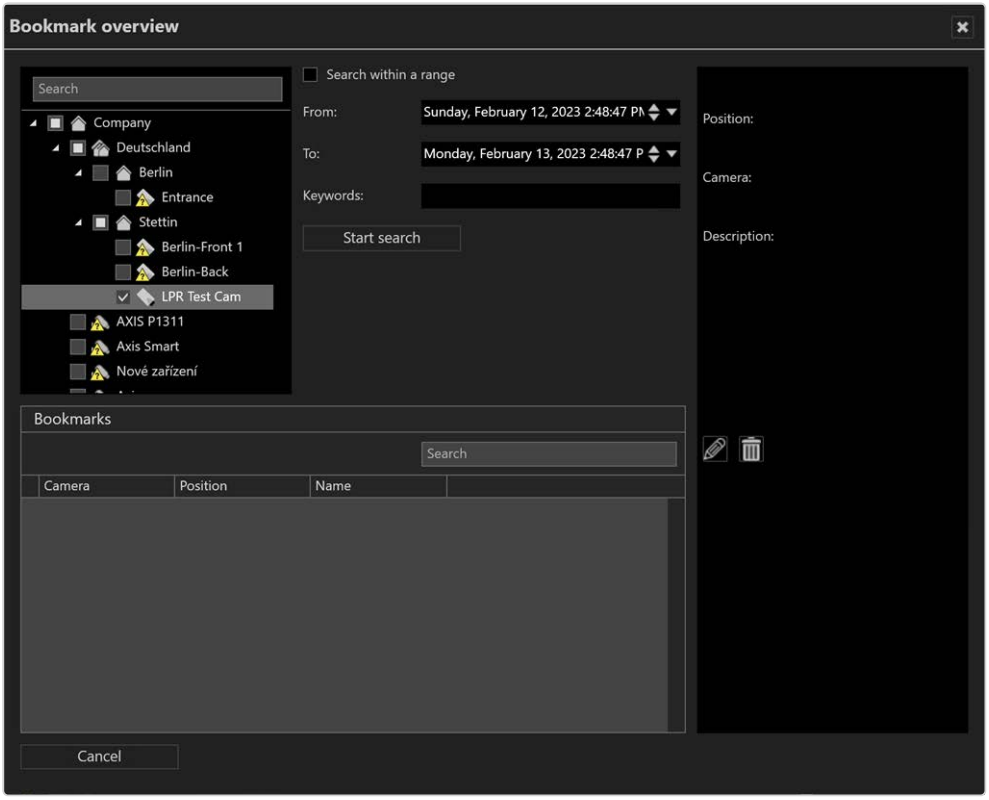


3. Enter a **Name** for the bookmark.
4. Select the **Camera** for which you want to bookmark the recording from the drop-down menu. The drop-down menu contains all cameras in that are currently displayed in the archive player. By default, the currently active camera in the archive player is selected.
5. Enter a description, if required.
6. Select **Add bookmark**. A flag will be added to the time line of the selected camera.

Bookmark overview

In the bookmark overview, bookmarks can be displayed, edited and deleted.

1. Select **Bookmark overview** ( ) in the Archive Player.



2. Select one or more cameras or click **Select all** to select all cameras displayed (i.e. cameras with bookmarks attached).
3. Optionally, search for the camera name or the bookmark.
4. Search bookmarks for all cameras even if only visible in the archive. Bookmarks from cameras of different installations can be searched simultaneously.
5. To deselect, click **Cancel selection** .
6. Enable **Search within a range** to narrow the time window for the search and specify the time interval.
7. Select **Start search** to display only the bookmarks within the specified time interval. The bookmarks are displayed in the "Bookmarks" section.
8. Select a bookmark from the "Bookmarks" section. The information associated with the bookmark (time, the assigned camera, and the description) is displayed in the right area.

9. Double-click on the bookmark to navigate to the corresponding time marker.
10. To edit the information, select **Edit** ( ) (see "Adding a bookmark" on page 178).
11. To **delete** the bookmark, select **Delete** ( ).

Bookmarks are not deleted with the video data, because they are stored in a separate event database. They are deleted automatically, once the oldest video image is newer than the time stamp of the bookmark.

Edge storage import

Edge storage uses the camera to store images on an internal storage media (e.g. SD card) to cover connection failures between the camera and the database server. If the connection between the camera and the server is interrupted, recording gaps on the DeviceManager will result.

After the connection is reestablished, the recording gaps on the server can be filled with the recordings from the camera's internal storage media. Time schedules for recording and maximal recording size are taken into consideration. (see "Image storage" on page 231).

Depending on the configuration of the camera (see "Edge storage" on page 240), edge storage data can be imported automatically or manually.

Manual edge storage import

1. For manual edge storage import, hold down the CTRL key when selecting **Update timeline** .

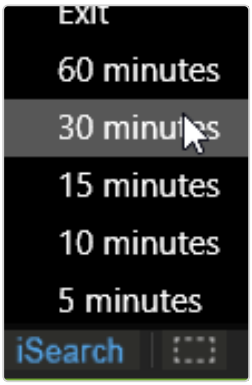
iSearch

iSearch in archive mode searches recordings for motion in specific image regions. The searchable time period is 5 to 60 minutes.

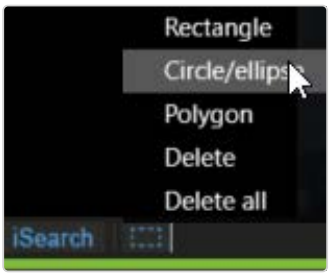
The performance of iSearch depends on the performance capability of the client hardware, since the search is carried out exclusively on the client.

Configuring iSearch

1. Select the related camera.
2. Click **iSearch** at the bottom of the video image and select a time range between 5 and 60 minutes. The maximum selectable time range depends on the access restrictions of the user for the archive (see "Rights options" on page 332).



A dotted rectangular icon is displayed on the right side of the iSearch button.



3. Click on the **area** icon and select the shape of the search area. The following shape options are available:
   - Rectangle
   - Circle / ellipse
   - Polygon
   - Delete shape
   - Delete all shapes

4. In the camera image drag the selected shape to the desired position. A semi-transparent area is laid over the image in the selected position.

> **If you selected the polygon for this purpose, click a point in the image for each corner and close the polygon by double-clicking the last point.**

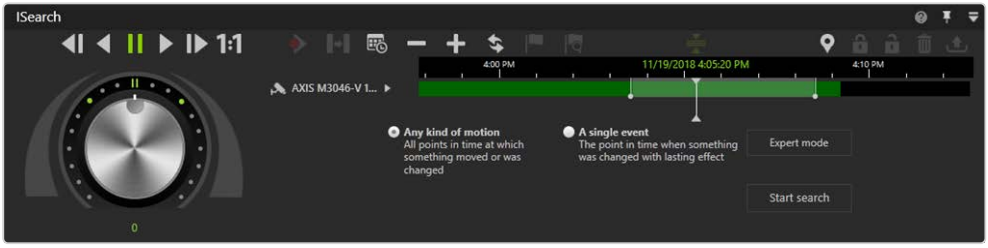


Fig. 86: Configuring iSearch

5. Within the selected area, select either **Any kind of motion** (default) or **A single event**.
   - **Any kind of motion**: This search method searches for all changes within the image in the specified period. The search can be performed for the whole image or for parts of the image as specified by the user. The search may take some time depending on the selection.
   - **A single event**: This search method is particularly quick. It is possible to search through several days of image material in a few seconds. However, this method only works if a single, lasting event has occurred in the camera's selected field.
6. Optionally select **Expert mode** to fine tune the search.

iSearch in expert mode

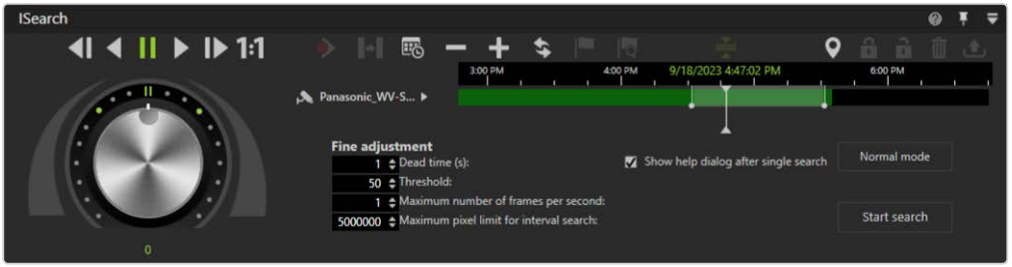


Fig. 87: iSearch in expert mode

1. Specify the desired settings and start the search. The following options are available:

- **Dead time** in seconds specifies how much time has to elapse after motion detection in the image or part of the image before another hit is displayed in the result list.
- **Threshold** detects changes in the image when the camera is operating in extreme light conditions. A change in the image is interpreted as "motion" if it exceeds the threshold. The higher the threshold, the greater the change in the image must be before it is considered to be "motion".
- **Maximum number of frames per second** if not all of the recorded frames have to be searched. This can speed up the search significantly.
- **Maximum pixel limit for interval search**: The maximum pixel limit for an interval search only has an impact on searches for a lasting change. The specified start and end points of the period in which the search is to be carried out are compared continuously. If the two points currently diverge by more than the specified pixel limit, interval bisection is interrupted, and a serial search with greater increments is started until the pixel limit is adhered to again. The interval search is then resumed from this point. This setting improves the search under extreme lighting conditions (strong contrast between light and dark areas or objects passing).
- **Show help dialog after single search**, if appropriate. On completion of the search, you can specify in a dialog whether or not the event has been found and whether you want to switch to archive mode with the event found.

2. To exit expert mode, select **Normal mode**.

Deleting a search area

1. Click the search area, and select **Delete** to delete only the selected area.
2. Optionally, select **Delete all** to delete all areas.

9

Report mode

Report mode gives you an overview of the events that have occurred in the form of a list. Distinctions are drawn between:

- User events (display of events that concern specific users)
- Alarm events (events that have occurred)
- Camera usage (display of events that concern a specific camera)
- System messages (display of events that concern specific services)

In addition, the camera usage of users can be tracked and the user can see which changes have been made to the configuration and by whom.

> **The maximum number of events to be displayed can be specified in the client configuration (see "Client configuration" on page 64).**

1. To switch to report mode, click the **Report mode** icon on the mode bar.

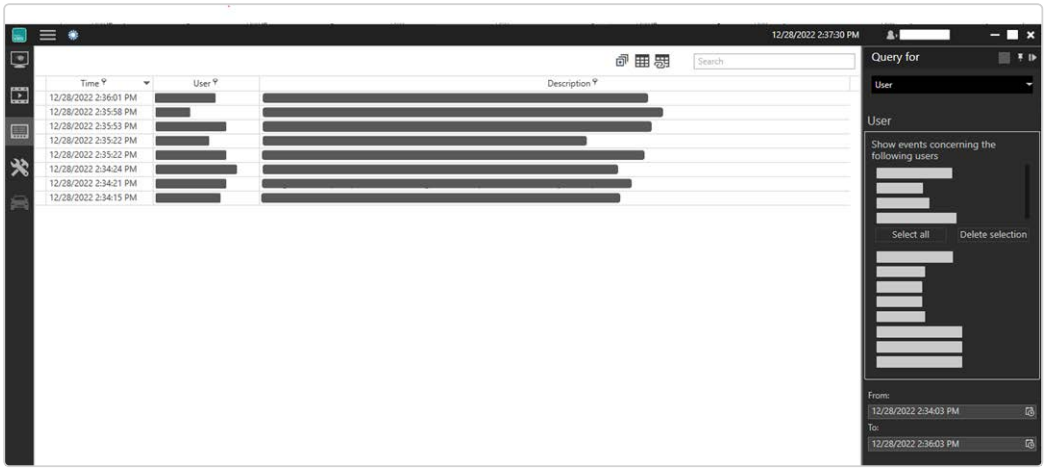


Fig. 88: Report mode

2. Click a column header in the main window to sort the events in ascending or ascending order based on the column's category (date / time, user, description).

Filtering the query

In report mode, the following event types can be evaluated:

- Alarms can be filtered for alarm scenarios
- Users can be filtered for:
  - Users
  - Camera configuration
  - Archive
  - Export
  - Patrols
  - Actions
  - Log on or log off
  - Failed logins
  - Change mode
  - Sharing and restriction events
- Camera usage can be filtered for:
  - Camera (only if the DeviceManager records camera usage)
  - Users

- System can be filtered for:
  - Core services
  - Image storage

Depending on the area, the query results can be filtered.

1. To filter the events on the basis of specified criteria, select the type of event you are searching for on the **Query for** control bar.
2. Select the user or users related to the events to be searched for.
3. Select the desired events. The items are displayed in the list below.
4. Select specific items by clicking the check box in front of the item's name or click **select all**.
5. To deselect, select **Delete selection**.
6. To further narrow the selection, specify dates and times to define the time period.
7. **Start** the query. Only the events that meet the selected criteria are displayed in the main window.

Exporting the analysis as spreadsheet file

You can also export the result as a comma-separated file (*.csv).

1. **Export** the result in order to analyze it in a spreadsheet program.

Saving a query as report template

Additionally, the search criteria can be saved for future queries.

1. In the report mode window, select **Save**.

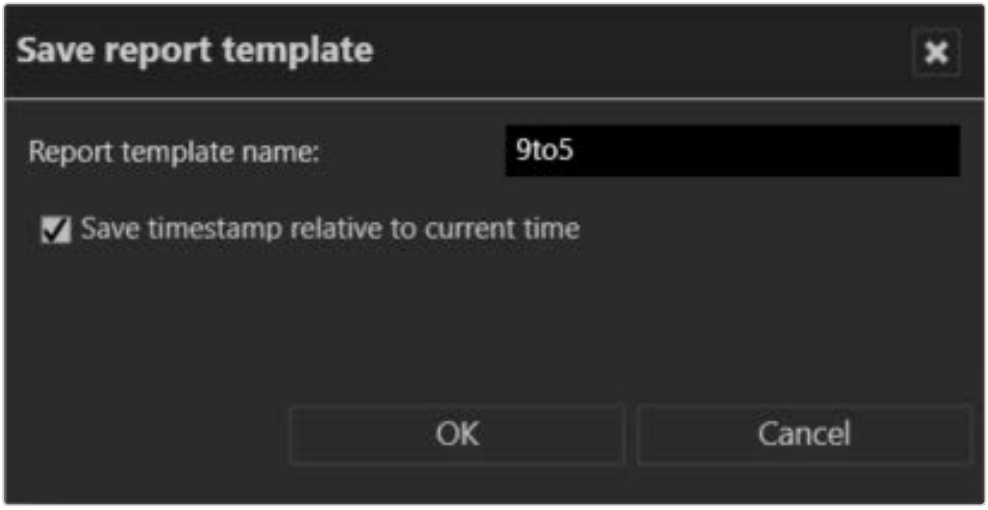


Fig. 89: Saving a query as report template

2. Enter the **Report template name**.
3. Optionally, select **Save timestamp relative to current time**. This option will use the time interval of the current query for the next query.
   Example The current query searches for events within the last 24 hours. When the query is saved with a relative time stamp, the next query will also search within the last 24 hours - relative to the next query.
4. Select **OK** to save the query.

Using a previously saved query

1. Select the name of the query in the drop-down menu and select **Start query**.

Deleting a saved query

1. To delete the saved query, select the query from the drop-down menu and select **Delete**.

10

Configuration mode

> **Adequate administrator rights are required for configuration mode.**

> **It is highly recommended to obtain a basic understanding of the concept of the underlying rights management before configuring the system (see "Concept" on page 24).**

In configuration mode all of the settings for e.g. the hardware, network, company, maps, alarms and users are made.

The Administration control allows you to assign hardware (e.g. cameras), actions and the authorization manager to the specified administration, and manage new objects such as alarm scenarios.

1. To change to configuration mode, click the **Configuration mode** icon in the mode bar (see "The mode bar" on page 126).

Additional settings

- See "Company and branches" on page 199 for further settings for the company.

Functions

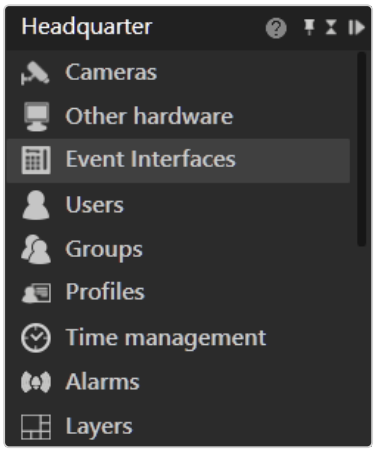


Fig. 90: Functions

Depending on the available hardware, the network architecture, and the Qognify VMS license, the following functions can be configured:

- **Cameras**: This function allows you to configure and manage the camera hardware and the associated video server (see "Cameras" on page 211).
- **Other hardware**: This function allows you to configure and manage additional devices (see "Other hardware" on page 272).
- **Event Interfaces**: This function allows you to configure third party safety systems which can be integrated by plug-ins (see "Event Interfaces" on page 322).
- **Users**: This function allows you to configure and manage the users (see "Users" on page 329).
- **Groups**: This function allows you to configure and manage the user groups (see "Groups" on page 338).
- **Profiles**: This function allows you to configure and manage the user and group profiles (see "Profiles" on page 345).
- **Time management**: This function allows you to configure and manage the time templates to coordinate the standard image recording of individual or multiple cameras as well as validity in alarm scenarios (see "Time management" on page 351).
- **Alarms**: This function allows you to configure and manage the alarm scenarios (see "Alarms" on page 356).

- **Layers**: This function allows you to configure and manage the layers to display multiple cameras or maps in surveillance mode (see "Surveillance mode" on page 131).
- **Maps**: This function allows you to configure and manage the graphical maps of the site or building under surveillance, including the location of the surveillance hardware (see "Maps and "Advanced Maps"" on page 377).
- **Buttons**: This function allows you to configure and manage the sequences of actions that can be triggered in the controller in surveillance mode (see "Buttons" on page 386).
- **Web pages**: This function allows you to embed web pages in the layer (see "Web pages" on page 389).
- **Patrols**: This function allows you to configure and manage multiple cameras, set positions, maps and layers one after the other for a user-definable time (see "Patrols" on page 391).
- **Sequences**: This function allows you to configure and manage the sequences of actions in which multiple set positions are approached one after the other and/or actions are triggered (see "Sequences" on page 394).
- **Video walls**: This function allows you to configure the arrangement of video wall screens. You can drag and drop camera images, layers, maps and web pages to display them on video walls (see "Other hardware" on page 272 for information on how to configure the screens).
- **License plate groups**: This function allows you to configure and manage the number plate recognition function of the LPR module (see "License plate groups" on page 400).
- **Server**: This function allows you to configure the device services (see "Server" on page 402).
- **System**: This function allows you to configure and manage system-wide settings for the network, automatic backups, communication settings and event management settings (see "System" on page 428).

The configuration shortcuts

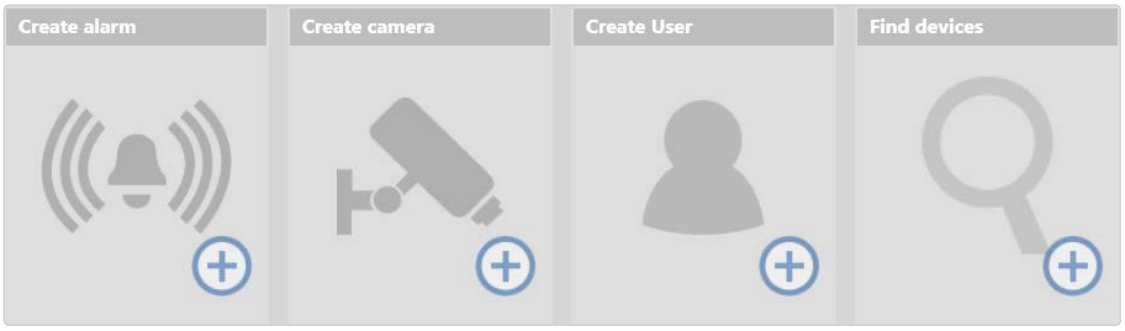


Fig. 91: The configuration shortcuts

You will find the configuration shortcuts on the starting page of configuration mode. They help you navigate to the settings for new cameras and alarms, and to find available devices on the network. You can use them to start settings for the following tasks:

- Creating alarms, see "Alarms" on page 356
- Creating cameras, see "Creating a camera manually" on page 212
- Creating users, see "Creating a user" on page 330
- Find available devices, see "Find devices" below

Find devices

By using the IP address assigned uniquely to a network device (e.g. cameras, encoders), the Device finder is able to find and display network devices. With the device finder, IP-cameras can be easily integrated into the Qognify VMS system.

1. Select **Find devices** in the Configuration mode view. All detected network devices (cameras) are displayed in the Device finder window. Unknown network devices (i.e. not yet configured cameras or routers) are displayed as gray text.

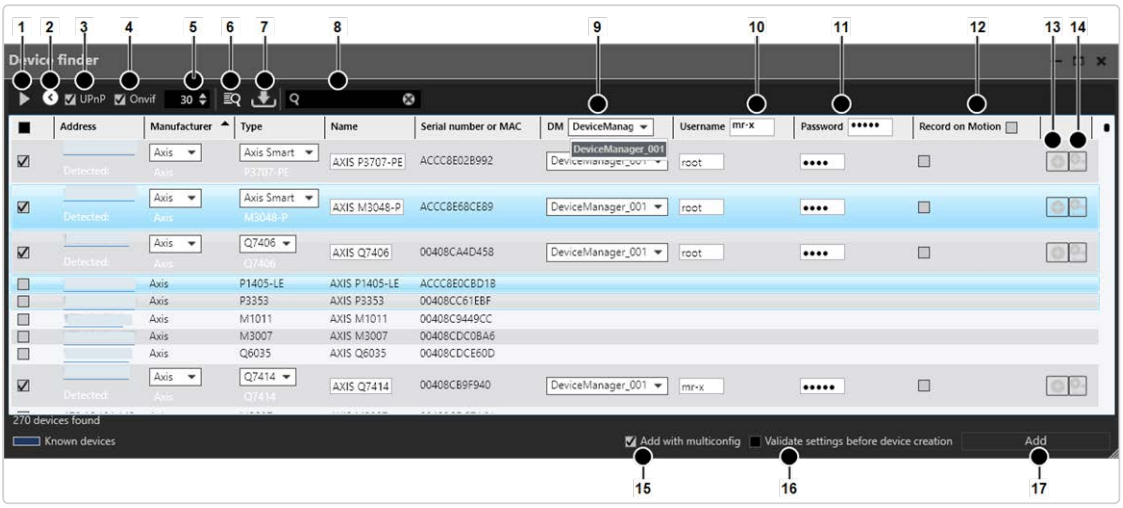


Fig. 92: Find devices

Filtering the search results

1. Click the **triangle** (1) to start a new network scan if not all network devices are found automatically after the first scan of the Device finder.
2. To display additional network options, click the **circle** (2). The Device finder supports ONVIF (3), UPnP (4), and Bonjour (available if installed on the system) protocols to search the network for devices.
3. Specify the **timeout** (in seconds) (5) for the protocols. This defines the time each protocol "listens" for new devices. After the timeout, the search has to be triggered manually.
4. Click the **search filter** (6) to toggle the display between all available devices or all unknown devices.
5. Click on one of the column header to sort the devices by **Address**, **Manufacturer**, **Type**, **Name**, or **Serial number or MAC** (MAC-Address).

6. To filter the results, enter one of the following search items in the search field:
   - IP address
   - manufacturer
   - device type
   - name
   - Serial number or MAC address

Adding individual devices

1. Select the camera to be added by clicking the check box in the first column.
2. Optionally click on the IP address to open the device-website in a web browser.
3. If required change the settings for **Manufacturer**, **Type**, and **DeviceManager** (DM).
4. Optionally, rename the camera or change user name and password.
5. Click **Add** (13) in the camera row or click **Add and Configure** (14). After clicking **Add and configure**, the configuration settings window for this device is displayed.
6. Configure the camera (see "Cameras" on page 211).

> **For adding a camera without the Device finder, see "Creating a camera manually" on page 212.**

Adding multiple devices

> **For all selected devices, the following settings can be made in the column header:**
>
> - Device Manager (9)
> - User name (10)
> - Password (11)
> - Record on motion (12)

1. Select the cameras to be added by clicking the check boxes in the first column.
2. Optionally click on the IP address to open the device-website in a web browser.

3. If required change the settings for **Manufacturer**, **Type**, and **DeviceManager** (DM).
4. Optionally, rename the camera or change user name and password.
5. To configure the selected cameras with the multi-configurations option, select **Add with multi-config** (15) (see "Configuring multiple cameras" on page 268).
6. Optionally activate **Validate settings before creation** (16) to check that the configured device settings are correct.
7. Click **Add** (17).

Camera import via CSV or XML files

With the camera import function camera configuration data can easily be imported based on structured csv or xml files.

Requirements

The files must adhere to certain requirements before the cameras can be imported.

CSV file requirements

The requirements for the importable csv file are:

- The entries must be separated by comma ","
- No spaces before or after a comma
- The first line must be a header
- The header must include the strings **IPAddress** and **DisplayName**
- If special characters (ß, ö, Ø, etc.) are used, the file must be encoded in UTF-8 format

> **The header strings are recognized automatically. The order does not matter.**

In addition the csv file can include the following values:

- MAC address
- DriverName: The value for driver should be the same as in Qognify VMS for *Manufacturer*, e.g. "Axis" instead of "AxisDriver"

- User Name
- Password

Example

```
DisplayName,MAC,IPAddress,Manufacturer,UserName,Password
Front Door,,172.16.101.153,Axis,root,pass
Back Door,0002D124EA0B,172.16.117.70,Vivotek,,
Entrance,ABCDEFABCDEF,1.2.3.4,Test,UserName,Password
```

XML file requirements

The requirements for the importable XML structure file are:

- The first element must be **<config>**
- The first child element must be **<Devices>**
- The **<Devices>** element contains all devices
- Each devices must contain the elements **<IPAddress>**, **<Manufacturer>**, and **<DisplayName>**.

In addition, the file "Device elements" can include the following values:

- MAC address
- DriverName
- User Name
- Password

Example

```
<config>
  <Devices>
    <Device1>
      <DisplayName>ImportTest2 - Axis</DisplayName>
      <MAC/>
      <IPAddress>172.16.101.153</IPAddress>
      <Manufacturer>Axis</Manufacturer>
      <Cameras>
        <Camera1>
          <DisplayName>ImportTest - Axis</DisplayName>
        </Camera1>
      </Cameras>
    </Device1>
    <Device2>
      <DisplayName>ImportTest2 - Vivotek</DisplayName>
      <MAC>0002D124EA0B</MAC>
      <IPAddress>172.16.117.70</IPAddress>
      <Manufacturer>Vivotek</Manufacturer>
```

```
      <Cameras>
        <Camera1>
          <DisplayName>ImportTest - Vivotek</DisplayName>
        </Camera1>
      </Cameras>
    </Device2>
    <Device3>
      <DisplayName>ImportTest2 - Unknown</DisplayName>
      <MAC>ABCDEFABCDEF</MAC>
      <IPAddress>1.2.3.4</IPAddress>
      <Manufacturer>Test</Manufacturer>
      <Cameras>
        <Camera1>
          <DisplayName>ImportTest - Unknown 1</DisplayName>
        </Camera1>
        <Camera2>
          <DisplayName>ImportTest - Unknown 2</DisplayName>
        </Camera2>
      </Cameras>
    </Device3>
  </Devices>
</config>
```

Importing the CSV file or XML file

1. Switch to configuration mode and click on **Find devices**.
2. Select **Import** .
3. Select the CSV file or the XML file and import it.

> **Depending on the amount and the type of devices to be imported the import process can take a while.**

- If the device finder is still running a search you will receive a message that the imported devices are not shown yet.
- When the device finder has finished searching, the imported configuration is added to the device finder's result list.
- For devices included in the imported configuration and which are also found by the device finder, adding their configuration is fast.
- For devices included in the imported configuration but not found by the device finder, Qognify VMS tries to complete the data. This might take a few seconds for each camera.
- The progress is shown in an overlay (not a dialog box) so that the user can continue working during the import.

- After the import has finished, a message about the import status and the different colors in the device finder is displayed. Devices that have been found by the device finder are highlighted in green, devices which were not found are highlighted in red.

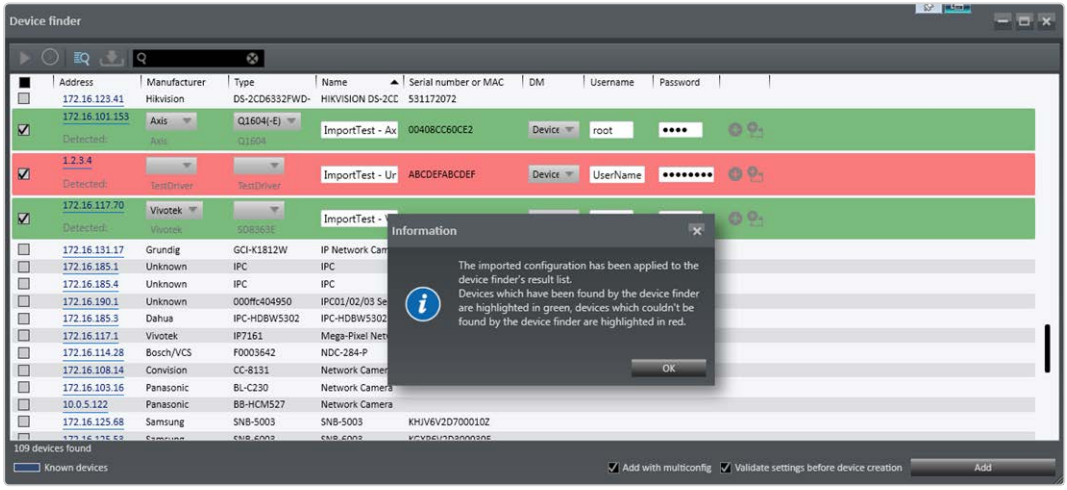


Fig. 93: Importing the CSV file or XML file

For further settings, see "Filtering the search results" on page 193.

Searching in configuration mode

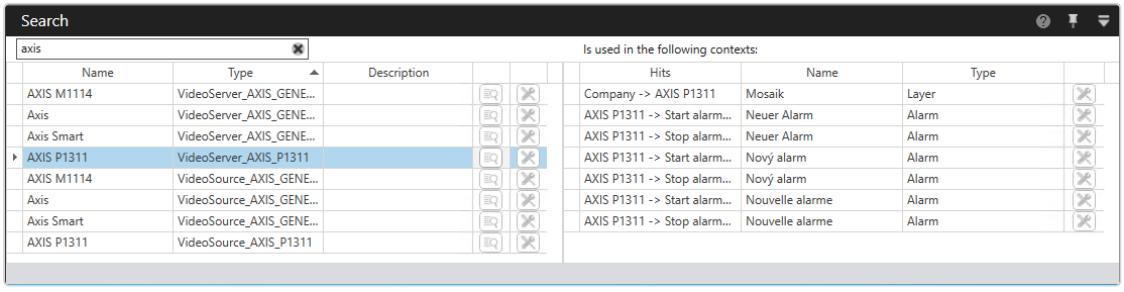


Fig. 94: The search control in configuration mode

The **Search** control below the work area helps you find the contents of the server database more quickly The search starts as soon as the second character is entered and shows a list of all the results.

1. Enter the search term, which can be an object name or a description. The search starts as soon as the second character is entered and shows a list of all results. Information on the type is also displayed.

2. Select **Show References** . The right column shows context belonging to the found term.
3. Select **Open setting** . The settings of the hit are opened. To edit items in the configuration mode, administration rights may be required.
4. Hover over the column title to define the filter for the selected column.

Company and branches

This control allows you to configure your company's branches and the hardware used at each location (see "Working with branches" on page 207). When the program is installed, one "company" (main branch) is set as the starting point. You can specify the name of the main branch and assign additional branch groups branches to it.

> **The main branch can have sub-branches, but branches cannot have sub-branches or branch groups.**

For the relationship between the "company" and the branches, see "Relationship between the main branch and its sub-branches" on the next page.

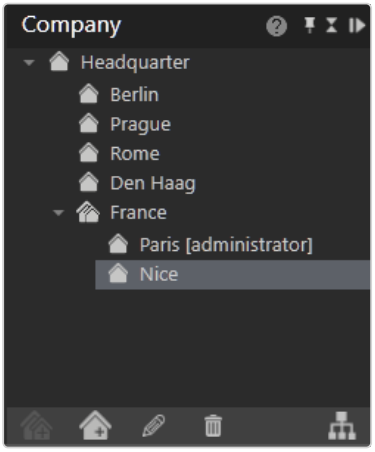


Fig. 95: Company and branches

Branches in Qognify VMS are subordinated to the "company" which can be considered as main branch. Therefore, the administration of the main branch can extend into the administration of a sub-branch, but not vice versa. Equally, one sub-branch cannot manage another sub-branch or the main branch itself. With the exception of cameras and DeviceManager servers, all other objects belong to the sub-branch (e.g. a map of a sub-branch cannot be connected to a camera in the main branch, but the map in the main branch can be connected to a camera in the sub-branch).

> **Administrative rights are NOT inherited from the main branch to the sub-branches, therefore they are also not inherited to branch groups. But administrative rights that are assigned to branch groups are applied to all subordinated branches or branch groups.**

Relationship between the main branch and its sub-branches

Concept

For configuration of the main branch and the sub-branches, the user must have the administrative rights for all relevant branches. For administrative rights of a sub-branch the user has to be assigned to the sub-branch or to the main branch.

Example

- User "A" has administrative rights for the main branch "X" and both sub-branches "Y" and "Z". He can configure all branches.
- User "B" has administrative rights for the sub-branch "Y", but not for the other branches. He can only configure sub-branch "Y".
- User "C" has administrative rights for the main branch "X" and the sub-branch "Z". He cannot configure sub-branch "Y" and branches.

Like the main branch, sub-branches can contain entities that are constricted to the branch itself. Entities of the main branch cannot be configured from the sub-branch. Entities, such as maps, cameras or layers, are configured with the Core Service Main (CSM) of the main branch for all Core Services. The entities thereby "refer" to a server (CSM or CSS). Basically, only references in the sub-branch, or from the main branch to the sub-branch are allowed.

> **There are no references between sub-branches.**

For the relationship between CSM and CSS see "Core Services and branches" on page 22.

> **The only exception for references from the CSS to the CSM are cameras and Device Management servers, where the camera of a sub-branch can be managed through the Device Management server of the main branch, thereby relieving sub-branches of installing their own Device Management server.**

Legal and illegal references

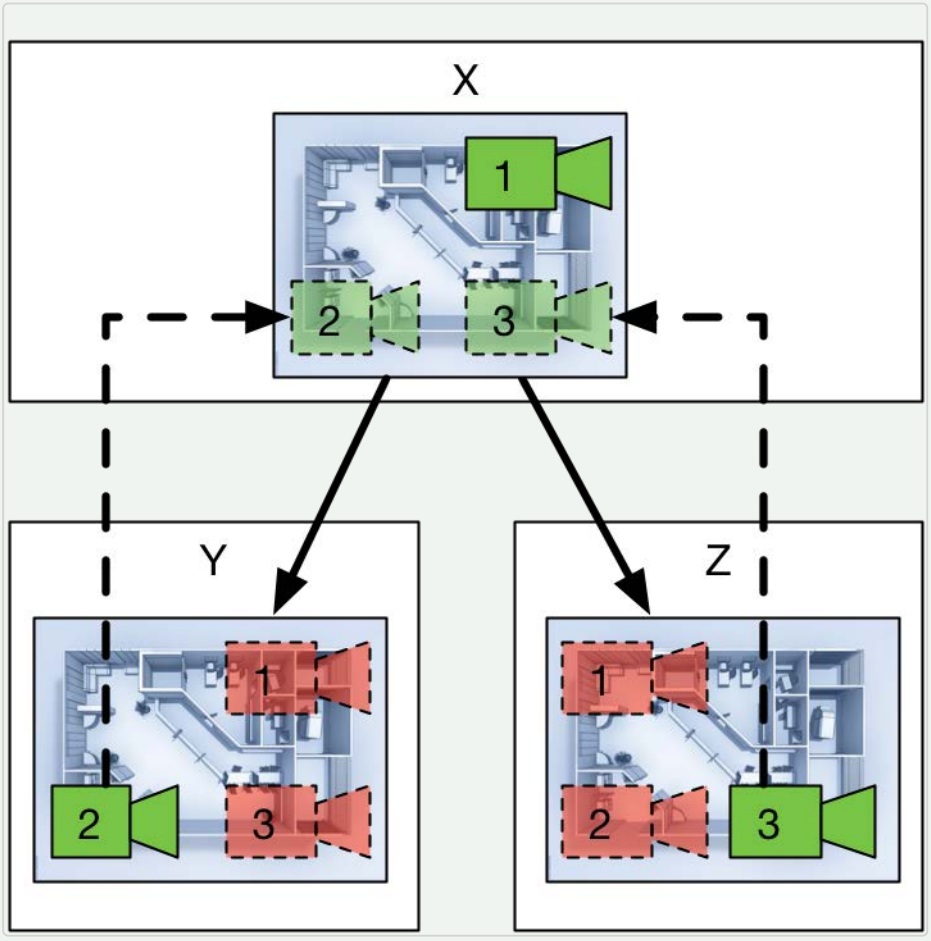
After entities or entity groups (such as maps with cameras) have been moved between-branches, all referenced entities ("objects") must be moved as well. "Legal" references are only possible if all entities of a group are accessible by the sub-branch to which they have been moved. Otherwise, "illegal" references to the main branch are caused.

The only exception are entities in the main branch, which may contain entities from the sub-branches.

Example

In the main branch "X", map "A" is created, consisting of cameras 1, 2, and 3. However, camera 2 is configured for the sub-branch "Y" and camera 3 is configured for the sub-branch "Z". Hence, cameras 2 and 3 are referenced into map "A".

When map "A" is moved to sub-branch "Y", references to camera 2 are "legal", but cameras 1 and 3 become "illegal" for sub-branch "Y", because camera 1 still resides on the main branch "X" and cannot be referenced into sub-branch "Y". Likewise, camera 3 still resides in sub-branch "Z" and cannot be accessed by sub-branch "Y", even if all cameras use the same DeviceManager in main branch "X".



Relationship table

The following table lists the items and their accessibility by the main branch or sub-branch in configuration mode depending on the area in which the item is created.

How to read the table

- An action for a camera is only accessible by the sub-branch if configured in the same sub-branch. Actions configured in the main branch cannot be accessed by the sub-branch.
- The lane configuration of the LPR module is accessible by the sub-branch, even when configured in the main branch. The related camera however must be configured in the sub-branch.

Entity	Navigation in configuration mode	Entities accessible from sub-branch when configured in main branch
All intervals (e.g. alarm scenarios)		-
Add hardware	DeviceManager	x
Wizard	DeviceManager	x
Camera server	General > DeviceManager	x
Camera	General > Action	-
	Recording	-
Archive	General > DeviceManager	x
GND	General > DeviceManager	x
SPS	General > DeviceManager	x
SPC	General > DeviceManager	x
Audio source	General > DeviceManager	x

Entity	Navigation in configuration mode	Entities accessible from sub-branch when configured in main branch
Lane	Lane configuration > LPR module	x
	Lane configuration > Camera	-
	Lane configuration > Assigned camera	-
Analytics	General > Analytics module	x
	General > Camera	-
Analytics API	General > Analytics module	x
	General > Camera	-
Buttons	General > Specified camera	-
	Action	-
	2. action	-
	Start alarm scenario	-
	End alarm scenario	-
	Start patrol	-
Maps		x[1]
Video walls		-

[1]Maps defined in the sub-branch may only contain entities from the sub-branch. Maps defined in the main branch may contain entities from the main branch and the sub-branches.

Entity	Navigation in configuration mode	Entities accessible from sub-branch when configured in main branch
Layers		x[1]
User	General > Groups	-
	User rights	x[2]
	Administrative rights **Administrative rights are not inherited by the branch**.	x[3]
Groups	General > Trigger	-
	User	-
	User rights	x[4]
	Administrative rights **Administrative rights are not inherited by the branch.**	x[5]

[1]Layers defined in the sub-branch may only contain entities from the sub-branch. Layers defined in the main branch may contain entities from the main branch and the sub-branches.

[2]User rights defined in the sub-branch only have access to entities in the sub-branch. User rights defined in the main branch have access to entities from the main branch and the sub-branches.

[3]Administrative rights defined in the sub-branch only have access to entities in the sub-branch. Administrative rights defined in the main branch have access to entities from the main branch and the sub-branches.

[4]User rights defined in the sub-branch only have access to entities in the sub-branch. User rights defined in the main branch have access to entities from the main branch and the sub-branches.

[5]Administrative rights defined in the sub-branch only have access to entities in the sub-branch. Administrative rights defined in the main branch have access to entities from the main branch and the sub-branches.

Entity	Navigation in configuration mode	Entities accessible from sub-branch when configured in main branch
Profiles	General > Layers	x
	General > Patrols	x
	Videowall module mapping > Mapping, defined in branch	-
	Videowall module mapping > Mapping, defined in company	x (modules)
Alarms	Start > Start events	x
	Buttons	-
	End > End events	x
	End > Buttons	-
	Visualization	x
	Profiles	-
	Server > Action start	x
	Server > Action end	x
	Email and FTP	-
Wizard, CopyWizard	Start events	x
	Cameras	x (actions)
	Persons involved > Profiles	-
	Cameras	x (actions)
	Persons involved > Profiles	-
Patrols		x
Sequences		x
Server	Transcoding server	x

Entity	Navigation in configuration mode	Entities accessible from sub-branch when configured in main branch
FailOver servers cannot be transferred from another sub-branch. **For a DeviceManager in the sub-branch, the FailOver DeviceManager from the main branch cannot be used**.	>DeviceManager	
	DeviceManager > General > FailOver	-
	LPR module > General > FailOver	-
	Analytics module > General > FailOver	-
	Analytics API module > General > FailOver	-
	Server motion detection module > General > FailOver	-
System	Event management > System events > Actions	-
	Event management > System events > Email	-
	Event management > System events > Profiles	-
Client	Logo action > Layers	x

Working with branches

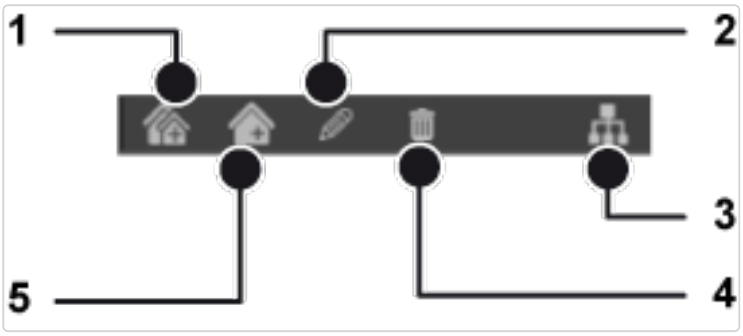


Fig. 96: Working with branches

Creating a branch or branch group

1. To create a new branch or branch group, click **New branch group** (1) or **New branch** (5).
2. Specify the name of the branch or group, and click **OK**. The new branch or group is displayed.

Editing the name of a branch or branch group

1. To edit the name of a branch or branch group that has been created, select the branch or group in the window of the control.
2. Click **Edit** (2).
3. Enter a new name for the branch or group, and click **OK**.

Organizing branches in groups

Branches can be organized into branch groups to facilitate navigation. The branch groups are displayed as folders in the Company control as tree views (archive tree, LPR tree etc.).

1. To move a branch or branch group into another branch group, select a branch (or branch group) and drag it on the target branch group.
2. To remove a branch from a branch group, select the branch and drag it on the company name.

Deleting a branch or branch group

1. To delete a branch or branch group, select it, and click **Delete** (4).

   > **When deleting a branch that contains at least one entity (e.g. camera, button, alarm scenario) a warning displays that this branch is not empty. Additionally, a statistic about the content of the branch is displayed.**

2. Click **Delete**.

Working with the site map

1. Click **Site map** (3) to display the site map for the installation.

Fig. 97: Site map

The site map provides the following functions:

- Arranging objects (entities) in branches and folder by drag & drop.
- Checking consistency of the logical structure of the relations of the objects distributed in branches is valid (see "Relationship between the main branch and its sub-branches" on page 200).

Moving objects between branches

> **Moving objects between branches requires administrator rights for the main branch. Administrators of sub-branches do not have access to the main branch.**

1. To move an object (entity) between the main branch ("company") and a sub-branch, select the main branch.
2. Select the object in the administration control.
3. Drag and drop the selected object into the branch.

Performing a consistency check

> **Moving objects between branches may cause inconsistent references. Therefore it is recommended to perform a consistency check immediately after moving objects to another branch.**

1. Select **Show video servers with multiple video sources as one device** to display an encoder with multiple cameras as one device. Otherwise, all cameras belonging to one encoder will be displayed as separate devices.
2. Select **Show all entities** to display all objects like users, alarms and servers.
3. Click **Consistency check** to display any inconsistencies. For "legal" and "illegal" references, see "Relationship between the main branch and its sub-branches" on page 200.

Editing menu on the administration control

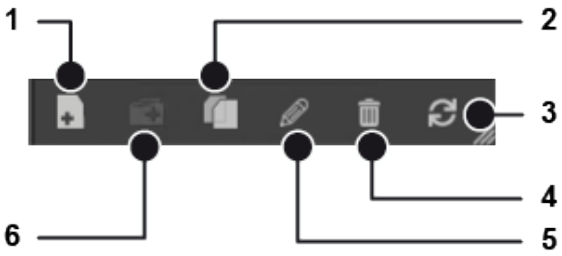


Fig. 98: Editing menu on the administration control

The following editing modes are available on the **Administration** control:

- Create new object (1)
- Duplicate object (2). Only one object can be selected.
- Refresh view (3). Depending on the context, a sorting icon is displayed.
- Delete object (4).
- Edit object (6). Depending on the context, many different configuration pages or a multiple configuration can be open.
- Create new folder (2).

Cameras

The **Camera** function on the control bar allows you to configure and manage the video hardware like IP cameras and video encoders.

Creating a camera manually

> For creating multiple cameras quickly with the device finder, see "Find devices" on page 192.

1. Click **Create new object** in the camera control bar.

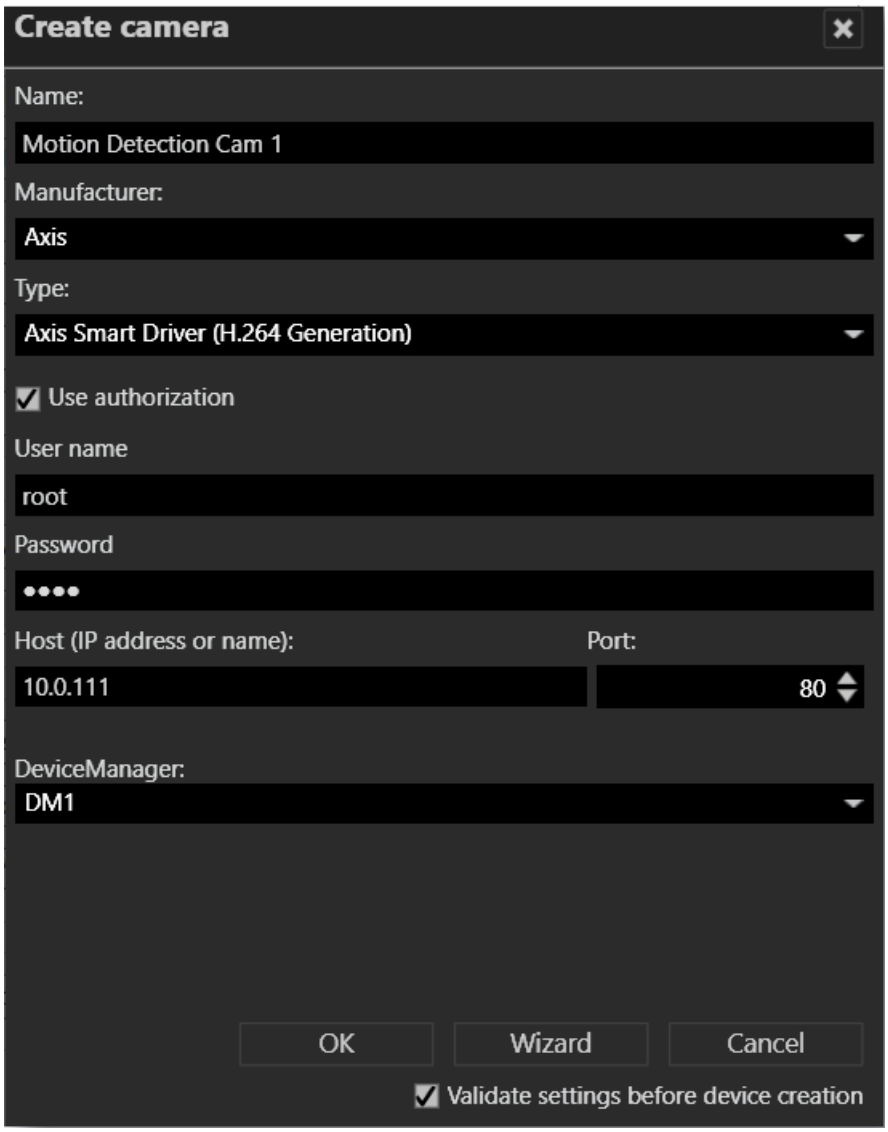


Fig. 99: Creating a camera

2. In the Create camera window, enter the name for the new camera. If you want to configure the new camera using the configuration wizard, click **Wizard** (see "Creating a camera with the wizard" on page 215).

   > **The wizard cannot be used for creating a camera using generic drivers. The generic driver only receives the standard image stream (RTSP stream) from the camera.**

3. Select the **manufacturer** and **type** of the camera.
   - **Generic video driver**: The generic video driver can be used to integrate cameras that are not integrated into the Qognify software. The functions are restricted to displaying and recording the camera image. The video parameters, e.g. the resolution and the frame rate, must be configured on the camera directly. Qognify does not accept liability for correct operation of cameras that are integrated by the generic video driver.
   - **Smart camera driver**: The vendor-specific camera drivers obtain the supported features directly from the camera. Qognify provides camera drivers for several manufacturers. All models available at the time of the current release are supported (for details, see the related PDF document in the download section of the Qognify partner website).

     > **Some models that are different from the manufacturers' standard can cause different behavior of the generic camera driver. Any camera planned to be used with a generic driver should be tested before making any binding agreements. Approved devices are listed in the document "Supported 3rd Party interfaces".**

     > **Generic camera drivers do not support offline configuration. For projects with many cameras of the same type, at least one camera per model must be connected and configured. Afterwards, the cameras may be duplicated and configured as often as required.**

   - **ONVIF Driver/ ONVIF Profile-S Driver**: The ONVIF video driver can be used to integrate cameras that are not integrated into the Qognify software. The functions are restricted to displaying and recording the camera image. The video parameters, e.g. the resolution and the frame rate, and motion detection can be configured depending on the ONVIF version. Qognify does not accept liability for correct operation of cameras that are integrated by the ONVIF video driver.
   - **Qognify Archive**: A Qognify Archive camera allows the import of recordings that appear as a regular camera in the archive mode (see "Archive mode" on page 163).

- **Qognify JPEG Camera Emulator**: Video streams can be composed from JPEG-files that are stored in a specific folder in the file system (e.g. cameras upload their images to an FTP-server). Therefore the video stream is independent from the camera hardware. Very slow frame rates (e.g. 1 frame per minute) are also possible.

4. Select an **authorization**, if required, and enter a **User name** and **Password**.
5. Enter the **Host** name or IP address of the camera.
6. Select the **DeviceManager**, if applicable. If multiple servers have been installed for storing the image data (see "Installation of a distributed server" on page 38), the available servers are displayed.
7. Optionally activate **Validate settings before device creation**. This checks if the camera can be implemented properly.

   > **If the check fails, the camera can be loaded anyways and the settings can be changed afterward.**

8. Click **OK** to confirm your entries. The new camera is displayed in the camera control bar and can be configured (see "Configuring a camera" on page 223).

Creating a camera with the wizard

With the camera configuration wizard you can integrate a camera with a few steps. The settings correspond to the steps in the Cameras control (see "Creating a camera manually" on page 212).

> **The wizard cannot be used for creating a camera using generic drivers. The generic driver only receives the standard image stream from the camera.**

General settings

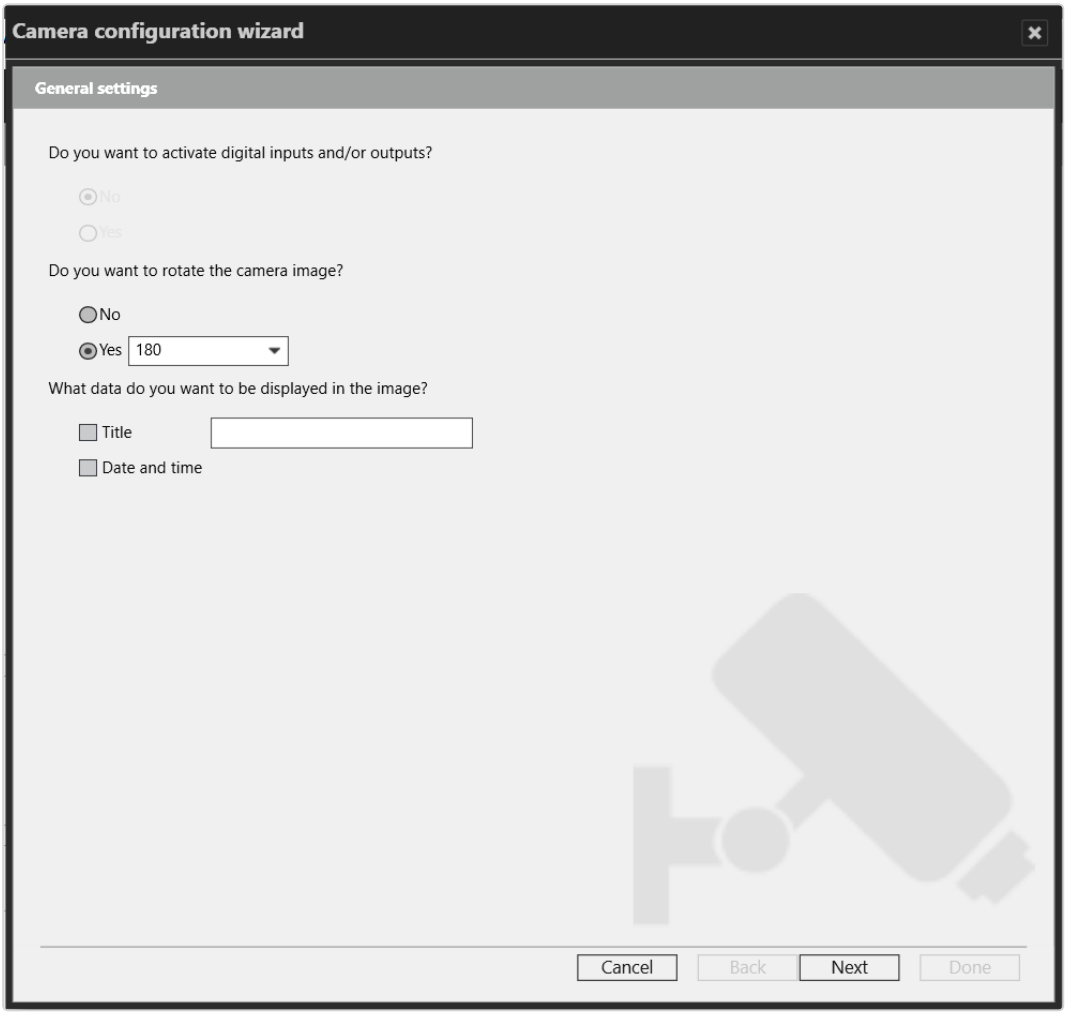


Fig. 100: General settings

1. Select **Yes** to activate digital inputs or outputs (if available on the camera) or **No** to deactivate them.
2. If the camera needs to be rotated, select the rotation angle.
3. Select and enter the type of data displayed in the camera image.
4. Select **Next** to define the standard recording settings.

Standard recording

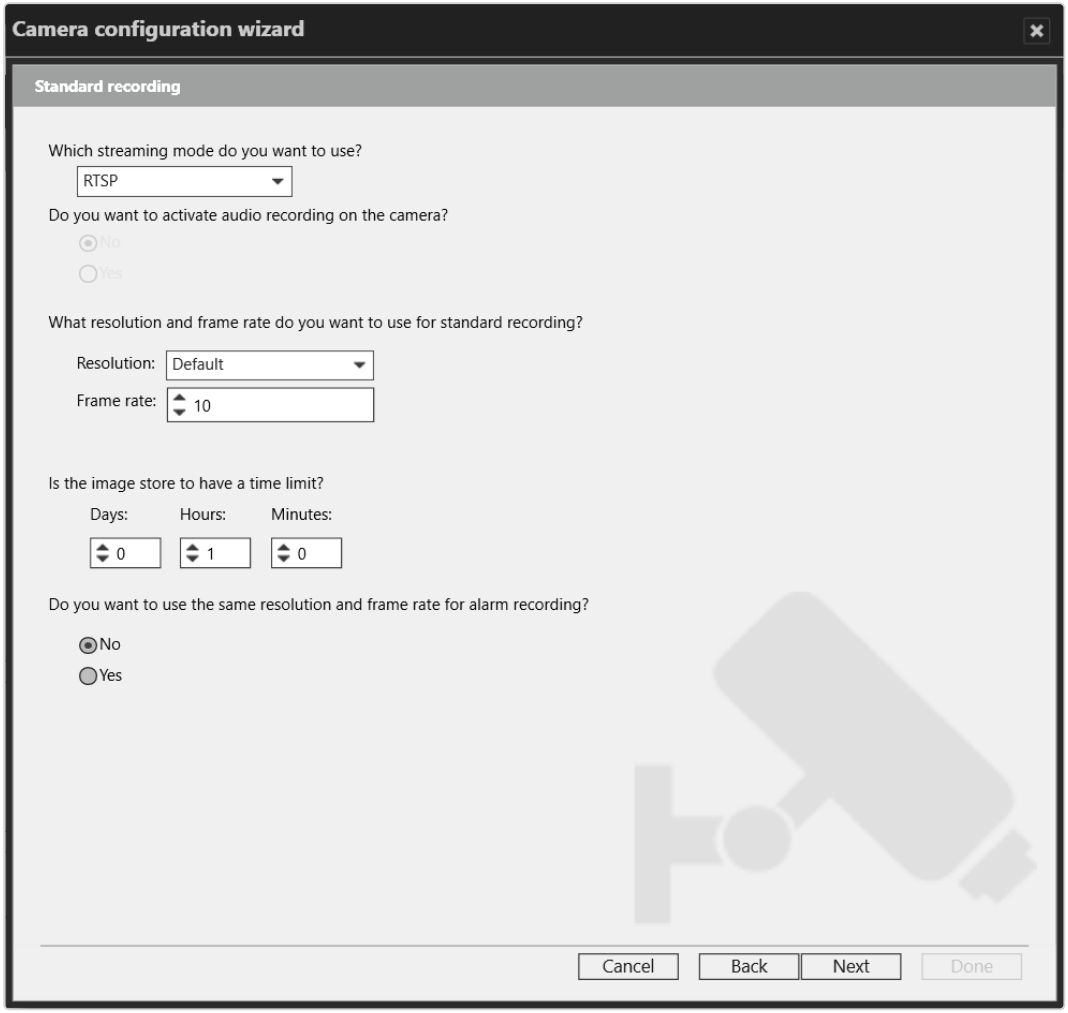


Fig. 101: Standard recording

1. Select the streaming mode (e.g. M-JPEG, H.264, H.265, RTSP).
2. Activate audio recording (only available on MPEG-4, H.264 or H.265 streams).
3. Select **Resolution** and **Frame rate** for the standard recording.
4. Define the time limit for the image storage.
5. Select **Next** to define the alarm recording settings.

Alarm recording

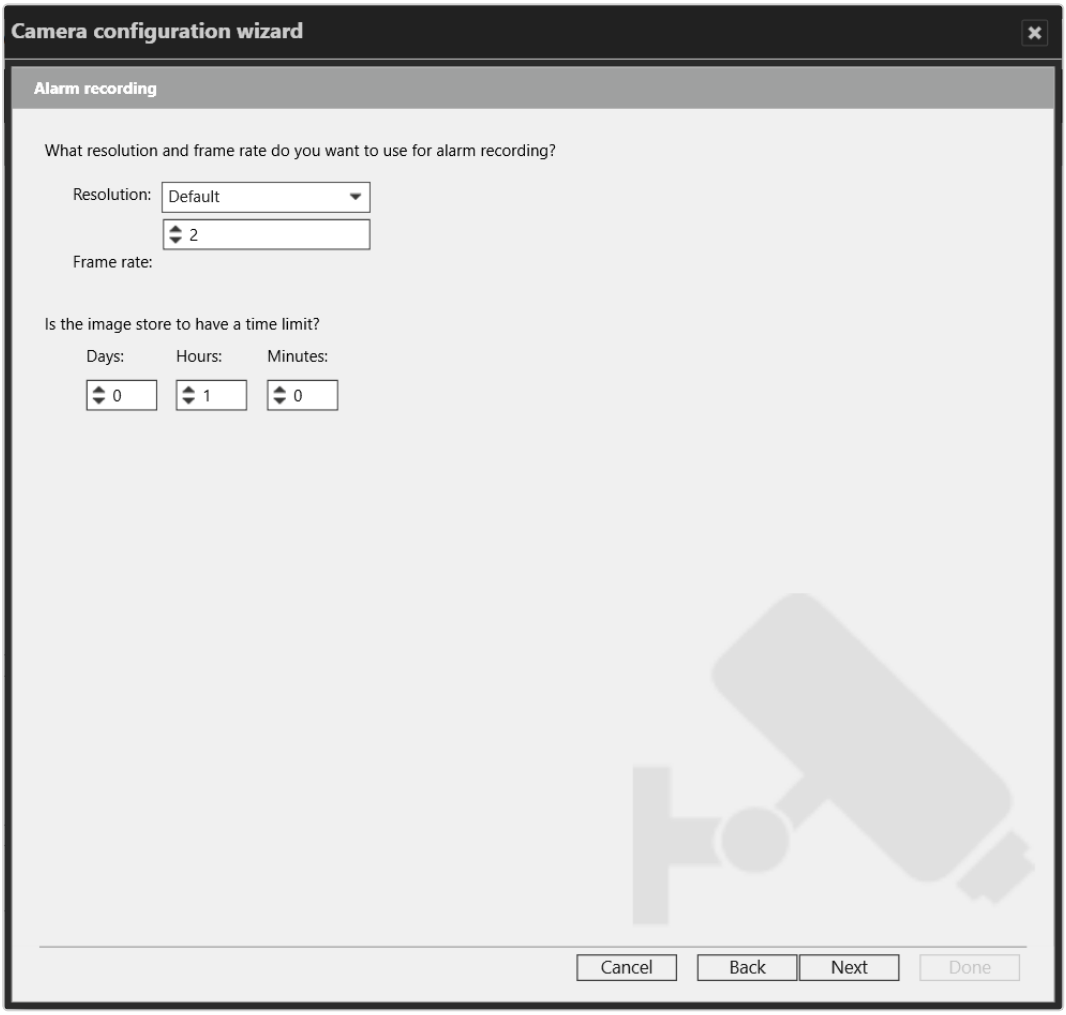


Fig. 102: Alarm recording

1. Select **Resolution** and **Frame rate** for the alarm recording.
2. Define the time limit for the image storage.
3. Select **Next** to see a summary of your settings.

Summary

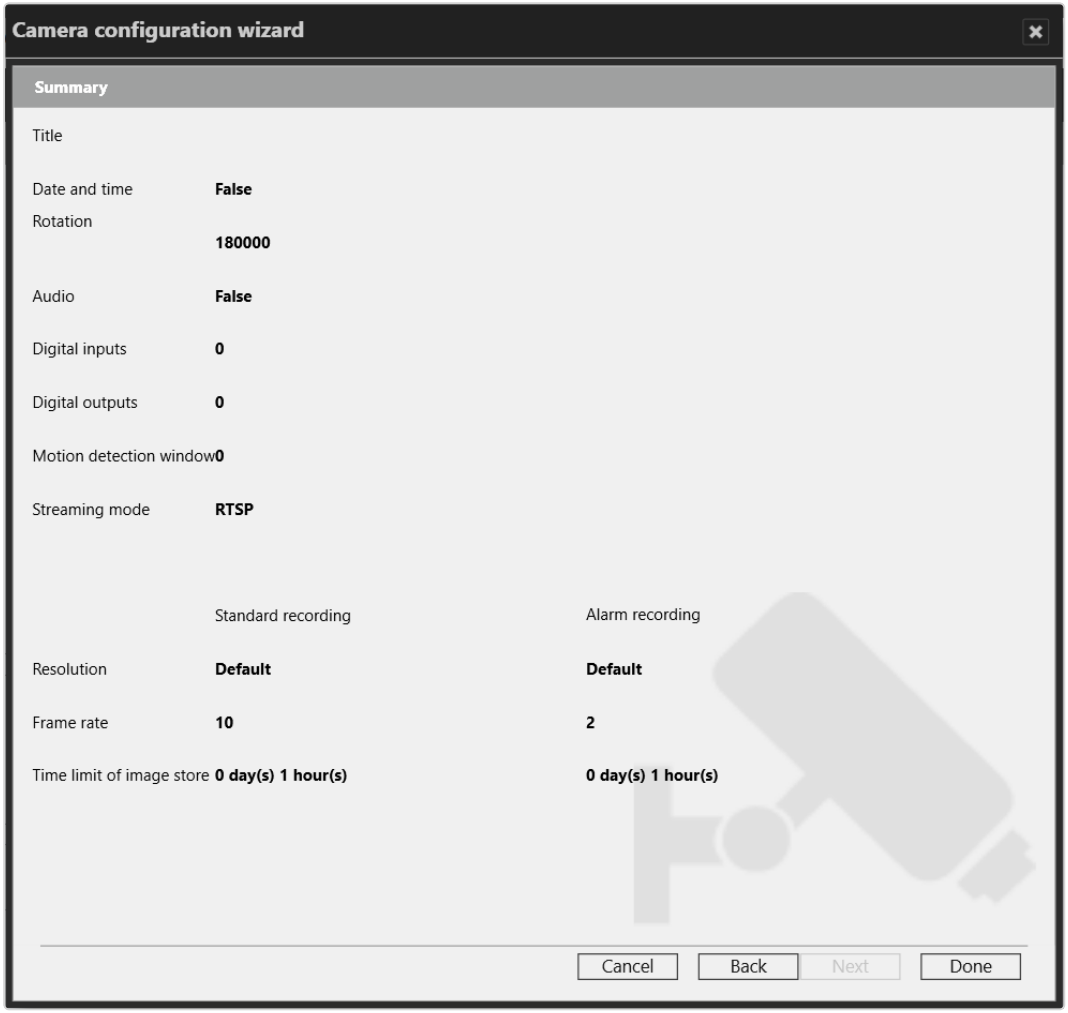


Fig. 103: Summary

1. Check the settings.
2. To make changes, select **Back** and change the settings.
3. To apply the settings, select **Done**.

The AXIS body-worn camera controller

The AXIS Body Worn System Controller (BWSC) offloads and temporarily stores video from each AXIS body-worn camera, and sends it to Qognify VMS. For this, a connection file must be created during set-up that must be uploaded to the BWSC.

The BWSC must be licensed to use. If not licensed, the web server port is not opened and no connection between the body-worn controller and Qognify VMS is established.

After the video import process is finished, the temporary files are deleted from the local hard drive.

Each body worn camera user is mapped to a separate video channel and requires a license even if a body worn camera is shared with other users (one license per channel).

System requirements & prerequisites

- Make sure to reserve enough free disk space per body worn camera for temporary video files storage on the local drive. The amount of space needed depends on the number of cameras used.
- Use a network adapter with at least 1 Gbit/s transfer rate.
- Use a NTP time server to synchronize the time between Qognify VMS and the body-worn system. Otherwise recordings from the body-worn system might be imported with a wrong timestamp.
- Body-worn system administration (cameras, camera settings, users, etc.) must be done by the Body Worn Manager.

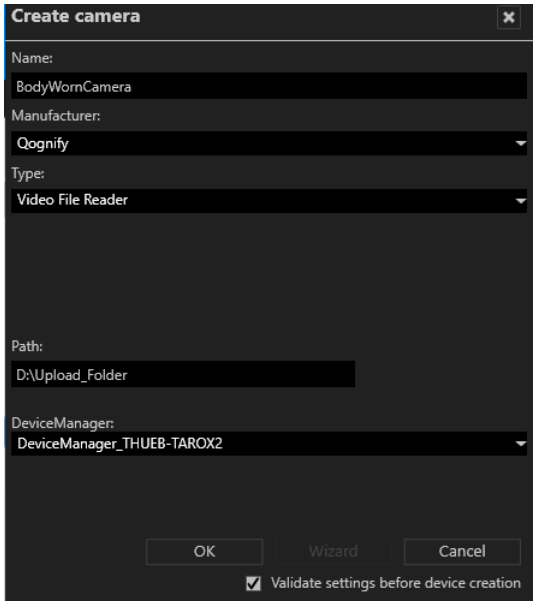
> **You can add the Body Worn Manager browser interface as a website to Qognify VMS for administrators.**

Known limitations

The communication between VMS and AXIS Body Worn Camera System Controller can only be used over HTTPS. By default, all TLS versions can be used for the HTTPS connection between VA and Axis controller. We recommend switching off SSL 3.0/TLS 1.0 and TLS 1.1 Windows-wide as described in our hardening guide.

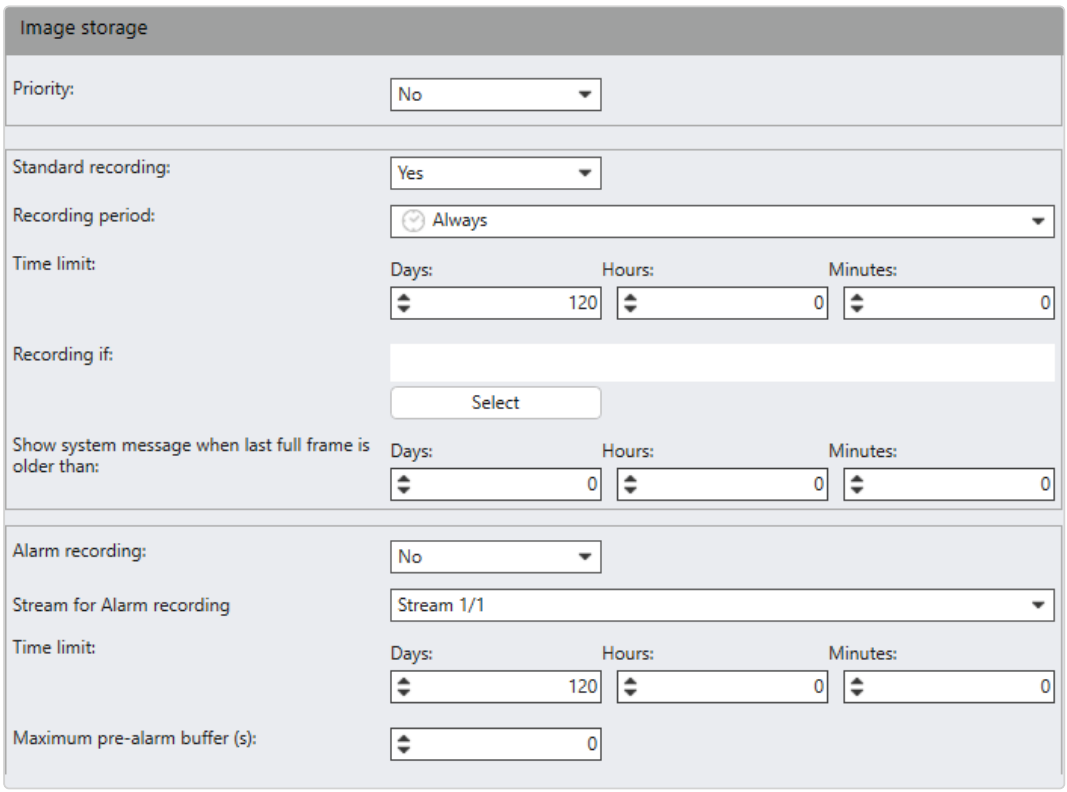
Configuring the body-worn camera connector

Prerequisite: A “Body Worn Camera Connector” has been created in the VA Administration tool (see "Adding a body-worn camera connector module" on page 492).



1. Create a new camera and enter “Qognify” as **Manufacturer**, and “Video File Reader” as **Type**.
2. Specify a directory on the local drive that will be monitored by the driver. This is the directory used by Qognify VMS to import the video files.
3. Select **OK**. A new virtual camera is created. Use the same directory as specified for the AXIS Body Worn Camera VA Module where the recordings from the body-worn system are temporarily stored.

4. Record a video with an AXIS Body Worn Camera and put it into the docking station, so the video files can be imported into Qognify VMS.
   - For each user a video channel is automatically created once his first recording is imported.
   - Each body worn user gets a separate channel that is also available in Archive Mode.



5. Specify the video retention period for the **image storage**. The initial period is 120 days.

   Configure a retention period long enough to handle situations when people forgot to dock a camera for a long time, or a camera was lost and found again. If the retention period is too short to cover the time when a recording was created, this recording will be deleted right after import.

Configuring a camera

Network cameras consist of a video server unit (encoder) and at least one camera unit. Accordingly, the settings of a network camera are always subdivided into video server settings and camera settings. The video server settings include all of the connection-specific parameters, while the camera settings include all of the image quality and image storage settings.

1. Select the camera in the overview. The settings of the camera are displayed in the main window.

Encoder / camera: general

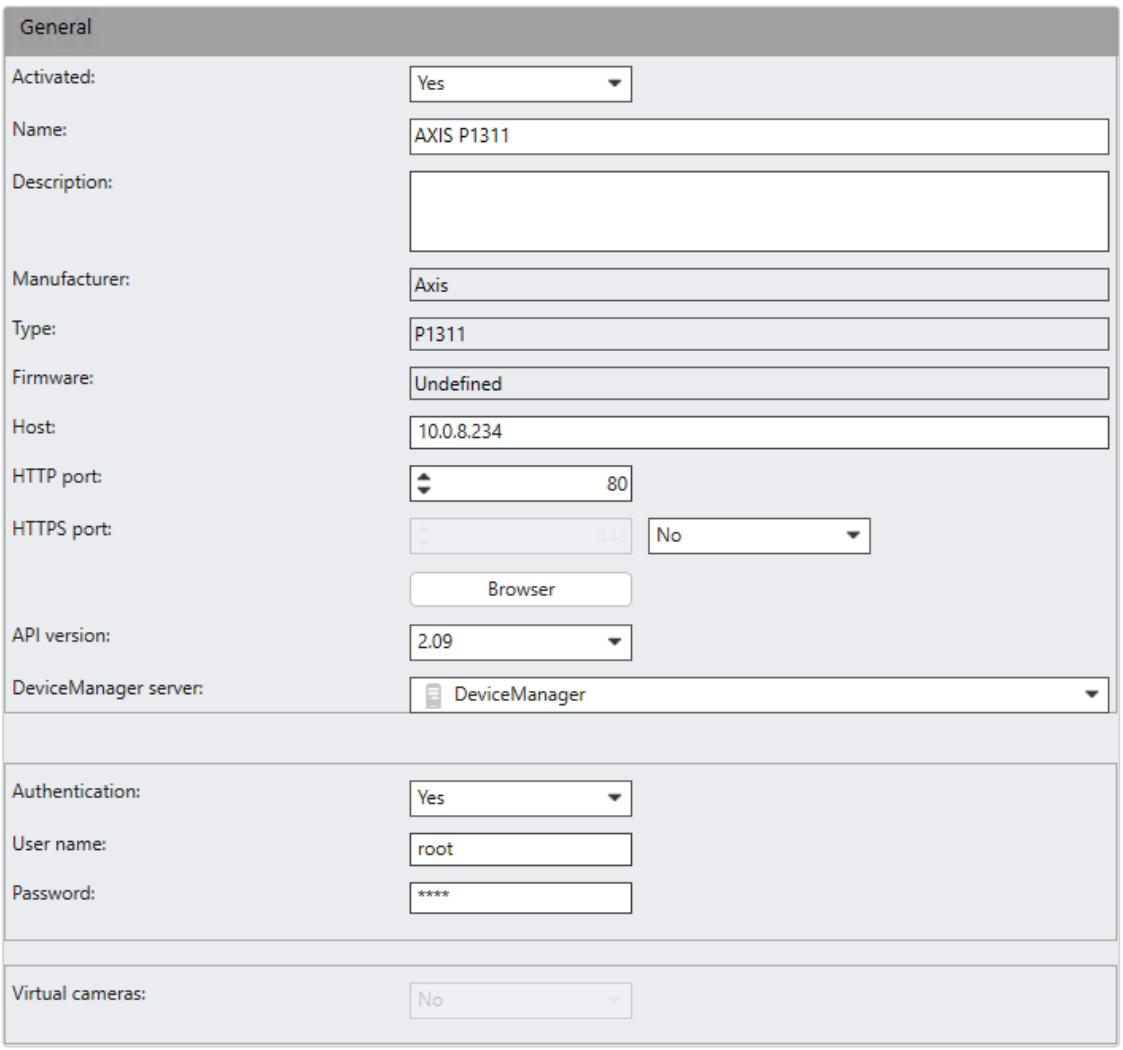


Fig. 104: Encoder / camera: general

1. **Activate** the camera or encoder.

   In case of a multichannel encoder the connected cameras are not accessible anymore.

2. Click **Query Device** e.g, settings have changed directly on the camera.

   The feature is only available if the camera is integrated with the ONVIF driver or Smart driver.

3. Enter a unique **Name** of the network camera.
4. Enter a descriptive text of up to 1000 characters. The description will be included in the export and can also be set for multiple cameras. The description is also available in the configuration export tool and is displayed in the configuration mode search (see "Searching in configuration mode" on page 198).
5. Select the protocol type (**http** or **https**), and change the **Port** number, if necessary.
6. To test the incoming camera signal, click **Browser**. The browser defined in the system settings ("standard browser") starts up, and the camera's web interface is displayed in the browser window.
7. The application programming interface (**API version**) is identified automatically.
8. Define a **Stream network timeout (s)** between 5 and 20 seconds. Set a value for the stream network timeout between 5 and 20 seconds. If the network connection to the camera is temporarily lost, an error message is suppressed for the duration of the set value and the last received image remains in the camera view.

   The feature is only available if the camera is integrated with the ONVIF driver or Smart driver.

9. If necessary, change the **DeviceManager server**.

   Changing the DeviceManager will delete all existing recordings.

10. Specify if **Authentication** is required for the camera and, if necessary, enter a **User name** and **Password**.
11. Select **Virtual cameras** to display and save multiple image details from a camera as a separate camera.

    This function is only available for specific camera models.

After activation of the virtual camera function, multiple virtual cameras are automatically created. The number of virtual cameras depends on the camera model. They are configured similarly to a standard camera. The image details can be specified in the virtual camera configuration (see "Virtual camera (image detail)" on page 230).

Maintenance

> **This feature applies to Axis SD and Bosch SD cameras.**

Pushing the password

The maintenance feature supports modifying the camera password in a bulk operation instead of setting the password for each camera individually.

Fig. 105: Maintenance

1. Set the camera password and confirm by repeating.
2. Select **Push password**. The camera is restarted with the new password.

Digital inputs

Some cameras provide digital inputs that can trigger camera specific features, such as restarting the camera or switching on the camera light.

Fig. 106: Digital inputs

1. Select the digital inputs and specify unique names for **Name for CLOSED** and **Name for OPEN**.
2. Specify the interval for the **dead time** (in seconds) after which a signal is analyzed again. That prevents the event database from becoming unnecessarily large when events in rapid succession occur. This setting may also be used to trigger an alarm (see "Alarms" on page 356).
3. **Apply** the set values if you want to make further settings.
4. **Save** the set values to apply the values and conclude input.

Digital outputs

Some cameras provide digital outputs. A state change can be used e. g. as a start event in a alarm scenario.

Fig. 107: Digital outputs

1. Select the digital outputs and specify unique names for **Name for CLOSED** and **Name for OPEN**.
2. Specify the **hold time** for the time (in seconds) within which an output is opened or closed (0 = infinite).

Camera general

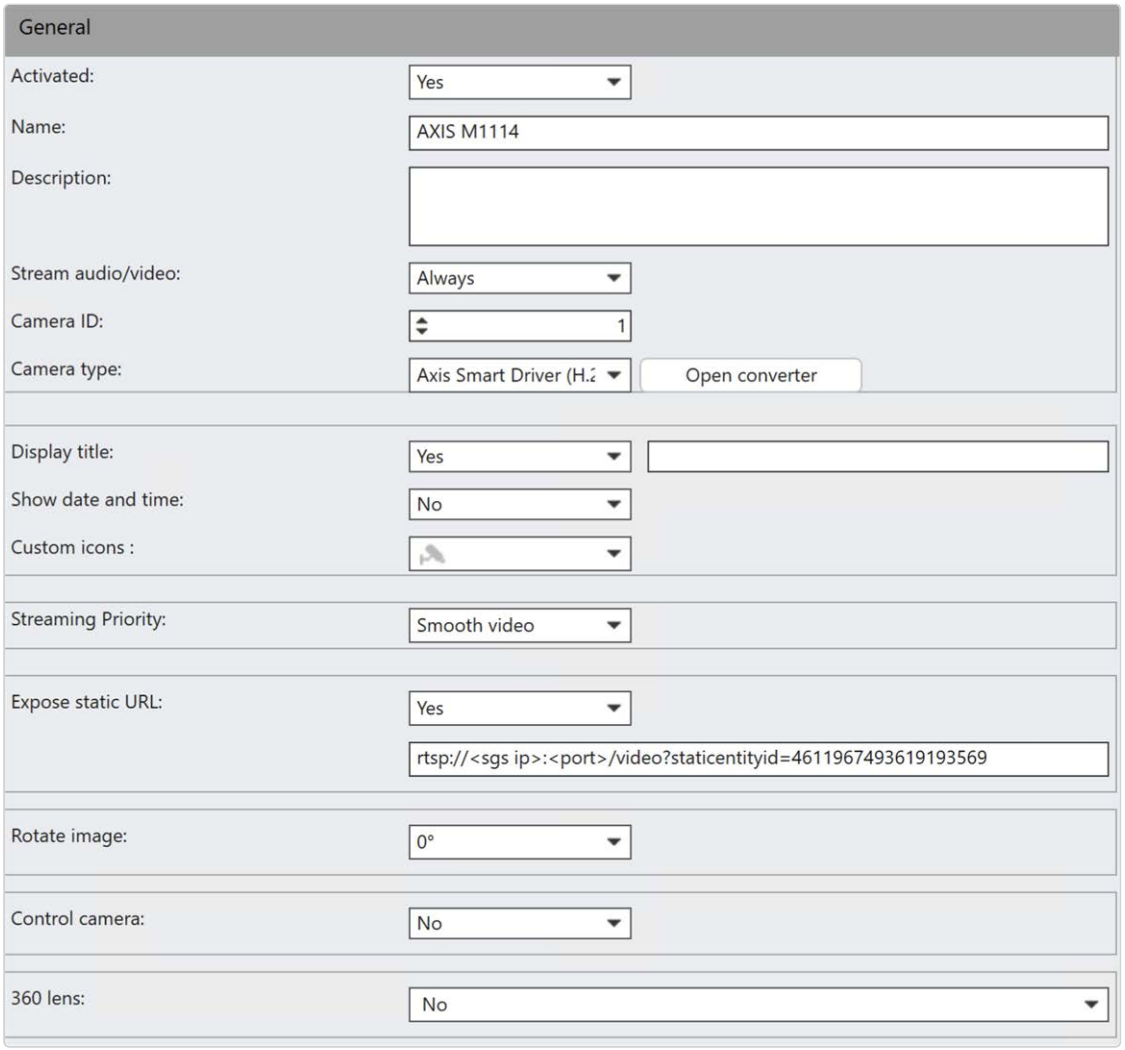


Fig. 108: Camera general settings - 1

1. Activate or deactivate the camera.
2. If necessary, alter the **Name** of the camera.
3. Optionally, select **Stream Audio / Video** to enable video streams continuously or on demand (trigger-based). This feature can reduce the network traffic e.g. in LTE environments.
   - **Always** (default): Video streaming from the camera to the Device Manager is available and can be recorded or delivered to the client immediately on request.
   - **On demand**: There is no video stream from the camera at all. Video streaming can be started e.g. by an alarm event (see **Actions at start of alarm** in "Server" on page 369) or a button action (see "Action" on page 387). It can take while to establish the video stream.
   - **On demand – quick start**: Video streams from the camera are discard by the Device Manager. Video streaming can be started e.g. by an alarm event (see **Actions at start of alarm** in "Server" on page 369) or a button action (see "Action" on page 387). When needed the related video stream is available immediately.
4. If necessary, change the **Camera ID** and adapt the ID of the associated camera to the hardware. The camera ID is only required for some camera controllers.
5. Select the **Camera type**:
   - **Camera**: The camera is used with or without the PTZ control functions, depending on the camera type.
   - **External PTZ**: If the camera does not have its own PTZ control unit, you can divert the control signals of an encoder to another camera with a connected PTZ control unit. A separate RS-485 port of the encoder is required for each diversion.
6. To change the camera type, click **Open converter** (see "Converting a camera" on page 271).
7. Specify whether a title is to be displayed in the camera image, and enter the **Title**.
8. Select whether the **Date and time** are to be displayed in the camera image.
9. Select a **Custom icon** for the camera (see "Managing sound and icon files with custom media" on page 447)

10. Change the **Streaming Priority** if required from Smooth Video to low latency:
    - **Smooth Video** (default): The video images from the camera are dynamically buffered in the random-access memory (RAM) on the Qognify client before they are displayed. This normalizes fluctuations in the live video display based on problematic situations like network jitter, limited bandwidth, non equidistant frames, jumping frame rates, etc.
    - **Low Latency**: The video images from the camera are displayed in real-time without buffering. Therefore insufficient bandwidth can result in jerky video .
11. Set **Expose static URL** to “Yes” to enable a static IP address for the camera for the video stream URL.
    - The placeholders for the IP address and the port number must be replaced by the address and the port of the SGS gateway the camera is connected to (see "Configuring the Gateway-Service (SGS) module" on page 419).
    - When using the RTSP protocol, make sure that “RTP_Over_RTSP_Over_TCP” is selected as the transmission mode (see "Editing a video stream" on page 243).
12. If the camera was not mounted upright, use the **Rotate image** function to rotate the image in 90° steps (90°, 180°, 270°). If the camera cannot rotate by itself, the client will do the rotation. Camera side rotation always has the priority, however.

Settings for PTZ cameras

1. Select **Control camera** (available for PTZ cameras only) if you are configuring a PTZ camera or a control unit in order to give the user the option of controlling the camera in surveillance mode.
2. Specify the **PTZ sensitivity** (available for PTZ cameras only) of the camera control.
3. Select the **Camera position** (available for PTZ cameras only) to give the user the option of defining and using the preset camera positions in surveillance mode.
4. Select **Invert PTZ control** (available for PTZ cameras only) to correctly control cameras, e. g. cameras that are mounted upside down.

13. If the camera has a **360°-angle lens** (wide-angle or fish eye lens), select the manufacturer of the lens and its parameters.
    - If available at the camera, select the **Dewarping mode** and set the **Position of the camera**. The dewarping mode determines the extent to which the distortion of the image produced by the fish eye lens is rectified.
    - After selecting an appropriate camera, set the dewarping mode to **Panorama** or **Virtual PTZ**, and the camera position to **ceiling**, **table**, or **wall**.

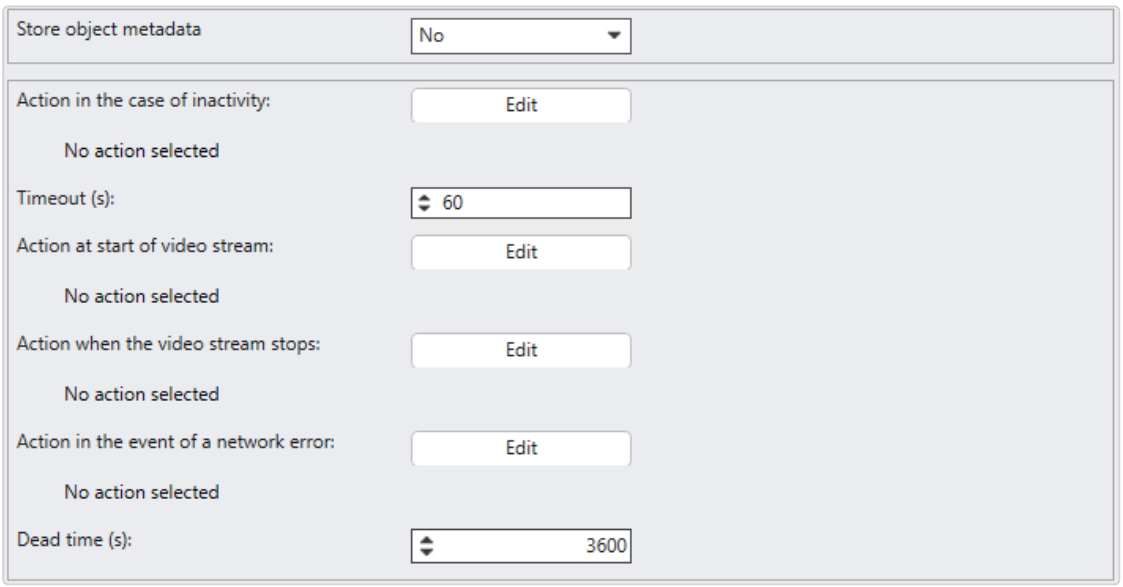


Fig. 109: Camera general settings - 2

14. Specify the setting for **Store object metadata**.
    - If set to "Yes", the Device Manager will forward the metadata to the QogniFinder.
    - If set to "No", the Device Manager will not forward any metadata, and the camera will not be shown in QogniFinder.
15. Make a selection for **Action in the case of inactivity** to specify which action is to be performed if a PTZ camera is not controlled. The selected action is displayed.
16. Specify for **Timeout (s)** in seconds the time after which the action is to be performed if the PTZ-camera is inactive.

17. Make entries for **Action at start of video stream** and **Action when the video stream stops**. The selected actions are displayed.
    - The **Action at the start of the video stream** is triggered if a user has the camera in surveillance mode in the foreground, i.e. is viewing the current live image of that camera.
    - The **Action when the video stream** stops is triggered if the current camera is closed or a different layer is moved to the foreground.
18. Select the **Action in the case of network error** to specify an action if the camera is inactive due to network error. The selected action is displayed.
19. Define a **Dead time (s)** in seconds for the selected action in which a network error will not trigger the action again. The default value is 3600s.

Geo coordinates

Camera can be located on a map with GPS coordinates. The coordinates are provided as web mercator mappings. Longitude is the east-west position, latitude is the north-south position. The coordinates are synchronized with the feature "Advanced Maps" (refer to "Maps and "Advanced Maps"" on page 377).

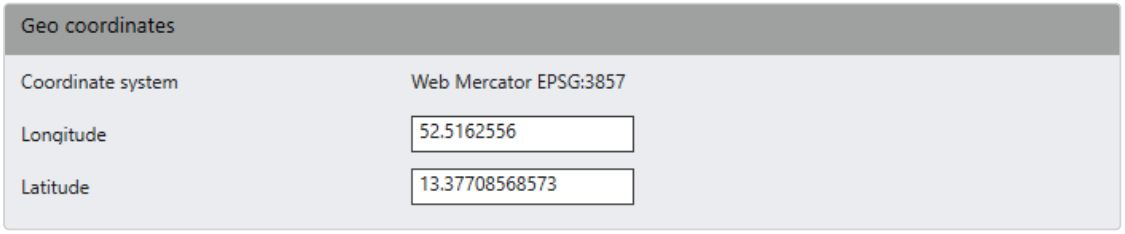


Fig. 110: Geo coordinates

1. Enter the geo coordinates of the camera for the longitude.
2. Enter the geo coordinates for the camera for the latitude.

Virtual camera (image detail)

If the feature "virtual camera" is activated (see "Encoder / camera: general" on page 223), all virtual cameras except the first are deactivated by default.

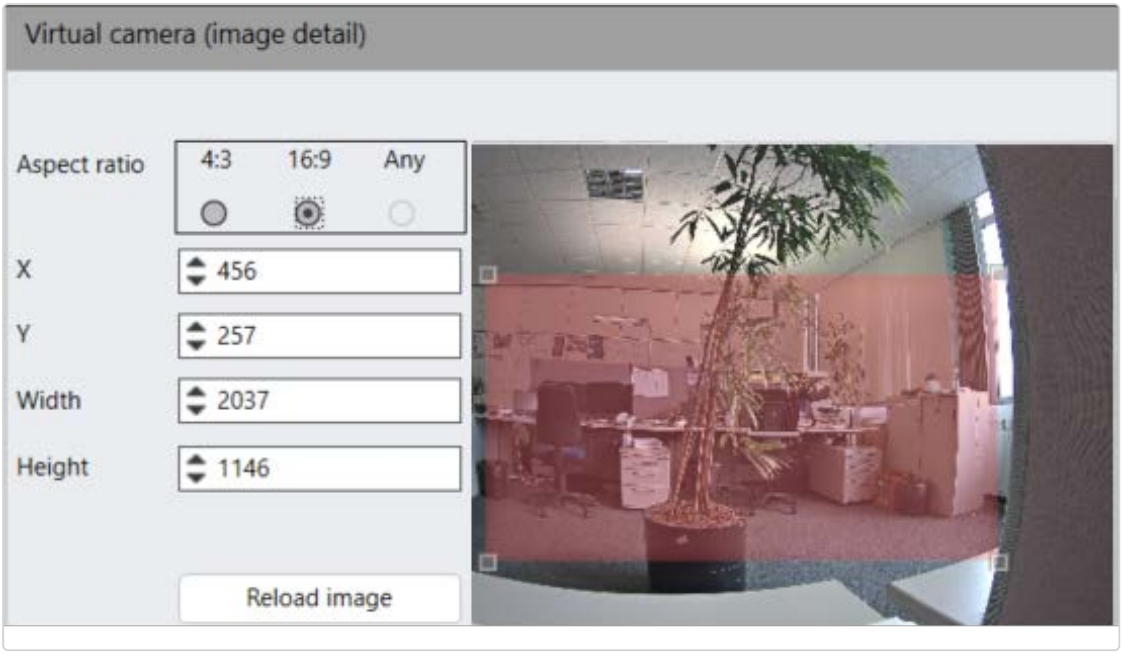


Fig. 111: Virtual camera (image detail)

1. Select the **Aspect ratio** of the virtual camera (4:3, 16:9, or Any).

   > **"Any" is only available if supported by the camera.**

   > **We recommend to select the same aspect ratio in the video stream settings (see "Video streams" on page 242), because otherwise the image could become cropped.**

2. Enter the x and y coordinates of the top right corner of the red rectangle which defines the image section).
3. Enter the width or height of the image section to be displayed.
   - If width is selected, the height will be scaled automatically depending on the selected aspect ratio
   - If height is selected, the width will be scaled automatically depending on the selected aspect ratio.
   - Optionally, the field of view can also be scaled by dragging the corner points.
4. To change the position of the selected area in the image, click into the selected area and move the selection with the mouse button pressed.
5. Click **Reload image** to create a new snapshot of the scene.

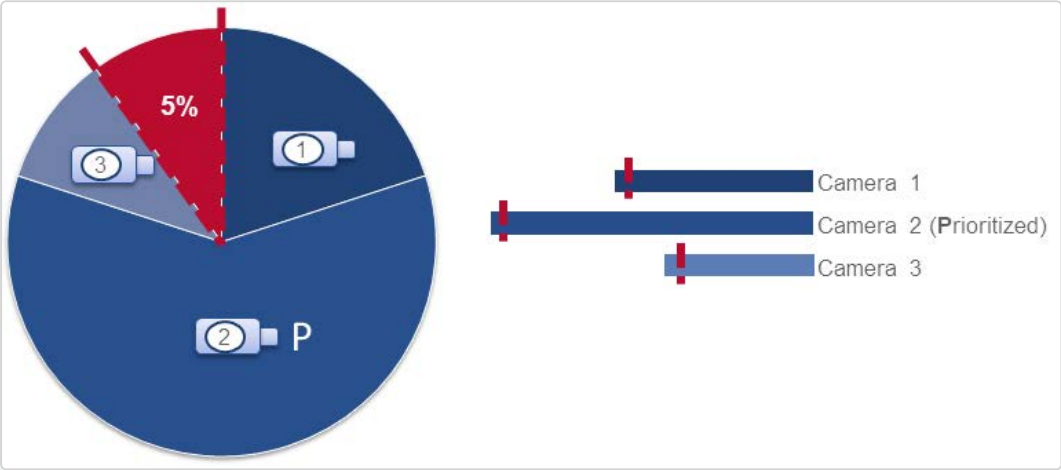
Image storage

This section describes the configuration of conditions for standard and alarm recordings, as well as the "Edge Storage" and "Record On Motion" behaviors.

Multimedia database

Video recordings are stored according to the so called "ring buffer" queue in the multimedia database. For a brief overview, see the following illustration.

Overview



*When the storage capacity reaches **85%**, a **Zone almost full**-message is send via SNMP, email or as message to the client. As soon as the storage capacity reaches **95%**, the ring buffer system starts deleting the oldest video data to create free disk space for new recordings. The image data of the prioritized cameras (**P**) are the last to be deleted.*

All of the image storage settings (e.g. the size of a camera's storage area on the hard disk) are configured here. To prevent sensitive image data from being over-written, standard and alarm recordings are configured separately.

When storage capacity reaches 95%, the oldest recordings will be deleted in the following order:

1. Standard recordings
2. Alarm recordings
3. Prioritized standard recordings
4. Prioritized alarm recordings

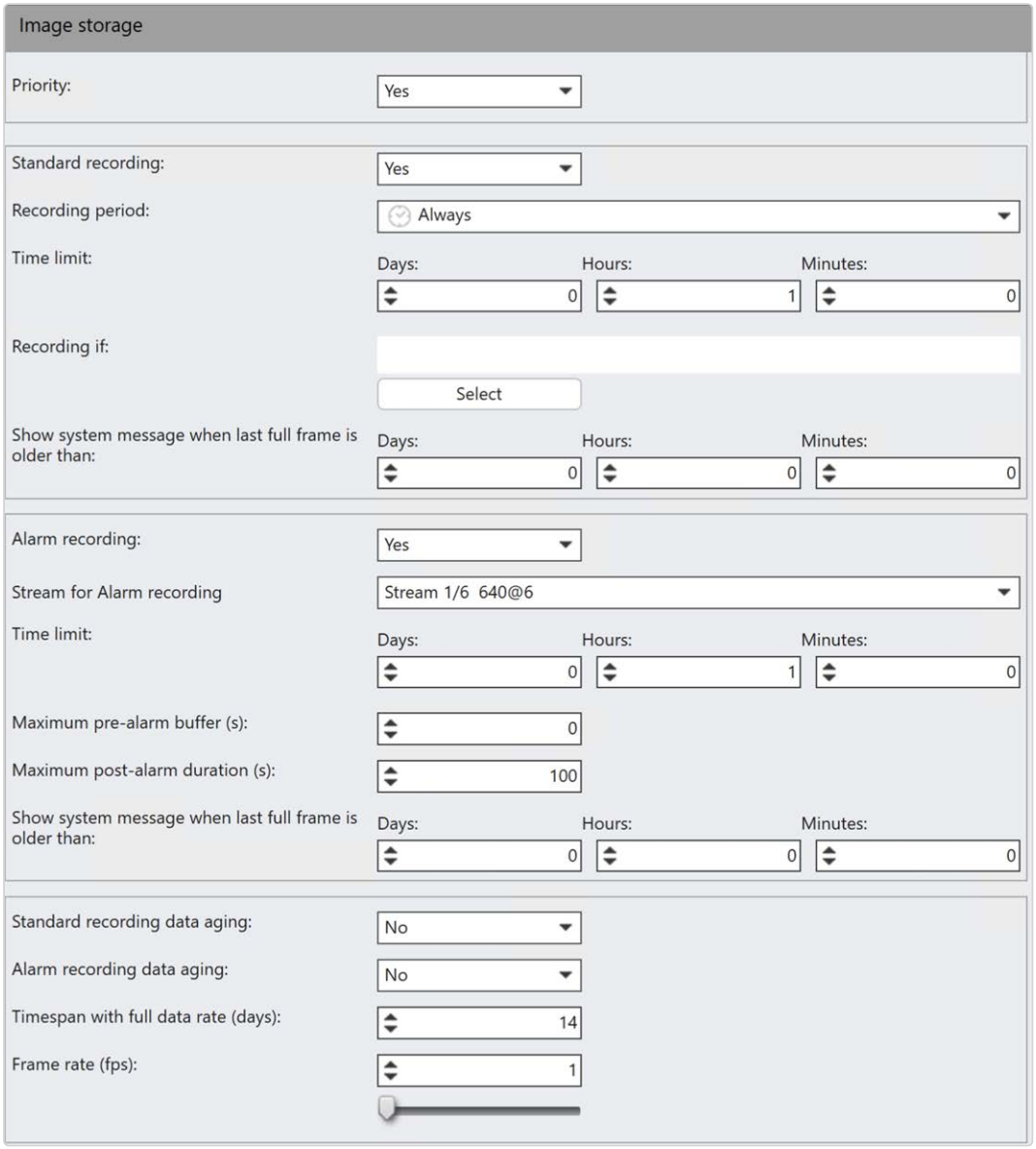


Fig. 112: Multimedia database settings

1. Select **Multimedia database** from the Image storage menu.
2. Select whether the image recording has a **Priority**: If the storage capacity reaches 95%, the ring buffer system starts deleting the oldest image data. The recorded image data of the prioritized cameras are the last to be deleted (see order of deletion above).
3. Select whether **Standard recordings** are to be carried out with this camera.
4. Select the **Recording period**. You specify the exact period using a time template that you create in the time management (see "Time management" on page 351). By default, continuous recording is started ("Always").

5. Select the **Time limit** and enter the maximum storage duration. If the time limit is exceeded, recordings older than the specified time limit will be deleted.
6. In section **Recording if** you can select a condition on available digital inputs for starting image recording.

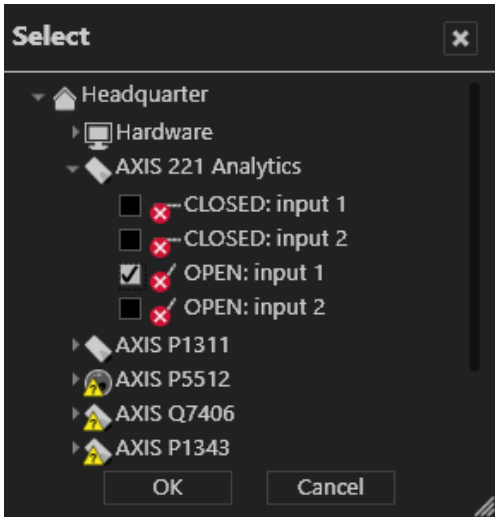


Fig. 113: Multimedia database - select condition

7. Specify the time interval after which a message is displayed when the last full frame of the standard recording is reached. This helps to monitor the storage space required for standard recordings.
8. Select whether **Alarm recordings** are to be carried out with this camera.
9. Select a **stream for alarm recording**. To use this feature the multi-stream function must be supported by the camera and has to be configured (see "Video streams" on page 242)
10. Select the **Time limit** and enter the maximum storage duration. If the time limit is exceeded, the recordings older than the specified time limit will be deleted.

11. Specify a **Maximum pre-alarm buffer** (up to 3600 seconds) to record a period if a standard recording is deactivated or an additional stream for alarm recording is defined. The pre-alarm buffer defines the maximum length of pre-alarm duration that can be configured in an alarm scenario (see "Server" on page 369 settings in for the alarm-configuration). The data recorded in the buffer memory is transferred to the alarm recording track when manual recording is started (see "Manual alarm recording" on page 144).

    > **The pre-alarm buffer is taken into account only if there is no standard recording available.**

12. Specify a **Maximum post-alarm duration** for manual alarm recording to record a period after the alarm is triggered for manual alarm recordings in surveillance mode (see "Manual alarm recording" on page 144). If manual alarm recording is not stopped, the recording will stop automatically at the end of the specified post-alarm duration.
13. Specify the time interval after which a message is displayed when the last full frame of the alarm recording is reached. This helps to monitor the storage space required for alarm recordings.
14. Activate automatic reduction of the frame rate of standard recordings or alarm recordings after a specified period (**Standard recording data aging** or **Alarm recording data aging**). On expiration of the specified period, the frame rate of the stored recordings is reduced to save memory (data aging).

    > **The data aging process only compresses the image data of the day before the configured day.**

    Example You record an H.264 stream with 20 images a second with an I-frame interval of one second. Data aging reduces the frame rate to one image a second, because all P-frames are deleted. Tracking data and audio recordings are always deleted.
15. Specify the **Time limit** after which the recordings are to be compressed and released from the audio track.

16. Specify the **Frame rate** (in fps) at which the recordings are to be stored after the time limit is exceeded. This reduces the image data to the set frame rate.
    - Motion JPEG recordings will be reduced to the defined frame rate.
    - MPEG-4 / H.264 / H.265 recordings will be reduced to i-frames (the p-frames will be deleted).
17. Set a time frame after which a system notification message is triggered if the last full frame recorded is older than the specified time. To receive the message "The last archive image is older than the configured value", the Event Manager must be configured correspondingly (see "Configuring the Event Manager" on page 433).

Gap filling

Gap filling fills recording gaps on the zone with the recordings from the edge storage device.

> **For other settings than gap filling, see "Edge storage" on page 240.**

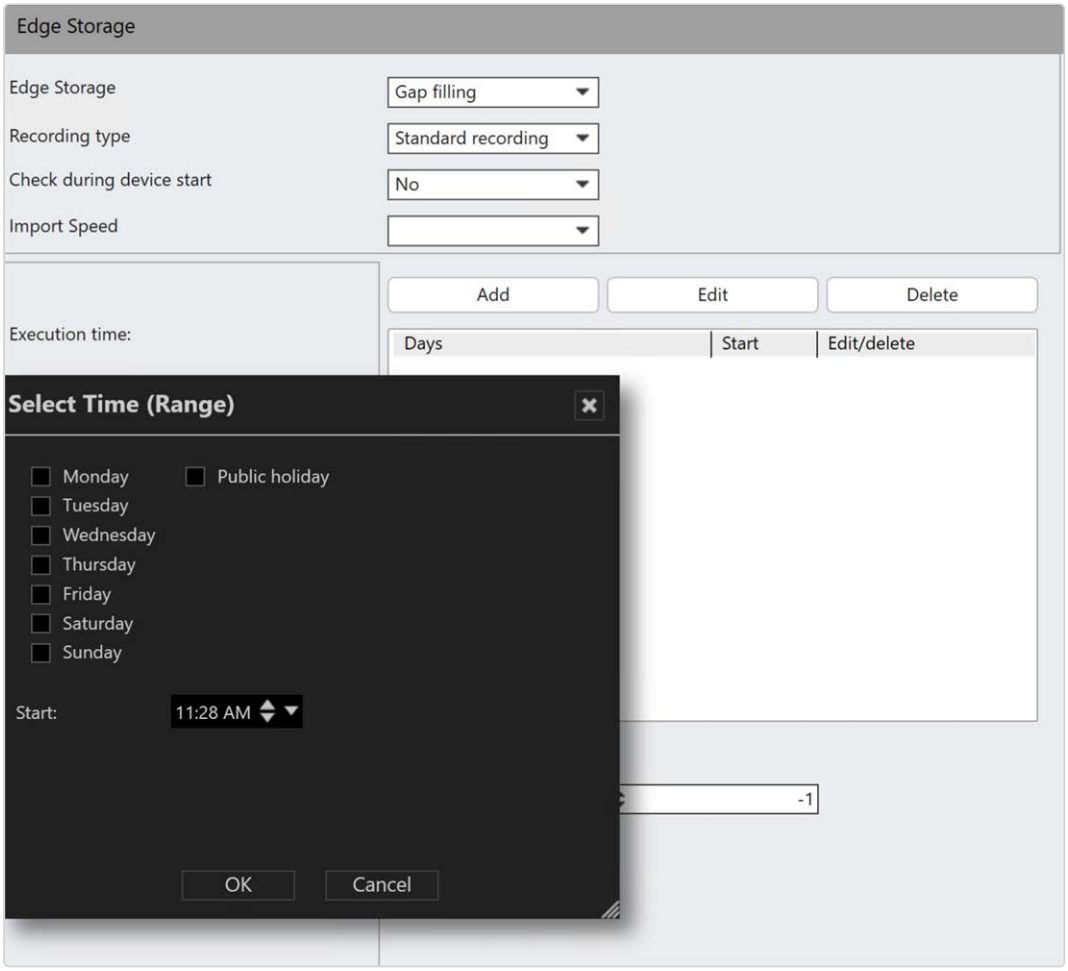


Fig. 114: Gap filling - 1

1. For **Edge storage**, select **Gap filling**.
2. For **Recording type**, select if the imported image data should be treated as **Standard recording** or **Alarm recording**.

3. For **Execution time** add at least one schedule and select the time when Qognify VMS looks automatically for gaps in the recordings and fills them up.

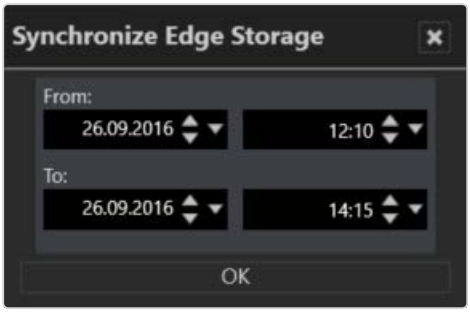
   > **A daily system check is recommended.**

4. To trigger gap filling by an alarm scenario or a sequence, set **Activate trigger** to **Yes**.
5. Activate **Optional time range (in minutes)** and specify the number of minutes of excess time before and after the actual gap filling. The data from the camera will deliver not only the missing time frame, but also a surplus to prevent gaps.

Full import

Full import overwrites all recordings on the zone with the recordings imported from the edge storage device.
The files can only be imported manually in archive mode (see "Archive mode" on page 163).

1. For **Edge storage**, select **Full import**.
2. For **Recording type**, select if the imported video sequences should be treated as **Standard recording** or **Alarm recording**.
3. Switch to archive mode.
4. Press CTRL and click **Update timeline** ( ) in the Archive player (see "Archive player" on page 164).



5. In the pop-up menu, define the time range and click **OK**.

Record on motion

The feature Record on motion allows a quick and simple configuration of an alarm recording.

> **Record on motion does not replace a complete alarm scenario (see "Alarms" on page 356).**

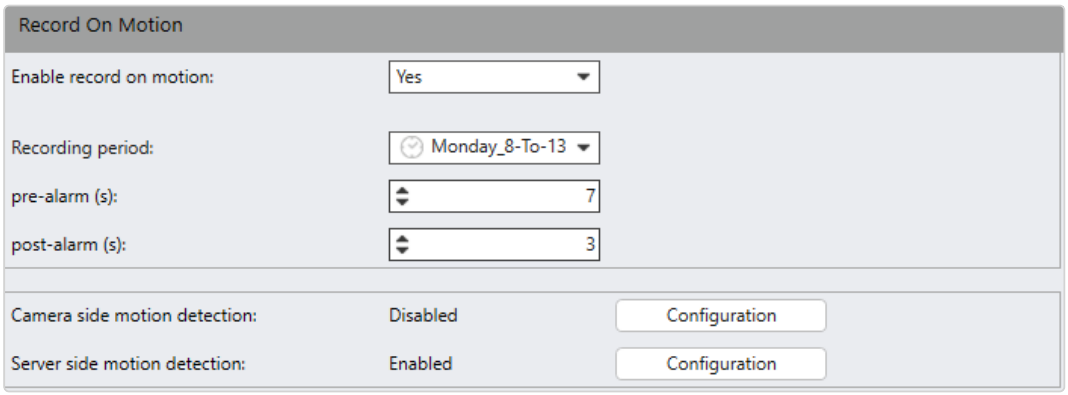


Fig. 115: Record on motion

1. Select **Enable record on motion**:
   - Select **Yes** if there should be an alarm recording as the result of an enabled server-based or camera-based motion detection.
   - Select **No**. You will be asked if server-based motion detection should be deactivated.
2. Select the **Recording period** as specified in the time management (see "Time management" on page 351). Any trigger outside of the selected time interval will be ignored. Triggers at the threshold are included in the corresponding pre- and post-alarm recording.

3. Specify a **pre-alarm** duration in seconds.
4. Specify a **post alarm** duration in seconds.

Edge storage

The menu item "Edge storage" is only displayed if supported by the selected camera.

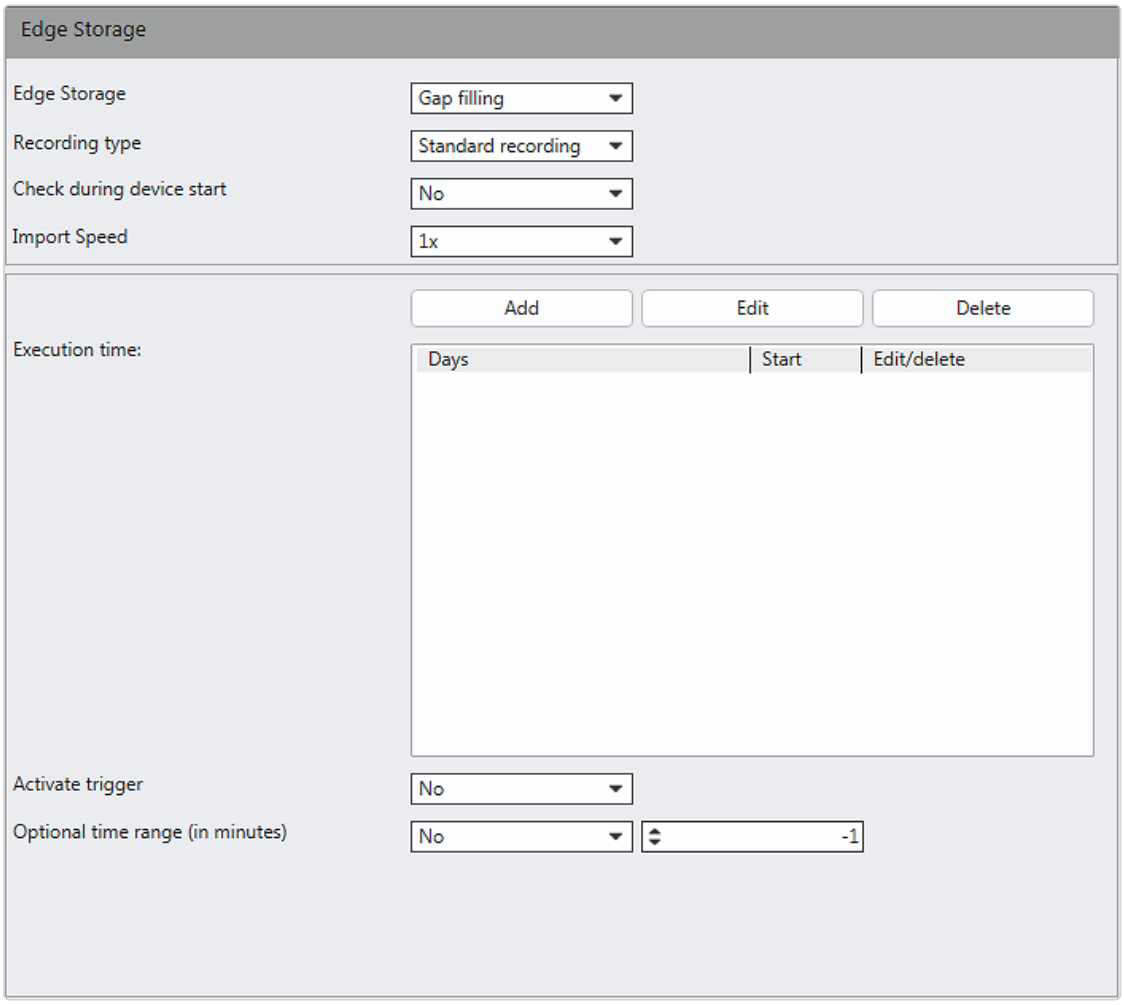


Fig. 116: Edge storage

Edge storage uses the camera to store images on an internal storage media (e.g. SD card) to cover connection failures between the camera and the database server. If the connection between the camera and the server is interrupted, recording gaps on the DeviceManager will result.

After the connection is reestablished, the recording gaps on the server can be filled with the recordings from the camera's internal storage media. Time schedules for recording and maximal recording size are taken into consideration.

Both use cases require configuration on camera side (see "Technical_Guides_Qognify_Qognify VMS_7.5_EN.pdf"). Both use cases require a license which includes edge storage functions.

There are various options to configure edge storage in configuration mode:

- Check on device start: If a device is started or reconnects after network failure, the import will be triggered.
- Import speed: Depending on the camera brand and model different values can be selected, e.g.
  - 1x: The import speed is identical to the playback speed of the recording
  - 2x: The import speed is double the playback speed of the recording
  - Max: Depending on the camera manufacturer, some cameras allow a higher import speed. By selecting this value, the Qognify VMS client will import the recordings at the highest possible speed available for the camera (for settings in the DeviceManager configuration, see below).
- Import triggered by schedule (see "Gap filling" on page 237).
- Manual import of a time range in archive mode (see "Full import" on page 238).
  - Optionally, a time range can be defined. If no time range is defined, all data since the last import will be imported.
  - If a time range is defined, only data within this range will be imported.
- Import triggered by an alarm scenario.

Remarks

- To prevent network flooding, only one device at a time will retrieve video from edge storage. If the importing or gap filling is triggered for several devices at the same time, they will be lined up in a queue.
- Do not change the configuration of the device while gap filling or full import is active as this may result in data loss.
- Make sure that the camera date / time is synchronized with the date, daytime, daylight savings time and time on the Qognify server.
- Edge storage does not work in a failover scenario (productive DM is offline and the redundant DM is recording images at that moment).

- Gap filling: In configuration mode > Camera > Image Storage > MultimediaDatabase you can activate **only record if**: This option will be ignored when checking for missing recordings. If there is a recording gap because of this feature, the missing recording will be transferred from the camera to the MDB although no recording is intended.
- It is possible to check manually for missing recordings (and update them): Open the camera in archive mode and click on update timeline. Depending on the missing recordings the update will take some time.
- Time schedules, holidays, maximum recording time range will not be ignored.
- Gap filling: If checking once a day for gaps, make sure to have recordings for two days on the device to make it work properly. Also make sure that the SD card has enough storage space for two days of recording.
- Recordings that are overwrite-protected will not be replaced by edge storage imports.
- Inserted recordings in the MDS will be shown in report mode.
- Gaps will be filled only after the first access to the camera.
- If the recording fails often, Qognify cannot ensure that the edge storage functionality is working properly. In this case the camera problem or network problem must be fixed first.

Video streams

In the video streams section, different profiles for the transmission of image data from the camera should be specifies and configured. Qognify VMS creates a base stream during installation of the camera. The base stream cannot be deleted.
If supported by the camera, multiple video streams can be configured, e.g. to use a different video quality in surveillance mode, for alarm recording, and for analytics purposes.

Creating a new video stream

If supported by the camera, different settings can be applied to one video stream, e.g. to use a different video quality in surveillance mode and for alarm recording. The different recordings are captured from the base stream. The base stream cannot be deleted.

1. In the configuration tree click on "Video streams". The configured video streams are listed.

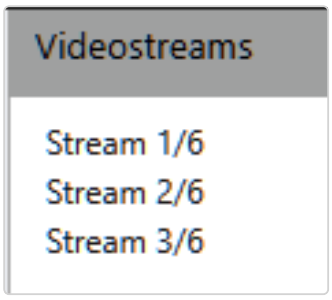


Fig. 117: Creating a new video stream

2. Click **New** to create a new video stream.

> **The maximum number of streams depends on the camera type.**

Editing a video stream

1. Select the video stream, and click **Edit** to make the required settings.
2. Select the **capture mode**.

> **Capture mode can only be selected if supported by the camera. The available capture modes are dependent on the camera type. With multi-channel devices or virtual cameras, changing to the capture mode affects all devices of this video server. Therefore capture mode can only be defined for the base stream (displayed by a home icon), but affects all subsequent streams of the selected camera. Depending on the setting selected, the camera provides different frame rates and resolutions. The camera may restart and be inaccessible for a few minutes.**

3. Select the type of the **video** stream. The following video streams are available, depending on the hardware:

Motion JPEG (M-JPEG)

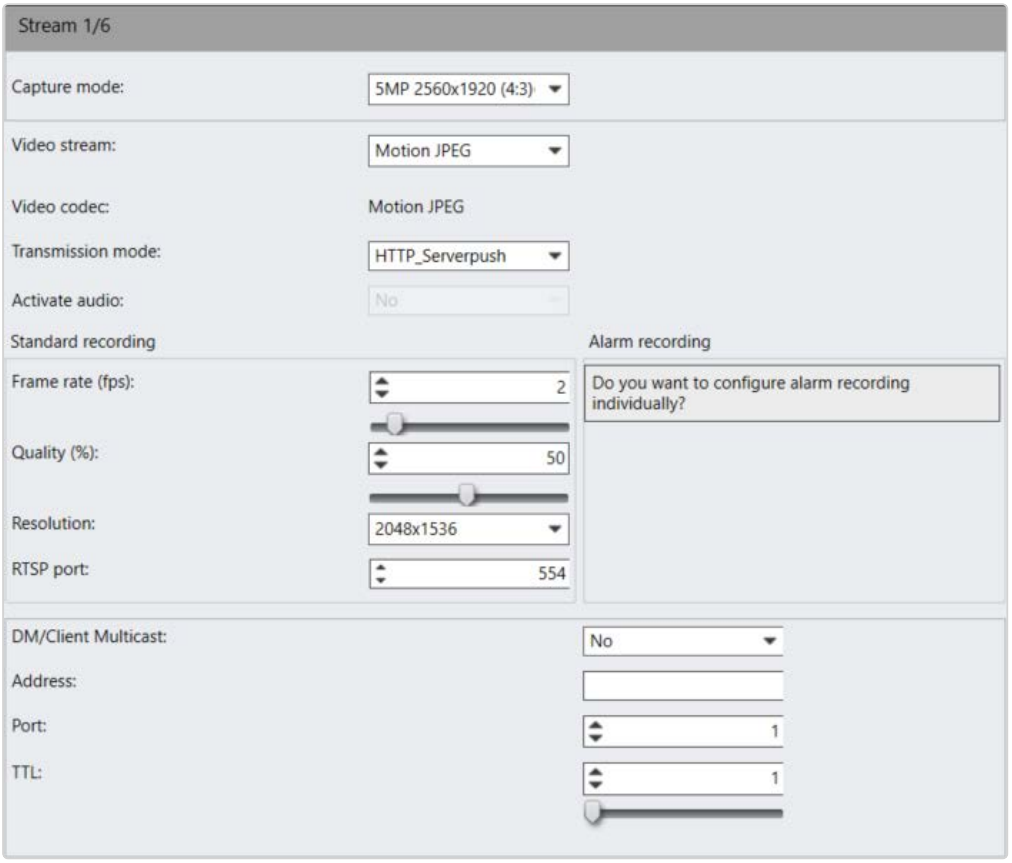


Fig. 118: Motion JPEG (M-JPEG)

1. Select the **transmission mode**: HTTP server push (only available mode for Motion JPEG) - also known as HTTP streaming - is a mechanism for sending unsolicited (asynchronous) data from a (camera) web server to the DeviceManager.
2. Specify the **Frame rate** (fps) for standard recording.
3. Specify **Quality** separately for standard recording.
4. Select a suitable **Resolution** for the camera image for standard recording.
5. Specify an **RTSP port**. The default RTSP port is 544.

6. Optionally configure the alarm recording separately.

> **It is not recommended to specify different alarm recording settings. If there are differences in the settings for standard and alarm recording, it can take several seconds to switch from standard to alarm recording. The length of time taken depends on the camera. There may be no recording available at all during this period.**

> **If a different video quality is required for alarm recording, it is recommended to define a separate video stream that can be assigned in the alarm recording settings (see "Multimedia database" on page 232).**

H.264 / H.265 / (MPEG-4)

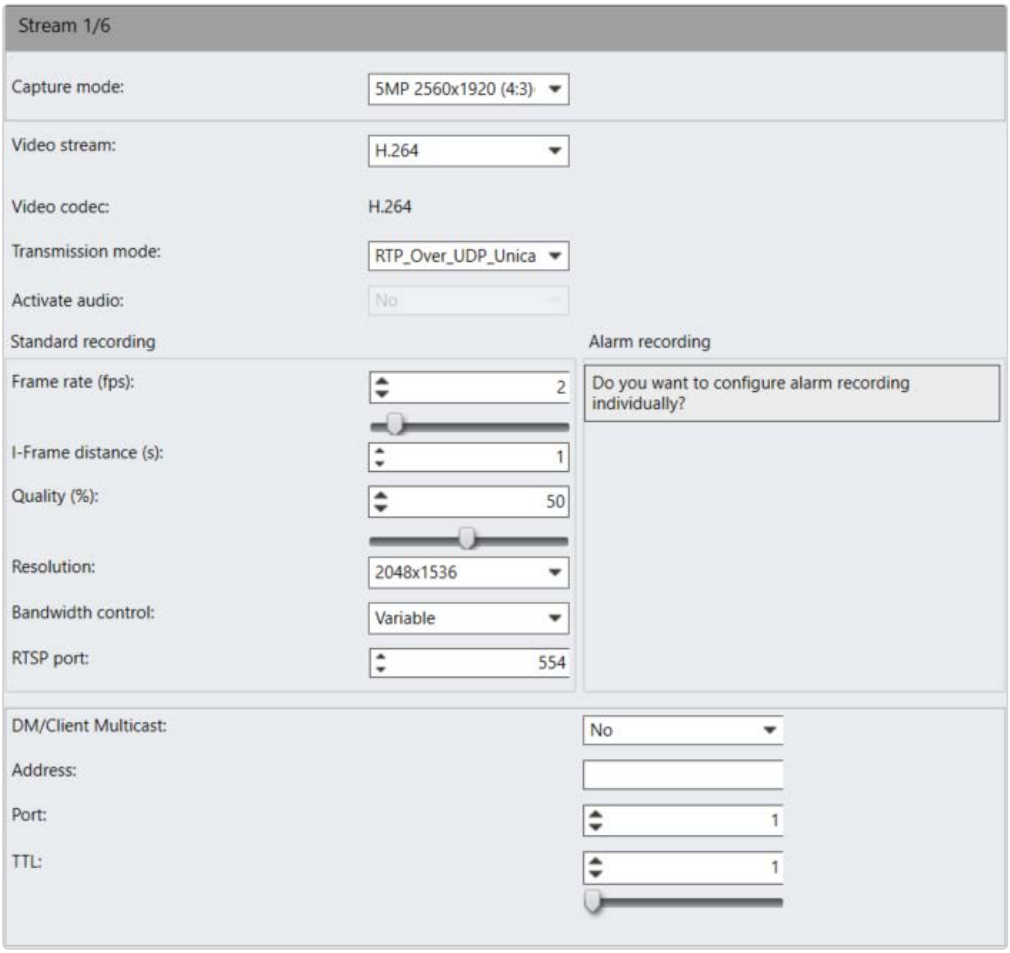


Fig. 119: H.264/ H.265 (MPEG-4)

1. Select the **Transmission mode**. The following transmission modes are available depending on the camera:
   - **RTP over UDP Unicast** (default setting): Communication between the Qognify server and camera is via TCP port 554 (RTSP port). Image transmission from the camera to the server is via a negotiated UDP port.
   - **RTP over UDP Multicast**: Communication between the Qognify server and camera is via TCP port 554 (RTSP port). Image transmission is via a multicast address provided by the camera. RTP over UDP Multicast should only be used if third-party systems (e.g. Barco or eyevis) and the server access the camera simultaneously.
   - **RTP over RTSP over TCP**: Communication between the Qognify server and camera and image transmission is via TCP port 554 (RTSP port). This setting is recommended for poor network connection between servers and camera. Latency times may occur due to repeated transmission of corrupt data.
   - **RTP over RTSP over HTTP Unicast**: Communication and image transmission is via a HTTP tunnel (port 80 TCP). This setting is recommended for poor network connection between servers and camera. Latency times may occur due to repeated transmission of corrupt data.
2. **Activate audio** for the transmission of audio signals. This function is available only if the camera can process audio signals in MPEG-4-based video streams.

   > **If activated, the audio stream is also recorded and therefore available in archive mode.**
3. Specify the **Frame rate (fps)** for standard recording.
4. Define the **I-frame distance** for MPEG-4 / H.264./ H.265
5. Specify **Quality** separately for standard recording.
6. Select a suitable **Resolution** for the camera image for standard recording.

7. Select the type of **Bandwidth control** for MPEG-4/H.264/H.265 streams:
   - **Variable Bitrate**: VBR is used if sufficient resources and bandwidth are available. VBR delivers constant image quality at static scenes and motion.
   - **Constant Bitrate**: CBR is used if only reduced bandwidth is available. CBR delivers good image quality at static scenes and reduced image quality on motion.
8. Specify an **RTSP port** (default port: 554).
9. Optionally configure alarm recordings separately.

> **It is not recommended to specify different alarm recording settings. If there are differences in the settings for standard and alarm recording, it can take several seconds to switch from standard to alarm recording. The length of time taken depends on the camera. There may be no recording available at all during this period.**

> **If a different video quality is required for alarm recording, it is recommended to define a separate video stream that can be assigned in the alarm recording settings (see "Multimedia database" on page 232).**

Video classifications

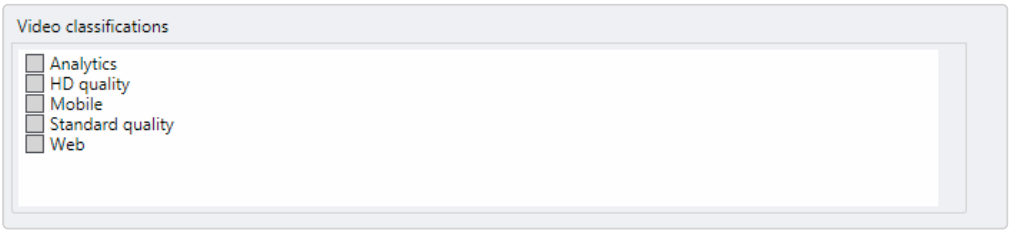


Fig. 120: Video classifications

Video classifications are available only when multiple video-streams are specified for a camera. In this case, each stream has to be classified. Classified streams can be used for multiple purposes. For example, the classification “Standard quality” is used for standard recording and alarm recording while the classification “HD quality” is used for displaying the camera image on the client depending on the user profile (see "Image settings" on page 348).

1. Select the appropriate video classification (see "Configuring the video classification" on page 429).

DM / Client Multicast

Fig. 121: DM / Client Multicast

1. Select **DM / Client Multicast** streaming to display a single video stream simultaneously on multiple clients. Multicast should only be used if there is low bandwidth between the DeviceManager and clients.

   > **Multicast-capable network hardware is required for multicast streaming.**

2. Enter the network **Address** and **Port** number of the multicast server.
3. Specify the **TTL** ("Time-to-live") period after which the client has to log in to the multicast server again. A short TTL results in a higher network load.

Deleting a video stream

1. In the configuration tree click on "Video streams". The configured video streams are listed.
2. Select the video stream and click **Delete**.

Audio

If the camera supports transmission of audio signals, the audio codec can be configured. However, the adjustments in the camera control in surveillance mode override

the camera settings (see "Audio" on page 154). To use the transmission of audio signals from the camera to the client, the transmission has to be activated in the video stream settings (see "Video streams" on page 242).

Camera selection is only necessary for multi-channel devices.

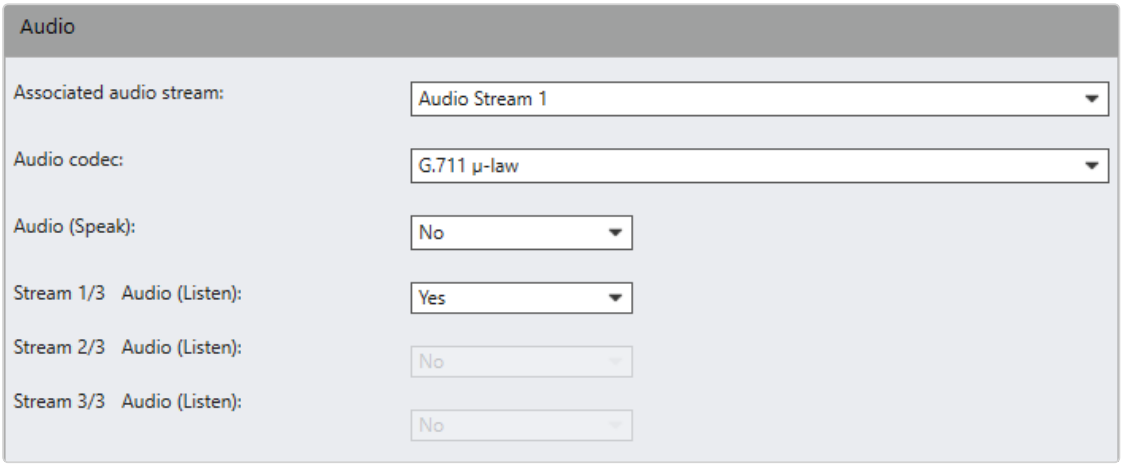


Fig. 122: Audio

1. Select the MPEG-4/H.264/H.265 mode for video streams in the video stream settings (see "Video streams" on page 242).
2. Select the **associated camera**.
3. Select the corresponding **audio codec.**
4. If supported by the camera, select **Audio (Speak)**. When set to "Yes", an audio communication to the camera is possible in surveillance mode (see "Audio" on page 154).
5. For each video source that supports audio select the available audio stream and set to "Yes" to enable audio. If the device supports multiple audio streams, each audio stream can be assigned to exactly one video source.

   If the audio stream is selected on another video source, it is removed from the first video source.

Camera positions / digital presets

If the selected camera supports PTZ the menu item is "Camera positions".

If the selected camera does not support PTZ, this menu item changes to "Digital Presets". All camera positions will be defined using the digital zoom. The number of camera positions is limited by the camera.

Camera positions can be created and deleted as "presets" by the user in surveillance mode and by the administrator in configuration mode.

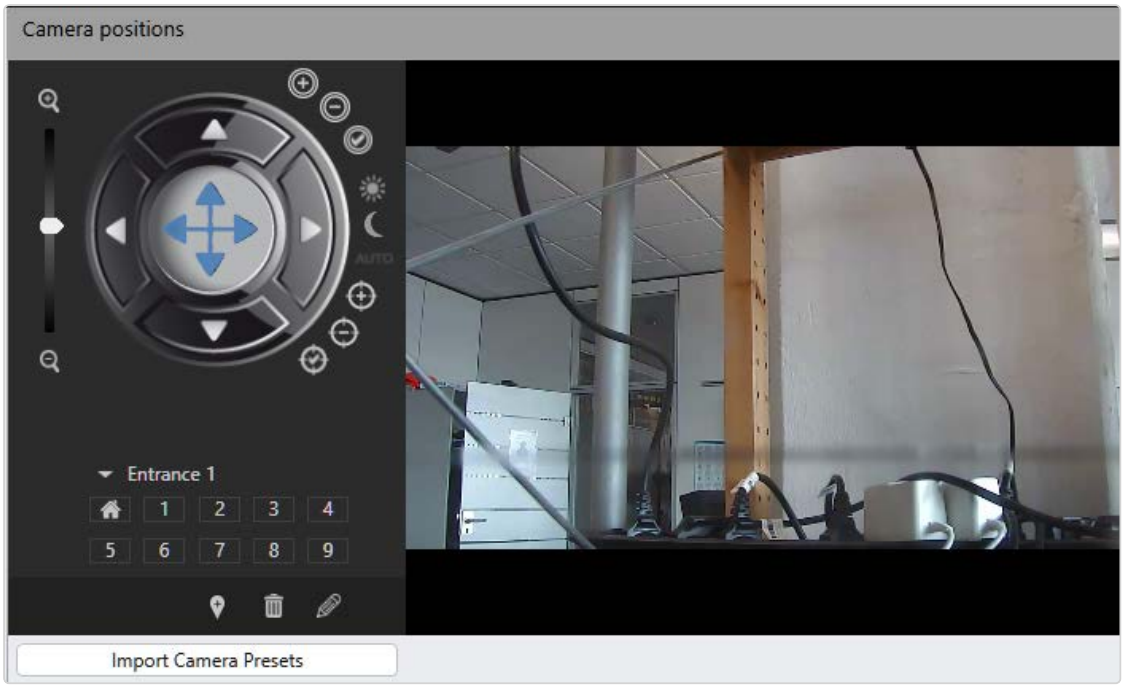


Fig. 123: Camera positions / digital presets

Depending on the camera the following features are available:

- Iris +
- Iris -
- Auto iris
- Day mode
- Night mode
- Auto mode
- Close-up focus
- Long-range focus
- Auto focus

Creating camera positions / digital presets

Admin presets are created and managed by the administrator.

1. Use the PTZ controller or an external controller device to move the camera to the required position.
2. Click **Add new camera position**.
3. Enter the **name** of the new preset position, and click **OK**. The name is displayed in the column, and the preset position is assigned the next free position number. If there are not enough position numbers, the additional positions are added in a drop-down list.

Editing preset positions / digital presets

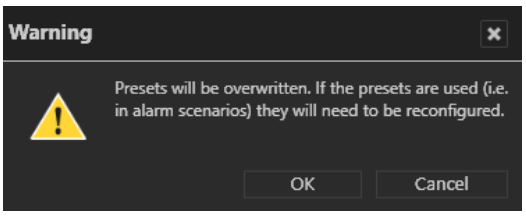
1. Click on the position you want to edit or select it from the list.
2. Click **Edit current preset**.
3. Use the PTZ controller or an external controller device to move the camera to the required position.
4. Change the positions name if required.
5. Click **Save current changes**.
6. To delete a preset position, click on the selection, select the name from the list, and click **Delete current camera position**.

Importing camera positions / digital presets

Positions that are already configured on the camera can be imported into the Qognify configuration.

> **The import presets option is available only when the user has rights to create presets (see "Manage user rights" on page 333) and camera position needs to be enabled in the general camera configuration (see "Camera general" on page 226).**

1. Click **Import Camera Positions**.



> **When importing preset positions from a camera, all positions in the Qognify configuration will be overwritten!**

2. Click **OK**. The import process starts.

Video Backup/Export

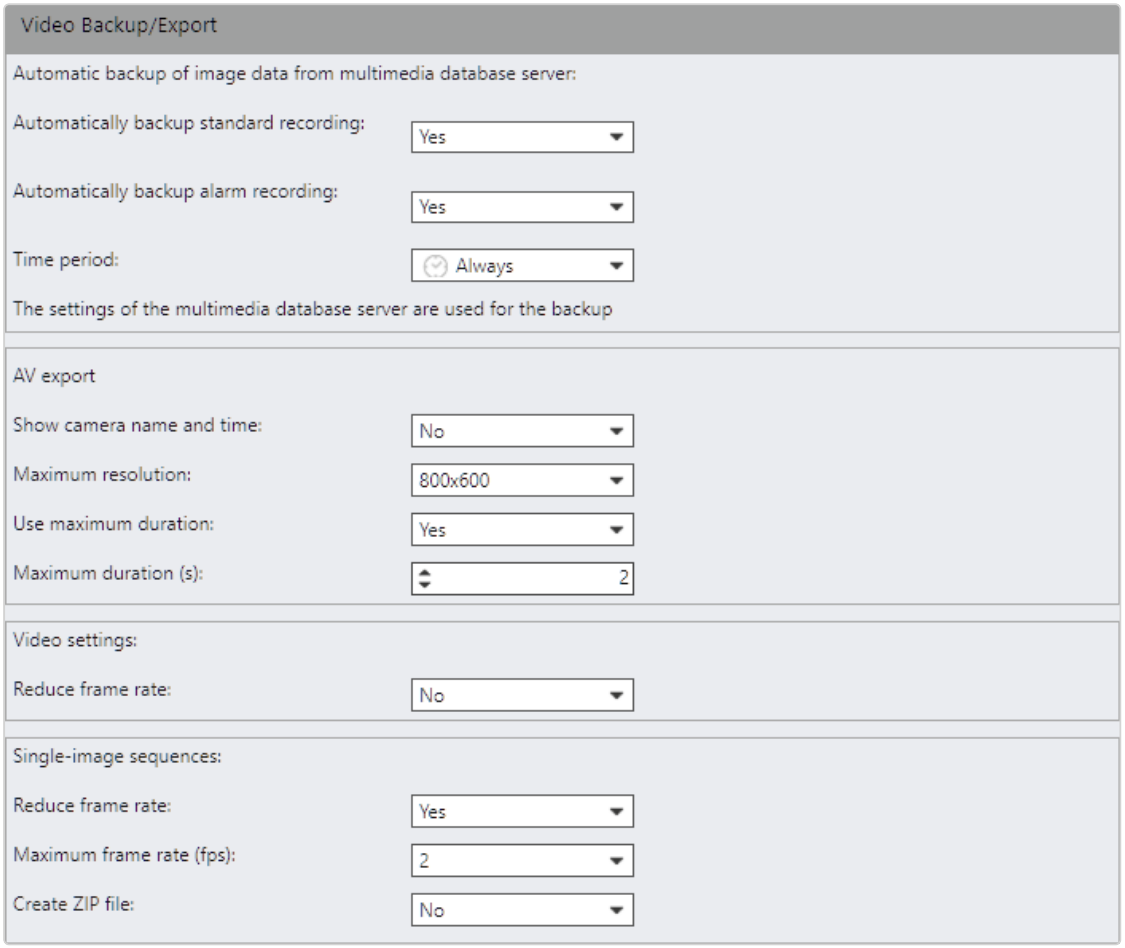


Fig. 124: Video backup / export

Automatic export of image data from the database server

Recordings can automatically be exported to a path on the DeviceManager e. g. for long-time archiving of recordings or backup purposes.

By default, backups are created daily as backup jobs. Before starting the transfer, Qognify VMS checks if the path to the backup folder is available. If the path is not available or the backup process fails, Qognify VMS will retry to connect once every minute and resume the backup process as soon as the connection is established. If the backup content is no longer available (e.g. when a camera is removed during an unfinished backup). the backup job is removed.

> **If the export process is interrupted, e.g. due to a network error, it will be automatically resumed as soon as possible.**

1. Specify whether standard recordings and alarm recordings are to be backed up automatically.

   The path for the automated export must be configured in the DeviceManager configuration (see "Configuring the DeviceManager (DM)" on page 404). Otherwise automatic export is not possible!

2. Specify the **Time period** to be exported. Time periods can be defined in time templates in the time management (see "Time management" on page 351).

AV export

AV export can be triggered by an alarm. The process converts alarm recordings into unencrypted H.264 (MPG) or M-JPEG sequences which can be attached to an E-Mail or stored on an FTP Server (see "Email and FTP" on page 372).

> **The FTP-Server settings need to be specified in the VA Administration Tool (see "Qognify VMS VA Administration Tool" on page 476).**

1. Specify whether the **Camera name and time** of recordings are also to be exported and displayed in the AV export. The camera name and time are specified in the exported sequence at the bottom of the image.
2. Select the **Maximum resolution** for the export.
3. Specify whether the **Length** of the recording is to be limited.
4. Enter the **Maximum duration (s)** of the export (in seconds).

   > **It is recommended to reduce the size of the export files as much as possible by reducing resolution and duration of the video sequence.**

5. In Video settings (for MPG based streams, e.g. H.264), optionally activate **Reduce frame rate**, so only I-frames will be exported.
6. In single-image sequences (MJPG) optionally activate **Reduce frame rate**, so the specified maximum frame rate (fps) will be exported.
7. Select **Create ZIP file** to compress the exported data after export.

Server side functions

The configurable server side functions are:

- Motion detection (see "Motion detection" on the facing page)
- Reference image comparison (see "Reference image comparison" on page 257)
- Tampering detection (see "Tampering detection" on page 258)

The server side functions detect motion within the image, tampering attempts on the camera, and differences to a reference image. For the server side functions, images are analyzed by motion detection modules on the server (see "Adding a server-based motion detection module" on page 485). For example, a server side motion detection event can be used to trigger an alarm.

> **Server side image analysis by the motion detection module causes high resource load. Therefore it is recommended to use the camera side motion detection (see "Camera side functions" on page 259).**

1. Select the server side operation menu.
2. Select a video classification (see "Video streams" on page 242).

   - The video classification determines which video stream is used for motion detection.
   - The video streams are ordered according to their use of network bandwidth ("HD quality" requires a broadband connection, whereas "Mobile" decreases the image quality for slow networks).

3. For image comparison, select a video stream for low bandwidths.

   > **Motion detection, reference image comparison and tampering re-size the images to 320 x 240 pixels internally if they are larger.**

Motion detection

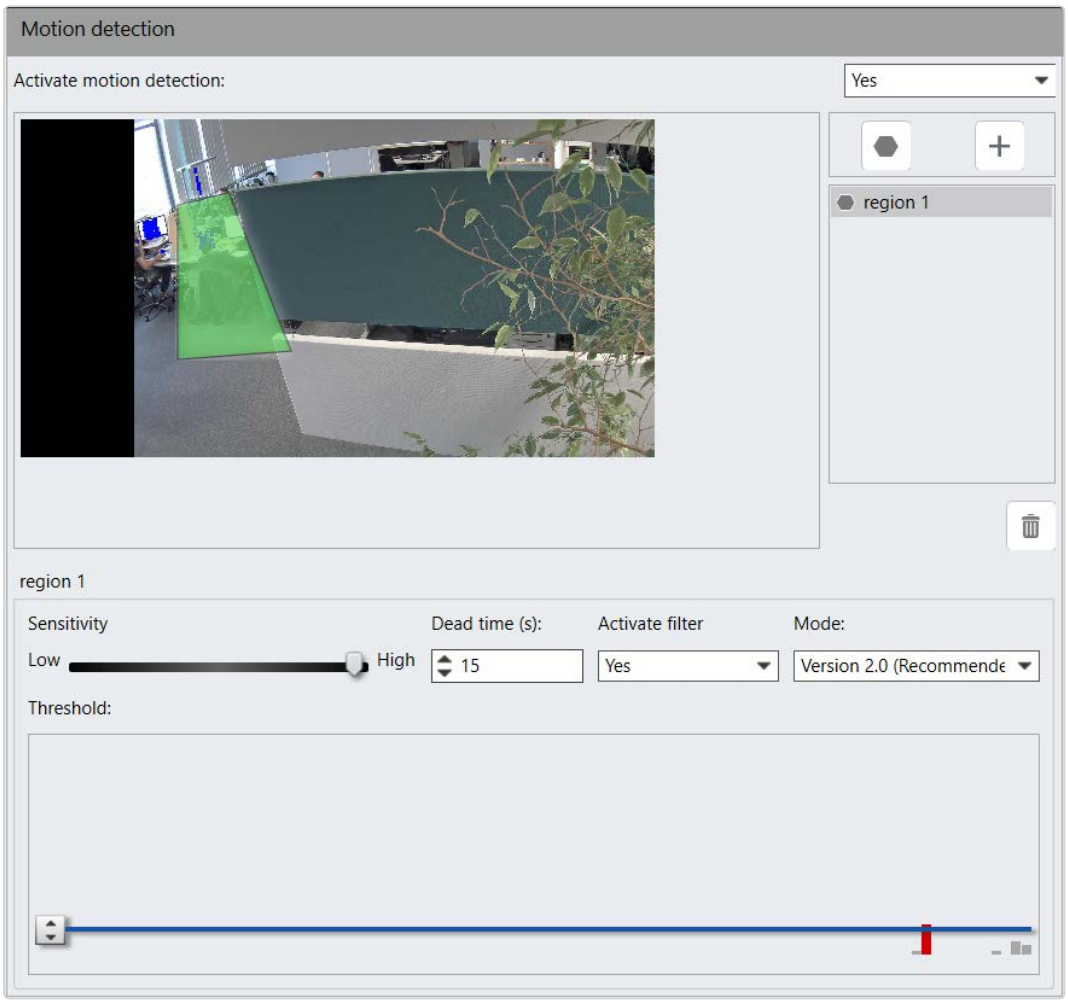


Fig. 125: Motion detection

The server side motion detection analyzes a single channel gray image stream and is therefore highly efficient. Nevertheless, it is recommended to prefer the camera side motion detection for reducing the hardware requirements of the server (see "System requirements" on page 31).

> **The motion detection feature delivers the best results with indoor use. You can create up to 10 regions for each camera with individually configured sensitivity, dead time, and threshold values**

1. Select **Motion detection** from the Server side operation menu (you may have to click on the triangle in front of the menu).
2. To activate the motion detection, select **Yes** from the drop-down menu.
3. Click the plus sign to the right of the camera image.

4. Use the polygon tool to draw the region on the camera image. Different sections are only required if different alarm scenarios are to be triggered for each section.
5. Enter a name for the region(s).
6. Adjust the motion **sensitivity** by moving the slider as appropriate. The sensitivity value determines how big or small a difference in the image has to be in order to count as motion. Increase the value if too many false negative results are obtained, or decrease the value if too many false positive results are obtained.
   - With a high value, even small changes in the image will be treated as motion.
   - With a low value, only big changes in the Image will be treated as motion.
7. Specify the interval for the **dead time** (in seconds) after which a signal is analyzed again.
8. Select **Activate filter** to optimize the image by a blur filter to reduce image noise which might appear (e.g. due to low light conditions).
9. Choose between **Version 1.0** and **Version 2.0** by using the drop-down menu in the middle.

> **It is strongly recommended to use Version 2.0, since it has a much better performance and only a slightly reduced quality. The mode type has to be the same for every region in one camera.**

10. Adjust the **threshold** by moving the blue line. The threshold determines how big the motion in the images needs to be in order to trigger a alarm.
    - Set the threshold to a high value if only big motions are supposed to trigger an alarm.
    - Set the threshold to a low value if small motions are supposed to trigger an alarm. The rectangles in the threshold slider window are a visual help for the threshold adjustment. They show the motion amplitude of the last seconds and colors them red, if the current threshold value would have triggered an alarm.
    - The colored pixels in the image show where motion was detected.
      - A blue colored pixel signifies that motion was detected
      - A red colored pixel signifies that a alarm was triggered
11. Save the settings.

Reference image comparison

The live camera image is compared to a defined reference image of the same camera view (see "Manual reference image comparison" on page 114). An alarm will be triggered if the images do not match and triggers a second alarm when the original camera view is restored.

1. Select **Reference image comparison** in the server side operation menu.
2. To activate the automatic image reference comparison, select **Yes** from the drop-down-menu.
3. Select **Create reference image** to select an image from the camera that serves as a backdrop for the motion detection.
4. Select **Show differences only** to show only the differences between the live-image and the reference image.
5. Adjust the **Alert threshold (tolerance)** in percent. An alarm will b e triggered only if the differences between the live image and reference image are above the threshold.
6. Select if the image to be compared is a live image in Surveillance mode or a recorded image from Archive mode. The recorded image has to be specified by selecting the time by selecting **Calender direct input**  .

7. Specify the values for the **Execution time point** by defining the time interval (in minutes, at a certain day time or on certain days per week at a specific time) for the comparison between the reference image and the live image.

Tampering detection

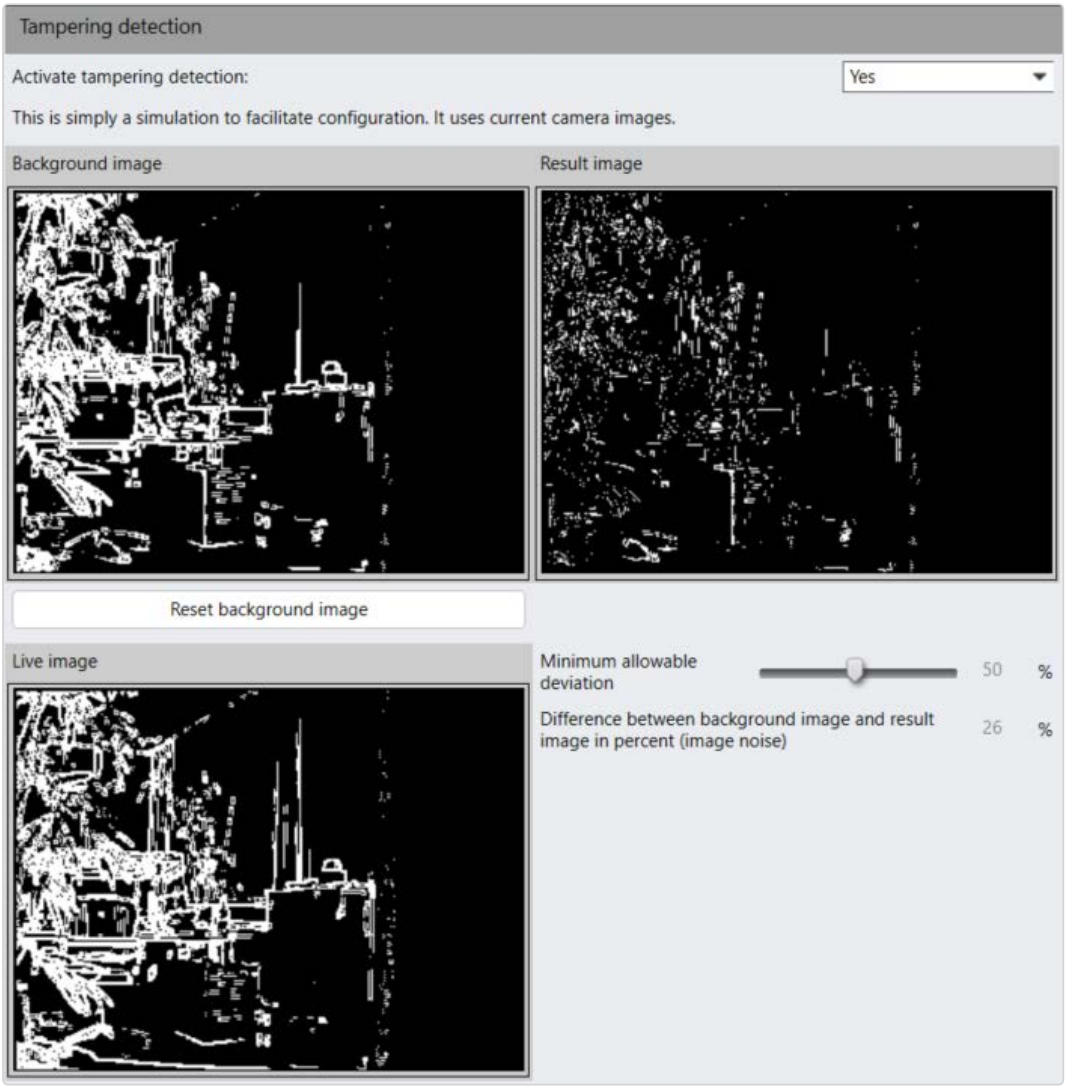


Fig. 126: Tampering detection

The tampering detection recognizes manipulation of the camera orientation but uses edge detection for comparison. The reference images are generated automatically from every image and compared to the following. Specific tampering events can be used as triggers for an alarm scenario. After an alarm, the reference image will be recreated.

1. To activate the tampering detection, select **Yes** from the drop-down-menu.
2. Select **Reset background image** to define a new reference image.

3. Set the **Minimum allowable deviation** for the live image (in percent) to specify the threshold value that triggers the motion detection. The higher the value, the less sensitive the image detection will be.

   > **To trigger an alarm, an alarm scenario has to be configured for the camera (see "Creating an alarm scenario" on page 357).**

4. Apply the set values if you want to make further settings.
5. Save the set values to apply the values and conclude input.

Camera side functions

If supported by the camera, the camera side functions detect motion within the image and tampering attempts on the camera.

> **Camera side functions have to be activated and configured on the camera itself.**

For example, a motion detection event can be used to trigger an alarm.

Motion detection

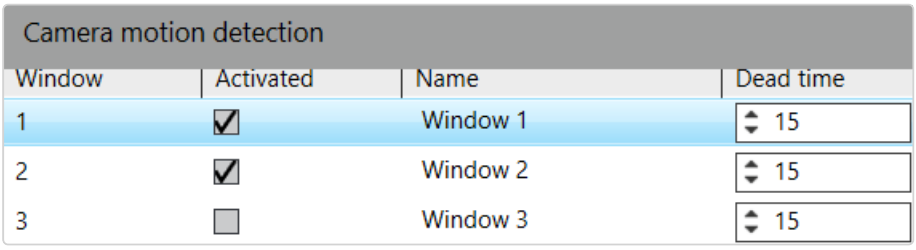


Fig. 127: Motion detection

1. Choose **Motion detection** in the Camera side operation menu.
2. Activate the appropriate number of windows, and enter a name and interval for the **dead time** (in seconds) after which a signal is analyzed again. This setting may also be used to trigger an alarm (see "Alarms" on page 356).

Tampering detection

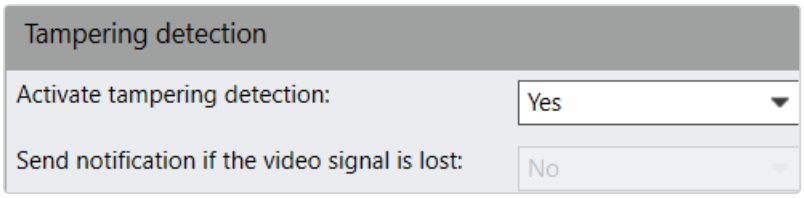


Fig. 128: Tampering detection

Depending on the camera model used, specific events can be used as triggers for an alarm scenario (see the respective camera manual for more information about the camera specific tampering features).

An action can be started once notification is received. This setting may also be used to trigger an alarm (see "Alarms" on page 356).

1. Choose **Tampering detection** in the Camera side operation menu.
2. Select **Yes** to activate camera side tampering detection.
3. If supported by the camera, select **Yes** to **Send notifications if the video signal is lost**. This will trigger a notification in the alarm list if the video signal drops out.

   This setting may also be used to trigger an alarm (see "Alarms" on page 356).

Event trigger

If the camera is integrated by a smart driver (generic driver) trigger as motion detection, tampering or other camera side events can be configured as event triggers.

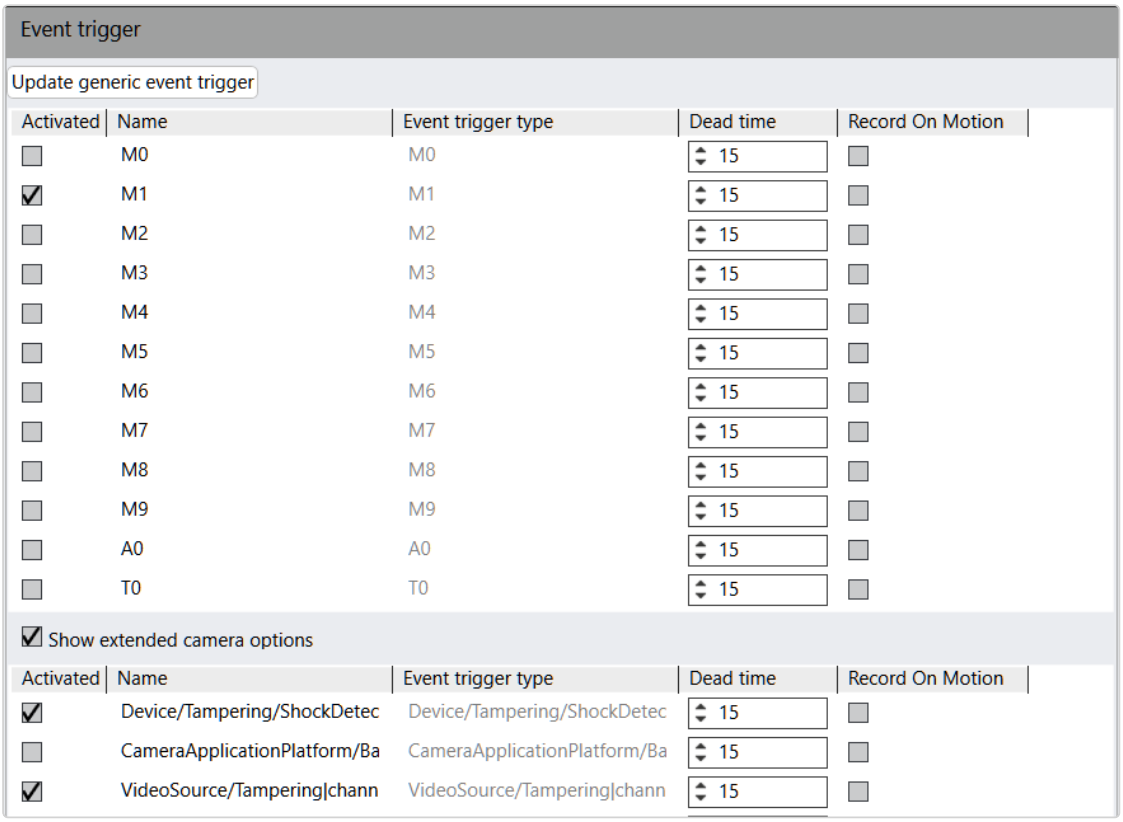


Fig. 129: Event trigger

1. Choose **Event trigger** in the Camera side operation menu.
2. If changes were made on the camera itself or if not all expected events appear, click **Update generic event trigger**.
3. Activate the appropriate number of events, and enter a **Name** and interval for the **Dead time** (in seconds) after which a signal is analyzed again. This setting may also be used to trigger an alarm (see "Alarms" on page 356).

The dead time is only used when the event trigger is used for by e.g. an alarm scenario. If the checkbox “Record On Motion” is also checked, the dead time will not be applied to the “Record On Motion” function.

> **Depending on the camera-type and driver extended camera options can be available.**

Privacy masking

Sensitive areas or movements in the image can be hidden by a mask. This prevents the user from seeing these areas. Depending on the user authorizations, the mask is displayed in surveillance mode and archive mode.

This function can be activated and disabled in surveillance mode and archive mode by administrators and users with corresponding rights.

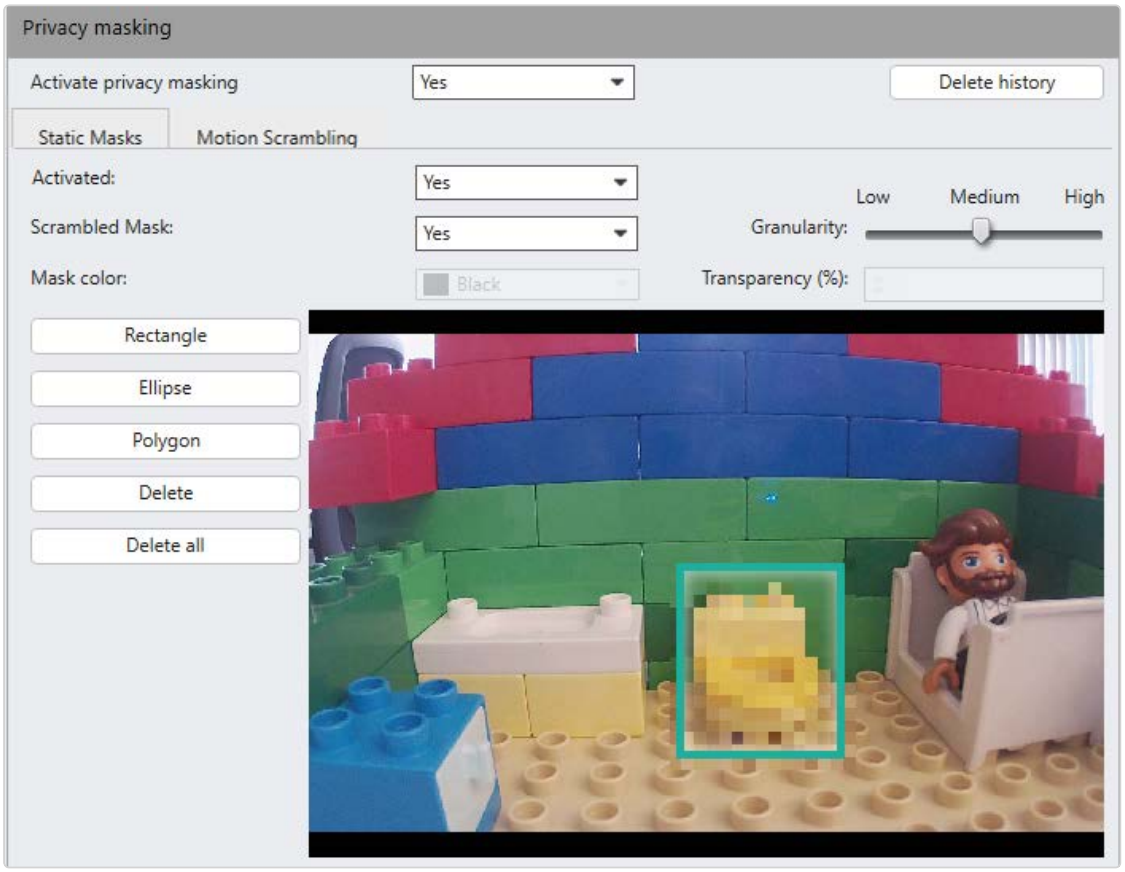


Fig. 130: Static objects

1. Activate **Privacy masking**.
2. Select **Static Masks** or **Motion Scrambling**.
   - You can use the **Static Masks** method to mask fixed individual areas of the camera image. The masking follows the camera so that it is always the same image detail that is masked.
   - You can use **Motion Scrambling** to mask changing or static image information. The **Moving objects** method of the Scrambling function allows you to mask moving objects like people or cars (see "Motion Scrambling" on the next page). **Office mode** of the scrambling function is based on reference image comparison and masks all differences from a reference image (see "Office mode" on page 265).

Static Masks

Scrambled Mask

1. Select **Static Masks** and activate.
2. Select the shape of the area to be scrambled, e. g. a rectangle or an ellipse.
3. Select **Scrambled Mask** and set the granularity of the details. The lower the granularity, the less coarse the selected area is displayed.
4. Drag the shape over the camera image.

Mask color

1. Select **Static objects** and activate.
2. Select the shape of the area to be masked, e. g. a rectangle or an ellipse.
3. Select **Mask color** and set the color and the transparency of the mask
4. Drag the shape over the camera image.

Deleting a mask

1. Select either **Delete** to delete a single mask or select **Delete all** to remove all masks.

Motion Scrambling

Moving objects

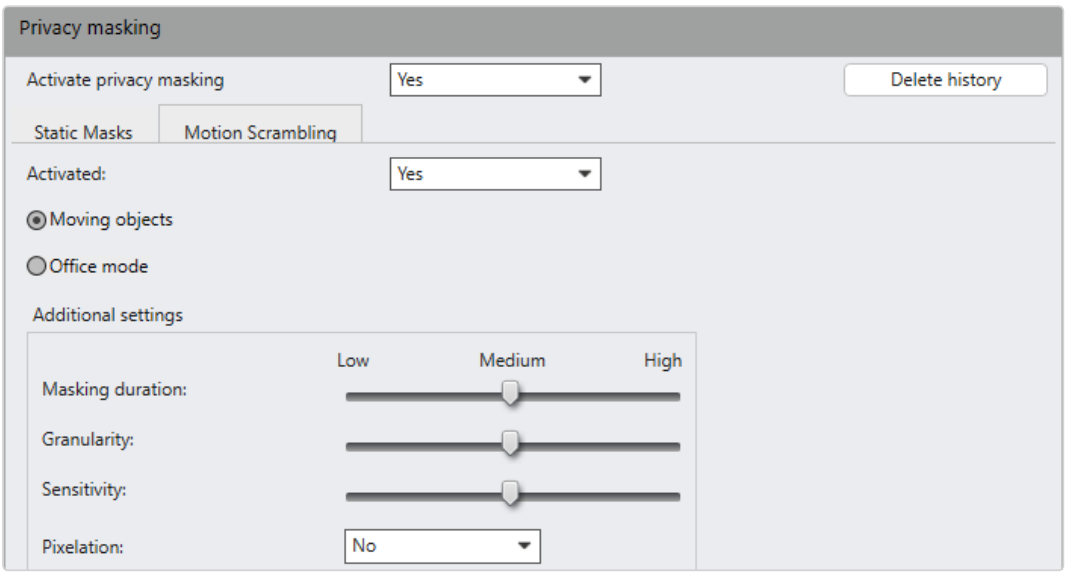


Fig. 131: Scrambling / moving objects

1. Select **Scrambling** and activate.
2. Specify how long the object is to be masked for after it comes to a halt (**Masking duration**), the pixel size to be used for masking (**Granularity**) and how sensitive the response is to a moving object (**Sensitivity**).
3. Select **Pixelation** to display the mask in black and white. Otherwise, the mask is displayed with coarse pixels in the original colors.

Office mode

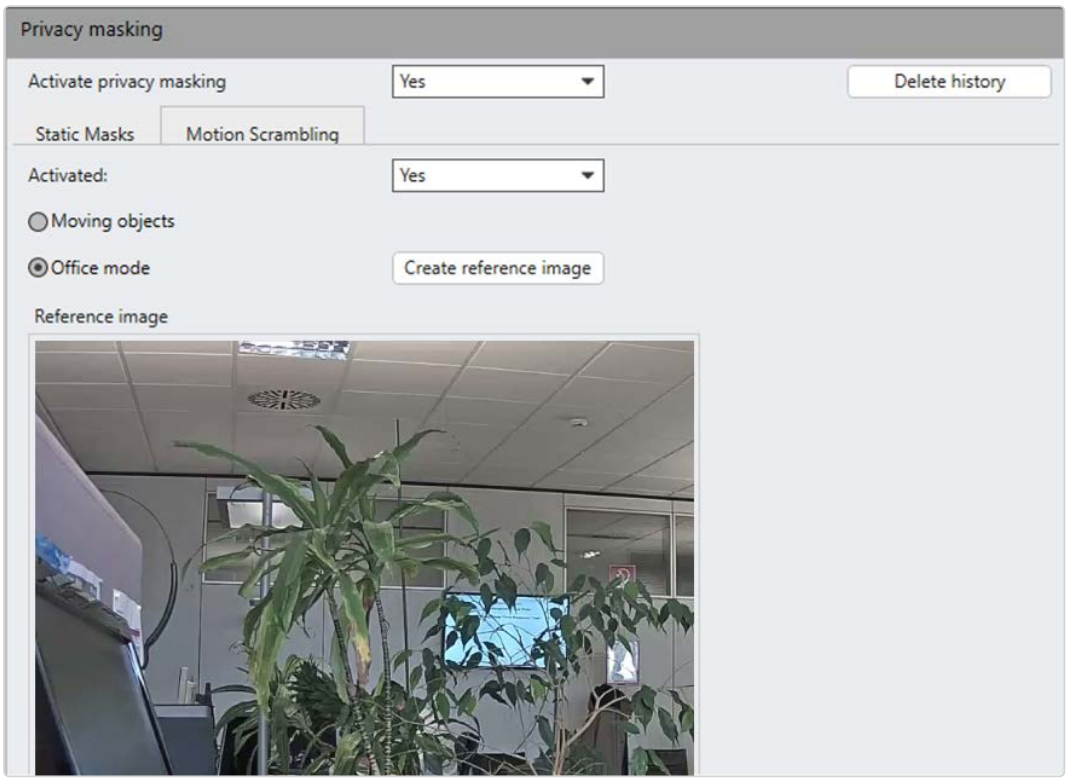


Fig. 132: Scrambling / office mode

1. Select **Office mode**.
2. Load a reference image. All differences to the stored reference image are masked.
3. To delete all masks in the archive, click **Delete history**.
4. Click **Yes** to confirm.

> **If privacy masking history is not deleted, privacy masks remain on the recordings even if the masking feature is deactivated. Therefore only users with the appropriate permissions are able to see the recordings.**

Click-2-Track

A person or object that moves across different camera views can be followed even without specifying the camera name of the following view. Instead, the person or object path is defined in surveillance mode by activating the area covered by the adjacent camera (see "Click-2-Track" on page 135).

This feature requires an appropriate license and is not included in the standard package.

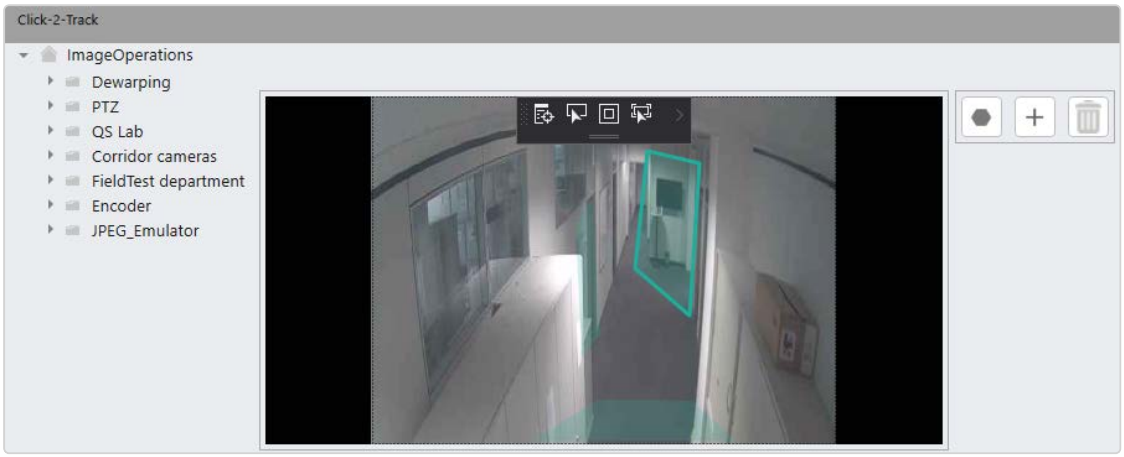


Fig. 133: Pursuit mode

1. Click **Add** + and click **Polygon** ⬣.
2. Draw a polygon in the image by clicking to define the corners. The polygon defines the regions for surveillance.
3. Close the polygon by double-clicking.
4. Open the camera tree to the left of the image and drag a camera into the region.
5. To change a region, click **Polygon** ⬣ and define a new region.
6. To check the settings, use the mouse to hover over the region for a preview of the linked camera image.
7. To delete a polygon, select the polygon and click **Delete** 🗑. The polygon and the link to the associated camera is deleted.

Configuring an Archive camera

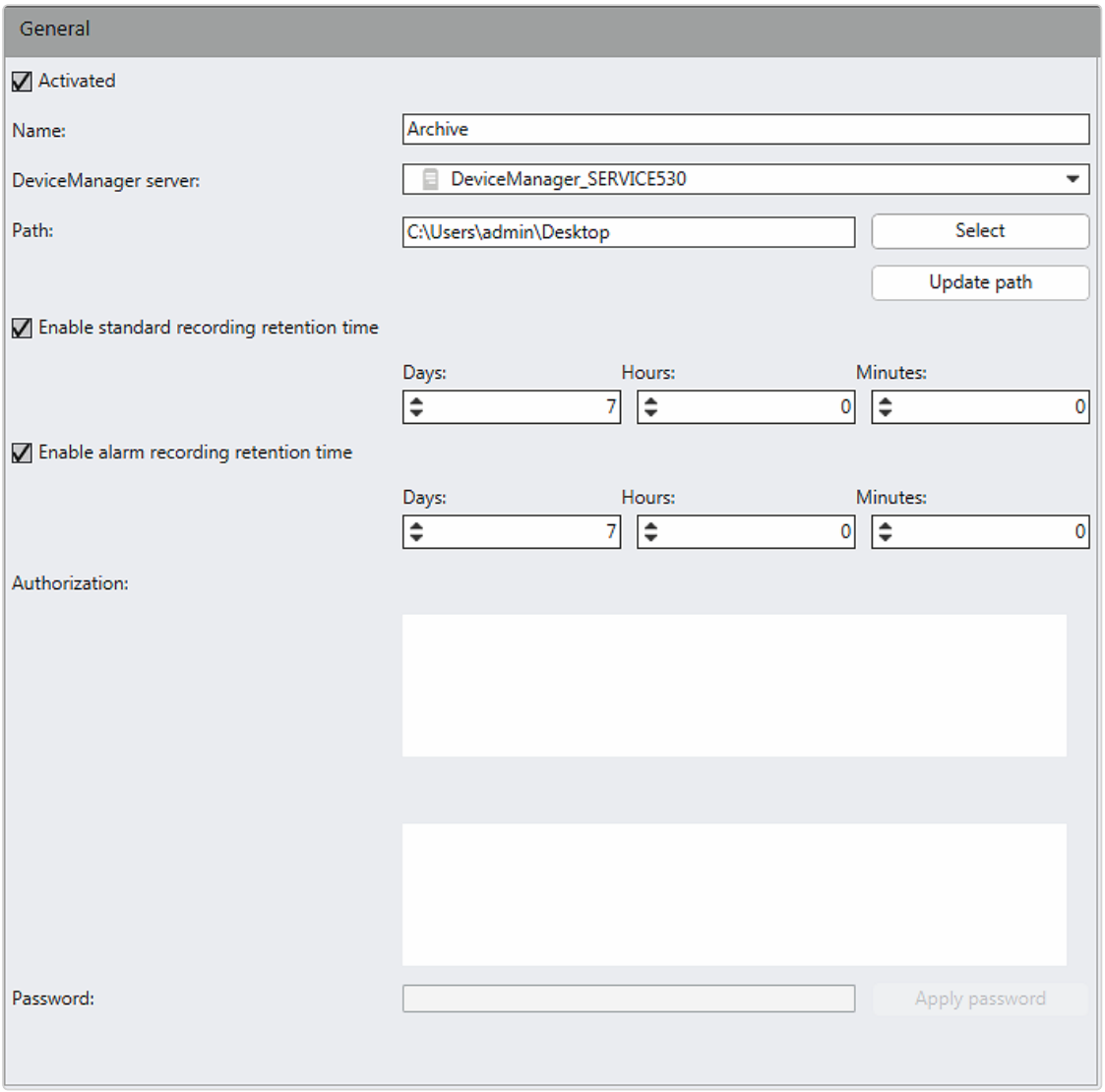


Fig. 134: Archive camera general settings

1. Activate or deactivate the camera.
2. If necessary, alter the **Name** of the camera.
3. If necessary, change the **DeviceManager server**.

   > **Changing the DeviceManager will delete all existing recordings.**

4. Define the input **Path**, where the recordings will be stored. You can search for the folder using **Select**.
5. To alter the file path, click **Update path**.
6. **Enable standard recording retention time** to specify the time frame for keeping the standard recordings.
7. Define the time frame in days, hours and Minutes.

8. **Enable the alarm recording retention time** to specify the time frame of keeping the alarm recordings.

The **Authorization** column shows the verified and unverified cameras found at the specified location.

9. Select an unverified camera and define the appropriate **Password** to validate the camera. This prevents unauthorized access to archive cameras.

> **The encryption uses AES 256 GCM with PBKDF2Sha256 as the password hashing algorithm.**

Configuring multiple cameras

To facilitate camera configuration, multiple cameras can be configured at once, even across different branches. However, not all settings are available. For the configuration of specific cameras, see "Configuring a camera" on page 223.

1. Close all camera configuration tabs.
2. Click **Cameras** in the company control.
3. Select the cameras you want to configure.
4. To configure multiple cameras at once, close all camera tabs in the work area.
5. Click **Edit**. The camera configuration view is displayed. Options that are not available on all selected cameras are greyed out. When configuring multiple cameras at once, only those settings can be changed that apply to all cameras.
6. Activate or deactivate the required settings. For setting details, see "Configuring a camera" on page 223.

Selecting and deselecting multiple cameras at once

1. To select a contiguous list of cameras, select the first camera in the camera control by clicking its check box. A check mark is displayed in the box.
2. Press the Shift key and select the last camera in the row by clicking its check box. All cameras in between are selected.
3. To deselect a contiguous list of cameras, deselect the first camera in the camera control by clicking its check box. The check box is empty.
4. Press the Shift key and deselect the last camera in the list by clicking its check box. All cameras in between are deselected.

5. Press the Shift key and click on the check box in front of the list name. All cameras are selected.

Moving cameras

You can move one or multiple cameras at once by cutting and pasting.

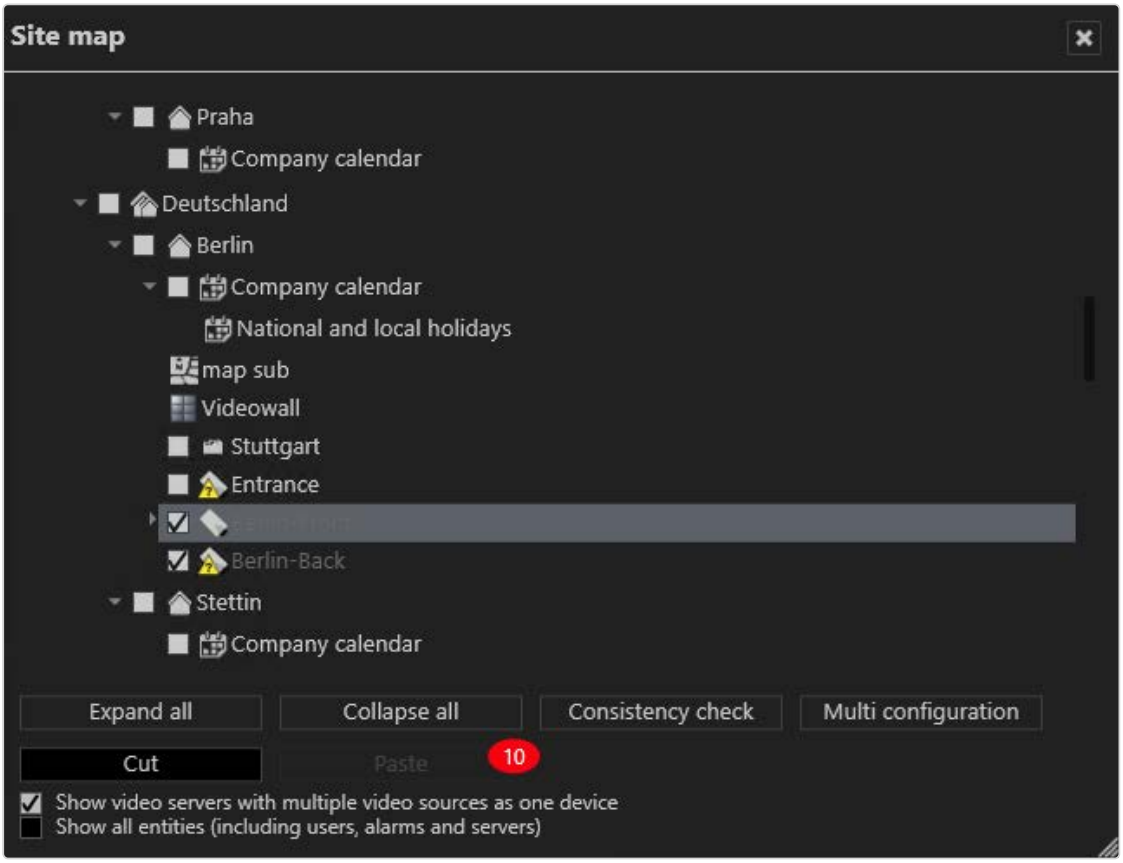


Fig. 135: “Moving” a camera

1. In the panel “Company”, select **Site map** .
2. Select the cameras by clicking the check boxes.
3. Select **Cut**. The selected items are grayed out and the number of selected items is displayed.
4. Select a branch or folder. Paste is enabled.

> **If more than 100 items are selected, a notice is displayed about the time the process takes to complete. Moving large numbers of entities can take a few minutes.**

5. Select **Paste** to move the cameras into the selected branch or folder.

Duplicating a camera

Duplicating a camera with the "Copying wizard" enables camera settings to be applied to a large number of identical cameras to save time.

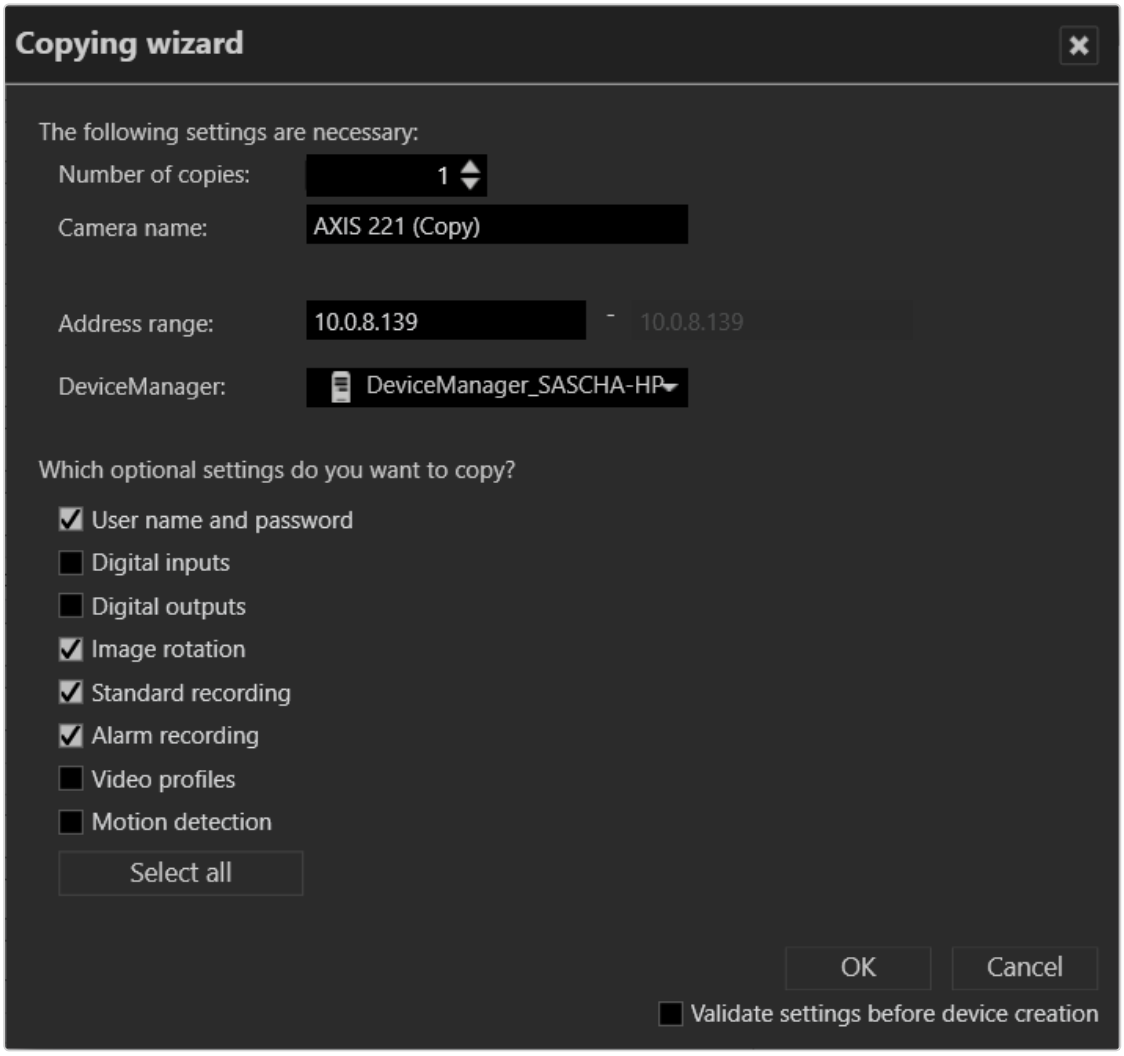


Fig. 136: Duplicating a camera

1. Select the camera in the overview.
2. Click **Duplicate object**, and specify the number of copies.
3. Enter the **name** of the duplicated camera. The names of the cameras are also assigned a number, which is automatically incremented. The name can also be changed after it has been set (see "Configuring a camera" on page 223)
4. Enter the IP address of the first copied camera in the **address range**. The IP addresses are automatically incremented based on the number of copies.
5. Select the **DeviceManager**.
6. Activate the properties that are to be transferred to the copied cameras.
7. Optionally, activate **Validate settings before device creation**.
8. Click **OK** to accept the name. The new camera is displayed in the overview.

Deleting a camera

1. Select the camera in the overview.
2. Click **Delete object**.

> **All saved recordings of the camera are deleted.**

Converting a camera

An installed camera can be converted into a new camera by transferring the camera configuration and recordings (driver conversion). Alarms, patrols and other settings are inherited by the new camera. This conversion can be used to install a new camera to replace a defective one.

> **Camera using the smart driver (generic driver) are not fully supported and may only be converted partially.**

> **If a native camera driver is converted into a smart driver, a RTSP stream has to be selected in the video stream configuration (see "Editing a video stream" on page 243).**

1. Select the camera in the overview.
2. Click **Open converter** in the general settings of the selected camera.

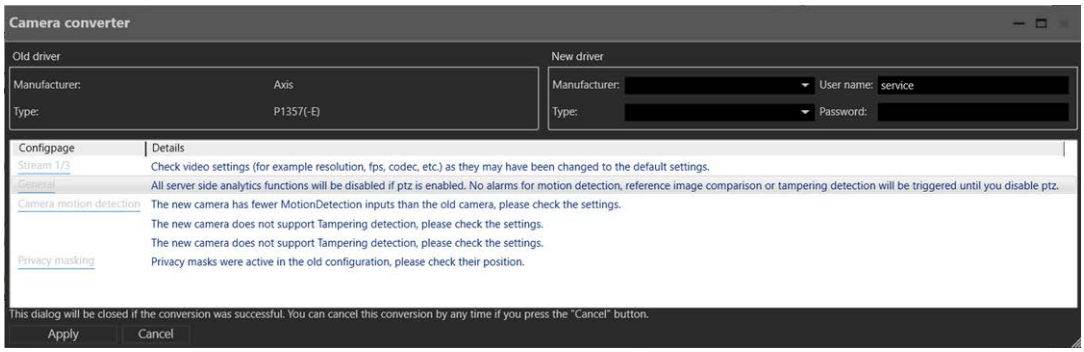


Fig. 137: Converting a camera

3. Select the **manufacturer** and the camera **type** of the new camera.
4. Enter **User name** and **Password**, if required.
5. Click **Verify conversion**. A list of possible conversion issues is displayed.
6. After resolving the issues, click **Apply** to start the conversion process.

Other hardware

The **Other hardware** function in the Administration control allows you to configure and manage additional devices. Additional devices include items such as network interfaces, video walls, alarm systems and I/O modules. The devices can be partly administered and actuated with Qognify VMS and also with software from third-party manufacturers.

1. Select the location in the **Company** control. The selected location is displayed in the title bar of the control bar.
2. Select **Other hardware** in the control bar.

Creating new hardware

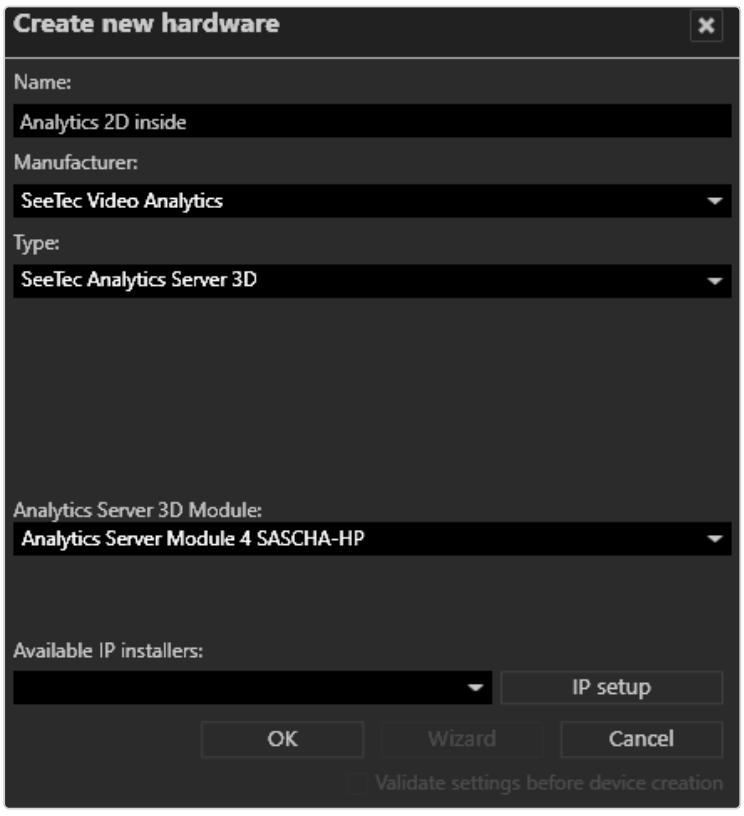


Fig. 138: Creating new hardware

1. Create a new hardware item.
2. Enter the **name** for the new hardware.

3. Select the **manufacturer** and **type** of the hardware. The following manufacturers and types are available:
   - **Third-party interface**: eyevis wall, SPC alarm system, Aritech Alarm Center, Schneider Intercom ICX Connection, Siemens SPC 4000/5000/6000.

     > **See Integrating other hardware or ask Qognify support about the use of third party interfaces.**

   - **Qognify**: network I/O, DisplayAgent and VoIP
   - **Qognify Video Analytics**: Generic VCA Channel, License plate recognition, LPR VCA, Qognify Analytics Basic / Enterprise / Premium, Qognify Analytics Server 3D
   - **Advantech**: ADAM 6050/6050W, ADAM 6052, ADAM 6060/6060W/6066
   - **AXIS:** A9161, A9188
   - **W&T**: WEB-IO 2x Digital IN/OUT
   - **Wago**: Wago System 750 I/O module
4. Select an **authorization**, if required, and enter a **user name** and **password**.
5. If necessary, enter the name of the **host** or the **IP address** of the device.
6. If necessary, select the **DeviceManager**.
7. Click **OK** to confirm your entries. The new hardware is displayed in the overview.

Configuring hardware

1. Select the hardware in the **Other hardware** overview.
2. Edit the settings for the hardware. The following options are available:
   - "Third-party interfaces" on the next page
   - SeeTec
   - "Qognify Video Analytics" on page 290
   - "Advantech" on page 314
   - "AXIS" on page 316
   - "W&T" on page 318
   - "Wago" on page 320

Deleting hardware

1. Select the hardware in the **Other hardware** overview.
2. Click the **Delete object** icon.

Third-party interfaces

This section includes the configuration of the following interfaces:

- Aritech Alarm Center
- eyevis Wall
- Schneider Intercom ICX Connection
- Siemens SPC 4000/5000/6000
- TDSi access control

Third-party interfaces have to be pre-configured on the side of the third-party component. This section describes only the configuration in Qognify Qognify VMS.

For configuration of the third-party interfaces of the components, see "Technical_Guides_Qognify_Qognify VMS_7.5_EN.pdf" or contact support (see "Support" on page 13).

Aritech Alarm Center

The Aritech Alarm Center sends alarms and events via the OH network receiver to the Qognify system, which acknowledges the events and processes them in the form of alarm scenarios. All messages sent to the Qognify system by the Aritech Alarm Center must acknowledged by Qognify VMS, otherwise they are sent again. The connection is unidirectional.

The systems communicate via TCP using the Security Communications Protocol - “SIA Format” Protocol - for alarm system communications, SIA DC-03-1990.01(R2003.10).

For installation or configuration of the Aritech Alarm Center, see "Technical_Guides_Qognify_Qognify VMS_7.5_EN.pdf" or contact support (see "Support" on page 13).

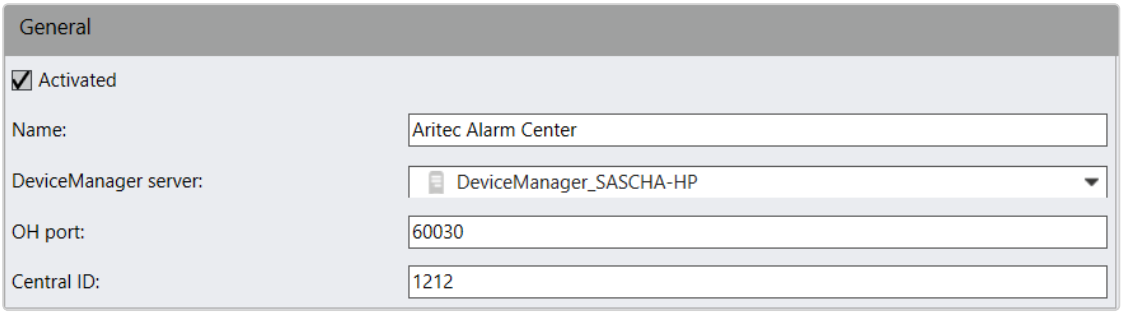


Fig. 139: Configuring the Aritech Alarm Center - 1

1. Add a new **Other hardware manufacture**r by selecting "3rd Party Interface" and **Type** "Aritech Alarm Center".
2. Choose which **DeviceManager server** should manage the Alarm Center. The Aritech System has to send its events to this server.
3. Enter the **OH port** for the events to be sent to from the OH network receiver via the logging appender. The port can be found in the file seetec.properties. This file can be found in the installation directory of the OH Network Receiver.
4. Enter the **Central ID**.

   > **You will receive this ID from the installer of your Aritech Alarm Center.**

Rules

A rule consists of a name, a zone ID, an area ID and an event.
The following items from the Aritech Alarm Center events can be used in a rule:

- Alarm [SIA code: BA]: Alarm
- Tamper [SIA code: TA]: Tamper events
- Armed [SIA code: CL]: Alarm center is armed
- Disarmed [SIA code: OP]: Alarm center is unarmed
- Mask [SIA code: BT]: A sensor reports that a zone is masked
- Excluded [SIA code: BB]: Zone was deleted
- Arm Forced [SIA code: CF]: Alarm center is armed although there are open problems

Creating rules

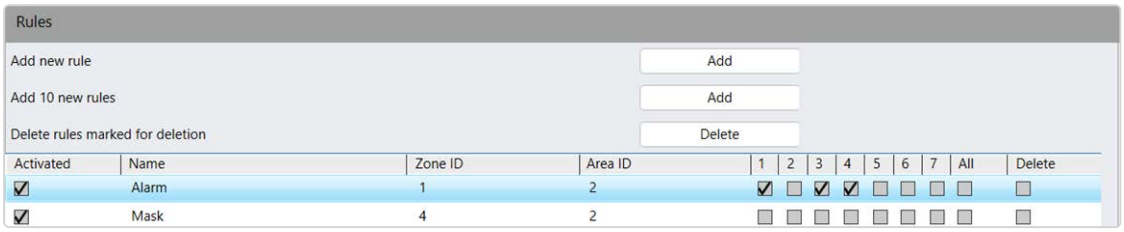


Fig. 140: Configuring the Aritech Alarm Center - 2

1. Select **Add one rule** or **Add 10 rules**.
2. Activate the rule.
3. Enter a rule name.
4. Enter **Zone ID** to the corresponding zone.
5. Enter **Area ID** to the corresponding area.
6. Select the desired event (column ‘1’- ‘7’). Multiple selections are possible. You will receive the zone ID and area ID from the installer of your Aritech Alarm Center.

eyevis wall

eyevis provides video wall systems that are controlled by a Qognify VMS client.

General

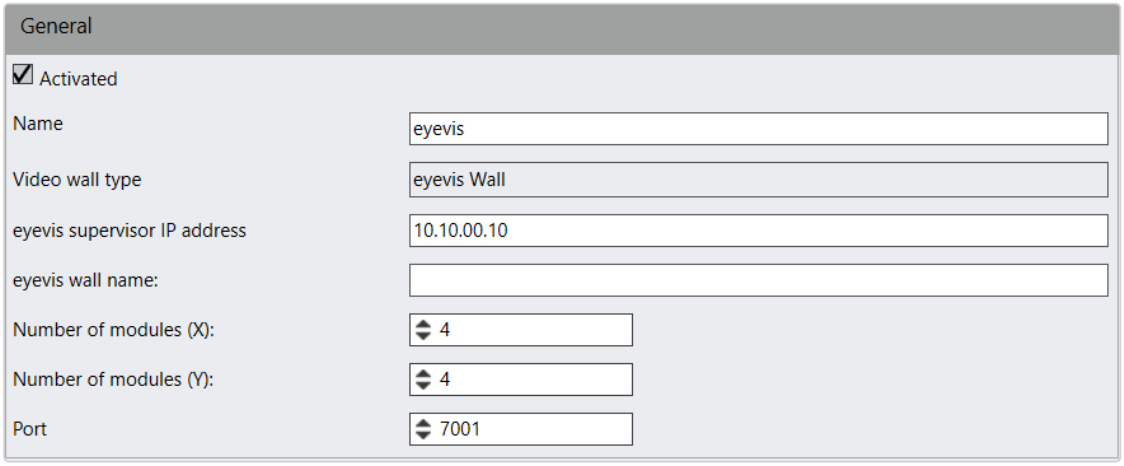


Fig. 141: General

1. Activate or disable the module.
2. If necessary, alter the **name**.
3. Enter the **eyevis supervisor IP address**.
4. Specify the **eyevis wall name**.

5. Split the available image area on the eyevis video wall into individual video wall modules by entering the values for **Number of modules (X)** and **Number of modules (Y)**.
6. Enter the port at which the **eyevis supervisor** can be reached.
7. **Apply** the set values if you want to make further settings.
8. **Save** the set values to apply the values and conclude input.

> **Additional settings have to be configured in the video wall configuration (see "Video walls" on page 398).**

Schneider Intercom ICX connection

For the communication with the Schneider Intercom a proprietary protocol is used (ICX protocol, version 1.1/0910 "PRELIMINARY"). The events are provided via this protocol. There is no conversation data within the protocol stream, only information like “X establishes a connection with Y“. There are no active protocol features implemented. This Qognify VMS server is only listening for events. Qognify VMS is not able to send any commands to the Schneider Intercom Server.

> **For installation or configuration of the Schneider Intercom ICX connection, see "Technical_Guides_Qognify_Qognify VMS_7.5_EN.pdf" or contact support (see "Support" on page 13).**

General

The Schneider Intercom device server is configured by the separately provided Schneider software. The terminal identification is also carried out with the Schneider software.

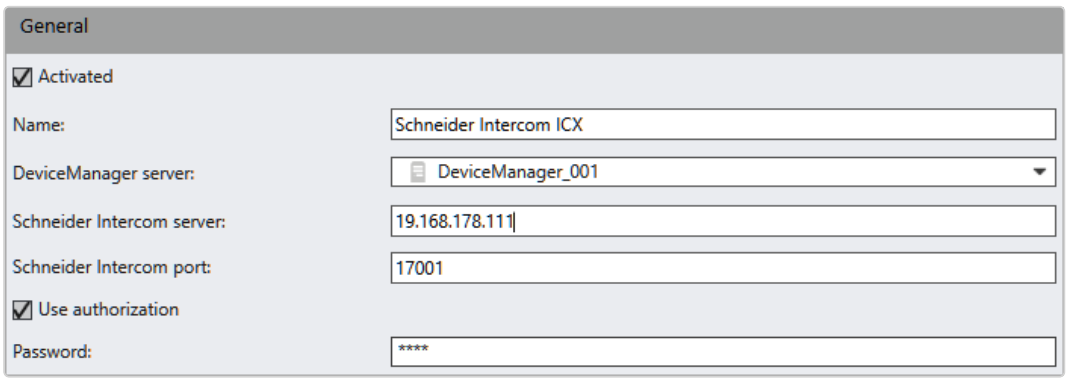


Fig. 142: Schneider Intercom ICX connection - General

1. Create a new module with the following settings:
   - Manufacturer: 3rd Party Interface
   - Type: Schneider Intercom ICX
2. Activate the module.
3. Select the **DeviceManager** to manage the Schneider device.
4. At **Schneider Intercom server** and **Schneider Intercom port** enter the IP address and the port of the Schneider Intercom server.
5. Optionally, activate **Use authorization** to restrict access and enter the password.

Rules

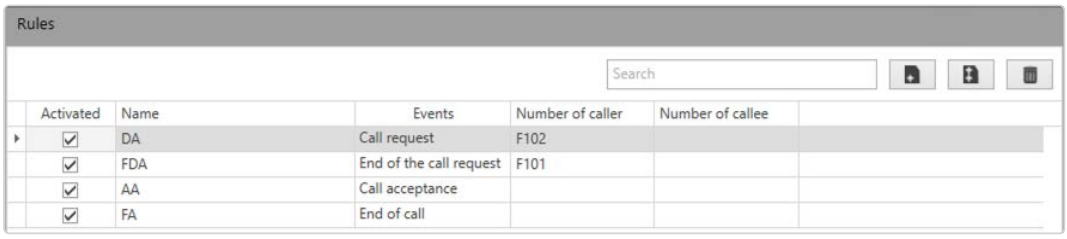


Fig. 143: Schneider Intercom ICX connection - Rules

A rule consists of a name, an event-type, and a caller or callee number.

1. To add a rule, select **Add** .
2. To add multiple rules (10) at once, select **Add multiple rules** .
3. To delete a rule or multiple rules, select the rules and click **Delete** .

4. Specify the following events to be managed by Qognify VMS within a rule:
   - Nothing selected
   - Call request (ICX Code Task 5B Type 21)
   - End of call request (ICX Code Task 5B Type 30)
   - Call acceptance (Connection is started) (ICX Code Task 42 Type 12)
   - End of call (ICX Code Task 42 Type 10)
   - Call discrete ((ICX Code Task 42 Type 13))
   - Call group (ICX Code Task 42 Type 0B)
   - Call request emergency (ICX Code Task 5B Type 22)

   > **From Qognify VMS R12 onward, "Call 2" is handled in a different event, customers may need to change their existing configuration. Before the change, "Call 2" was included in the normal "Call" event, now it is an event on its own.**
5. Enter the caller and the callee numbers. There are two possible data formats: 4-digit and 8-digit hexadecimal digits.
6. Fill the unused digits with “F” to a full block.

> **Example**
>
> | Number (=terminal ID) | >4 digits | 8 digits |
> |---|---|---|
> | 101 | F101 | - |
> | 12321 | - | FFF12321 |

7. Create an alarm scenario and select the according rule as start-event (see "Creating an alarm scenario" on page 357).

Siemens SPC 4000/5000/6000

The Siemens alarm center can send alarms and events to the Qognify VMS system. The Qognify VMS system acknowledges the events and can process them in the form of alarm scenarios.

General communication between the two systems is via TCP. The Siemens alarm center always establishes a TCP connection. All messages sent to the Qognify VMS

system by the Siemens alarm center are acknowledged by Qognify VMS, otherwise they are sent again.

General

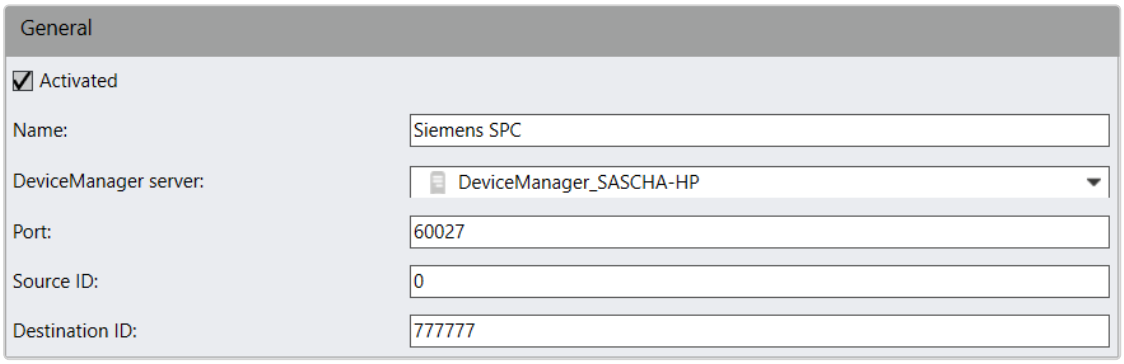


Fig. 144: General

1. Activate or disable the module.
2. If necessary, alter the **Name**.
3. If necessary, change the server for managing the devices (**DeviceManager**). The alarm system sends the messages to this server.
4. If necessary, change the receiver IP **Port** for the transmission of messages from the Intrusion Control Panel (Standard: 60027). Use a separate port for each Intrusion Control Panel.
5. Enter the installation ID as **Source ID**. This ID is used to acknowledge messages. The IDs must be identical in Qognify VMS and in the Siemens Intrusion Control Panel. The source ID can be found in the configuration of the SPC alarm system.
6. Enter the receiver ID as **Destination ID**. The destination IDs must be identical in Qognify VMS and in the Siemens Intrusion Control Panel (default: 777777). The destination ID can be found in the configuration of the SPC alarm system.

> **The corresponding module entries of the SPC alarm system (source ID) and the entries of the Qognify system (destination ID) must be identical.**

Areas

You can activate up to 64 areas for each Intrusion Control Panel. Each area can be set to armed or disarmed and can be used as a trigger event for a Qognify alarm scenario.

Fig. 145: Areas

1. Activate the area and enter the **name of arming** and the **name of disarming**. If an event is triggered, the term specified is displayed instead of a number (e.g. "window open" or "window closed").

The state of an area can be visualized in the map (see "Maps and "Advanced Maps"" on page 377). The area is shown red (armed) or green (unarmed) after 10-15 seconds.

Rules

A rule consists of a name, an event type, and a corresponding zone. A rule represents a zone. It is called a rule because each zone can have one type but two events (alarm / restore). Therefore two different types are needed in Qognify VMS to use them with alarm scenarios.

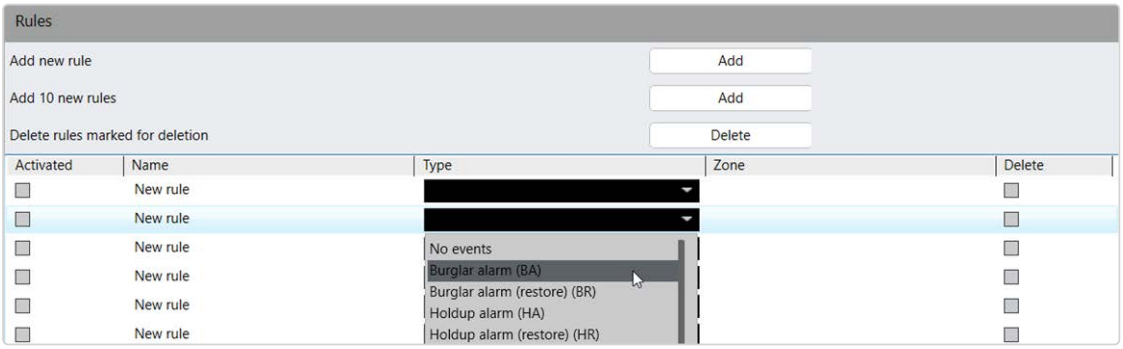


Fig. 146: Rules

1. Click **Add new rule** or **Add 10 new rules** to create one or ten new rules.
2. Activate the desired rules and change the **name**.
3. Select the **event** that is to trigger an alarm message. The alarm system distinguishes between the burglar alarm and panic alarm events. Specify the type of alarm in the rule.
4. Enter the **detector group** to set the ID of the device that sends the alarm signal.
5. **Apply** the set values if you want to make further settings.
6. **Save** the set values to apply the values and conclude input.

The following event types sent by the Siemens Intrusion Control Panel can be processed as rules by Qognify Qognify VMS:

- Burglar alarm (BA)
- Burglar alarm restore (BR)

- Panic alarm (PA)
- Panic alarm restore (PR)
- Medical alarm (MA)
- Medical alarm restore (MR)
- Sabotage alarm (BT)
- Sabotage alarm restore (BJ)
- Sabotage alarm (TA)
- Sabotage alarm restore (TR)
- Technology alarm (UA)
- Technology alarm restore (UR)
- Holdup zone fault (HT)
- Holdup zone fault restore (HJ)
- Panic zone fault (PT)
- Panic zone fault restore (PJ)
- Medic zone fault (MT)
- Medic zone fault restore (MJ)
- Technology fault / sabotage (UT)
- Technology fault / sabotage restore (UJ)
- Network connected (NR)
- Network disconnected (NT)

Outputs

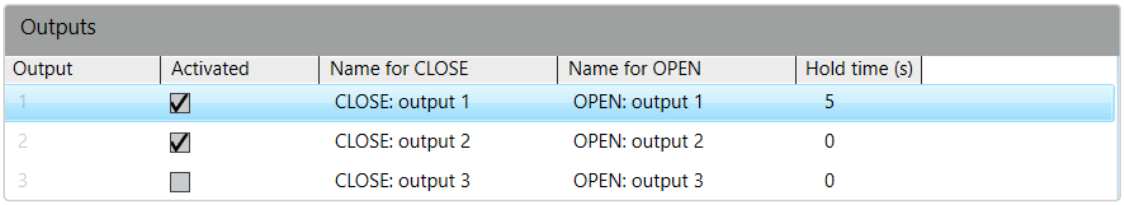


Fig. 147: Outputs

You can activate up to 8 outputs for each SPC panel. Each one can be set to CLOSE or OPEN.

1. Activate the output
2. Optionally, change the names

Hold time is not used in Qognify VMS but configured in the SPC panel.

TDSI Access Control

TDSi is an access control system from Time and Data Systems International Limited.
The TDSi system is connected by the export of the text-files from TDSi which are read by the Qognify system.

Configuring the TDSi connection

1. Create a new module with the following settings:
   - Manufacturer: 3rd Party Interface
   - Type: TDSi access Control

General

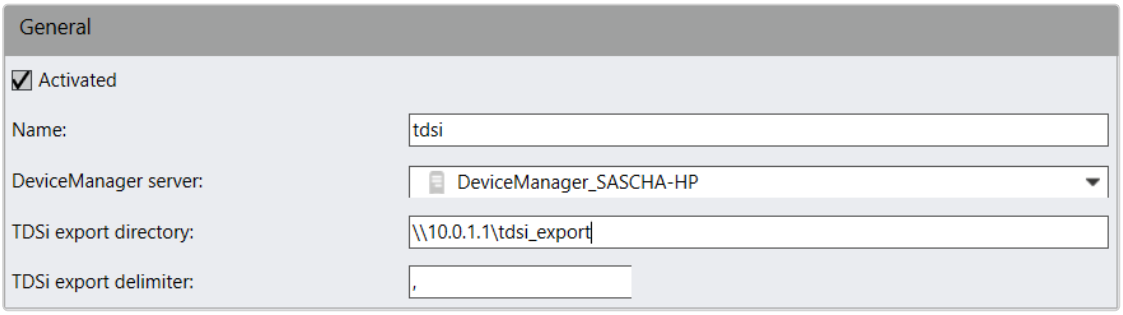


Fig. 148: TDSI Access Control - General

1. Activate access control.
2. Optionally, change the **name** of the device.
3. Select the **DeviceManager server** to manage the TDSi connection.
4. Specify the **TDSi export directory** where the EXgarde Event Exporter will store events.
5. If the directory was not created locally on the Qognify server, enter the full UNC path.
6. Enter the **TDSi export delimiter**.

Event groups

Creating of event groups is optional. Event groups will be used in a rule as starting event for alarm scenarios. Thereby always the same alarm scenario can be started, regardless of the event.

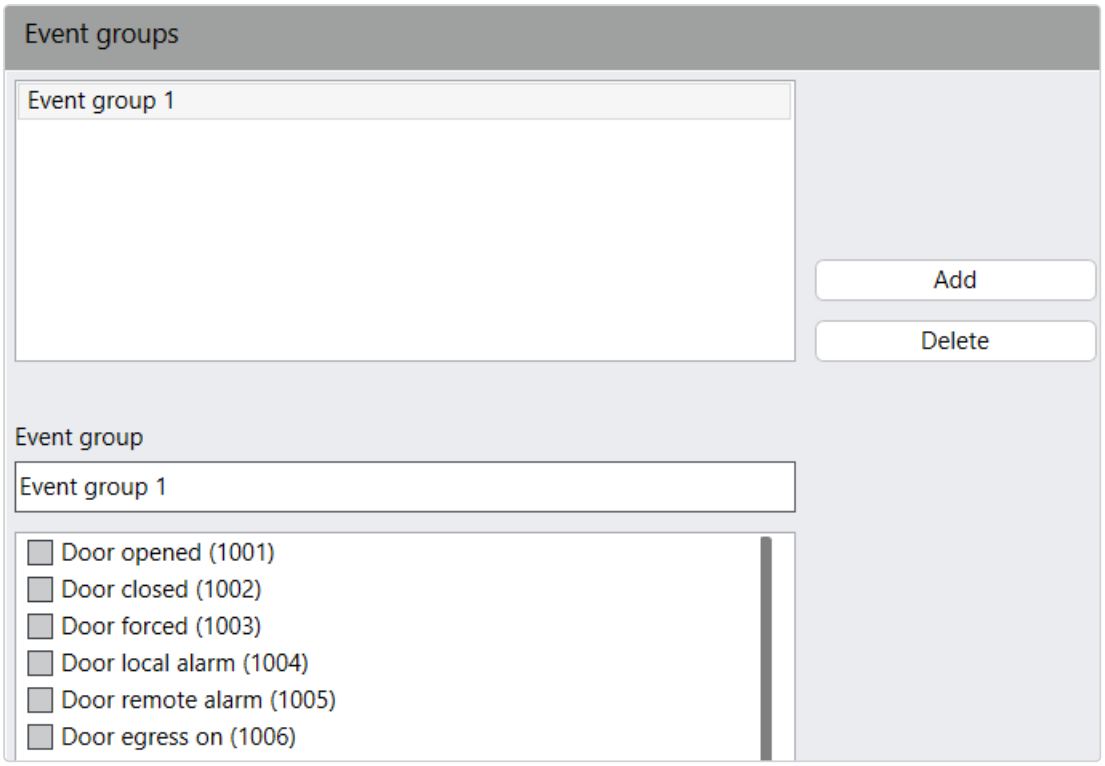


Fig. 149: TDSI Access Control - Event groups

1. To create a new event group, click **Add**.
2. Set the name of the event group in the text field.
3. In the **Event group** list, select one or more events assigned to the event group.

Rules

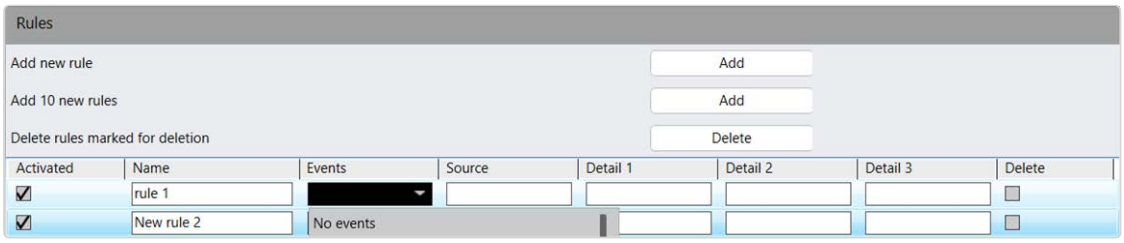


Fig. 150: TDSI Access Control - Rules

1. Click **Add one rule** or **Add 10 rules** to add one or 10 rules at once.
2. Set the name of the rule in the **Name** column of the table.
3. For the event, select a single event or an event group that you have previously created.

4. Optionally, fill out **Source**, **Detail 1**, **Detail 2** and **Detail 3** fields. The fields correspond to the fields in the EXgarde Explorer overview.

> **The case (upper/lower case) in the field “Source” as well as Detail 1 through Detail 3 must be exactly the same in the EXgarde Event Exporter and the Qognify configuration. Otherwise the alarm scenario will not be triggered.**

> ### Example
>
> Door opened is selected as Event, Front Entrance is selected as Source and user Testuser as Detail 1.
> The corresponding alarm scenario will only be started when user Testuser opens the door Front Entrance.

Qognify

Other hardware from Qognify includes the configuration of

- Network input and output
- DisplayAgent video wall
- VoIP

For a description on how to configure, refer to the sections below.

Qognify network I/O

Qognify can provide network I/O, e.g. to trigger a hardware function over the network.

General

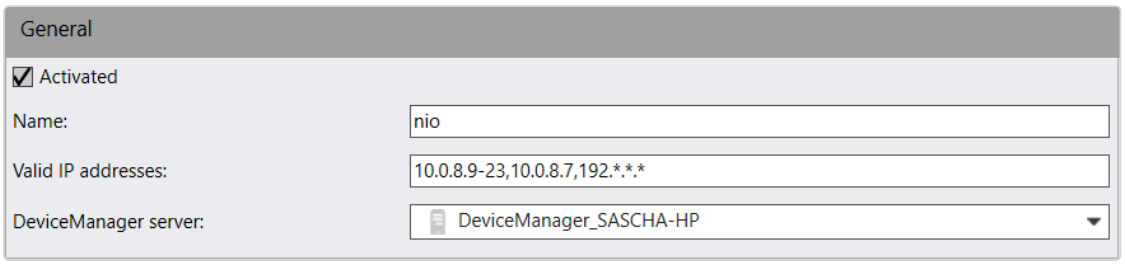


Fig. 151: General

1. Activate or disable the module.
2. If necessary, alter the name.
3. If necessary, enter the **valid IP addresses** or IP address ranges to create a mask within which input operations are to be run. This is optional. You can specify any number of masks separated by commas (no spaces). The placeholders * and - can be used in a mask. If no mask is assigned, every incoming connection is accepted.

   > *Example*
   > *10.0.8.9-23,10.0.8.7,192.*.*.**
   > *Three restrictive masks have been defined:*
   > *Mask 10.0.8.9-23 allows all IP addresses in the range 10.0.8.9 to 10.0.8.23.*
   > *Mask 10.0.8.7 allows the individual IP address.*
   > *Mask 192.*.*.* allows the complete sub-net 192.*

4. If necessary, change DeviceManager server (see "Installation of a distributed server" on page 38).

Inputs

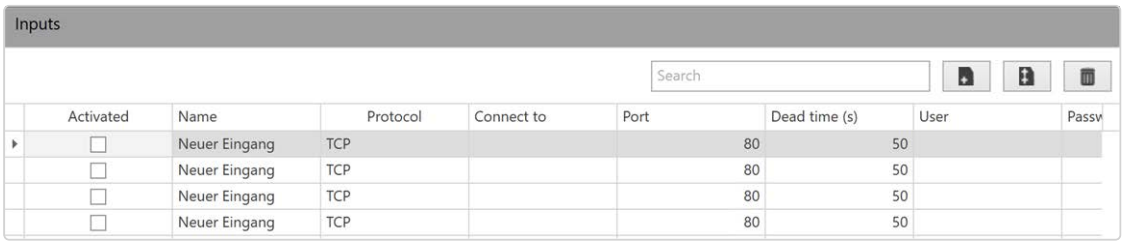


Fig. 152: Inputs

1. Click **Add new input** or **Add 10 new inputs** to create one or ten new inputs.
2. Click **Activated** to activate or deactivate an input. To set the activation state for multiple inputs, hold down the shift or control key on the keyboard while selecting other inputs.
3. Change the **Name** of the input.
4. Select the network **Protocol** for the input. The following protocols are available:
   - TCP for connections within the network,
   - TCP (permanently) for permanent connections within the network,
   - HTTP for connections over the Internet.
5. In column **Connect to** enter the IP address and the **port** number for the incoming input connection.
6. Specify the interval for the **Dead time** (in seconds) after which a signal is analyzed again.
7. If the HTTP protocol is selected, enter the **User** name and **Password** for accessing the hardware.
8. Select the **Type** of the text which can be transmitted, when there is an input connection. If ASCII is selected, only upper- and lower-case letters and numbers can be used, not special characters. With HEX, all characters are permissible.
9. Enter the **text** to be displayed as soon as the hardware is accessed
10. Optionally specify the **Control characters** encoding for the correct display of paragraph changes, for example.
11. To delete inputs, select the inputs you want to delete, and click **Delete** inputs marked for deletion. To delete multiple inputs hold down the shift or control key while selecting the inputs.

Outputs

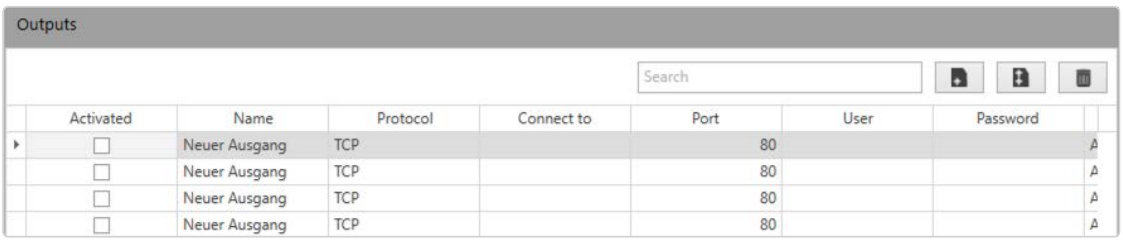


Fig. 153: Outputs

1. Click **Add new output** or **Add 10 new outputs** to create one or ten new outputs.
2. Click **Activated** to activate or deactivate an output. To set the activation state for multiple outputs, hold down the shift or control key while selecting the outputs

3. .Change the **name** of the output.
4. Select the network **Protocol** for the output. The following protocols are available:
   - TCP for connections within the network,
   - HTTP for connections over the Internet,
   - HTTPS for encrypted connections over the Internet.
5. Enter the IP address and the port number with which the output is to establish a connection. You can assign the same IP address to multiple outputs.
6. If the HTTP or HTTPS protocol is selected, enter the **User name** and **Password** for accessing the hardware.
7. Select the **Type** of password encryption. If ASCII is selected, only upper- and lower-case letters and numbers can be used, not special characters. With HEX, all characters are permissible.
8. Enter the **Text** to be displayed as soon as the hardware is accessed.
9. To delete outputs, select the outputs you want to delete, and click **Delete outputs marked for deletion**.To delete multiple outputs hold down the shift or control key while selecting the outputs.

Qognify DisplayAgent (video wall)

The Qognify DisplayAgent is integrated in the Qognify client. With the DisplayAgent any client computer (see "System requirements" on page 31) and the connected monitors can be used as a fully featured monitor wall.

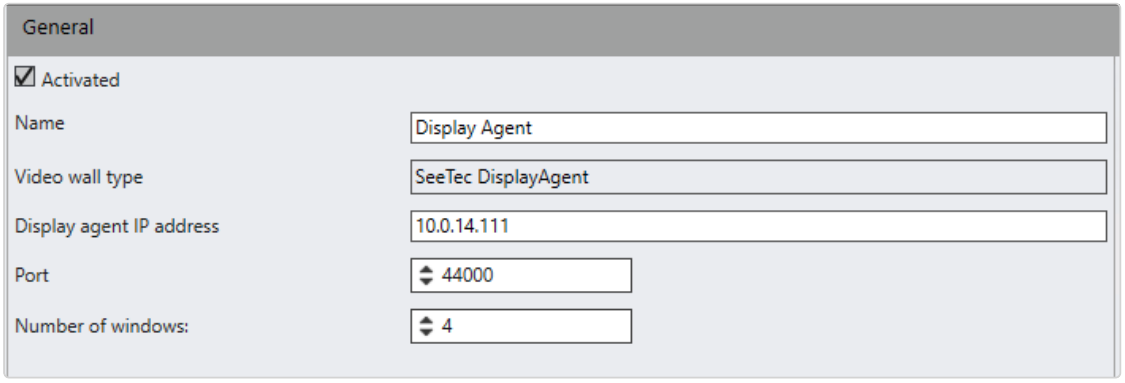


Fig. 154: Qognify DisplayAgent (video wall)

1. Activate or disable the module.
2. If necessary, alter the **name**.
3. If necessary, change the **IP address** of the computer on which the Qognify DisplayAgent is installed.

4. Specify **the number of windows** to set the monitors on the computer on which the Qognify DisplayAgent was installed. It is recommended to specify one window per monitor.

> **Further settings have to be done in the video wall configuration (see "Video walls" on page 398)**

VoIP

The configuration sets suitable hardware (VoIP-capable devices such as Mobotix cameras and door intercom systems).

General

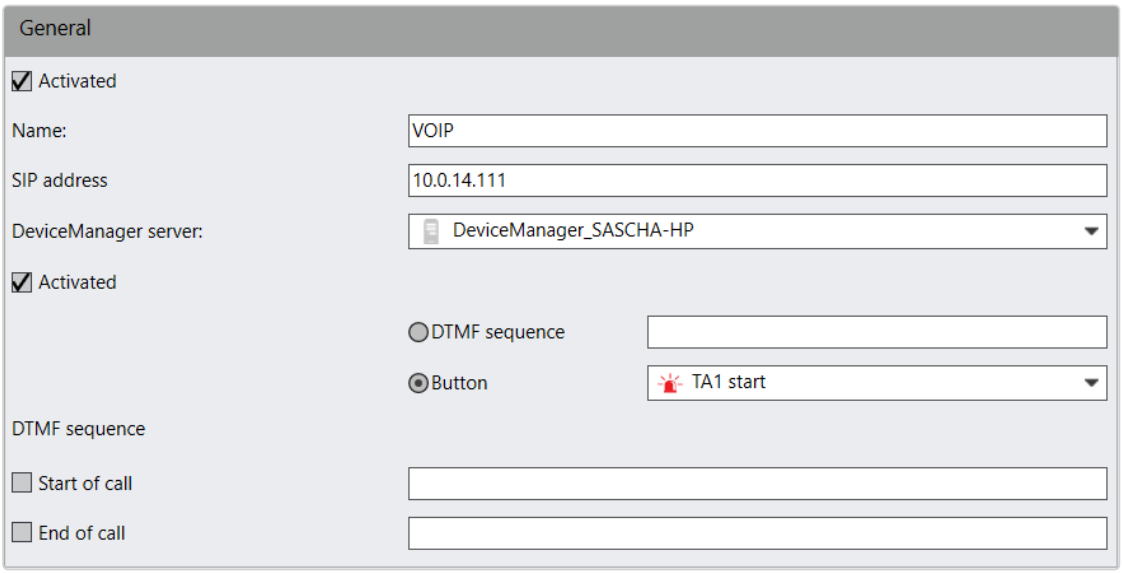


Fig. 155: General

1. Activate or disable the module.
2. If necessary, alter the **Name**.
3. If necessary, change the **SIP address** of the computer on which the VoIP is installed.
4. Select the **DeviceManager**.
5. Select **Activate** define whether the DTMF function key in surveillance mode (see "Audio" on page 154) is to trigger a **DTMF sequence** or a **Button**.

- If necessary, specify the DTMF sequence, which can be found in the manual supplied by the device manufacturer, or select a Qognify button (see "Configuring a button" on page 386).

6. Specify the **DTMF sequences** for the start and end of the call. The DTMF Sequence is to be send by the client in surveillance mode when starting or ending a call (see "Audio" on page 154).

Voice over IP recording

Voice over IP sessions can be defined as standard VoIP recordings or Alarm VoIP recordings.

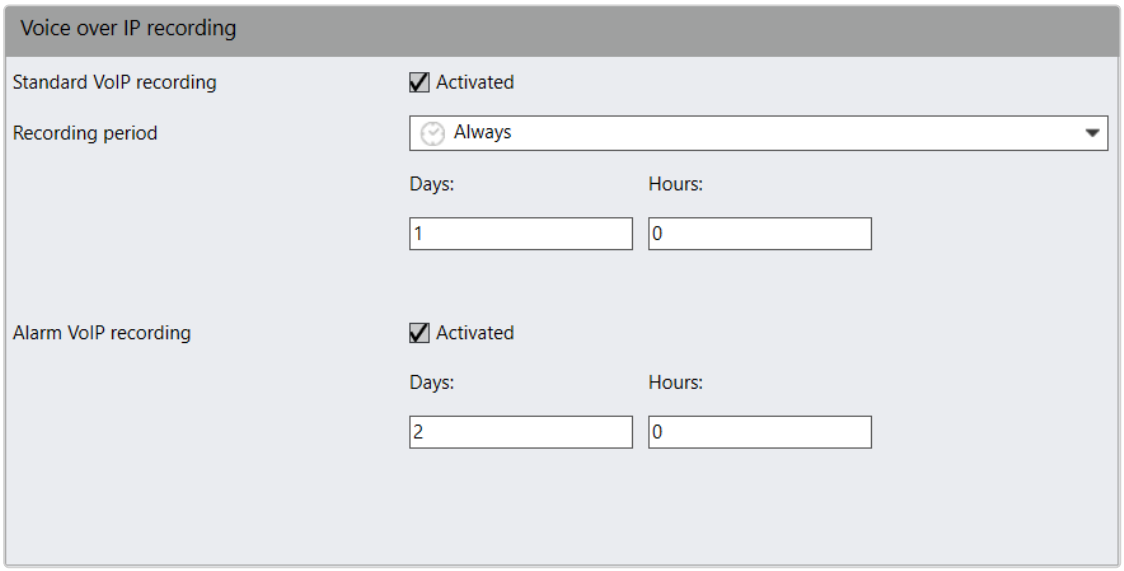


Fig. 156: Voice over IP recording

1. Activate **Standard VoIP recording**, select the **Recording period** depending on a time template (see "Time management" on page 351).
2. Enter the maximum number of days and hours for the total recording time.
3. Activate **Alarm VoIP recording**.
4. Enter the maximum number of days and hours for the total recording time.
5. **Apply** the set values if you want to make further settings.
6. **Save** the set values to apply the values and conclude input.

Qognify Video Analytics

Because the attention of the observers falls as the number of monitors that are observed increases, the Qognify VMS software gives you the option of performing intelligent video analysis. Intelligent video analysis reduces the stress on the personnel and significantly improves the surveillance quality.
The section SeeTec Video Analytics includes the configuration of:

- Generic VCA channel (see "Generic VCA channel" below)
- License plate recognition (see "License plate recognition" on page 293)
- LPR VCA (see "LPR VCA - License plate recognition" on page 297
- Qognify Analytics (obsolete, no longer distributed) (see "Qognify Analytics" on page 301)
- Qognify Analytics Server (see "Qognify Analytics Server" on page 309)

For performance reasons, the video analysis modules should be installed on a dedicated server (see "Custom installation" on page 41).

Generic VCA channel

The generic VCA (Video Content Analytics) channel module is used to connect APIs from third-party suppliers via Qognify Application Interface (QAI). The interface sends image data to Qognify Qognify VMS and receives events that, for example, require an alarm to be triggered.

To configure a generic VCA channel module, you first have to create it in the Qognify VA administration tool (see "Qognify VMS VA Administration Tool" on page 476).

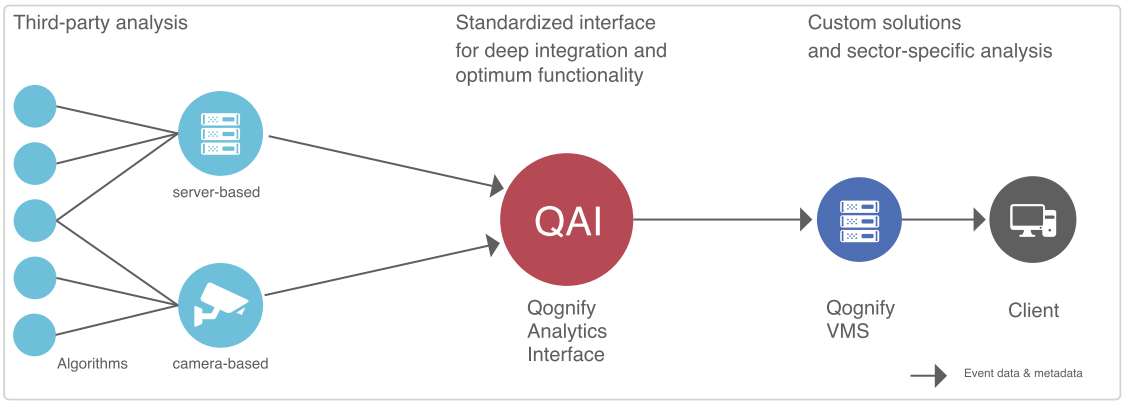


Fig. 157: Generic VCA channel

The QAI (Qognify Analytics Interface) provides the following plug-ins:

- **IPS / Axis**: for cameras with on-board image analysis, metadata are triggered (tracking data can be visualized in Qognify VMS)
- **IVA / Bosch**: for Bosch cameras with on-board image analysis
- **CogVis**: image analysis is server based
- **Traficon Flir**: Flir cameras with on-board image analysis. The Traficon plug-in is used for traffic analysis.
- **SafeZoneEdge** (compliant with ACAP version 1.0.4521)

- **AxisPerimeterDefender** (compliant with the ACAP Axis Perimeter Defender version 2.7.2).

In order to be detected correctly when the software starts up, the API must be stored in the "\VersatileApplications\VCAPlugin" sub folder of the Qognify installation folder.

General

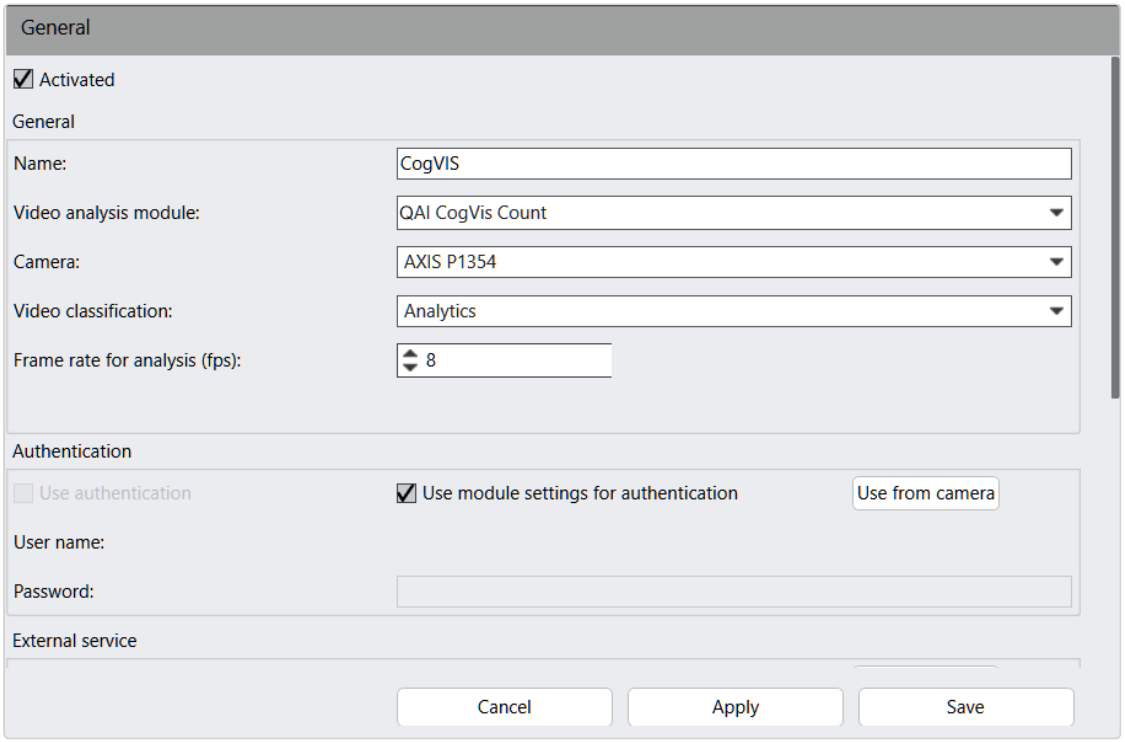


Fig. 158: Generic VCA channel - General

1. Activate the module and, if necessary, alter the **name**.
2. Select the **Video analysis module**.
3. Select the appropriate **camera**.
4. Select the appropriate **Video classification**. The video classification determines which video stream is used in surveillance mode for the various modes (normal, selected, alarm).
5. Enter the **Frame rate for analysis (fps)**. A different frame rate than the one configured in the selected video classification only influences MJPG based video streams.
6. **Apply** the set values if you want to make further settings.
7. **Save** the set values to apply the values and conclude input.

For information about configuring third party analytics systems, see "Technical_Guides_Qognify_Qognify VMS_7.5_EN.pdf" or contact support (see "Support" on page 13).

License plate recognition

The Qognify LPR module (License Plate Recognition) is an add-on module for Qognify VMS for the automatic recognition of license plates in stationary and moving traffic. It can read international license plate formats, including even with Arabic and Cyrillic characters, on up to eight lanes per server.

The module is configured entirely in the Qognify VMS client, and the recognition of the plates is carried out either continually or trigger-controlled. The LPR module can be used with any IP camera supported by Qognify VMS and is integrated into the system. For optimal detection even in difficult light conditions, special LPR cameras (IP cameras or analog cameras via video encoders) should be used.

All LPR related events like license plate from a certain list, unknown license plate, license plate on the wrong lane etc. can be used to trigger an alarm.

To configure an LPR module, you first have to create it in the Qognify VMS VA administration tool (see "Qognify VMS VA Administration Tool" on page 476).

Lane configuration

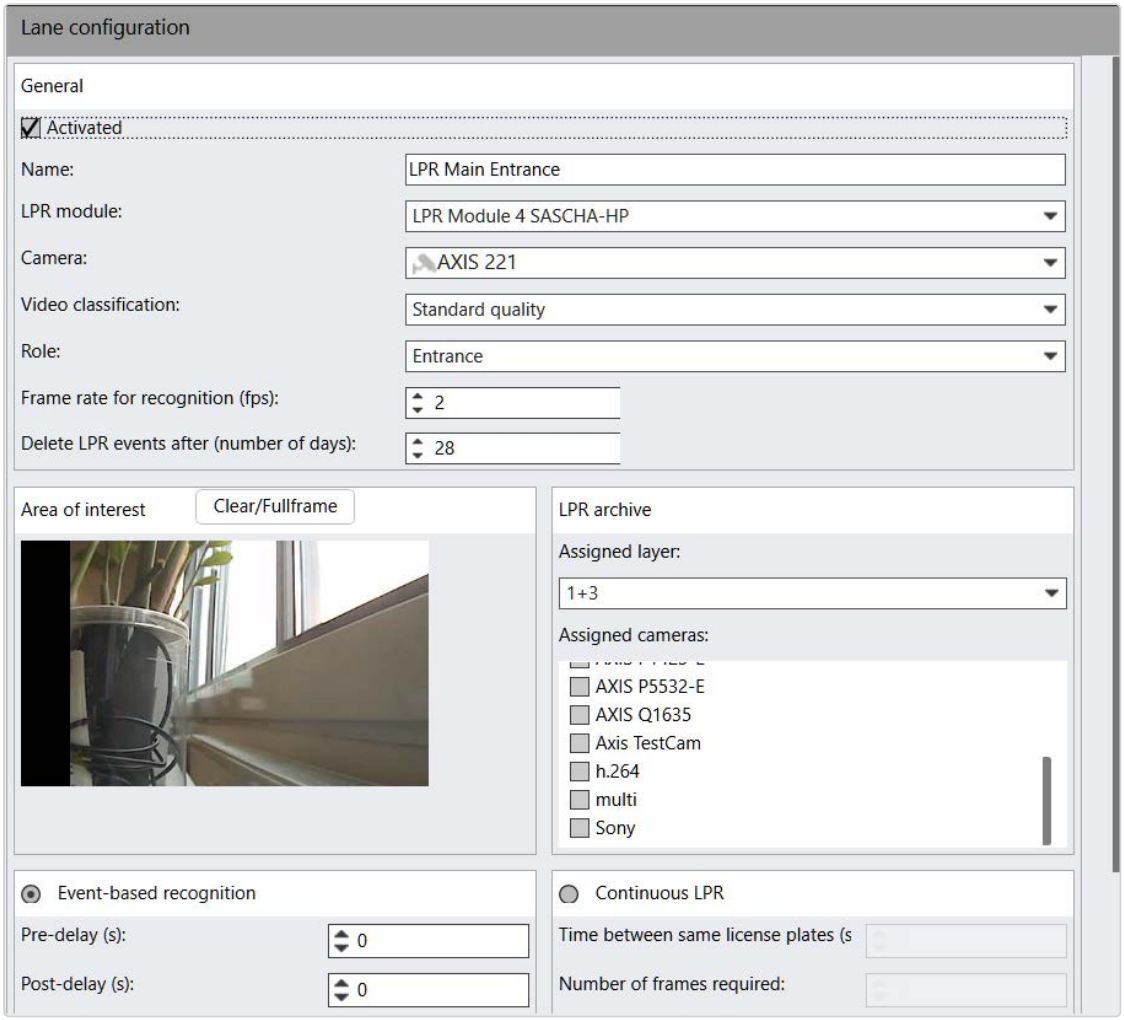


Fig. 159: Lane configuration

1. Activate the module and, if necessary, alter the **name**.
2. Select the appropriate **LPR module**.
3. Select the appropriate **camera**.
4. Select the appropriate **video classification**. The video classification determines the video profile used in surveillance mode for the various modes (normal, selected, alarm). With MPEG-4, H.264 or H.265 streaming the frame rate for recognition must correspond to the frame rate for default recording on the selected camera, while any desired value can be entered for Motion JPEG.
5. Select the desired **role**. For example, in LPR mode you can restrict the search to all entrances and you do not need to selected every entrance lane manually.

6. Enter the **frame rate for recognition** to specify the number of images per second that are to be transmitted to the module. With MPEG-4/H.264 streaming the frame rate for recognition must correspond to the frame rate for default recording on the selected camera, while any desired value can be entered for Motion JPEG.
7. Specify the number of days after which LPR events (recognized license plates, changes to master data, etc.) are to be deleted.
8. Select the **assigned cameras** and **assigned layers** that are to be displayed in LPR mode in addition to the camera.
9. Select **Event-based recognition** or **Continuous LPR**. With event-controlled recognition license plate recognition is only started after an event, e.g. if a vehicle passes through a light barrier. The event-based recognition is triggered e.g. by an alarm scenario.

   > **For performance reasons the use of event-based recognition is strongly recommended.**

10. Enter the **pre-delay** and the **post-delay** in seconds for event-based recognition. This period is used for recognition of the license plate, i.e. the images of this period are sent for OCR recognition.
11. Activate **Export at next trigger event.** As soon as this function is activated, the images are exported at the next trigger event to the LPR mode for license plate recognition and stored in the "VersatileApplications" folder in accordance with the pre-delay, post-delay and frame rate parameters.

    > *Example Frame rate: 2 fps*
    > *Pre-delay: 1s*
    > *Post-delay: 2s*
    > *At the next trigger event six images are saved to the "VersatileApplications" directory (pre-delay+post-delay * 2fps).*

    > **This setting is only applicable for the coming event and is used to check the parameters. It is applicable for only one event and is disabled after export.**

12. Enter the **time between identical license plates** for continuous recognition. This specifies how long the same license plate must be viewed.

    > *Example License plate recognition at a gas station: The time between same license plates is set to 60 seconds.*
    > *Scenario 1: Car 1 arrives -> license plate recognition is started - car 1 leaves -> start 60 seconds - car 1 returns within 60 seconds -> no license plate recognition because the car returned within 60 seconds.*
    > *Scenario 2: Car 1 arrives -> license plate recognition is started - car 1 leaves -> start 60 seconds - car 1 returns after 60 seconds -> license plate recognition again because the car did not return within 60 seconds*

13. Specify the number of images within which the license plate must be clearly recognized in the **Number of required frames** box.
14. Click **Create new list** to save one or more license plate lists. Select a list and assign a license plate group to it to be able to analyze it.
15. **Apply** the set values if you want to make further settings or **Save** the set values to apply the values and conclude input.

List configuration

With the help of lists, you can easily classify the license plates of vehicles, e.g. into "employees" and "suppliers" or "invalid license plates". For example, an alarm can be triggered if a license plate from list "invalid license plates" is detected.

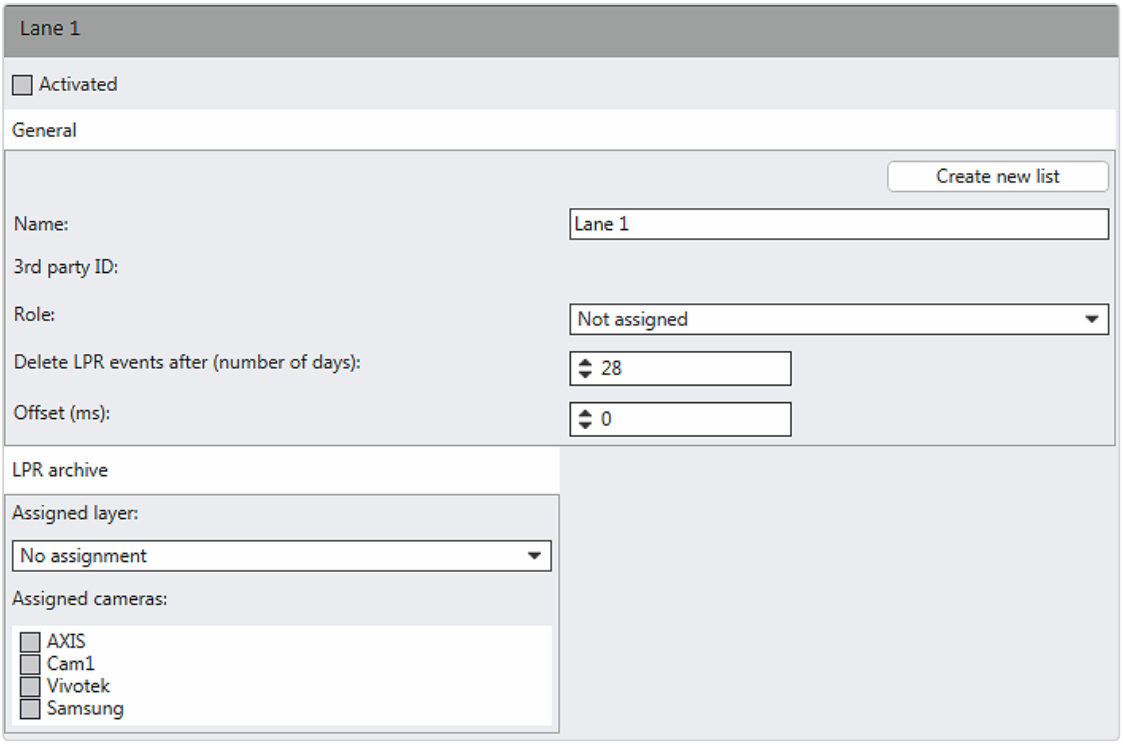


Fig. 160: List configuration

1. Select a list.
2. Activate the list and, if necessary, alter the **name**.
3. Select the **license plate groups** that are to be analyzed (see "License plate groups" on page 400). In the associated alarm scenario the user can specify, for example, that an alarm is triggered by a license plate from list 1 and that a barrier is automatically opened for a license plate from list 2.
4. **Apply** the set values if you want to make further settings or **Save** the set values to apply the values and conclude input.

LPR VCA - License plate recognition

The LPR-VCA (Video Content Analytics) channel module is used to connect APIs from third-party LPR suppliers via Seetec Application Interface (SAI). The interface sends image data and events to Qognify VMS which for example can trigger an alarm.
All LPR related events like license plate from a certain list, unknown license plate, license plate on the wrong lane etc. can be used to trigger an alarm.

> **In order to be detected correctly when the software starts up, the API-files and the signed xml-file must be stored in the "\VersatileApplications\VCAPlugin" or "\VersatileApplications64\VCAPlugin" subfolder of the Qognify installation folder.**

Adding new LPR VCA module

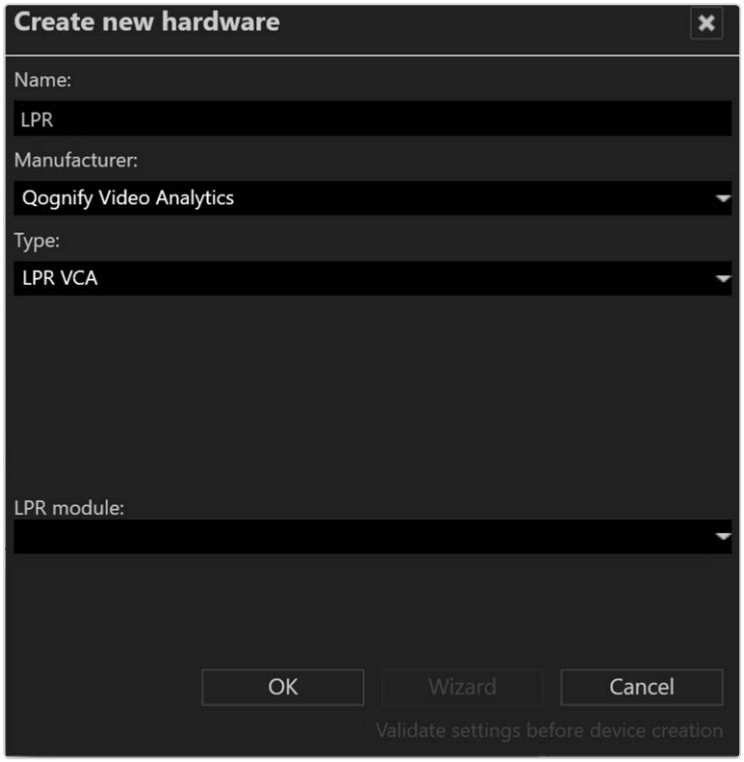


Fig. 161: Creating new hardware

1. Select **Other hardware** and create a new object.
2. Enter a **Name**.
3. For **Manufacturer** select "Qognify Video Analytics".
4. For **Type** select "LPR VCA".
5. Enter the **Host** (IP address or name) of the module.
6. Select the installed **LPR module** to specify the LPR VCA analysis channel to analyze the image data (see "Configuring the LPR module" on page 413).
7. Click **OK**. The new LPR VCA module is available within the selected company item for further configuration.

General LPR VCA settings

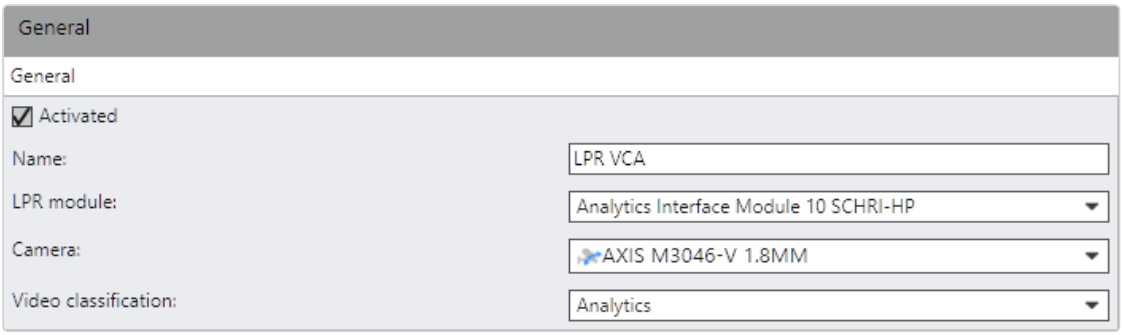


Fig. 162: General LPR VCA settings

1. Activate or disable the module.
2. If necessary, alter the **name**.
3. Select the appropriate **LPR module**.
4. Select the appropriate **camera**.
5. Select the appropriate **video classification**. The video classification determines the video profile used in surveillance mode for the various modes (normal, selected, alarm). With MPEG-4, H.264 or H.265 streaming, the frame rate for recognition must correspond to the frame rate for default recording on the selected camera, while any desired value can be entered for Motion JPEG.
6. Select the authentication method and enter the user name and password, if required.
7. To use an external LPR service depending on the camera manufacturer, enable **Use external service** and specify the **Host (IP address or name)** and the **Port** number of the service.

   > **Depending on the external service, the external software may provide additional parameters that can be configured.**

8. **Apply** the set values if you want to make further settings or **Save** the set values to apply the values and conclude input.

Lane configuration - General

Some 3rd party LPR modules are able to support multiple lanes with one channel (e.g. megapixel cameras watching multiple lanes at the same time). Therefore the LPR VCA plug-ins support assigning multiple lanes for the same LPR 3rd party channel.

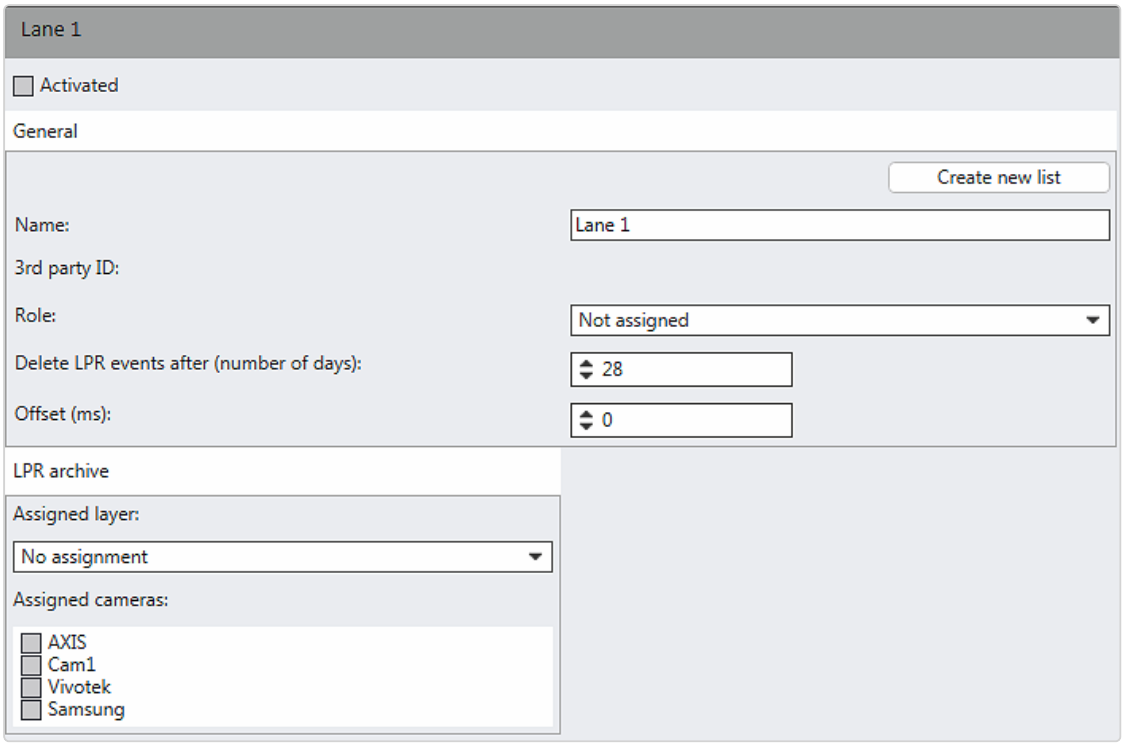


Fig. 163: Lane configuration - General

1. Activate the lane and, if necessary, alter the **name**.

   Each activated lane requires a license.

2. Click **Create new list** to create one or more license plate lists (see "Lane configuration - Lists" on the facing page).
3. Select the desired **Role**. For example, in LPR mode you can restrict the search to all entrances and you do not need to select every entrance lane manually.
4. Specify the **number of days** after which LPR events (recognized license plates, changes to master data, etc.) are to be deleted.
5. Define the **Offset** to compensate the camera signal offset.
6. Assign a layer in archive mode where the LPR image will be displayed.
7. Select the LPR camera.

   A maximum of two cameras can be assigned.

8. **Apply** the set values if you want to make further settings or **Save** the set values to apply the values and conclude input.

   While the configuration window is opened, any changes made by the plug-in will not be shown. To see the changes, configuration of the module / lane needs to be closed and reopened.

Lane configuration - Lists

With the help of lists, you can easily classify the license plates of vehicles, e.g. into "employees" and "suppliers" or "invalid license plates". For example, an alarm can be triggered if a license plate from list "invalid license plates" is detected.

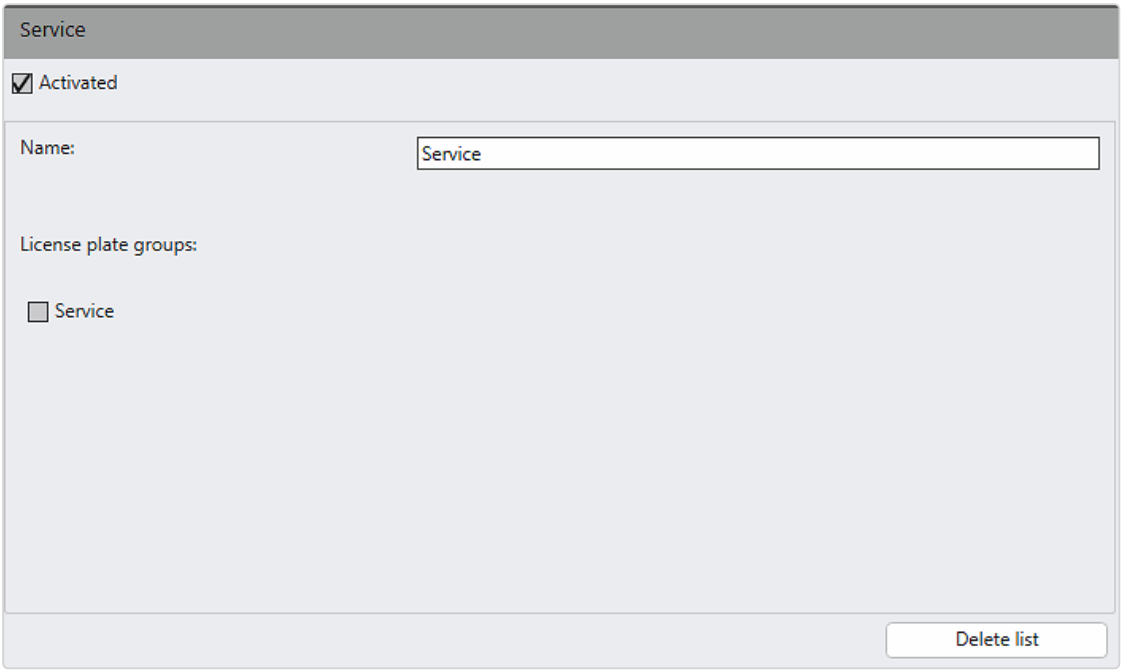


Fig. 164: Lane configuration - Lists

1. Activate the list and, if necessary, alter the **Name**.
2. Select the **license plate groups** that are to be analyzed. In the associated alarm scenario the user can specify, for example, that an alarm is triggered by a license plate from list 1 and that a barrier is automatically opened for a license plate from list 2.
3. Click **Delete list** to delete the selected list.
4. **Apply** the set values if you want to make further settings or **Save** the set values to apply the values and conclude input.

Qognify Analytics

The classic Qognify Analytics is obsolete and no longer distributed since Qognify VMS R9! It is available for migration purposes only. The feature is replaced by Qognify Analytics Server (for details, see "Qognify Analytics Server" on page 309).

The Qognify VMS server must send the camera images to the Qognify Analytics module for intelligent video analysis. Based on the analysis, alarms can be triggered.

To configure a Qognify Analytics module, you first have to create it in the Qognify VA administration tool (see "Qognify VMS VA Administration Tool" on page 476 and "Creating new hardware" on page 272). Alternatively it will be installed with a user defined installation of the analytics module (see "Server components" on page 43).

Overview of the Qognify Analytics packages

The Qognify solution offers different Qognify Analytics packages:

- Qognify Analytics Basic
- Qognify Analytics Premium
- Qognify Analytics Enterprise

	Qognify Analytics Basic	Qognify Analytics Premium	Qognify Analytics Enterprise
Area of Interest	X	X	X
Object Classification	X	X	X
Tripwire (also non-linear)	X	X	X
Multi-segment tripwire	X		X
Entering		X	X
Exiting		X	X
Appearing		X	X
Disappearing		X	X
Left behind			X
Taken away			X

Adding the Qognify Analytics module

1. Select **Other hardware** and create a new object.
2. Enter a **Name**.
3. For **Manufacturer** select "Qognify Video Analytics".

4. For **Type** select "Qognify Analytics Basic", "Qognify Analytics Premium", or "Qognify Analytics Enterprise".
5. Select the **Video Analysis module** to specify which video analysis channel is to analyze the image data.
6. Click **OK**.

General

1. Activate the module and, if necessary, alter the name.
2. Select the video analysis module to specify which video analysis channel is to analyze the image data.
3. Select the camera for delivering the analytics video stream.

   > **Privacy masking must not be used on the selected camera. Qognify Analytics devices cannot be copied. If the camera is rotated after configuration, the Video Analysis module will terminate recognition in some circumstances.**

4. Select the **Video classification** to specify which profile is to be used for image transmission to the video analysis channel. This setting applies only to multistreaming. Qognify recommends using an additional stream from the camera for video analysis. A CIF resolution is generally adequate for analysis (compression: 20%). Select larger resolutions only after consultation.
5. Specify the **Frame rate for analysis** to set the number of images per second to be sent to the video analysis channel. Qognify recommends a frame rate of 12 frames per second (fps).

6. The **Channel state** shows the current state of the Qognify Analytics channel. The following states are possible:
   - **Known scene (Good View)**: The Qognify Analytics channel is running. The video data is being analyzed.
   - **No signal (Bad Signal)**: The Qognify Analytics channel is running. The video data is not being analyzed (Possible causes: the image quality is too poor, the contrast may be too low or the image is too dark). An alarm scenario can be started in this state. Select the "Video analysis failure due to insufficient light or obstruction" option as the trigger event for the alarm scenario.
   - **Invalid scene (Invalid View)**: Unknown error. The video data is not being analyzed.
   - **Unknown scene (Unknown View)**: The current scene does not correspond with the acquired scene (e.g. the camera was rotated). The video data is not being analyzed. An alarm scenario can be started in this state. Select the "Video analysis failed due to incorrect camera position" option as the trigger event for the alarm scenario.
   - **Search for known scene (Searching for View)**: The Qognify Analytics channel is in the acquisition phase. If the Qognify Analytics channel is activated, the state changes to "Known scene", "Unknown scene" or "Unknown".
   - **Unknown**: No connection to the Qognify Analytics channel.
7. Select the desired **Usage**.
   - **Inside.** All objects will be monitored inside of a room or building
   - **Inside and people only.** Only people will be monitored inside of a room or a building
   - **Outside**. All objects will be monitored in open areas
   - **Outside, but no people**. All objects except humans will be monitored in open areas
   - **Any.** Any of the above applies
8. Select whether the analysis is to recognize **people** or **vehicles**.
9. Select **Person** or **Vehicle** to create an area in the camera image to be used to calibrate the camera.
10. For spatial location of the vehicle select **Tires** and define the position of the tires.

11. In the specified area, specify the position of the body parts (head/foot) or the vehicle's upper point (e.g. roof).

> *Example If a person is selected, place the head icon (red) at the highest point of the body's image and the foot icon at the lowest point of the body.*

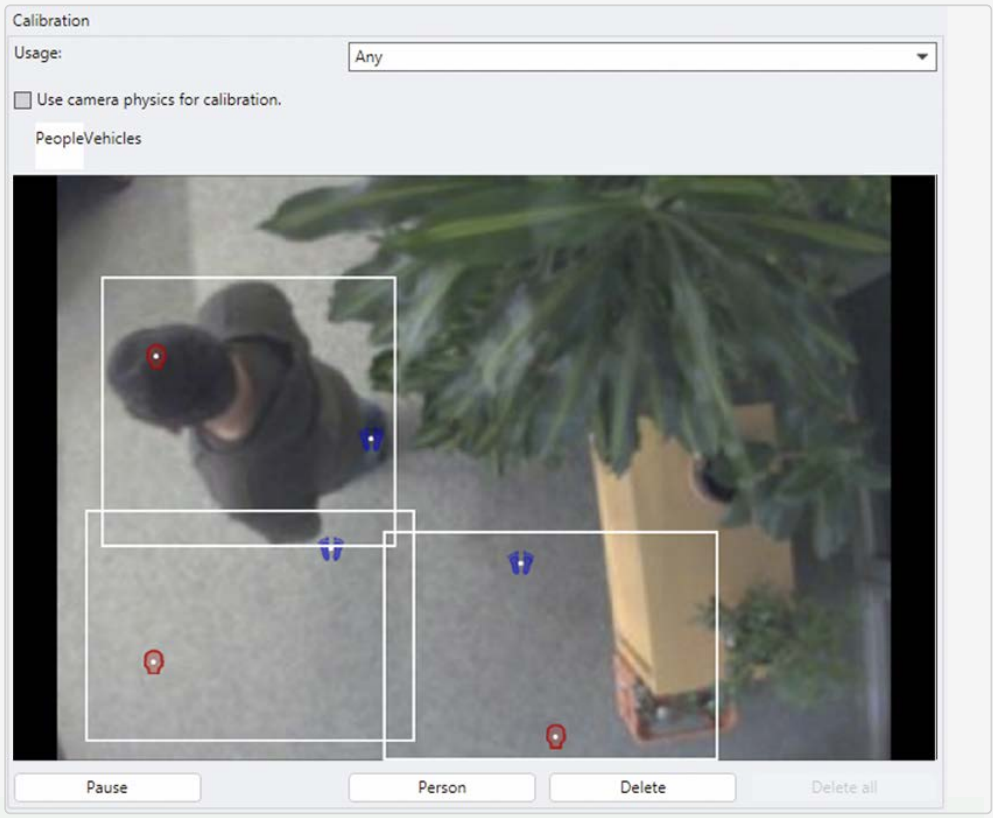


Fig. 165: General

12. If a vehicle is selected, place the cross icon at the highest point (roof) and select at least one wheel.

> **At least three persons or vehicles must be defined.**

13. To delete an area that has been created, select it and click **Delete**.
14. To delete all areas, select **Delete all**.
15. Enable **Automatically acquire new angles of view** to store the new position of the camera automatically as a new scene. An alarm scenario can also be optionally started if the camera was rotated.

16. Enable **Force new angles of view** to prevent circumstances in which the video data cannot be analyzed because the current scene does not correspond to the acquired scene. Unlike the "Automatically acquire new angles of view" option, you cannot start an alarm scenario by activating the Force new angles of view option.
17. Enable **Export single images in the event of an alarm** to save the images on which a motion or change is recognized separately as JPEG.
18. Specify the time period after which the exported images will be deleted. If you enter "0" as the time period the images will not be deleted.
19. Optionally enter the generic parameters that are to be taken into account in the analysis of the images.

    > **About the use of generic parameters, see "Technical_Guides_Qognify_Qognify VMS_7.5_EN.pdf" or contact support (see "Support" on page 13).**

20. Select **Add new rule** and enter a unique **name** for the rule.
21. Select the rule type. The following rules are available:
    - "Tripwire" below: As soon as the tripwire is exceeded in one or both directions, an alarm can be triggered.
    - "Area of interest (AOI)" on the facing page: An area in the camera image that can trigger an alarm.
    - "Scene change" on page 309: All changes in the visual field of the camera are detected if the camera image changes significantly.

> **A rule is not automatically activated after it has been created. Activate the rule during configuration of the rule (see below). Additional starting events can also be set for every rule.**

Tripwire

1. Activate the module and, if necessary, alter the **name**.
2. Activate **Classification of target** to assign the recognized object types. Multiple objects can be selected.
3. Click **Tripwire** to create a tripwire and record virtual tripwires in the camera image.
4. Click **MultiSegment TW** to create multi-segment tripwires. Multi-segment tripwires can be created at an angle.
5. Draw the virtual tripwires in the camera image.

6. Generate the corners of the tripwire by clicking on the camera image and drawing them.
7. If you have created a multi-segment tripwire, close it with a double-click.
8. Select the **parameters** for the directions from which the object is to be recognized.
9. Select the **filter for the minimum size** and the **filter for the maximum size** to specify the size of the object that is to be recognized.
10. Activate the filters with which the object is to be displayed. The color highlighting makes it easier to recognize the sizes of target objects in the foreground or background during configuration.
11. Select the additional filters:
    - **Salience**: Moving objects ignored, e.g. reflections, falling leaves or water motions.
    - **Maximum size change (%)**: Fast-changing objects are filtered, e.g. shadows.

    > *Example A shadow has a size of 100% in the first image, the size change is set to 50%.*
    > *If the shadow becomes larger, it is ignored until the size change exceeds 150%.*
    > *If the shadow becomes smaller, it is ignored until the size change falls below 50%.*
12. Click **Delete this rule** to delete the currently displayed rule.

Area of interest (AOI)

1. Activate the module and, if necessary, alter the **name**.
2. Activate **Classification of target** to assign the recognized object types. Multiple objects can be selected.

3. Select the trigger types to specify which object behavior is to trigger the event.
   - **Exiting**: Object exits the analysis area (including partially) and is still visible in the image.
   - **Entering**: Object enters the analysis area (including partially) and was still visible in the image beforehand.
   - **Disappearing**: Object exits the analysis area and is then not visible in the image.
   - **Appearing**: Object is in the analysis area and was not visible in the image beforehand.
4. Click **AOI** and specify the image detail.
5. Close the image detail with a double-click after it is marked out.
6. Select **additional parameters** for object recognition.
7. Enter a time period for **Time of loitering (s)** and **Left behind since (s)** after which a signal will be sent to trigger an alarm.
   - **Loitering**: Object has been in the analysis area for a longer time (over x seconds).
   - **Left behind**: Object is left behind in the analysis area for longer than x seconds (including partially).
8. Select the **plane** to specify the plane on which the object is found. This shows the differential background for the object recognition.
9. **Ground plane**: Recognition is to be on a horizontal area, e.g. a long corridor. The ground plane can be viewed as a carpet in the corridor that the object is in contact with.
10. **Image plane**: Every motion is to be detected. A detection at image plane can best be compared with traditional motion detection. However, detection at image plane also includes object classification.
11. In the **layer**, select whether detection is to be performed in an **image detail** or in the **full image**. Detection in the full image should be used if all unspecific motions are to be detected (person enters or exits the camera area). Because all motions are detected, it is also possible to receive a number of unwanted alarms. If detection is to be performed in the full image, some object behavior cannot be used and is therefore grayed out.
12. Select the **filter for the minimum size** and the **filter for the maximum size** to specify the size of the object that is to be recognized.

13. Activate the filters with which the area is to be displayed. The color highlighting makes it easier to recognize the sizes of target objects in the foreground or background during configuration.
14. Select the additional filters:
    - **Salience**: Moving objects ignored (e.g. reflections, falling leaves or water motions).
    - **Maximum size change (%)**: Fast-changing objects are filtered, e.g. shadows.

      > *Example A shadow has a size of 100% in the first image, the size change is set to 50%. If the shadow becomes larger, it is ignored until the size change exceeds 150%. If the shadow becomes smaller, it is ignored until the size change falls below 50%.*
15. Click **Delete this rule** to delete the currently displayed rule.
16. **Apply** the set values if you want to make further settings.
17. **Save** the set values to apply the values and conclude input.

Scene change

1. Activate the module and, if necessary, alter the **name**.
2. Select the **scene change** that is to trigger an event. All changes in the visual field of the camera are detected if the camera image changes significantly.
    - **Any change**: Combination of available options of the selection.
    - **Lighting on**: Change from dark to light
    - **Lighting off**: Change from light to dark
    - **Lighting on or off**: Change from light to dark or dark to light
    - **Unknown process**: Unclassifiable change
    - **Camera movement**: Camera is rotated
3. **Apply** the set values if you want to make further settings.
4. **Save** the set values to apply the values and conclude input.

Qognify Analytics Server

The Qognify Analytics Server provides two general variations of video analytics:

- **3D Analytics**
- **2D intelligent Motion Detection**

3D Analytics

The video 3D Analytics capacities of the Qognify Analytics Server is suitable for detecting human or vehicle intrusions in so called sterile zones. A sterile zone is an area where no human or vehicle is present (e.g. the area along a perimeter fence, a storage area at night time). The Qognify Analytics Server can be implemented at (examples):

- Perimeter protection of industrial sites or critical infrastructures
- Zone protection of sensitive facilities, storage and recycling sites, or any outdoor private areas
- Peripheral protection of stores, warehouses, company buildings, or private houses

Qognify Analytics Server can distinguish between

- People
- Vehicles
- People and vehicles

2D intelligent Motion Detection

In some cases Qognify Analytics 3D does not cover all video analytics requirements, e. g.:

- The calibration is not possible (e. g. test person is not allowed to walk in front of the camera)
- The camera position is too low or rolled
- The camera is inside – 3D Analytics does not work well inside because in most situations there are too many obstructing objects (person cannot be seen from head to toe) or the person is taking too much space on the field of view.
- There is no sufficient perspective (i.e. camera pointing directly on a wall or facade)

Architecture

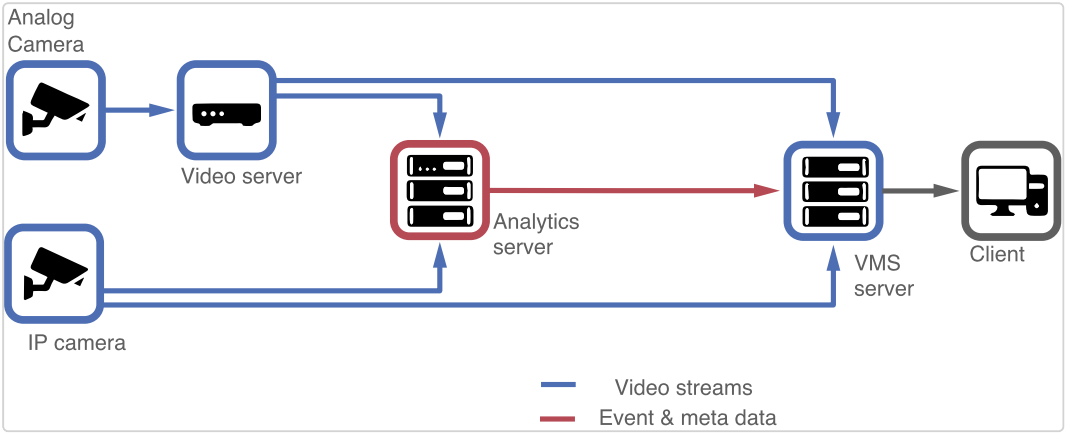


Fig. 166: Architecture of Qognify Analytics

Notes

- To add and configure a Qognify Analytics Server functionality, the required module must first be created with the Qognify VA administration tool (see "Qognify VMS VA Administration Tool" on page 476). Alternatively, it must be installed during a user-defined installation (see "Custom installation" on page 41).
- The Qognify Analytics hardware has to be added (see "Adding the Analytics Server module" on the next page).
- Camera side privacy masking may not be used.
- Qognify Analytics devices cannot be copied.
- If the camera is rotated after configuration, the Qognify Analytics Server module will terminate recognition in some circumstances.

Adding the Analytics Server module

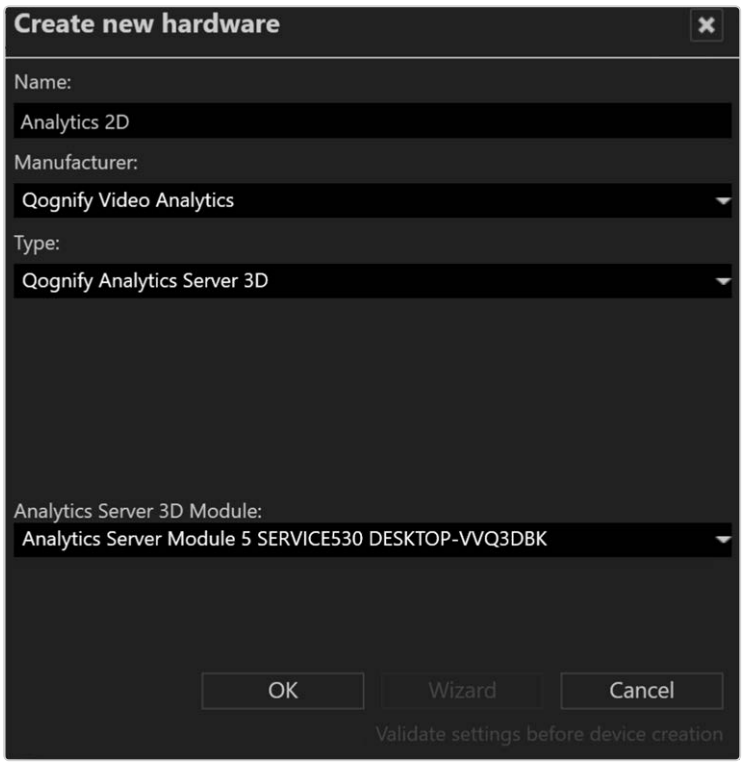


Fig. 167: Adding Analytics Server module

1. Select **Other hardware** and create a new object.
2. Enter a **Name** for the object.
3. For **Manufacturer** select "Qognify Video Analytics".
4. For **Type** select "Qognify Analytics Server 3D".
5. For **Analytics Server 3D Module** select the required "Analytics Server module" (see "Adding an Analytics Server module" on page 479).
6. Click **OK**.

> **For module configuration see "Configuring a Qognify Analytics Server module" below.**

Configuring a Qognify Analytics Server module

General

1. Select the Qognify Analytics Server module in the overview.

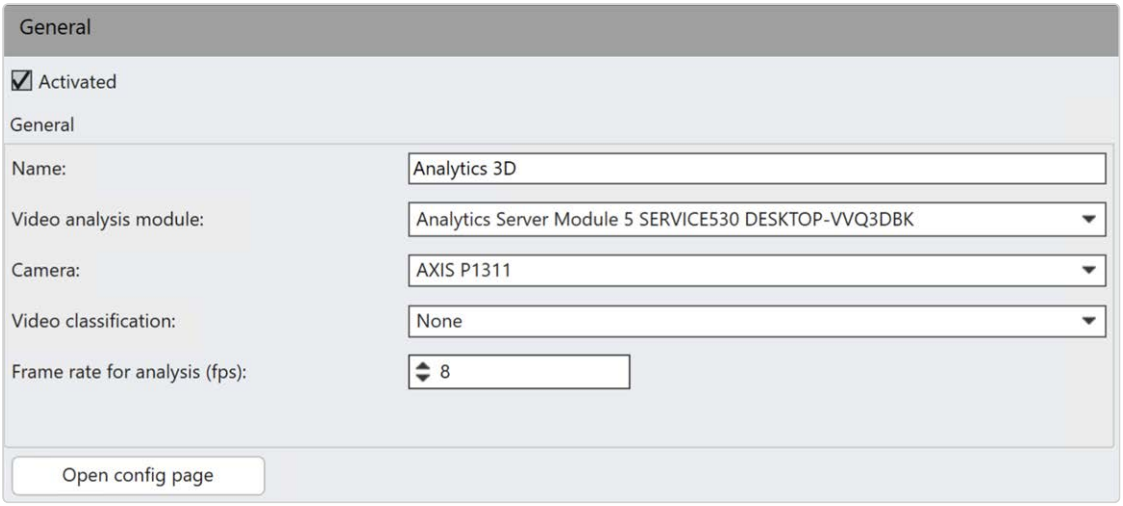


Fig. 168: Configuring a Qognify Analytics Server module

2. Activate the module and, if necessary, change the **Name**.
3. Select the **Video analysis module** to specify which video analysis channel is used to analyze the video data.
4. Select the **Camera** for delivering the video stream.
5. Select the **Video classification** to specify which profile is used for image transmission to the video analysis channel. This setting applies only to multistreaming (see "Video streams" on page 242).

It is recommended to use an additional stream from the camera for video analysis. A 4CIF resolution is generally adequate for analysis. Select larger resolutions only after consultation with the Qognify support (see "Support" on page 13).

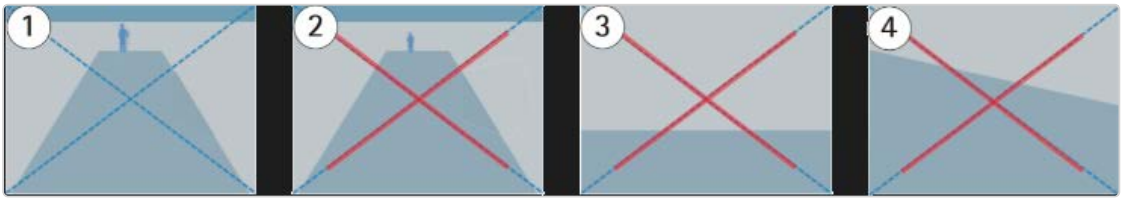


Fig. 169: Analytics scene setting

> **For the analytics to work properly, make sure you meet the following requirements.**

The scene in general should look like figure 1:

- The camera is installed at a minimum height of 2 m (6.6 ft) inside or 2,5 m (8.2 ft) outside, sufficiently tilted and with no roll
- The ground in the scene is mostly flat
- The lighting in the scene is sufficient to detect human activity
- The detection area is a sterile zone (usually free of moving objects)

- The height of a person is above 10% of the image height and above 7% if it is a thermal camera (negative example where person is too small see figure 2).
- The center of the image is below the horizon line (negative example with horizon line above the center of the image see figure 3).
- There is almost no camera roll (negative example with too significant camera roll angle see figure 4).

6. Specify the **Frame rate for analysis (fps)** to set the number of images per second to be sent to the video analysis channel.

   > **A frame rate of 8 frames per second (fps) is recommended.**

7. Click **Open config page** for configuring the Qognify Analytics server and defining analytics rules. If the config page for the module is open for the first time, select the type of analytics to be performed. The following types are available (see "Qognify Analytics Server" on page 309):
   - 2D intelligent Motion Detection
   - 3D Analytics

> **Make sure the Analytics setup tool is installed (see "Components for the custom installation" on page 42). For detailed configuration see the corresponding manual accessible from the setup tools help menu.**

Advantech

This section includes the configuration of the following interfaces:

- ADAM 6050 / 6050W
- ADAM 6052
- ADAM 6060 / 6060W / 6066

The ADAM remote I/O modules are versatile and robust computer interfaces for universal application in process control and automation. The modules are controlled by a microprocessor, and offer a simple and robust communication as well as analogue and digital I/O via Ethernet or RS-485.

General

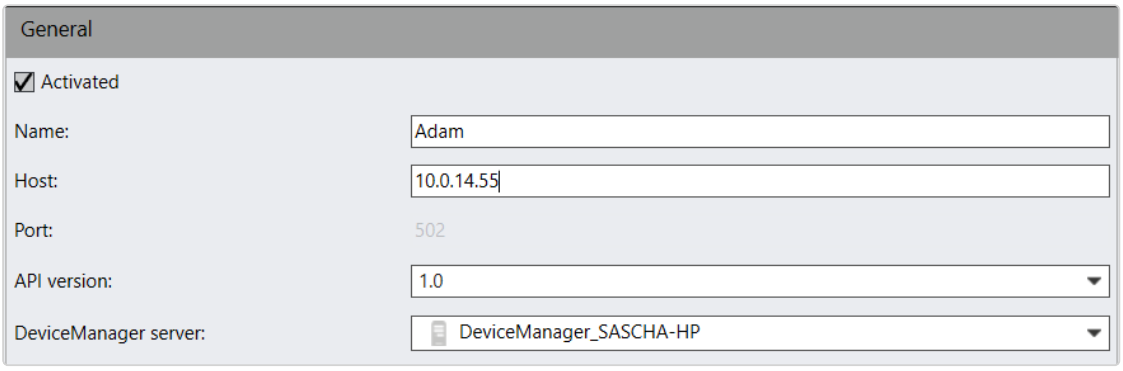


Fig. 170: Advantech Adam module - General

1. Activate or disable the module.
2. If necessary, alter the name.
3. If necessary, change the IP address or the name of the **host**.
4. If necessary, select the appropriate **API version**.
5. Change the server for managing the **DeviceManager server**.

Inputs

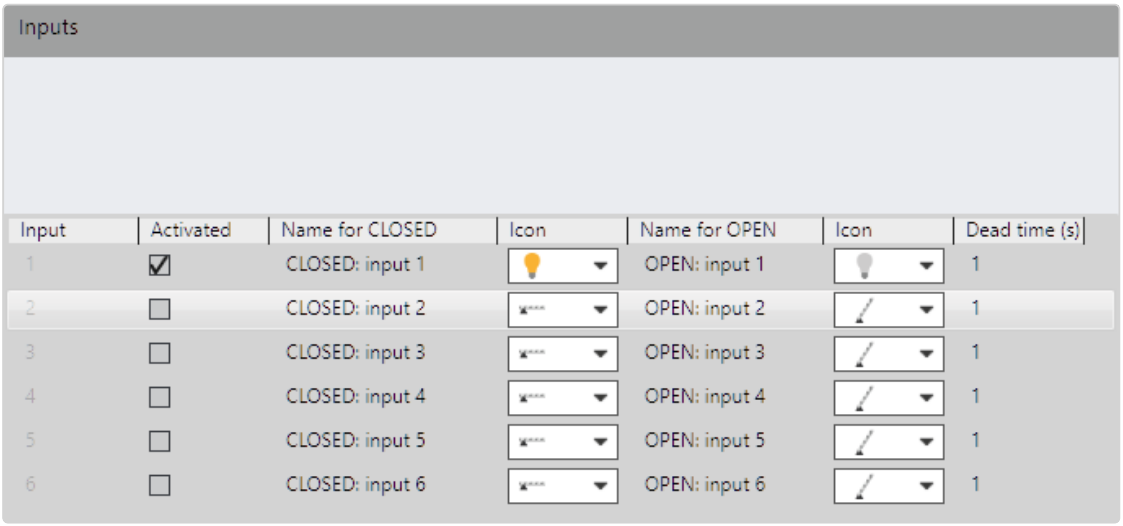


Fig. 171: Advantech Adam - Inputs

The number of inputs depends on the device type.

1. Activate the desired input and change the **name for CLOSED**.
2. Select the appropriate **icon** to display a graphic view of the current status of the input. You set the icon to be displayed in the map in the field of the same name.
3. Change the **Name for OPEN**.

4. Select the appropriate icon to display a graphic view of the current status of the input. You set the icon to be displayed in the map in the field of the same name.
5. Specify the interval for the **Dead time** (in seconds) after which a signal is analyzed again.

Outputs

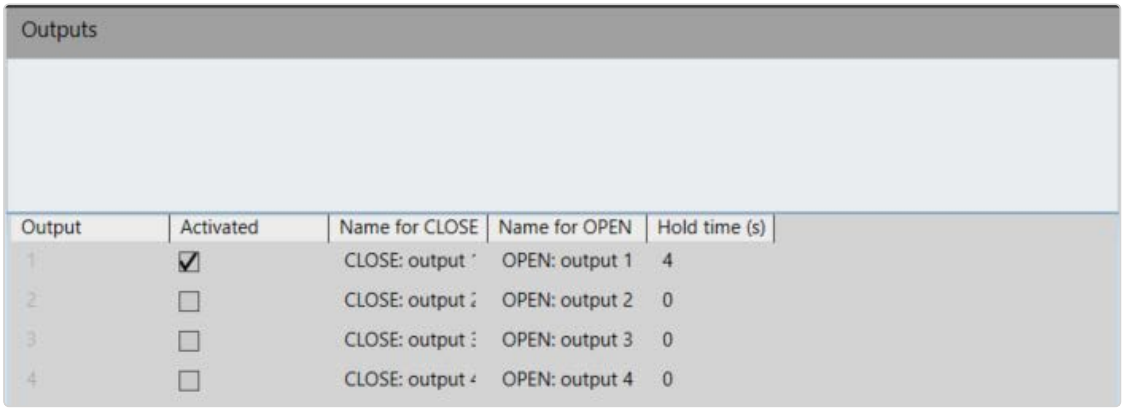


Fig. 172: Advantech Adam module - Outputs

The number of outputs depends on the device type.

1. Activate the desired output and change the **Name for CLOSE**.
2. Change the **name for OPEN**.
3. Specify the **hold time (s)** for the period for which the output is open or closed (0 = infinite).
4. **Apply** the set values if you want to make further settings.
5. **Save** the set values to apply the values and conclude input.

AXIS

This section includes the configuration of

- A9161
- A9188

The AXIS Network I/O Relay modules have configurable I/Os with supervised inputs and a relay. The module reacts on inputs, such as signals from PIR motion detectors or switches, to trigger actions. Their open platform enables a high level of integration with AXIS A1001 Network Door Controller, network cameras, and other facility systems. They also work standalone. Supplying power to I/O devices, they can extend the functionality of Axis products where additional I/Os or relays are needed.

General

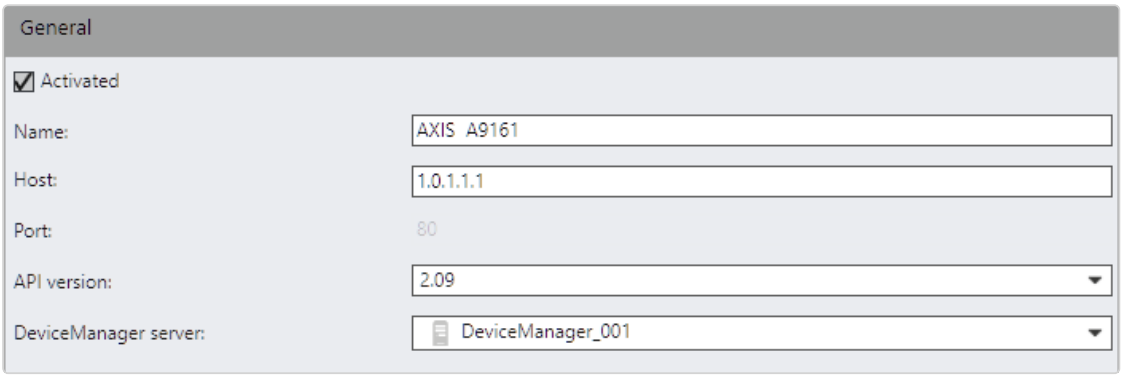


Fig. 173: AXIS - General

1. Activate or disable the module.
2. If necessary, alter the name.
3. If necessary, change the IP address or the name of the **host**.
4. If necessary, select the appropriate **API version**.
5. Change the server for managing the **DeviceManager server**.

Inputs

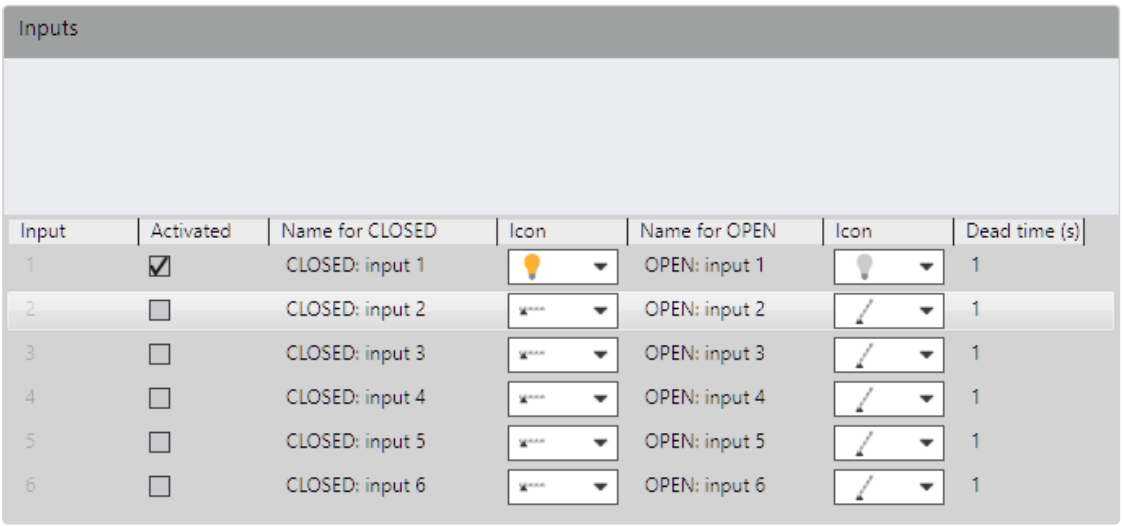


Fig. 174: AXIS - Inputs

> **The number of inputs depends on the device type.**

1. Activate the desired input and change the **name for CLOSED**.
2. Select the appropriate **icon** to display a graphic view of the current status of the input. You set the icon to be displayed in the map in the field of the same name.
3. Change the **Name for OPEN**.

4. Select the appropriate icon to display a graphic view of the current status of the input. You set the icon to be displayed in the map in the field of the same name.
5. Specify the interval for the **Dead time** (in seconds) after which a signal is analyzed again.

Outputs

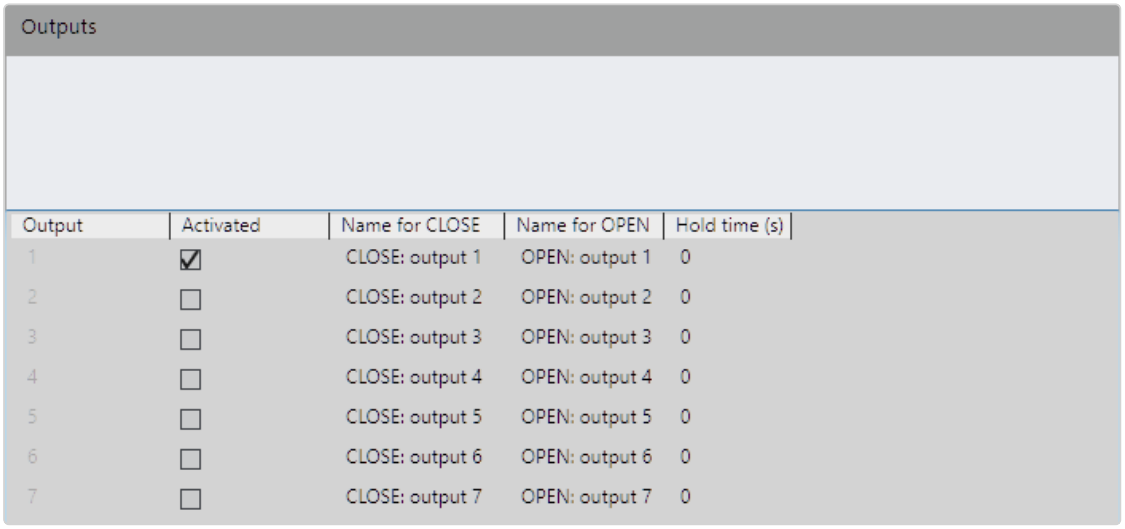


Fig. 175: AXIS - Outputs

The number of outputs depends on the device type.

1. Activate the desired output and change the **Name for CLOSE**.
2. Change the **name for OPEN**.
3. Specify the **hold time (s)** for the period for which the output is open or closed (0 = infinite).
4. **Apply** the set values if you want to make further settings.
5. **Save** the set values to apply the values and conclude input.

W&T

This section describes the configuration of the Web-IO 12x digital input, 12x digital output.
With the Web-IO digital you can control, acquire and monitor switching signals via TCP/IP Ethernet. Numerous web and network services are available for reporting changes on the inputs and outputs. Remote control over the internet mostly requires just a browser or a smartphone.

General

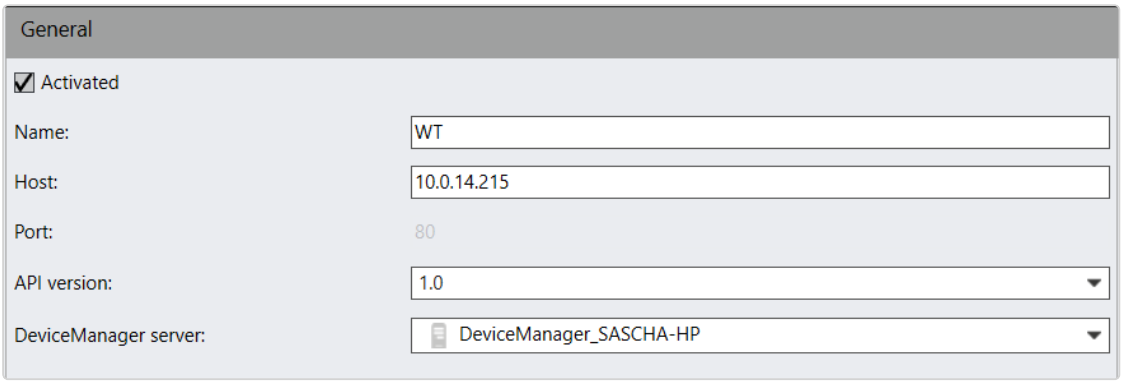


Fig. 176: W&T - General

1. Activate or disable the module.
2. If necessary, alter the name.
3. If necessary, change the IP address or the name of the **host**.
4. If necessary, select the appropriate **API version**.
5. Change the **DeviceManager server**.

Inputs

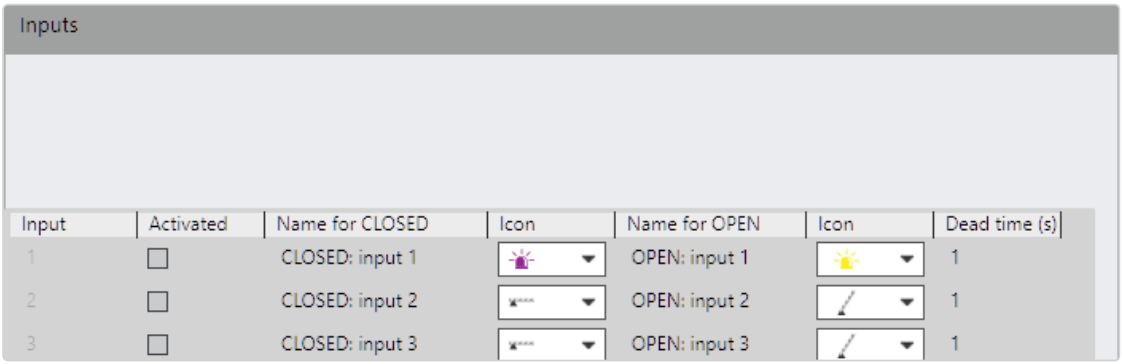


Fig. 177: W&T - Inputs

1. Activate the desired input and change the **name for CLOSED**.
2. Select the appropriate **icon** to display a graphic view of the current status of the input. You set the icon to be displayed in the map in the field of the same name.
3. Change the **name for OPEN**.
4. Select the appropriate **icon** to display a graphic view of the current status of the input. You set the icon to be displayed in the map in the field of the same name.
5. Specify the interval for the **dead time** (in seconds) after which a signal is analyzed again.

Outputs

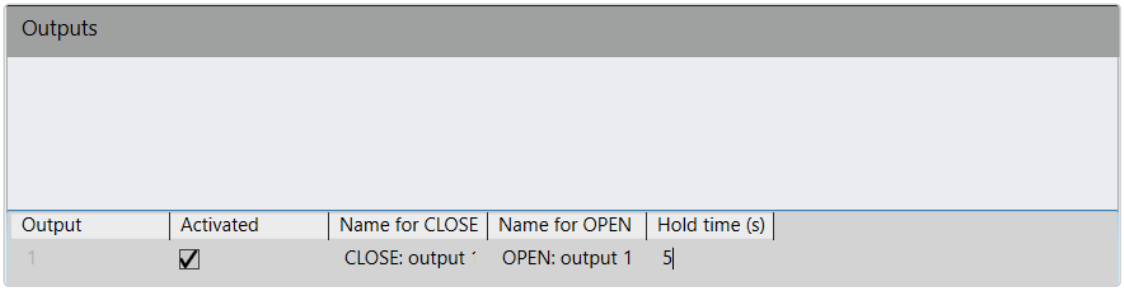


Fig. 178: W&T - Outputs

1. Activate the desired output and change the **name for CLOSE**.
2. Change the **name for OPEN**.
3. Specify the **hold time (s)** for the period for which the output is open or closed (0 = infinite).
4. **Apply** the set values if you want to make further settings.
5. **Save** the set values to apply the values and conclude input.

Wago

This section describes the configuration of the Wago System 750 I/O module.
Fieldbus couplers, fieldbus controllers and I/O modules found in the modular WAGO I/O-SYSTEM 750 receive digital and analog signals from sensors and transmit them to actuators or higher-level control systems.

General

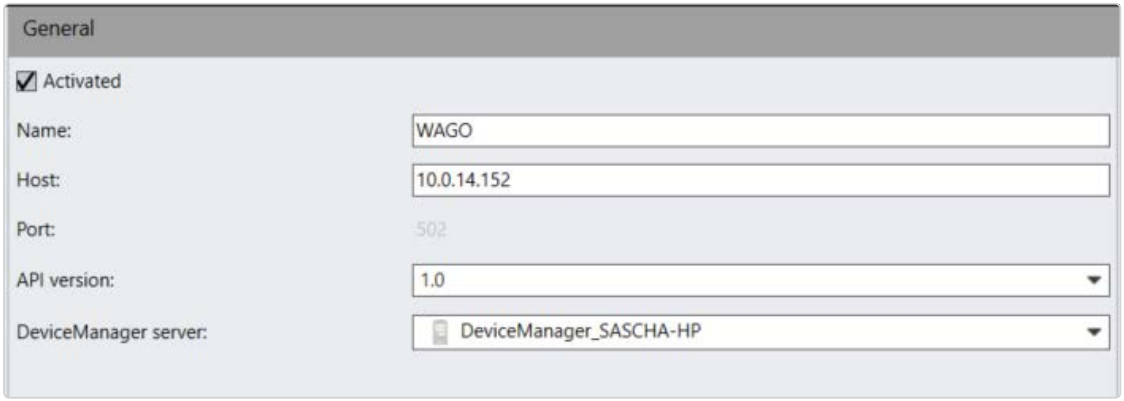


Fig. 179: Wago - General

1. Activate or disable the module.
2. If necessary, alter the name.
3. If necessary, change the IP address or the name of the **host**.
4. If necessary, select the appropriate **API version**.
5. Select the **DeviceManager server** for communication with the module.

Inputs

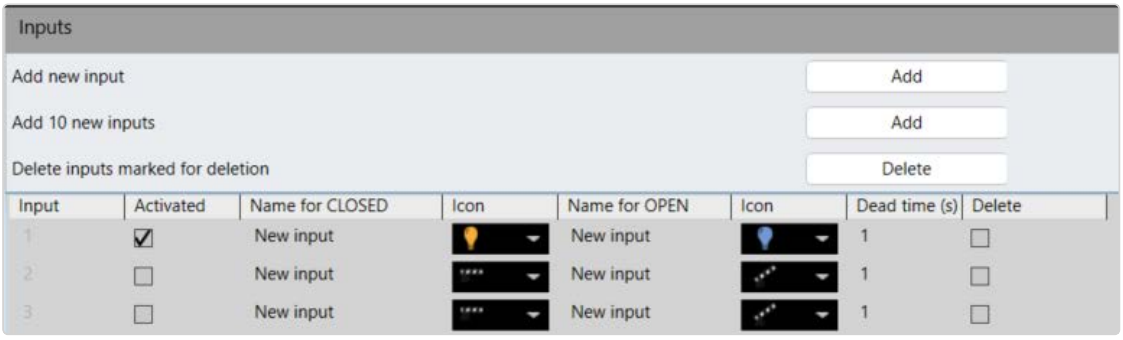


Fig. 180: Wago - Inputs

1. Click **Add new input** or **Add 10 new inputs** to create one or ten new inputs.
2. Aactivate the desired input and change the **name for CLOSED**.
3. Select the appropriate **icon** to display a graphic view of the current status of the input. You set the icon to be displayed in the map in the field of the same name.
4. Change the **name for OPEN**.
5. Select the appropriate **icon** to display a graphic view of the current status of the input. You set the icon to be displayed in the map in the field of the same name.
6. Specify the interval for the **dead time** (in seconds) after which a signal is analyzed again.
7. To delete entries, mark the entries that you want to delete and click **Delete inputs marked for deletion**.

Outputs

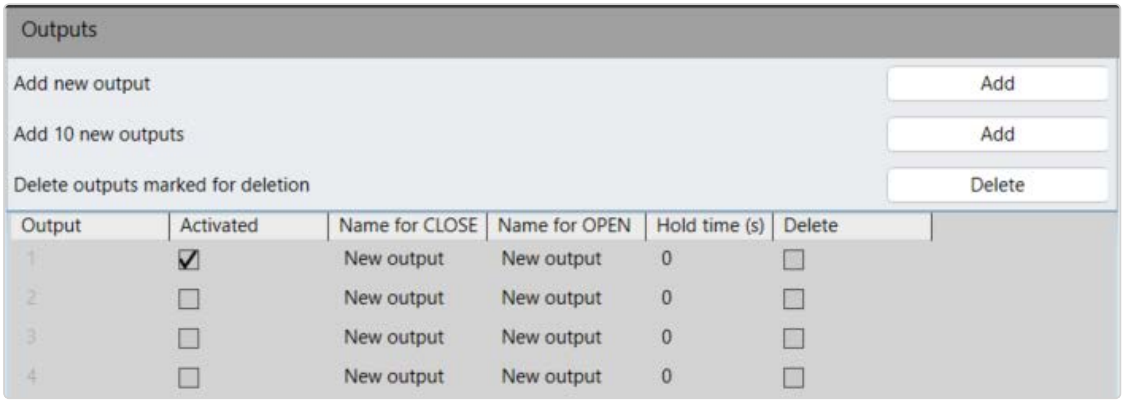


Fig. 181: Wago - Outputs

1. Click **Add new output** or **Add 10 new outputs** to create one or ten new outputs.
2. Activate the desired output and change the **name for CLOSE**.
3. Change the **name for OPEN**.
4. Specify the **hold time (s)** for the period for which the output is open or closed (0 = infinite).
5. To delete entries, mark the entries that you want to delete and click **Delete outputs marked for deletion**.
6. **Apply** the set values if you want to make further settings.
7. **Save** the set values to apply the values and conclude input.

Event Interfaces

The Qognify Event Interface function in the Administration control allows you to configure and manage third party safety systems that can be integrated into Qognify VMS on a generic basis, such as burglar alarm, fire panel, access control etc. These devices can be partly administered and actuated with the Qognify software and with software provided by the respective third-party manufacturers.

After the event interfaces or generic access controls have been configured, they can be connected to alarm scenarios (see "Alarms" on page 356) and the items can be added to maps (see "Maps and "Advanced Maps"" on page 377).

> **The Event Interfaces require some specific plug-in files which need to be copied into the Qognify VA-Plug-in directories ("C:\Program Files\Qognify\VersatileApplications64\AccessControlPlugins" or "C:\Program Files\Qognify\VersatileApplications64\EventPlugins"). For further information see technical guides or ask Qognify support about the use of third party event based plug-ins.**

To configure an event interface or a generic access control module, it must be created in the Qognify VA administration tool (see "Qognify VMS VA Administration Tool" on page 476).

For the Qognify generic access control at least one of the following access control modules has to be installed:

- Continental CardAccess3000Paxton Net2
- Lenel

1. Select the location in the **Company** control. The selected location is displayed in the title bar of the Administration control.
2. Select **Event Interfaces** in the control bar.

Unavailable items in the interfaces are not deleted, but hidden. They can be accessed at any time without reconfiguration.

Creating an event interface

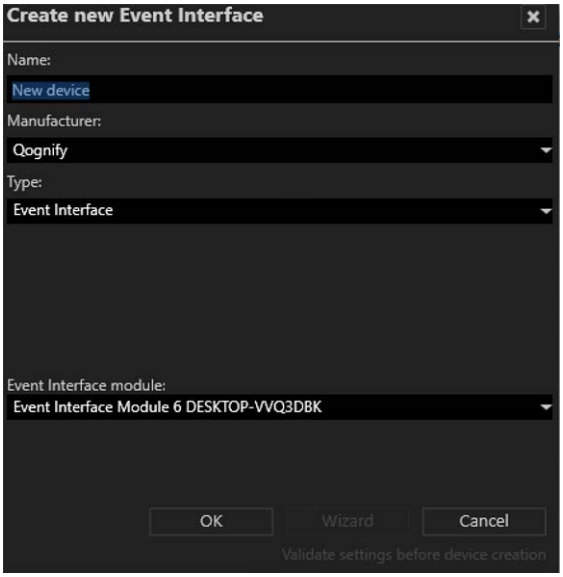


Fig. 182: Creating an event interface

1. Create a new **Event interface**.
2. Enter the **Name** for the new event interface.
3. Select the **Manufacturer**.
4. Select the **Type** Event Interface.
5. Select the installed **Event Interface module**.
6. Click **OK**. The new event interface is available within the selected company control.

Creating a generic access control

1. Create a new **Event interface** item.

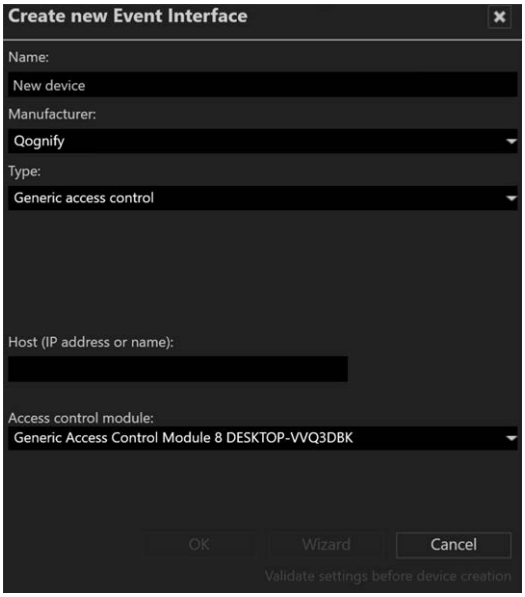


Fig. 183: Creating a generic access control

2. Enter the **Name** for the new generic access control.
3. Select the **Manufacturer**
4. Select the **Type** Generic access control.
5. Enter the **Host** (IP address or name) of the module.
6. Select the installed **Access control module** (refer to "Adding a generic Access Control module" on page 487).
7. Select **OK**. The new access control is available within the selected company item.

Configuring event interfaces

General

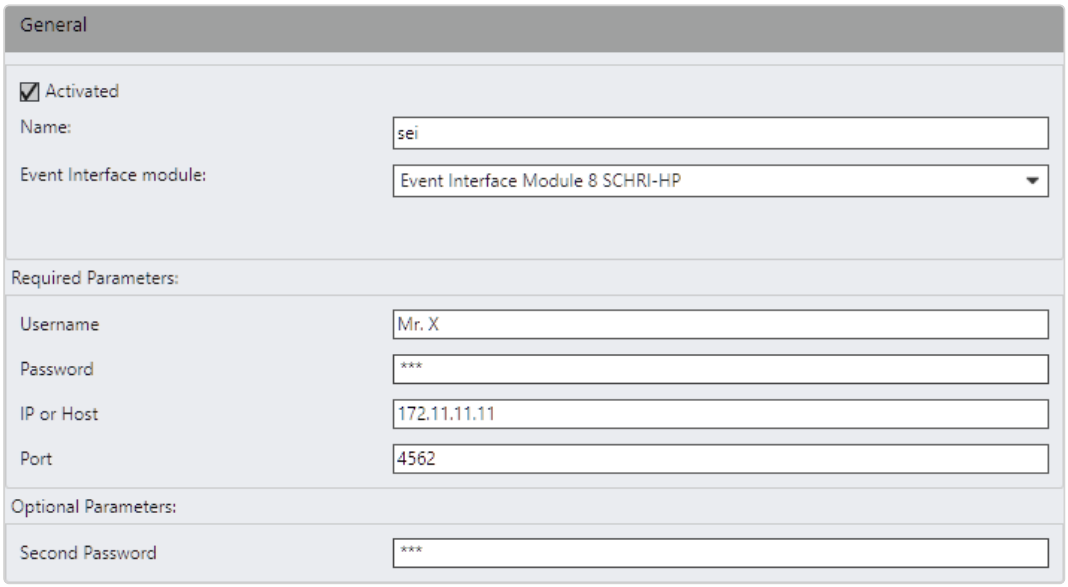


Fig. 184: Event interface settings - General

1. Select the event interface in the **Event interface** overview.
2. **Activate** the event interface
3. Edit the **Name**.
4. Select the **Event Interface module**.
5. Enter the required and optional parameters required by the plug-in:
   - **User name** and **Password** for the access control module
   - **Port** number and **IP** address of the module
   - **Second password** to access the module
6. Select **OK**.

Items

Depending on the plug-in, the Event Interface provides different objects such as the states of areas of an alarm system or the events from a 3rd party video analysis system. The available can be used in alarms (see "Alarms" on page 356) and maps (see "Maps and "Advanced Maps"" on page 377).

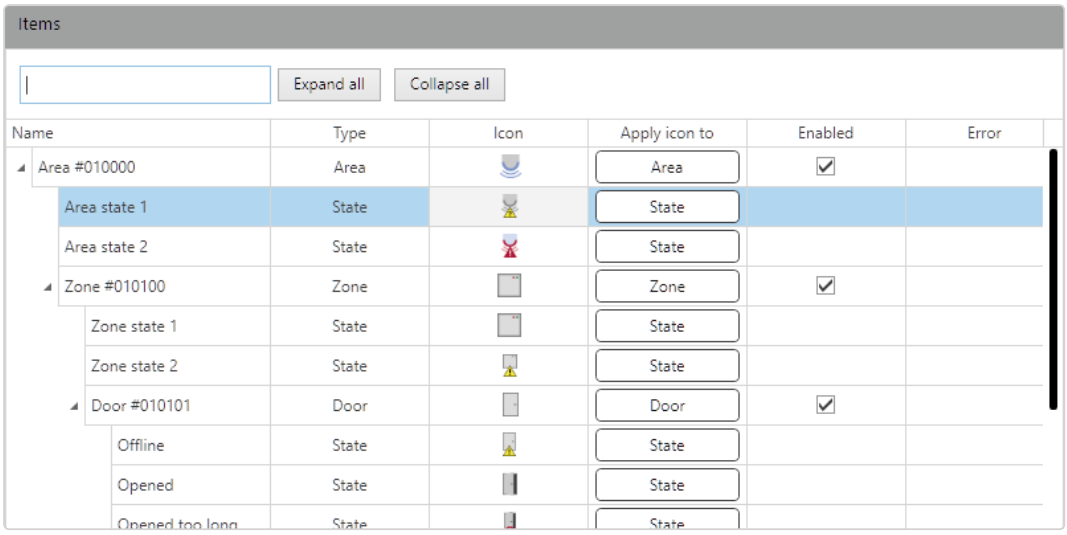


Fig. 185: Event interface items

Search Items

1. Enter a character string in the **search** field. The relevant items are listed and the string in the item name is highlighted.

Changing an icon

1. Click on the displayed icon.
2. Select another one. To use an icon that supports multiple states, refer to "Creating multiple-state icons" on page 328).
3. Click on the apply to item button.

Enabling or disabling an item

1. Click the **Enabled** check box. The state changes accordingly.

Rules

To group different event states, the single events or states can be collected in a so-called “rule”. This simplifies the administration of multiple events or states. The

rule is triggered when an event or state in it is changed or triggered.
The rules can be added to an alarm scenario (see "Start" on page 363).

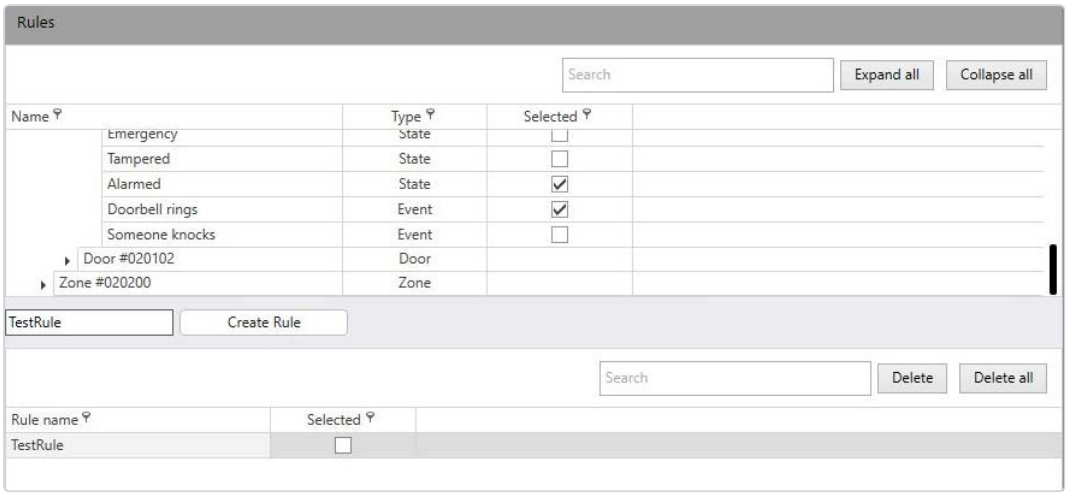


Fig. 186: Event interface settings - Rules

Creating a rule

1. Select events or states from the event list. If required, search for the event or decrease the number of displayed items by collapsing the list.
2. Name the rule and select **Create Rule**. The new rule is displayed in the rule list.
3. Repeat for multiple rules.

   Rules must not be named identically.

Deleting a rule

1. Select a rule in the rule list or search for the rule.
2. Select **Delete**.
3. To delete all rules in the list, select **Delete all**.

Unavailable items

The tab shows the items that are currently disabled, i.e. hidden, so that they can be activated without configuration. The unavailable items are displayed in the control

and marked with a red cross.

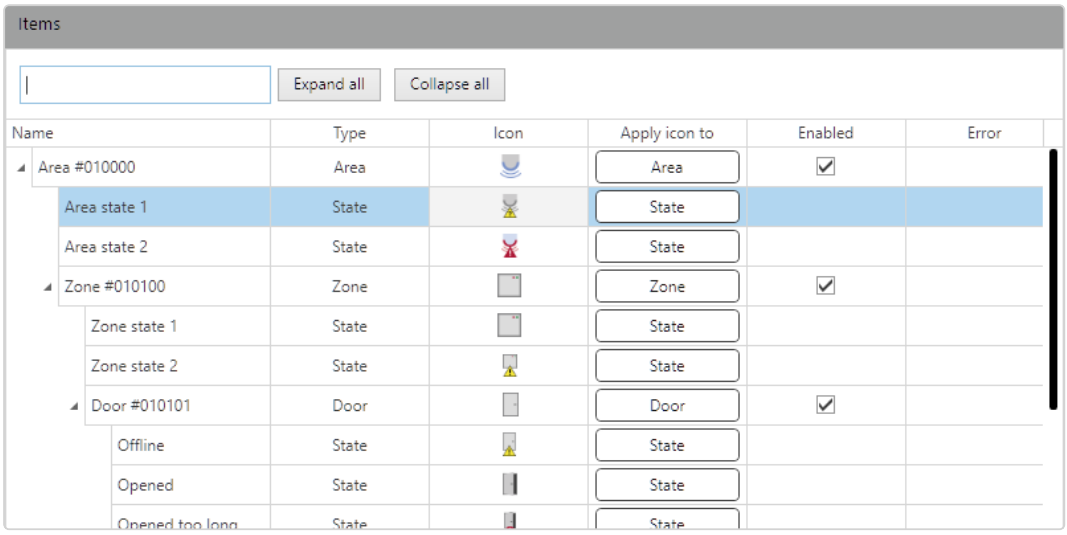


Fig. 187: Event interface - unavailable items

Activating an item

1. Select the item or enter the name of the item in the search field above the list.
2. Open the item by double-clicking.
3. Select **Active** (see "General" on page 325).

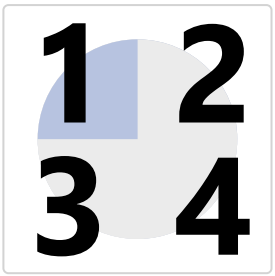
Deleting an item

1. Select the item and click **Delete**.
2. Click **Yes** to confirm deletion. The item is permanently deleted.

Creating multiple-state icons

Event interfaces in Qognify VMS support icons that can display up to four different states of a single event. The states of the icons are displayed as transparent overlays on top of the original icons on a map. Thereby, for a single event icon different states such as closed / open can be displayed.

The icons are not included in Qognify VMS but must be created according to the following requirements:



- The background is transparent so that it does not obscure the original icon below.
- The icon has a fixed size of 64 x 64 px.
- The image format is PNG.
- Each state only covers a quarter of the original icon.
- Each state is confined to the respective quadrant, e.g. the alarm state is displayed only in quadrant 1 and the rest of the icon is transparent.

Deleting event interfaces

1. Select the event interface (or generic access control) in the **event interface** overview.
2. Click **Delete object**.

Users

The **User** function in the **Administration** control allows you to create and delete user profiles. In addition, you can configure the connection to an existing Active Directory® Authorization Manager. The corresponding authorizations and profiles are assigned to the user, depending on whether he or she is logged in under a user name or as a group.
For a general description of administrative and user rights, see "Administrative rights and user rights" on page 24.

1. Select the location in the **Company** control. The selected location is displayed in the title bar of the **Users** control.
2. Select **Users** in the Administration control.

Creating a user

1. Select **Create new object** in the **Users** control. Two options are available:
   - Create Basic User. Creates a new user with user rights configured within Qognify VMS
   - Create Active Directory User. When an Active Directory (AD server is installed, the user and his group affiliation are connected to the user's account in Qognify VMS.

Creating a basic user

1. Select **Create Basic User**.
2. Enter the **Name** and **Password** of the new user.
3. Click **OK** to accept the name. The new user is displayed in the control.

Creating an Active Directory user

1. Select the **Object Type** "User".
2. Open the **Search Path** to the AD-server.
3. Enter the user name. The corresponding user account is displayed.
4. To search the user by name, select **Check names**.
5. Click **OK**.

Configuring a user

1. Select the user in the **Users** control.

Synchronizing AD users

The names of Active Directory users must be synchronized with the AD server, since the names cannot be edited in Qognify VMS.

1. **Select Reload**  in the users control.

General

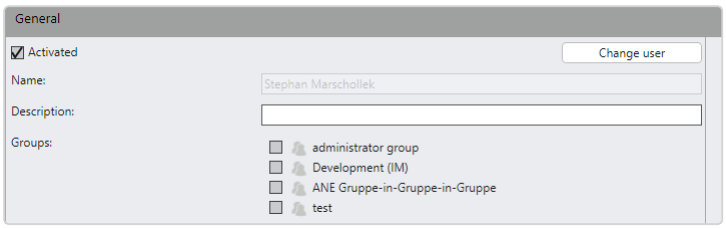


Fig. 188: User - General

1. **Activate** the user.

   > **The administrator cannot be deactivated.**

2. To change the name of the Active Directory user, select **Change group** and alter the user name in the dialog.
3. Enter a **Description** of the user account. This can be the name of the user, for example.
4. Activate the **Groups** to which the user account is to belong (see "Groups" on page 338). The association with a group is optional.

Password

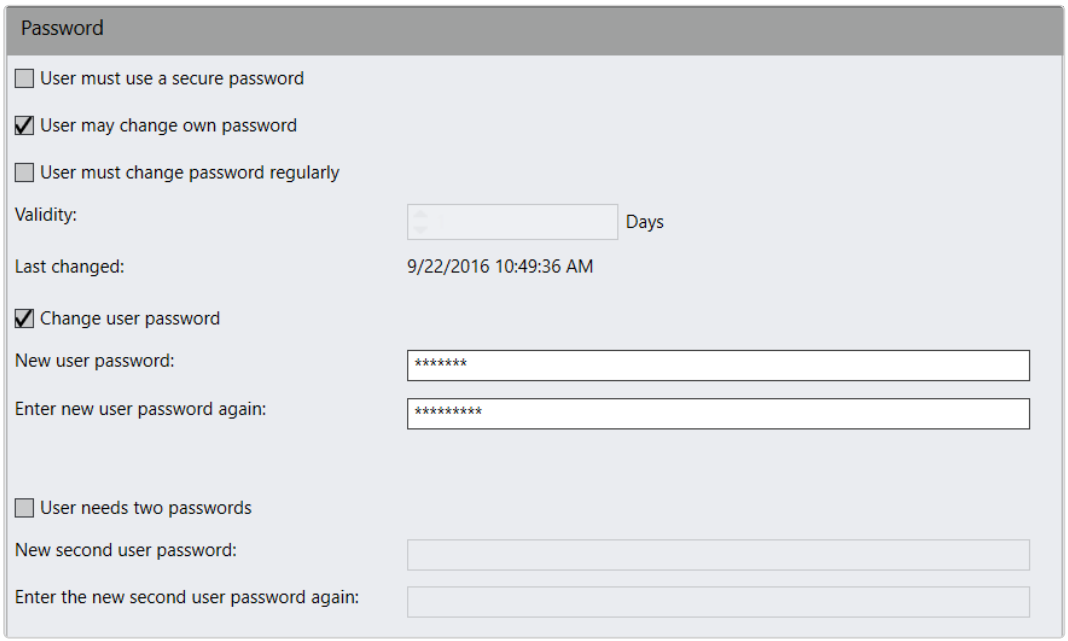


Fig. 189: User - Password

1. Select **User must use a secure password**. If the password does not meet the security requirements (see below), you receive a message to this effect.
2. Select **User may change own password** to permit the user to change his or her password.
3. Select **User must change password regularly** and specify the **Validity** period for the password. Before the period expires, the user is requested to change the password in order to be able to continue logging in.
4. Select **Change user password**, and enter a new user password.

   > **User passwords of AD accounts cannot be altered in Qognify VMS.**

   > **If you have selected "User must use a secure password", choose a password that consists of at least eight characters and contains at least one digit, one upper-case letter and one lower-case letter.**

5. Enter the user password again.
6. To create a second password on the "four-eyes principle", select **User needs two passwords** and specify a further password, which must adhere to the same security rules.
7. Enter the second password again.

   > **If you forget the administrator's password and have not added any users to the administrator group (see "Groups" on page 338), it is no longer possible to access configuration mode.**

Rights options

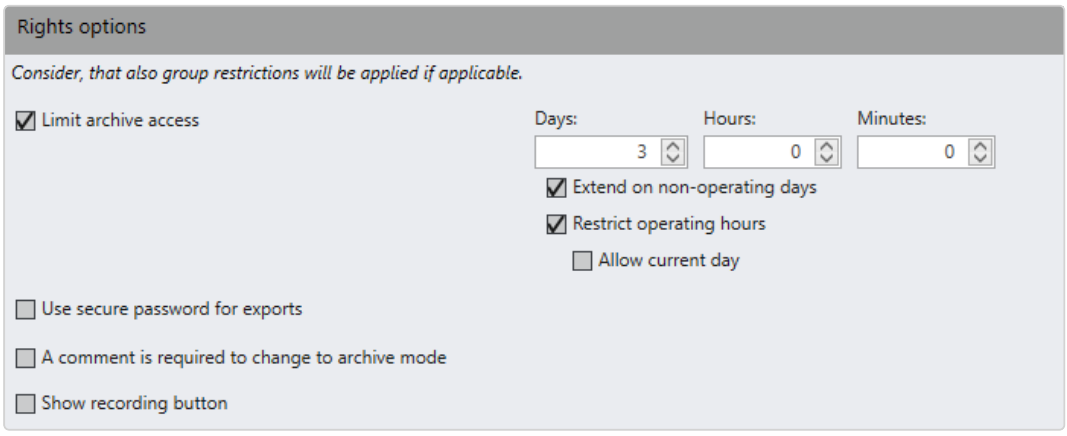


Fig. 190: User - Rights options

1. Select **Limit archive access** and specify the duration of the access period (in minutes) in order to limit the user's continuous access to the archive.
2. Select the number of days, hours, and minutes the user is allowed to have access to the recording archive.

> **If not visible, the following items are not part of the current license. Public holidays and non-office-days are not recognized for retention time and archive access.**

If a user is in a group, these settings are also taken into account. If the settings between users and groups contradict each other (e.g. 2 days archive access is set for the user, but 3 days for the group), the highest restriction applies (i.e. the user may only see 2 days of archive material).

- Enable **Extend on non-operating days** to include days such as public holidays or non-office days into the extended recording and access management.
- Enable **Restrict operating hours** to hide the archive for the configured area at operating hours.
- Select **Allow current day** as an exception so that the user has the right to view the archive during the opening hours on the current day.

> **Additionally, the extended recording and access management ("Operating days") can be restricted depending on the user (see "Manage group rights" on page 342).**

3. Select **Use secure password for exports**. If a user has the right to export recordings he has to provide a secure password.
4. Select **Comment necessary for changing to archive mode**.
5. Enable **Show recording button** to display the button **REC** in the camera layer.

Manage user rights

User rights as well as administrative rights are only positively inherited, i.e. if a user is assigned a specific permission as user right, but not as administrative right, he still owns both rights.

Example

User A has been assigned the right to delete recordings in "User / Manage user rights", but this right has not been assigned to him in "Groups / Manage user rights". The user may still delete recordings - even if he belongs to a group, that does not have the respective rights.
On the other hand, if user A belongs to a group that is allowed to define a Button, but the user himself has not been assigned this right, he still owns the group right.

This allows users to be members of a group and still own user-specific rights without causing conflicts.

User rights of users who belong to a group can also be administered via the group rights (see "Administrative rights and user rights" on page 24). A user's membership of particular groups is revealed by the colored fields (see "Groups" on page 338 for information on how to configure the colors of groups).

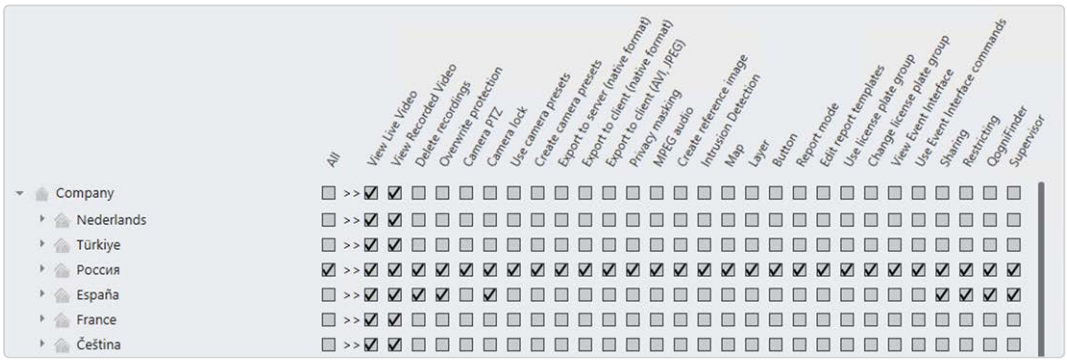


Fig. 191: User - Managing user rights

1. Select or deselect the rights for the selected user to perform specific actions on the installed devices and objects for all branches.
2. Optionally, open the Company tree and define the user rights specifically for each branch.

Depending on the device or object, the following rights are available, which can be selected or deselected individually or together.

- **All**: Selects or deselects all users rights for the corresponding device or object.
- **View Live Video**: The user can see a camera and its live images in Surveillance mode.
- **View Recorded Video**: The user can use cameras in Archive mode.
- **Delete recordings**: The user can delete recordings in Archive mode.
- **Overwrite protection**: The user can apply overwrite protection to recordings in Archive mode or remove overwrite protection from them.

- **Camera PTZ**: The user can use the PTZ camera including the digital zoom except for preset camera positions.
- **Camera lock**: The user can lock the position of the PTZ camera.
- **Use camera presets**: The user can use the predefined camera positions.
- **Create camera presets**: The user can create camera preset positions or delete predefined positions.
- **Export to server (native format)**: The user can save image data in the Qognify-specific format on the server.
- **Export to client (native format)**: The user can save image data in the Qognify-specific format on the client.
- **Export to client (AVI, JPEG)**: The user can save image data as an AVI or JPEG file on the client.
- **Privacy masking**: The user can deactivate privacy masking.
- **MPEG audio**: The user can use audio transmission.
- **Create reference image**: The user can use the manual reference image comparison from the Tools menu.
- **Intrusion Detection**: The user can use intrusion detection commands, e. g. on maps.
- **Map**: The user can use the corresponding map.
- **Layer**: The user can display defined layers.
- **Button**: The user can use buttons.
- **Report mode**: The user can view report mode.
- **Edit report templates**:The user can create and edit report queries in report mode and save them as templates.
- **Use license plate group**: The user can only use license plate groups when the LPR master data editor is opened automatically if an unknown license plate is detected.
- **Change license plate group**: The user can open the LPR master data editor from the View menu and can fully edit license plates.
- **View Event Interface**: The user can see the event interface items.
- **Use Event interface commands**: The user can change the state of an event interface item e.g on maps.

- **Sharing**: The user is allowed to share a camera with other users and any connected Active Directory group. *To share a camera, the user does not need administrative rights.*
- **Restricting**: The user can edit the restriction settings for cameras.
- **QogniFinder**: The user can search for objects using the QogniFinder in Archive mode.
- **Supervisor**: The user can only see, edit, delete, and potentially execute prepared exports on a branch level to prevent data misuse.

Manage administrative rights

A user with administrative rights can edit the system in configuration mode.

Example

A user can be specified as a system administrator for the branch "Hamburg" without even having access to the branch "Munich" (see "Relationship between the main branch and its sub-branches" on page 200).

The rights for users and groups are also checked on server side, so even if a hacked client (without any rights check) is used, it is still not possible to configure users, groups or their profiles.

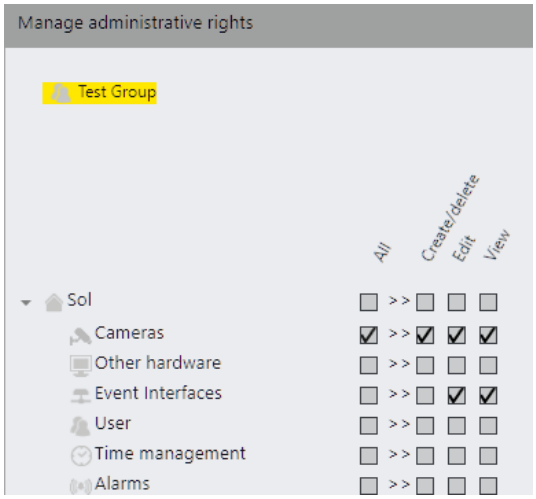


Fig. 192: User - Managing administrative rights

1. Select or deselect the rights of the selected user to make changes or settings. Three types of administrative rights are available:
   - **Create/delete**: The user has unlimited scope to manage the selected objects and can, for example, create, configure and delete cameras.
   - **Edit**: The user can change the settings of the selected objects, but cannot create or delete objects.
   - **View**: The user can view and operate the selected objects but cannot make settings or create and delete objects. This does not apply to layers created in surveillance mode ("temporary layers").
2. **Apply** the set values if you want to make further settings.
3. **Save** the set values to apply the values and conclude input.

Misc

To access a camera with a static IP address and port, the user must have the required permission.

Fig. 193: User - Misc

1. Select **Enable the static URL access** (IP address and port number) for the user.
2. Enter the password.
3. **Apply** the set values if you want to make further settings.
4. **Save** the set values to apply the values and conclude input.

Deleting a user

1. Select the user in the overview.
2. Click **Delete object**.

Duplicating a user

1. Select the user in the overview.
2. Click **Duplicate object**, and enter a **Name** for the duplicated user.
3. Click **OK** to accept the name. The new user is displayed in the overview.

Groups

The **Groups** function in the Administration control can be used to add users to groups and manage the rights of groups. The corresponding authorizations and profiles are assigned to the user, depending on whether the user is logged in with a user profile or a group profile.
For a general description of administrative and user rights, see "Administrative rights and user rights" on page 24.

1. Select the location in the **Company** control. The selected location is displayed in the title bar of the Administration control.
2. Select **Groups** in the Administration control.

Creating a new group

1. Select **Create new object** in the **Groups** control. Two options are available:
   - Create Basic Group. Creates a new user with user rights configured within Qognify VMS
   - Create Active Directory Group. When an Active Directory (AD server is installed, the user and his group affiliation are connected to the user's account in Qognify VMS.

Creating a basic group

1. Select **Create Basic Group**.
2. Enter the **name** for the new group.
3. Click **OK** to accept the name. The new group is displayed in the overview.

Creating an Active Directory® group

1. Select the **Object Type** “Groups”.
2. Open the **Search Path** to the AD-server.
3. Enter the group name. The corresponding group is displayed.
4. To search the user by name, select **Check names**.
5. Click **OK**.

Configuring a group

1. Select the group in the overview.

Active Directory groups that are grouped in AD retain their inherited rights from the parent group. A user that does not exist in Qognify VMS is allowed to log in if he is member of any parent group created in Qognify VMS.
The grouping a rights management is performed outside of Qognify VMS.

Synchronizing AD groups

The names and rights of Active Directory groups must be synchronized with the AD server, since the names cannot be edited in Qognify VMS.

1. Select **Reload** in the groups control.

General

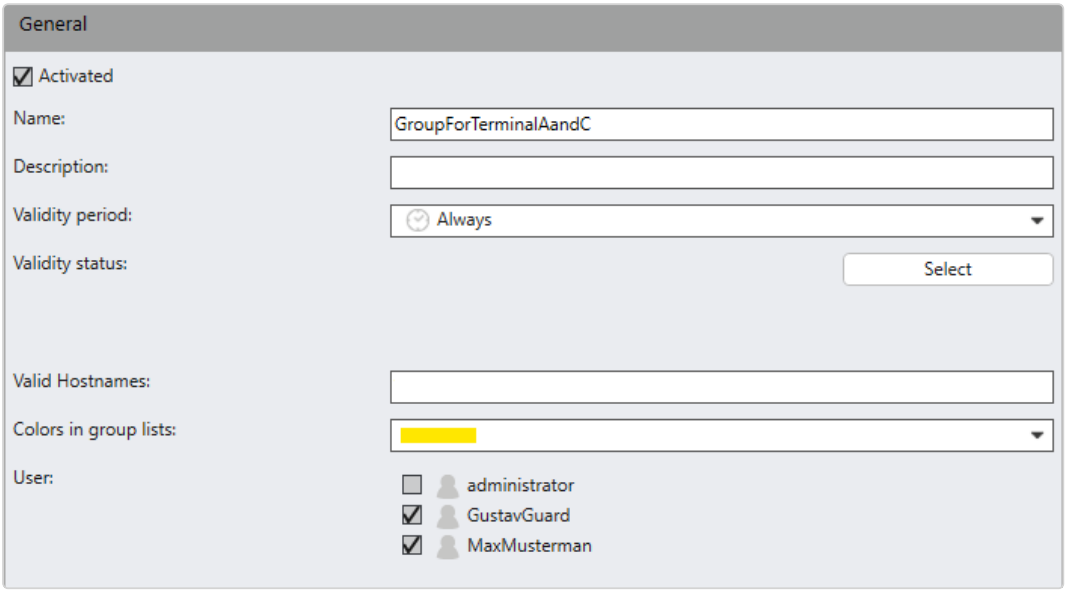


Fig. 194: Groups - General

1. **Activate** the group.
2. To change the name of the Active Directory group, select **Change group** and alter the group name in the dialog.
3. Enter a **description** of the group.
4. Select a **validity period** for the group, within which group members can access the system depending on their user rights. The possible periods are specified in the "Time management" on page 351.

   > **For a general description of administrative and user rights, see "Administrative rights and user rights" on page 24.**

5. Specify the **validity status** to activate or deactivate the group. All users belonging to this group can thus be prevented from accessing certain cameras.
6. If the group is restricted to one or more areas (hosts) within a multi-host setup, enter the **valid hostnames** separated by a comma (see "Restricting the use of multiple hosts" on the facing page).
7. Assign the group **colors in group lists**. Different colors for different groups facilitate the administration of user rights as each user inherits the rights and the colors of the group he or she belongs to.
8. Select the **users** to be assigned to the group.

Restricting the use of multiple hosts

The user can be restricted when accessing cameras to prevent that he can access cameras that are not part of his current job role (e.g. guard in building A, but not in building B). Whereas the role restricts the access to cameras (and entities) irrespective of the host he is connected to, this access can be further limited by defining only those areas (i.e. hosts) where he is currently logged in.
By this, the user not only sees the cameras assigned by his role, but also only the cameras associated with his current host.

Rights options

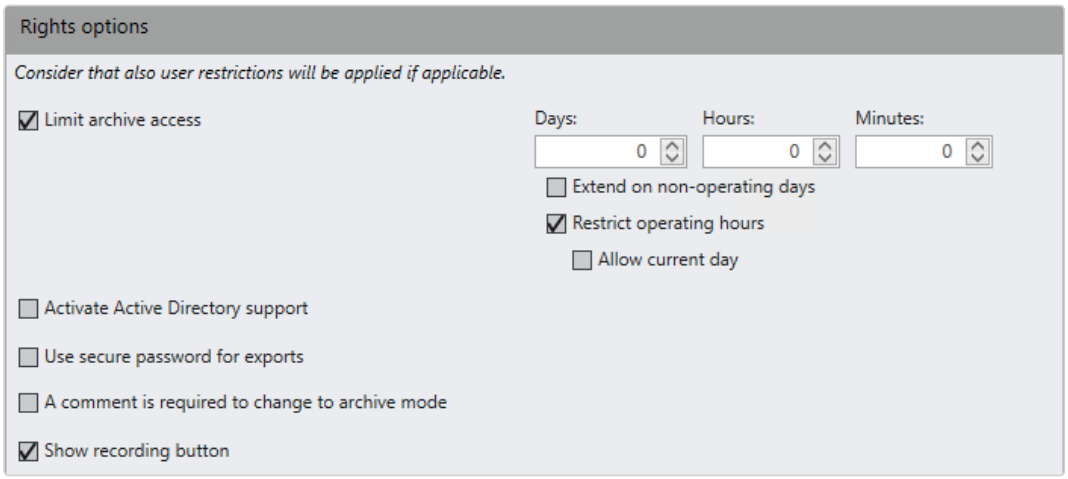


Fig. 195: Groups - Rights options

1. Select **Limit archive access** and specify the duration of the access period (in minutes) in order to limit the group members' continuous access to the archive.
2. Select the number of days, hours, and minutes the group members are allowed to have access to the recording archive.

> **If not visible, the following items are not part of the current license. Public holidays and non-office-days are not recognized for retention time and archive access.**

If a user is in a group, these settings are also taken into account. If the settings between users and groups contradict each other (e.g. 2 days archive access is set for the user, but 3 days for the group), the highest restriction applies (i.e. the user may only see 2 days of archive material).

- Enable **Extend on non-operating days** to include days such as public holidays or non-office days into the extended recording and access management.
- Enable **Restrict operating hours** to hide the archive for the configured area at operating hours.
- Select **Allow current day** as an exception so that the user has the right to view the archive during the opening hours on the current day.

Additionally, the extended recording and access management ("Operating days") can be restricted depending on the user (see "Manage user rights" on page 333).

3. Select **Activate Active Directory support** to apply the authorization settings of a connected Active Directory server.
4. Select **Use secure password for exports**. If a user has the right to export recordings, he has to provide a secure password.
5. Select **A comment is required when changing into archive mode** to force the user to enter a comment when changing into archive mode. This will prevent changing into archive mode without noticing.

Manage group rights

The rights for users and groups are also checked on server side, so even if a hacked client (without any rights check) is used, it is still not possible to configure users, groups or their profiles.

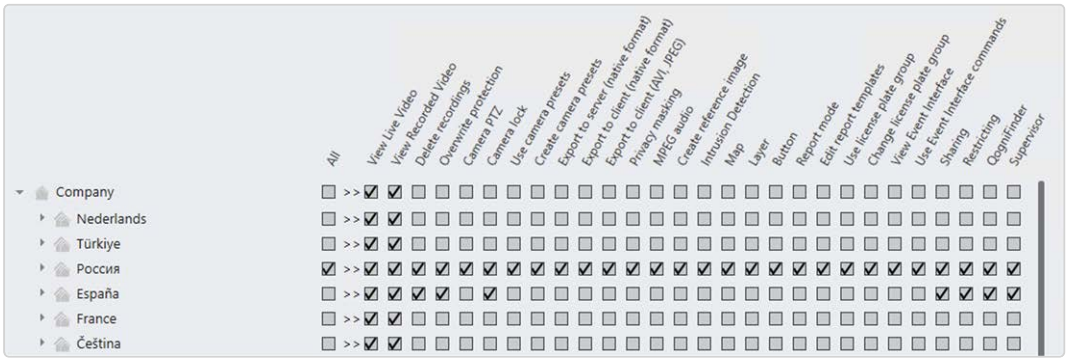


Fig. 196: Groups - Manage group rights

1. Select or deselect the rights to perform specific actions on the installed devices and objects for the selected group (for individual users, see "Manage user rights" on page 333).

Depending on the device or object, the following rights are available, which can be selected or deselected individually or together.

- **All**: Selects or deselects all users rights for the corresponding device or object.
- **View Live Video**: The user can see a camera and its live images in Surveillance mode.
- **View Recorded Video**: The user can use cameras in Archive mode.
- **Delete recordings**: The user can delete recordings in Archive mode.
- **Overwrite protection**: The user can apply overwrite protection to recordings in Archive mode or remove overwrite protection from them.
- **Camera PTZ**: The user can use the PTZ camera including the digital zoom except for preset camera positions.
- **Camera lock**: The user can lock the position of the PTZ camera.
- **Use camera presets**: The user can use the predefined camera positions.
- **Create camera presets**: The user can create camera preset positions or delete predefined positions.
- **Export to server (native format)**: The user can save image data in the Qognify-specific format on the server.
- **Export to client (native format)**: The user can save image data in the Qognify-specific format on the client.
- **Export to client (AVI, JPEG)**: The user can save image data as an AVI or JPEG file on the client.
- **Privacy masking**: The user can deactivate privacy masking.
- **MPEG audio**: The user can use audio transmission.
- **Create reference image**: The user can use the manual reference image comparison from the Tools menu.
- **Intrusion Detection**: The user can use intrusion detection commands, e. g. on maps.
- **Map**: The user can use the corresponding map.
- **Layer**: The user can display defined layers.
- **Button**: The user can use buttons.

- **Report mode**: The user can view report mode.
- **Edit report templates**:The user can create and edit report queries in report mode and save them as templates.
- **Use license plate group**: The user can only use license plate groups when the LPR master data editor is opened automatically if an unknown license plate is detected.
- **Change license plate group**: The user can open the LPR master data editor from the View menu and can fully edit license plates.
- **View Event Interface**: The user can see the event interface items.
- **Use Event interface commands**: The user can change the state of an event interface item e.g on maps.
- **Sharing**: The user is allowed to share a camera with other users and any connected Active Directory group. *To share a camera, the user does not need administrative rights.*
- **Restricting**: The user can edit the restriction settings for cameras.
- **QogniFinder**: The user can search for objects using the QogniFinder in Archive mode.
- **Supervisor**: The user can only see, edit, delete, and potentially execute prepared exports on a branch level to prevent data misuse.

Managing administrative rights

1. Select the corresponding rights in the administration settings for the selected group (see "Manage administrative rights" on page 336).
   - **Create/delete**: The group can administer the selected objects in full and, for example, create and delete cameras.
   - **Edit**: The group can change the settings of the selected objects, but cannot create or delete objects.
   - **View**: The group can view and operate the selected objects but cannot make any settings or create and delete objects.
2. **Apply** the set values if you want to make further settings.
3. **Save** the set values to apply the values and conclude input.

Deleting a group

1. Select the group in the overview.
2. Click **Delete object**.

Duplicating a group

1. Select the group in the overview.
2. Click **Duplicate object**, and enter the name for the duplicated group.
3. Click **OK** to accept the name. The new group is displayed in the overview.

Profiles

The **Profiles** function in the Administration control allows you to assign general settings to a user account or group that apply to the operation and interface settings of the client. For each user and user group a profile is generated automatically. The profiles for the administrator and the administrator group cannot be deleted. The administrator group profile is deactivated by default.

The rights for users and groups are also checked on server side, so even if a hacked client (without any rights check) is used, it is still not possible to configure users, groups or their profiles.

1. Select the location in the **Company** control. The selected location is displayed in the title bar of the Administration control.
2. Select **Profiles** in the Administration control.

General

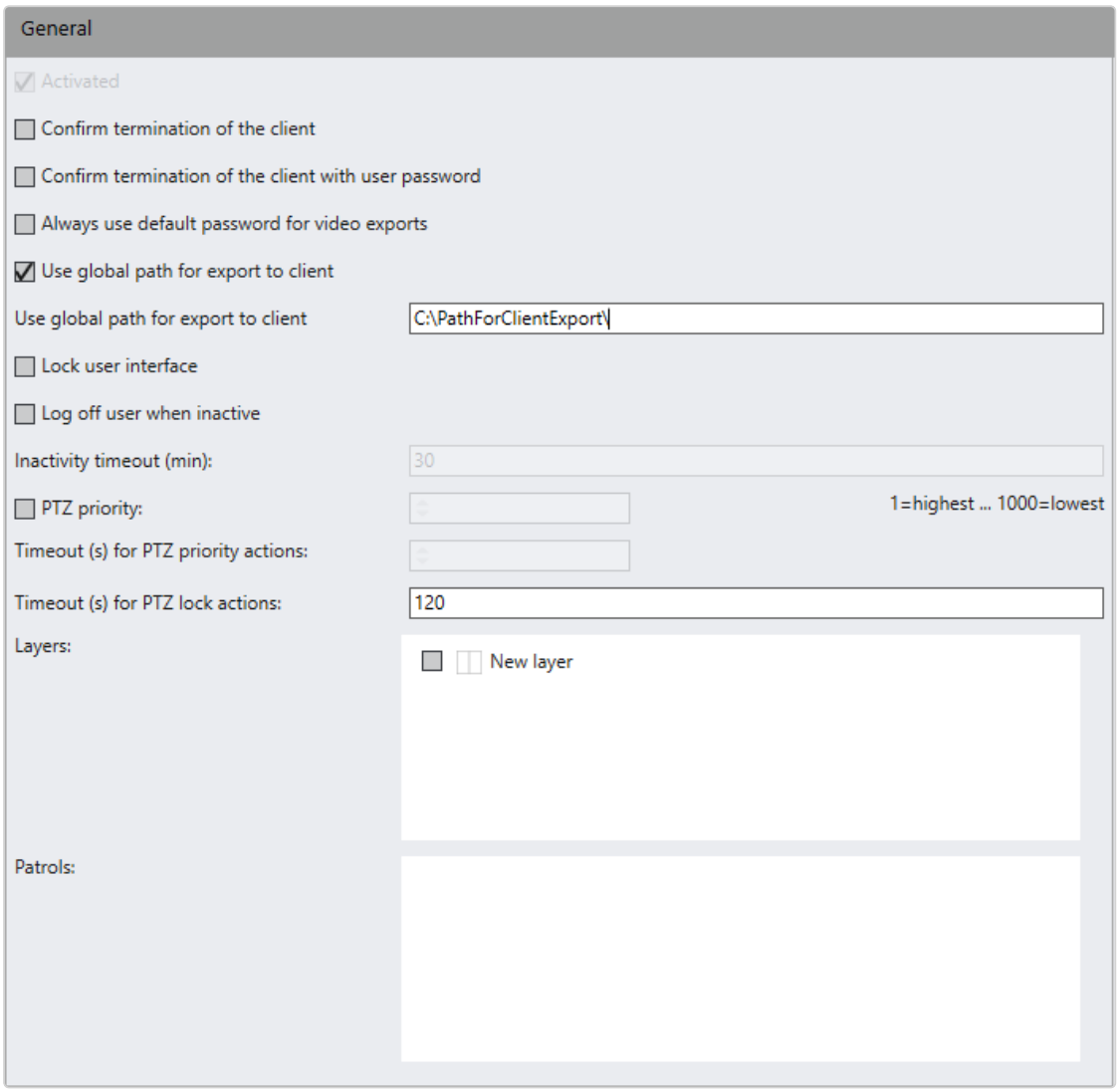


Fig. 197: Profiles - General

1. Activate or deactivate the selected profile.
2. Select **Confirm termination of the client** to display a confirmation on termination of the client.
3. Optionally, select **Confirm termination of the client with user password** to display a confirmation on termination that the user must confirm with his password.

4. Select **Always use default password for video exports** to prevent the user from using a specific password when exporting. The option for entering a specific password is disabled on video export (see "Export of native data to the client" on page 107).

   If the option is set, any user with this profile cannot export to AVI file or save single images even if he has the rights option "Export to Client (AVI, JPEG)" enabled (see "Manage user rights" on page 333).

5. Enable **Use global path for export to client** to make sure that all exports go to a predefined folder. When enabled, enter the path to the export folder. This path is used for all users with the profile for the following export options:

   - Multiple export (native export format to the client, export as *.AVI and *.JPG), see "Multiple export of image data" on page 104
   - Saving single images as *.JPG
   - All exports using the Export Designer, see "The Export Designer" on page 96

6. Select **Lock user interface** if the user should be prevented from changing the user interface (for example moving or resizing the Qognify VMS window).
7. Optionally, select **Log off user when inactive** and specify the **timeout** (time in minutes) after which the user is logged out of the system automatically if inactive.
8. Enter the **PTZ priority** counter between 1 and 1000 (the lower the number: the higher the priority) and specify the **Timeout for PTZ priority actions** in seconds. If the user does not activate any PTZ controls, the camera control is released again after the timeout.

   > **A user (or alarm, or server sequence) with a higher PTZ priority can override another user (or alarm or server sequence) when taking control of the camera.**

9. Enter the **Timeout for the PTZ lock actions** in seconds. If the user locks a PTZ camera in surveillance mode and does not unlock the camera manually, the camera is unlocked automatically after the specified timeout.
10. Select the **Layers** that can be displayed to the user or group (see "Layers" on page 374). The layers are displayed immediately in surveillance mode when starting the client with the related profile and cannot be closed.
11. Select the **Patrols** that the user or group can select if the client is started with the related profile (see "Patrols" on page 391).

Image settings

Image settings specify the quality of video images that are displayed in surveillance mode depending on the user profile.

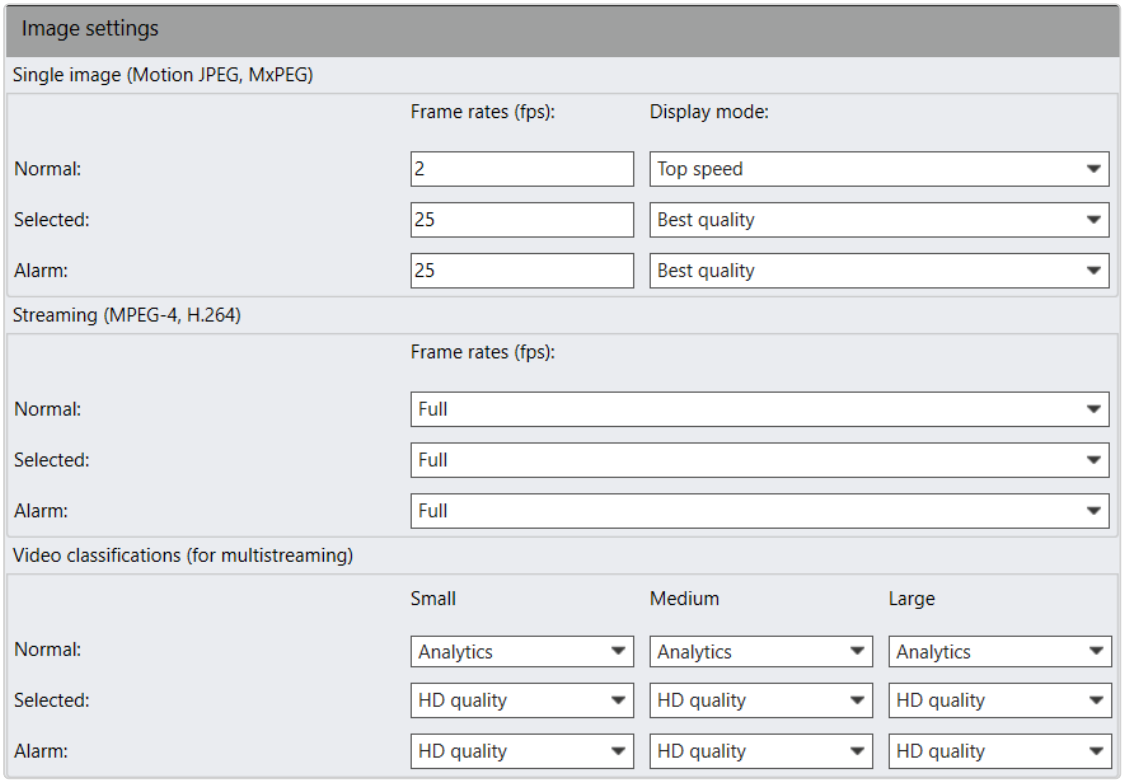


Fig. 198: Profiles - Image settings

Single Image (Motion JPEG, MxPEG)

The single image settings are used to specify how many images the client is to display per camera in a second if the camera sends Motion JPEG images.

> **These settings only affect the view in the client if Motion JPEG is activated as streaming mode in the camera configuration. They have no effect on the recordings.**

1. Specify the frame rates of the displayed **normal** and **selected** video image and of the **alarm** video image.
2. Select the **display mode** that influences the compression rate of the video image.

Streaming (MPEG-4, H.264)

Streaming (MPEG-4, H.264) allows you to specify the frame rate (fps) for MPEG-4, H.264 or H.265 streaming. You can select either full or reduced frame rate.

- **Full**: The complete image flow is transferred with the full frame rate. This can be a heavy load on the client computer if more than four cameras are displayed simultaneously and/or the computer hardware performance is too low.
- **Reduced**: The reduced frame rate only transfers the I-frames (full screens), which significantly reduces the CPU load for the client. The default setting for i-frames is one i-frame per second. In other words, with a reduced frame rate you only see one image per second in surveillance mode. The number of I-frames per second has to be changed the camera configuration (see "Configuring a camera" on page 223).

1. Specify the frame rates of the displayed **Normal** and **Selected** video image and the **Alarm** video image.

Video classification (for multistreaming)

The video classification setting allows you to specify the frame rate for three camera image sizes. If many cameras are displayed in a layer, the resolution of an individual camera can be decreased by selecting a different setting for each image display size:

- Small: for image display sizes up to 320 px
- Medium: for image display sizes between 320 px and 640 px
- Large: for image display sizes above 640 px

By decreasing the resolution, the system performance is improved. Accordingly, the streaming rate can be adjusted to accommodate for the available bandwidth (e.g. HD (high definition), web, mobile).

1. Specify the frame rates and the streaming rate of the displayed **Normal** and **Selected** video image and the **Alarm** video image. If nothing is selected, the streaming will be adjusted automatically.

Video wall module mapping

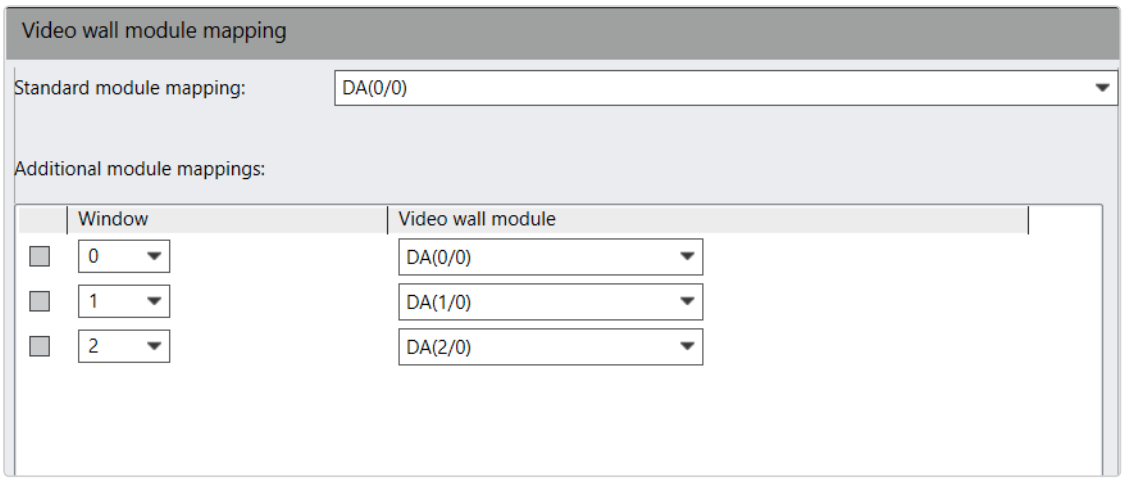


Fig. 199: Profiles - Video wall module mapping

Video wall module mapping allows you to specify whether and in which video wall module an alarm that occurs or a patrol is displayed for the selected profile.

Before video wall modules can be mapped, a video wall (see "eyevis wall" on page 276) or Qognify DisplayAgent (see SeeTec DisplayAgent (video wall)) has to be specified (see "Video walls" on page 398).

1. Select **Standard module mapping** or select which layer window is to be displayed on which video wall module. Standard module mapping is used if you have not defined video wall mapping for the specified Qognify window. Standard module mapping is configured in the video walls control (see "Video walls" on page 398).
2. If the number of module assignments is insufficient, add to the list by clicking the **Add** icon.
3. In **Additional module mappings**, select which window is to be displayed in which video wall module.

   > *Example The main window is displayed as 0/0 in the video wall module. The alarm scenario specifies that the alarm camera is to be displayed in the main window. The image of the alarm camera is displayed in the 0/0 module on the video wall by video wall module mapping.*

4. Select the modules you want to delete, and click **Delete**.
5. **Apply** the set values if you want to make further settings.
6. **Save** the set values to apply the values and conclude input.

Time management

The **Time management** in the Administration control allows you to create time templates that are similar to a schedule in order to coordinate the standard image recording of individual or multiple cameras as well as validity in alarm scenarios and user groups.
Additionally, the extended recording and access management ("Operating days") can be restricted depending on the user (see "Manage user rights" on page 333).

1. Select the location in the **Company** control. The selected location is displayed on the title bar of the Administration control.
2. Select **Time management** in the Administration control.

Configuring the extended recording and access management ("Operating days")

> **If not visible, the following items are not part of the current license. Public holidays and non-office-days are not recognized for retention time and archive access.**

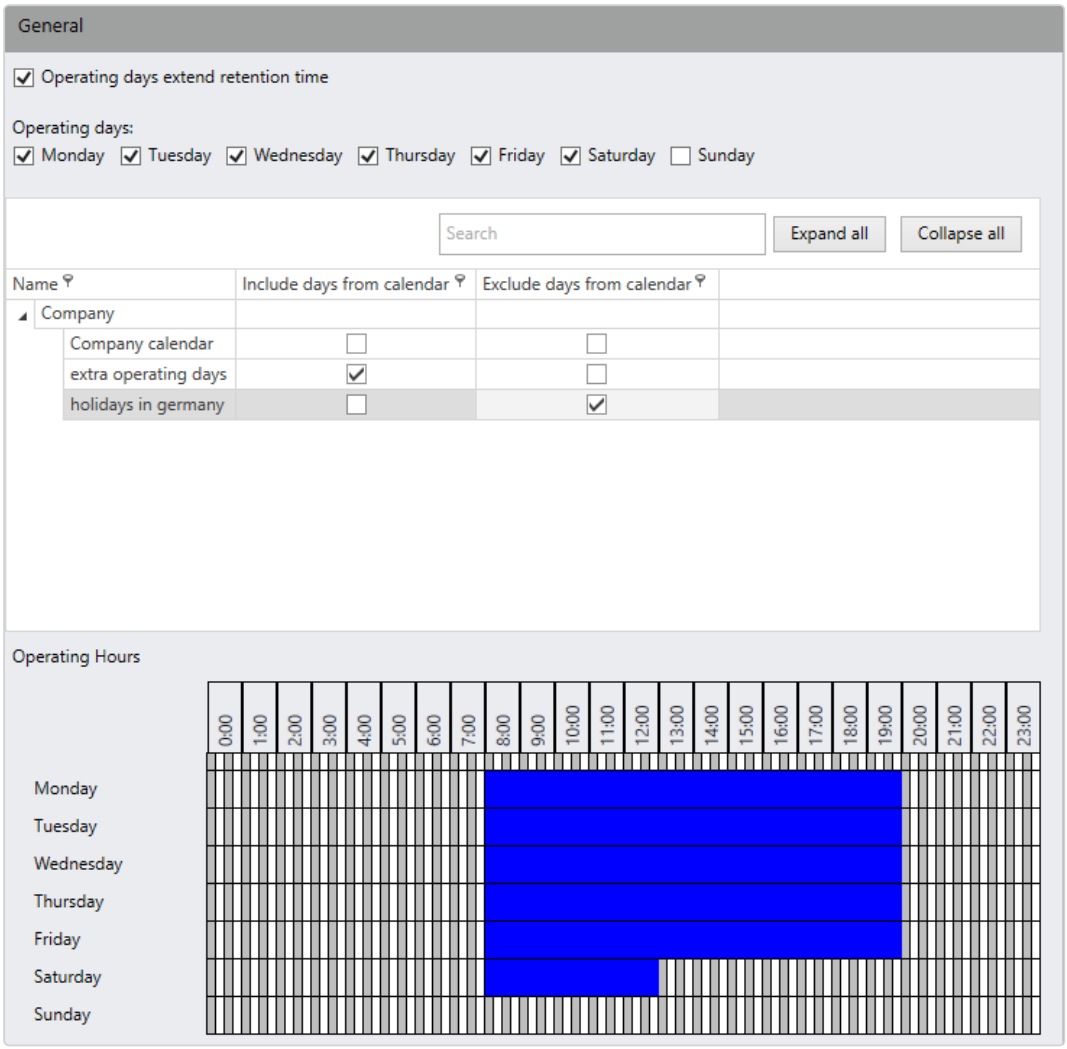


Fig. 200: Operating days

Each calendar day of the week can be marked as an operating day.

1. Select "Operating days extend retention time" to count only operating days for retention time. Non-operating days will extend retention time. Selected include and exclude calendars change the calculation accordingly, e.g. Monday to Friday are marked as operating days and on a camera there is a retention time of 5 days.

Example: Today is Saturday at 00:01: The retention time will be 5 days (Mo-Fr are 5 Days and all days are operating days => 5 Days).

2. Select the operating days.
3. Select the days to include or exclude

   - Include days that are excluded from business days, such as open Sundays.
   - Exclude days such as company holidays or public holidays that fall on a business day.

4. Click and drag the mouse across the calendar to mark the **Operating Hours**.

Creating a new time management template

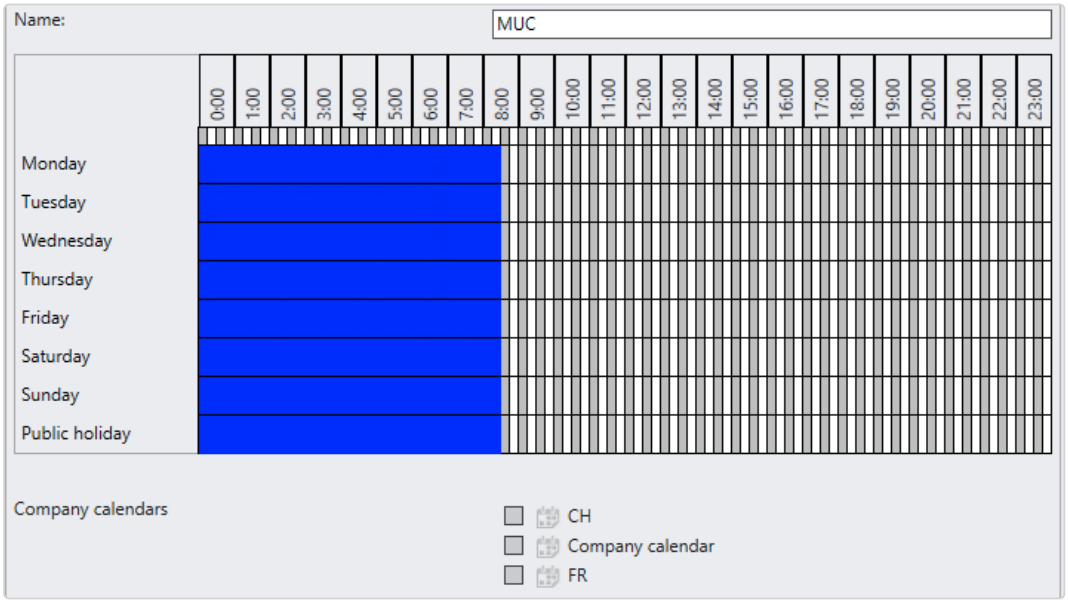


Fig. 201: Time management template

1. Create a new time management template.
2. Enter the name for the new time management template.
3. Click **OK** to accept the name. A calender for defining the time template is displayed.
4. In the calendar, select the periods in which actions are to be performed by holding down the mouse button and dragging the mouse pointer over the period.
5. To remove parts of the selected time sections, hold down the mouse button and drag again over the period.

Configuring a time management template

1. Select the time management template in the overview.
2. Select a branch time pattern if the time management should only apply to the branch, or select the central time management pattern that will apply to all branches.
3. In the calendar, select the periods in which actions are to be performed by holding down the mouse button and dragging the mouse pointer over the period.
4. Select the calendars for which the schedule apply. The calendars are defined in the company calendars (see "Company calendars" below).
5. **Apply** the set values if you want to make further settings.
6. **Save** the set values to apply the values and conclude input.

Deleting a time management template

1. Select the time management template in the overview.
2. Click the **Delete object** icon.

Duplicating a time management template

1. Select the time management template in the overview.
2. Click **Duplicate object**, and enter the name for the duplicated time management template.
3. Click **OK** to accept the name. A calender for defining the time management template is displayed in the overview.
4. Edit the calendar (see "Creating a new time management template" on the previous page).

Company calendars

Each branch of a company can have multiple calendars. Therefore the company as well as each branch has a category named "Company Calendars". The user rights are

managed in the section on user rights (see "Manage administrative rights" on page 336).
In each calendar, you specify the days to be handled in time templates separately from normal weekdays (e.g. public holidays or non-working days). Time templates are created in the time management (see "Time management" on page 351). They allow the precise specification of recording periods or times in which alarm scenarios are started.

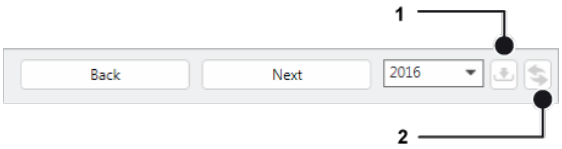


Fig. 202: Configuring the company calendar

1. Select the year for which you want to create a calendar template. Six months are displayed.
2. Click **Next** to display the following six months, or click **Back** to display the previous six months.
3. To navigate to the current date, click **Jump to the current date** (2).

Editing a company calendar

Configuring a calendar

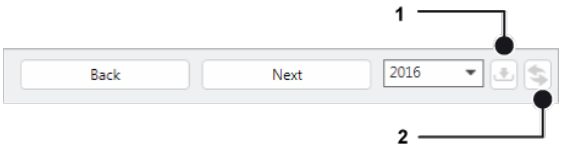


Fig. 203: Configuring a calendar

1. Select the calendar in the overview.
2. Click **Edit object** and enter the new name of the calendar.
3. Click **Import** (1) to enter the public holidays in the company calendar. The templates for public holiday import are in the Qognify installation folder in the "\Client\calendar folder as text files.
4. Select the desired federal states, as appropriate.
5. Activate **Replace holidays** to replace all manually entered public holidays, and click **OK**. The imported data is displayed highlighted in blue.
6. **Apply** the set values if you want to make further settings.
7. **Save** the set values to apply the values and conclude input.

8. Configure the timetables for the calendar days (see "Time management" on page 351).

Deleting a calendar

1. Select the calendar in the overview.
2. Click **Delete object** .

Duplicating a calendar

1. Select the calendar in the overview.
2. Click **Duplicate object**, and enter the **name** of the duplicated calendar.
3. Click **OK** to accept the name. The new calendar is displayed in the overview.

Alarms

Qognify VMS allows you to define complex alarm routines individually. All events that can start an alarm (e.g. motion detection, events from video analysis, license plate recognition (LPR), I/O contact, network I/O, button) can trigger a variety of different actions. These include alarm recording and visualization, sending triggers to third party systems via physical I/O contacts or network I/Os, sending video sequences via email and FTP, as well as launching external programs. Therefore, a customized work-flow can be set up for each alarm situation.
The **Alarms** function on the Administration control allows you to configure and manage alarm scenarios.

1. Select the location in the **Company** control. The selected location is displayed in the title bar of the Administration control.
2. Select **Alarms** in the Administration control.

Creating an alarm scenario

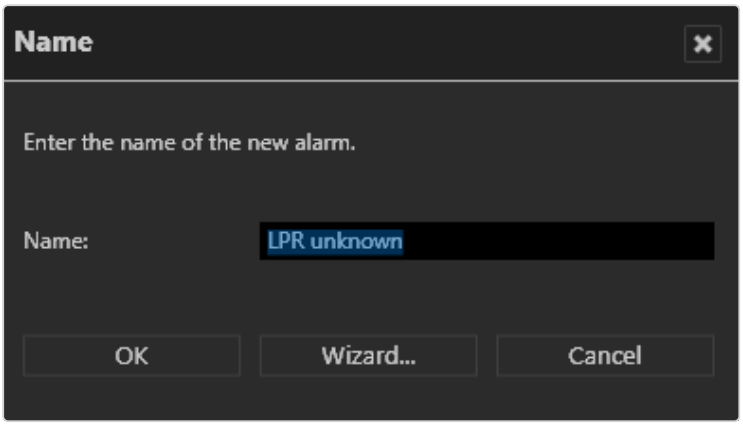


Fig. 204: Creating an alarm scenario

1. Select **Create new object** in the Alarm control.
2. Enter the name for the alarm scenario.
3. If you want to configure the alarm scenario using the configuration wizard, select **Wizard** (see "Creating an alarm scenario with the wizard" below) or confirm the name with **OK**. The new alarm scenario is displayed in the overview.
4. For configuration without the wizard, see "Configuring an alarm" on page 361.

Creating an alarm scenario with the wizard

The alarms are based on the detailed rights concept of Qognify VMS and can be assigned to individual users or user groups. The settings correspond to the steps in the Alarm control (see "Creating an alarm scenario" above).

Events

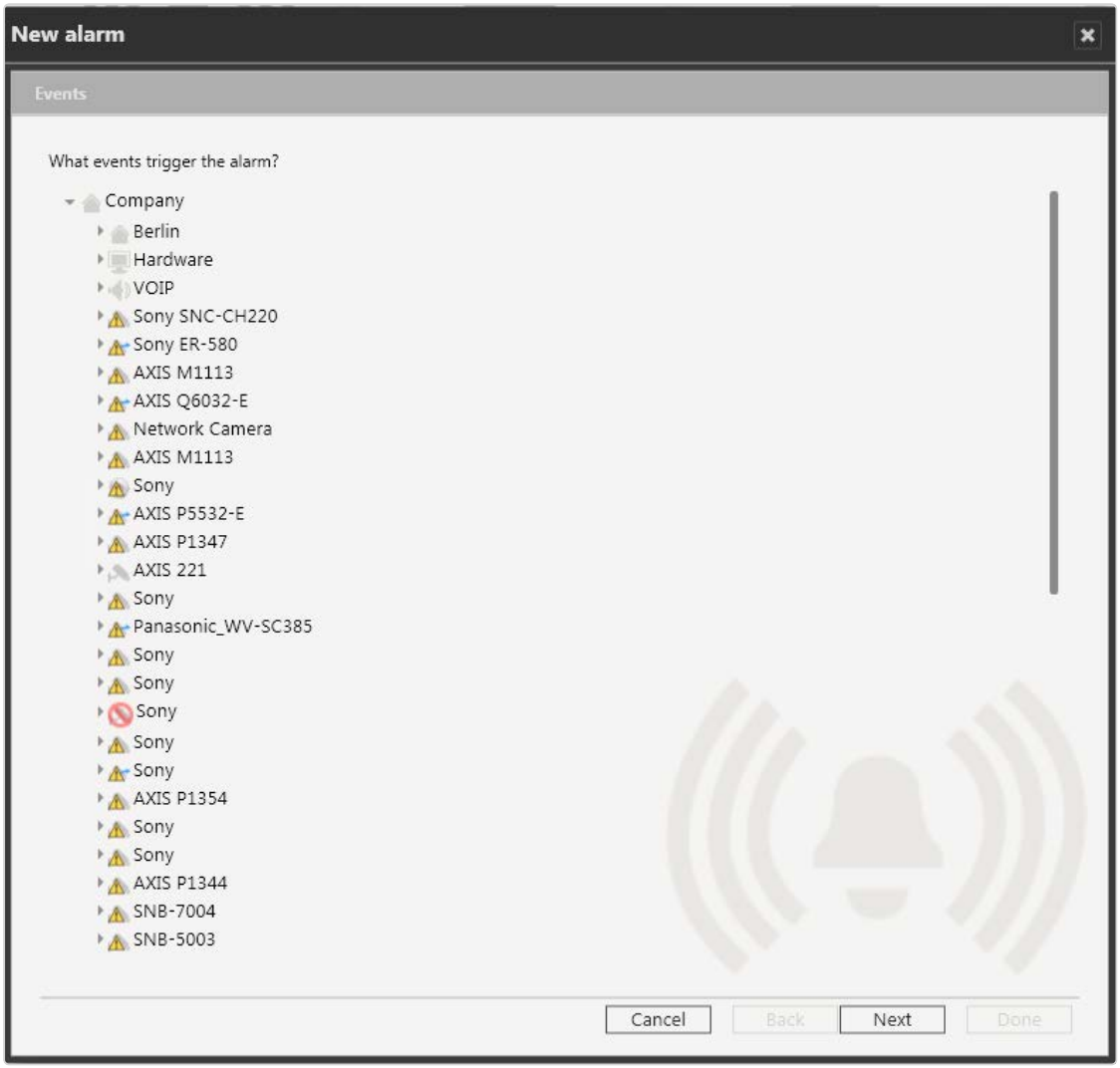


Fig. 205: Alarms - Events

1. Activate the objects that will trigger an alarm event.
2. Click **Next**.

Alarm camera

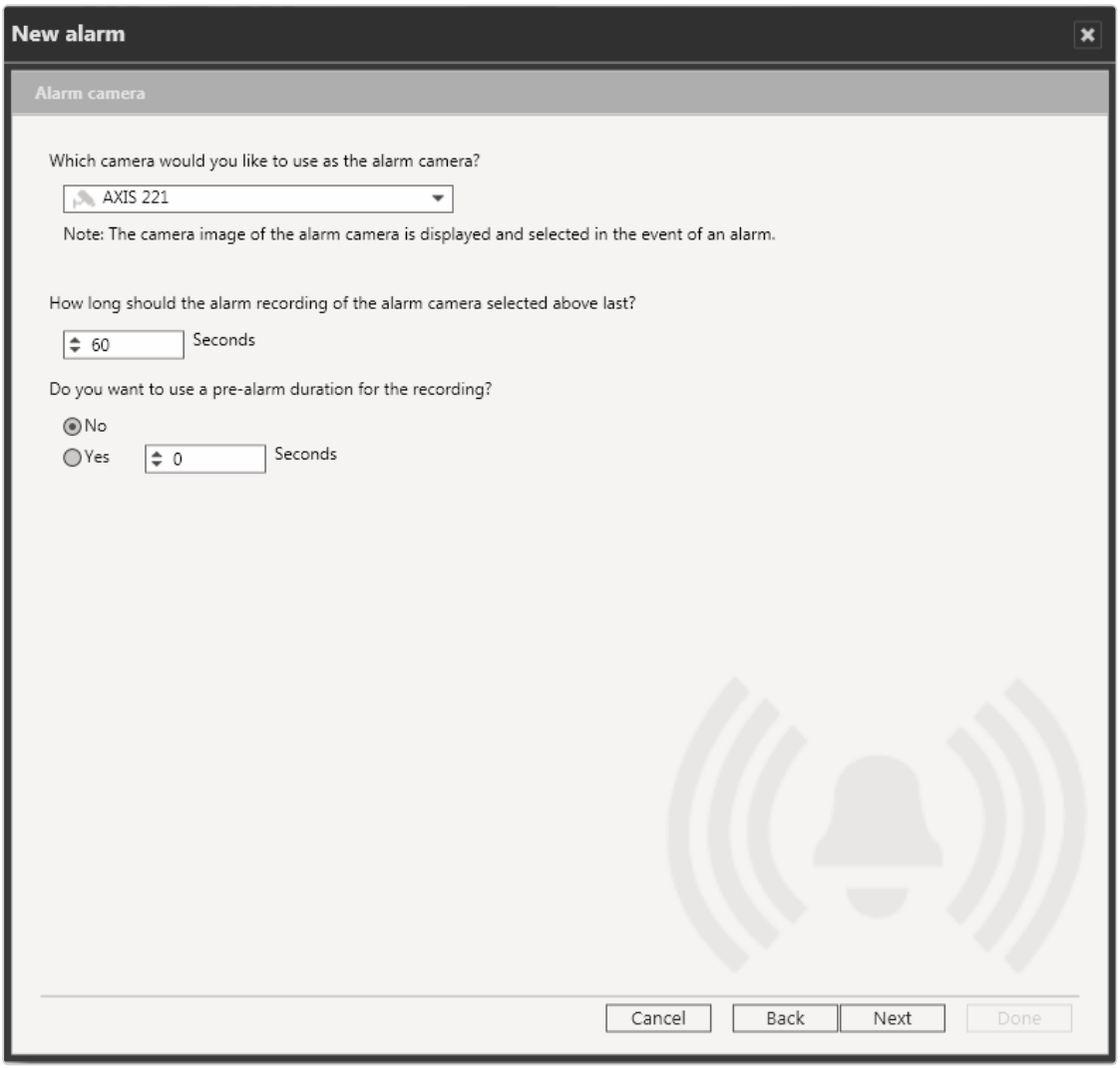


Fig. 206: Alarms - Alarm camera

1. Select the camera that is to be displayed as the alarm camera, and set the duration for alarm recording (in seconds).
2. Specify if you want to add a pre-alarm duration, and set the duration in seconds.
3. Click **Next**.

Users involved

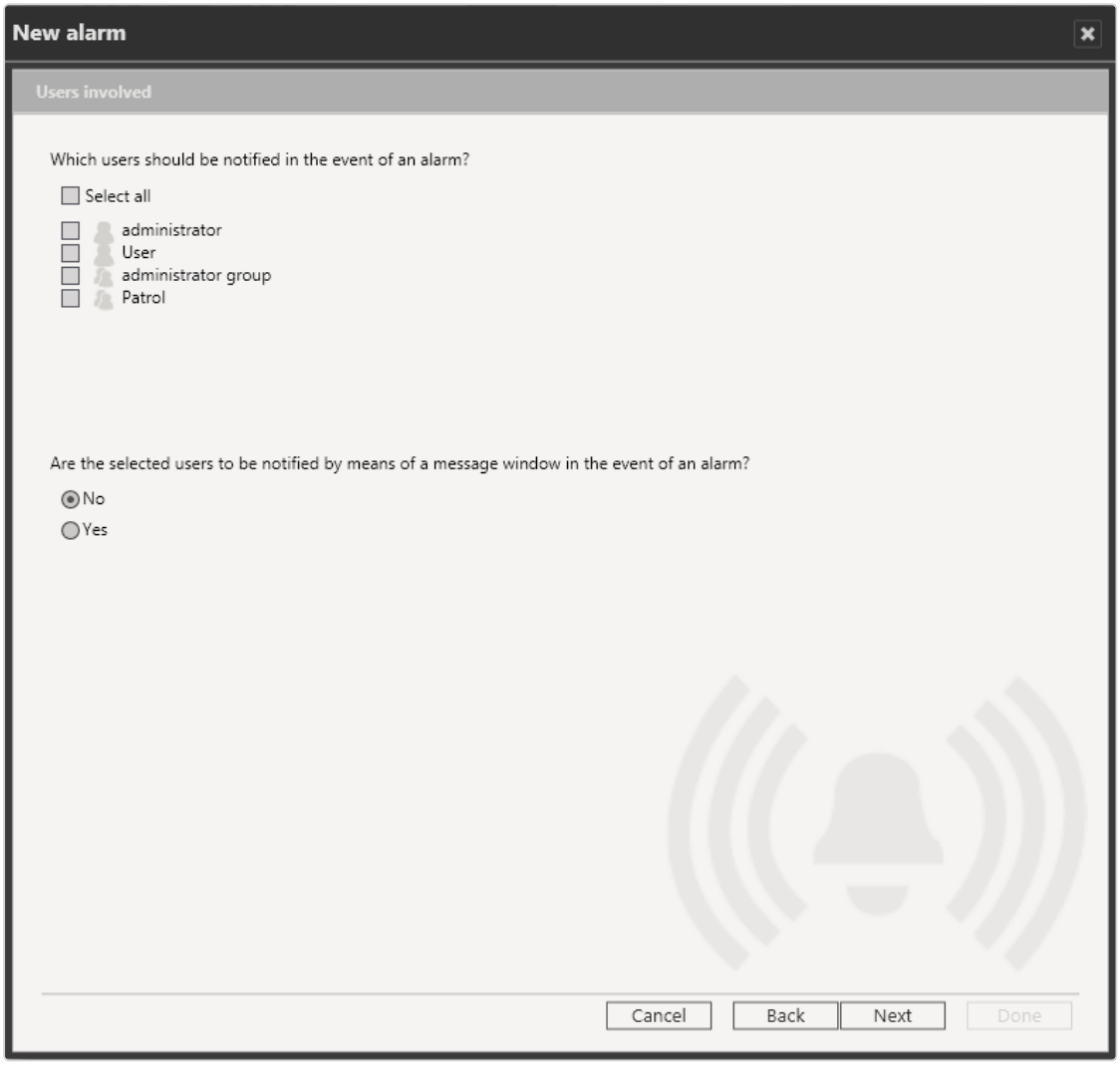


Fig. 207: Alarms - Users involved

1. Specify which user is to be notified by an alarm event. The user must first be created in the User control (see "Users" on page 329).
2. Specify if the user is to be informed of an alarm event by an alarm notification (see "Alarm messages" on page 158).
3. If the user should be informed by a message window, enter a short message.
4. Click **Next**.

Summary

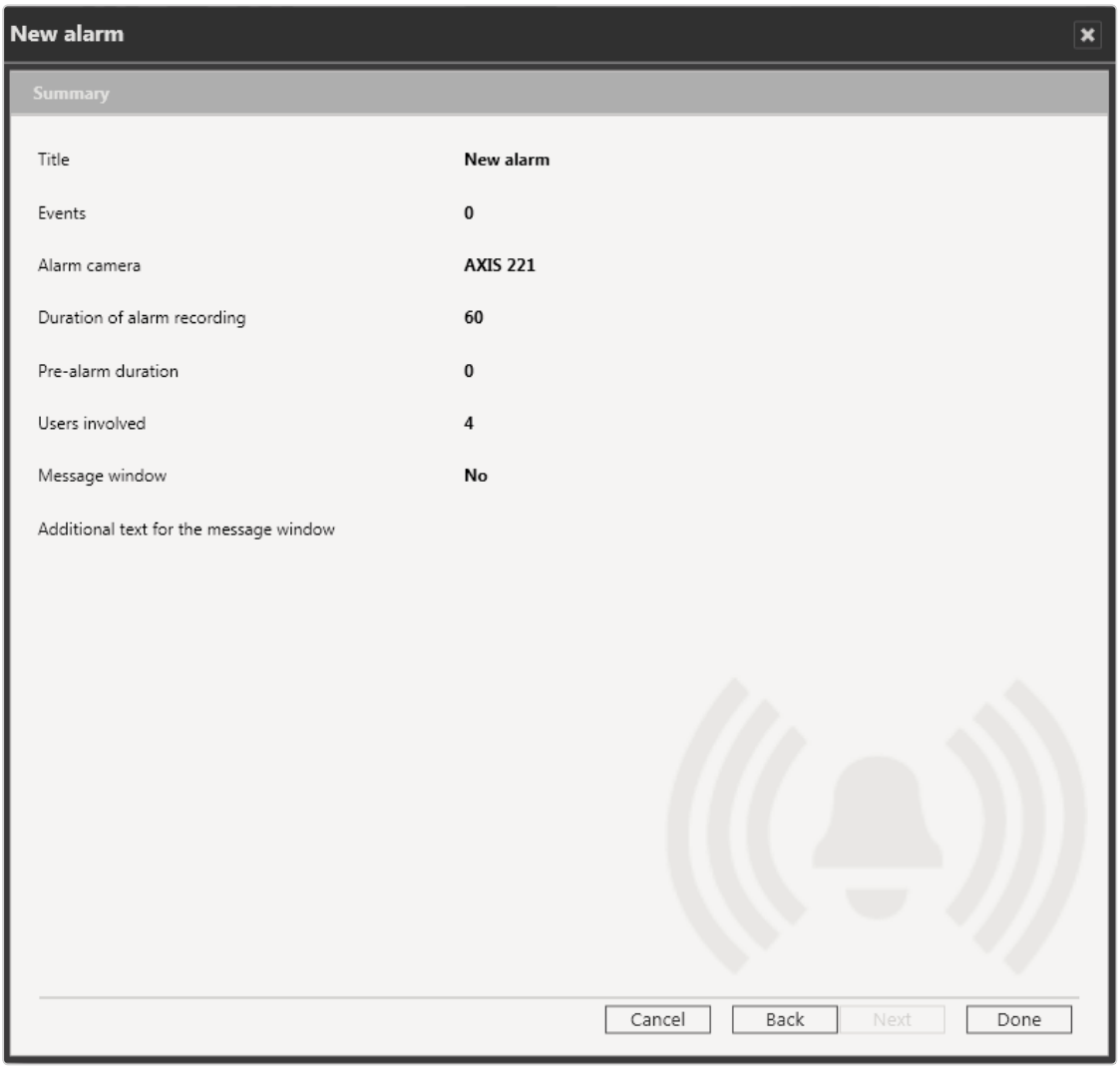


Fig. 208: Alarms - Summary

1. Check the settings.
2. To make changes, select **Back** and change the settings.
3. To apply the settings, select **Done**.

Configuring an alarm

1. Select the alarm in the alarm overview.

General

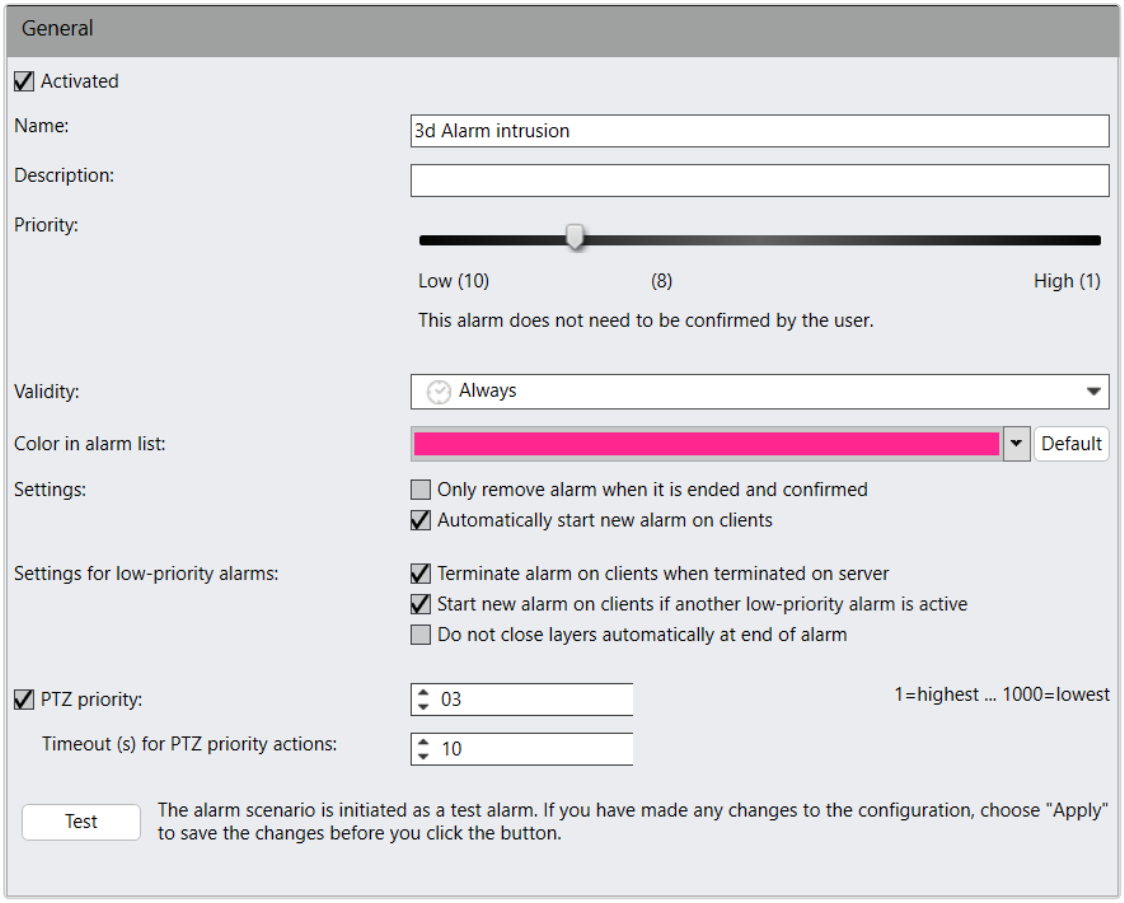


Fig. 209: Alarms - General

1. Select or deselect the alarm scenario.
2. If necessary, alter the **Name** of the alarm.
3. Enter a **Description**.
4. Use the slider to assign the alarm a **Priority**. The meaning of the priority level is displayed. An alarm with low priority can be stopped immediately at the end of the alarm. All dynamically opened components (layers, cameras and message windows) are closed again, and the previous layer is restored. Alarms with medium or high priority are not stopped until they have been confirmed. This is configurable in the settings for low-priority alarms (see below).
5. Select the **Validity** period for the alarm. The alarm is only active within the specified validity period. The possible periods are specified in the Time Manager (see "Time management" on page 351).
6. Select the **Color in alarm list**. The alarms are displayed in the alarm list in surveillance mode and in archive mode in the selected color.

7. Activate **Only remove alarm when it is ended and confirmed** to remove the alarm from the list only when its status has been set to "confirmed" and the alarm has ended (see "Alarm list and system messages" on page 158).
8. Deactivate **Automatically start new alarms on clients** to prevent the alarm from starting events. If deactivated, the user must start the assigned alarm events manually.
9. Select the **Settings for low-priority alarms**.
10. **Terminate alarm on clients when terminated on server**: The alarm is terminated on all of the clients involved and removed from the alarm list.
11. **Start new alarm on clients if another low-priority alarm is active**: A low-priority alarm displaces another active low-priority alarm. In other words, the current alarm is put aside, and the new alarm is displayed.
12. **Do not close layers automatically at the end of the alarm**: Prevents the layer from being automatically closed at the end of the alarm. This also keeps alarm cameras focused on the alarm tile even when the alarm is disabled (also refer to).
13. Enter the **PTZ priority** counter between 1 and 1000 (the higher the number: the lower the priority) and specify the Timeout for PTZ priority actions in seconds. If the alarm does not activate any PTZ controls, the camera control is released again after the timeout.

> **A user (or alarm, or server sequence) with a higher PTZ priority can override another user (or alarm or server sequence) when taking control of the camera.**

Start

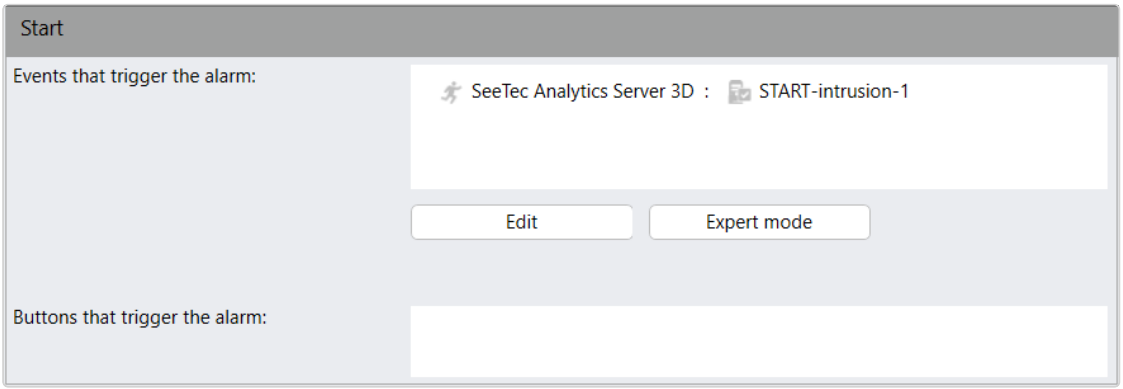
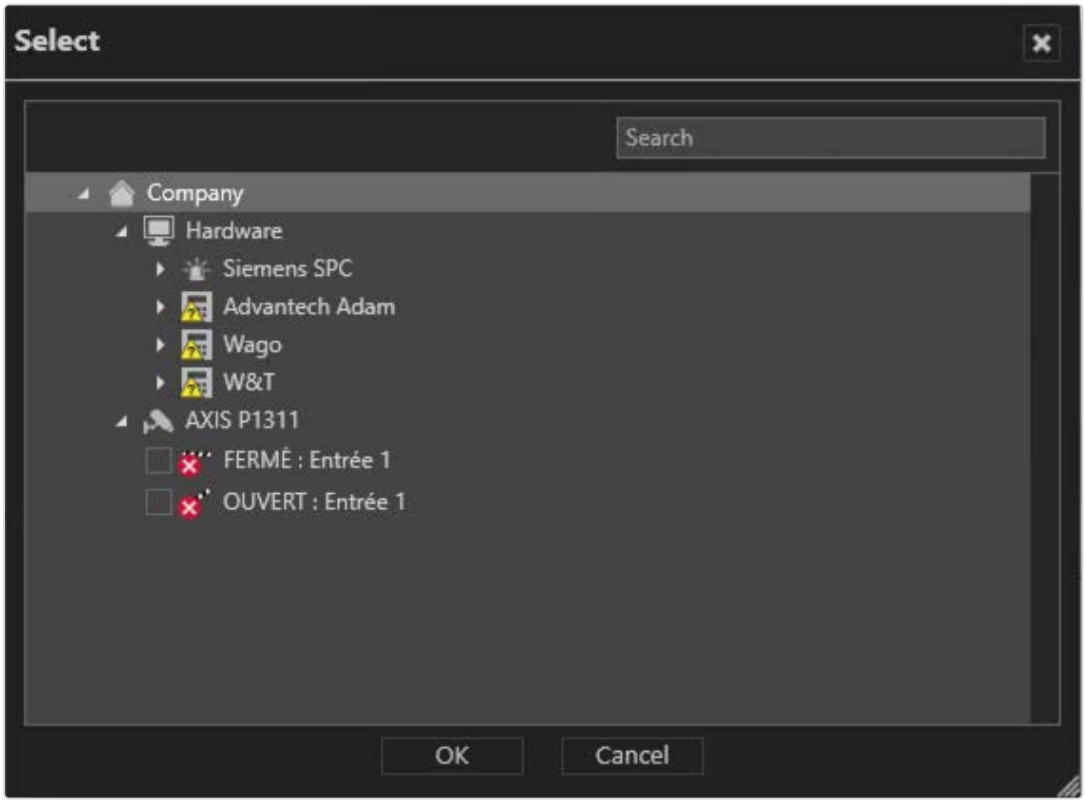


Fig. 210: Alarms - Start

Depending on the camera model or other hardware used, the following events can be used as triggers for an alarm scenario:

- Tampering: The camera angle is changed or the camera lens is covered.
- Video signal lost: The connection between the analog camera and the video server is cut.
- Motion detection: Significant motion has been detected in a defined area of the camera image.
- Digital I/O: An incoming digital signal triggers an alarm.
- VoIP events like starting or stopping a VoIP session
- Triggers from external interfaces like (access control systems, alarm systems)

1. Click **Edit** to select the **Events that trigger the alarm**. The hardware and event are displayed. You can select multiple objects.



The trigger must be created or activated before configuring the alarm scenario. One exception to this are buttons, which can be defined later in the buttons control (see "Buttons" on page 386). A starting event can be, for example, the receipt of a TCP signal from a camera when it detects motion. This is implemented via the Qognify network I/O.

2. Click **Expert mode** to specify the settings.

Expert mode

Expert mode can be used to create complex alarm scenarios. The alarm is triggered by different conditions that are logically linked (AND / OR conditions).

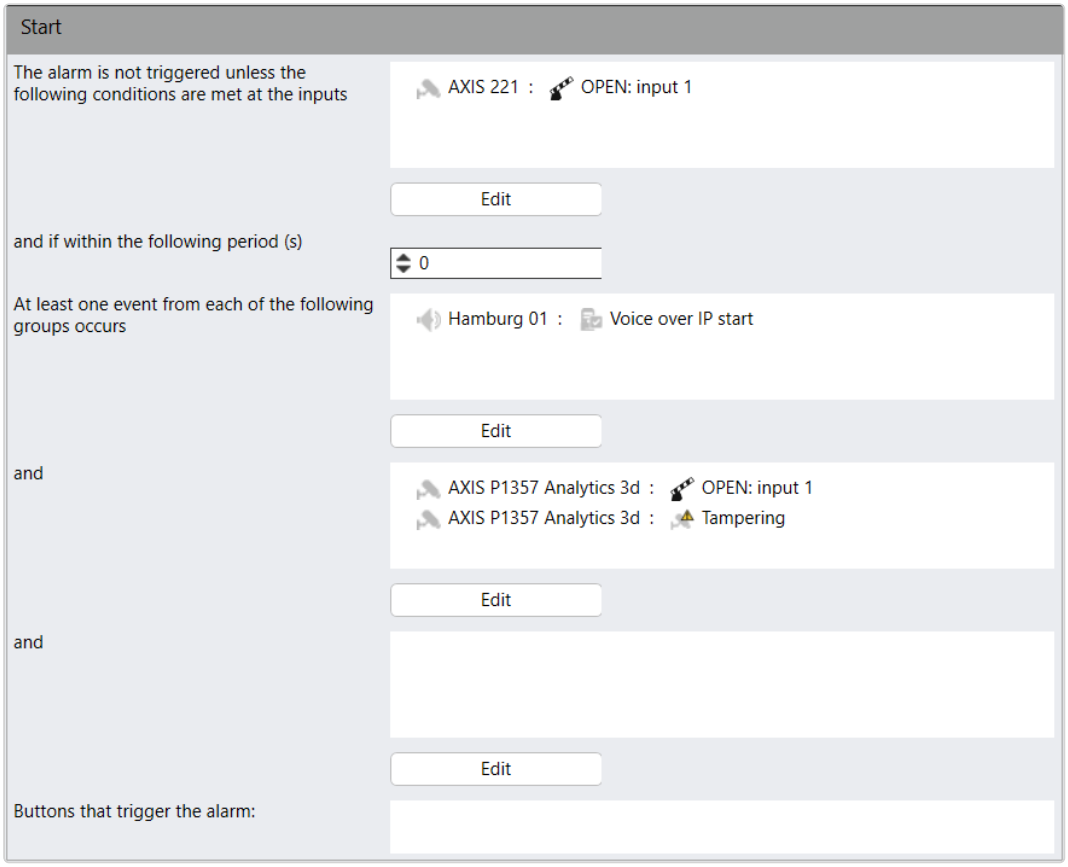


Fig. 211: Alarms - Expert mode

1. Click **Edit** and select the conditions at the (digital) inputs that must be fulfilled to trigger an alarm.
2. Set the **period** (in seconds) within which at least one of the following events from each group occurs.
3. To add the events to the condition, click **Edit** and select the relevant objects.

End

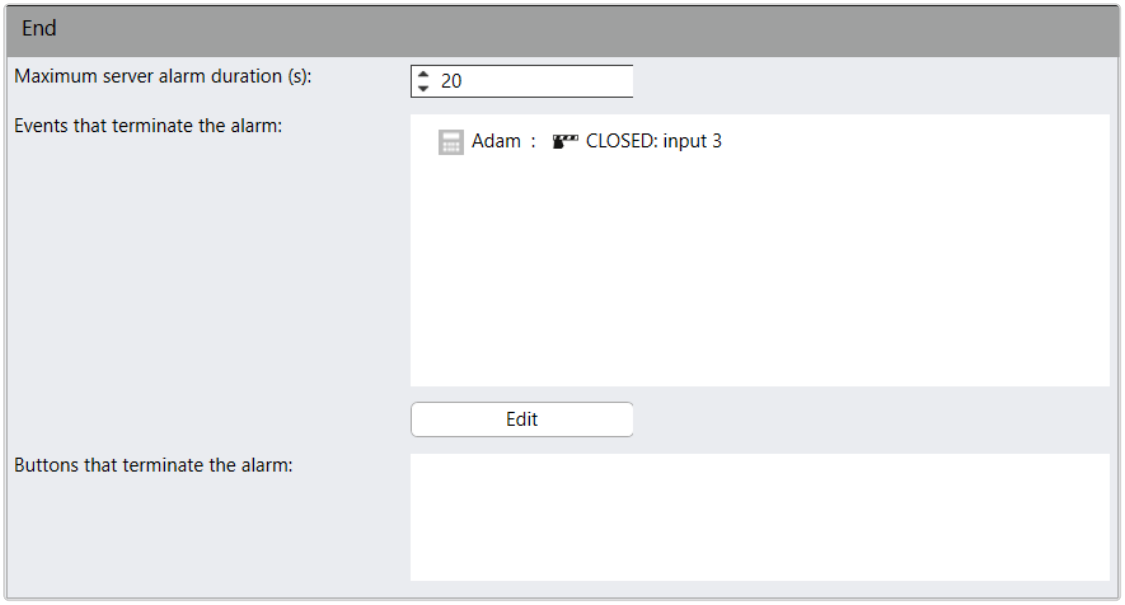


Fig. 212: Alarms - End

1. Specify the **Maximum server alarm duration** (in seconds) to specify how long the alarm is to be recorded for.
2. Click **Edit** to select the **Events that terminate the alarm earlier**. The hardware and events are displayed.

Visualization

In the visualization section you define how alarms are visualized on the client.

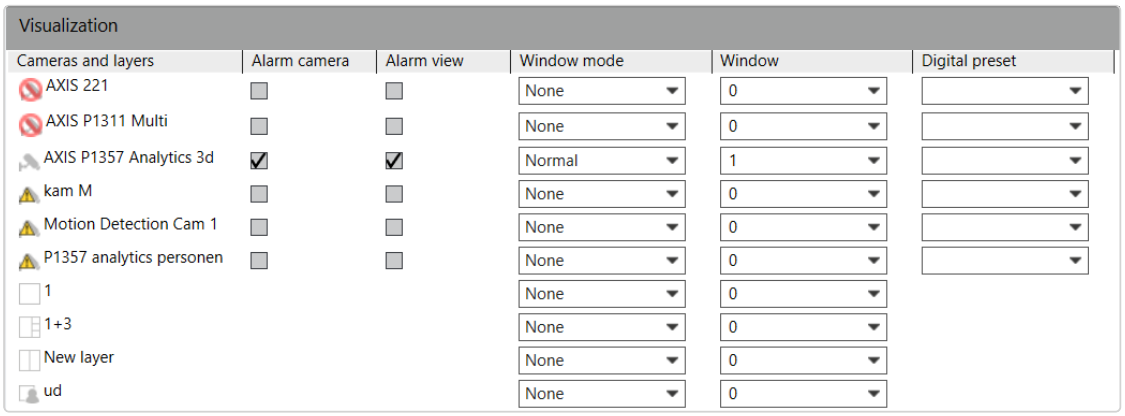


Fig. 213: Alarms - Visualization

There are three types of views which can also be combined:

- **Alarm camera**: The alarm camera is highlighted by a red frame in the various windows in surveillance mode.

- **Alarm views**: The alarm records of the selected camera are displayed in the selected window in four tiles in a 2x2 view: pre-alarm, post-alarm, alarm image (still image) and live image.
- **Layers**: Layers can include multiple cameras arranged in tiles. They can also include maps (see "Layers" on page 374).

An alarm with low priority is stopped immediately at the end of the alarm, i.e. all dynamically opened components (layers, cameras and message windows) are closed and the previous layer is restored. Alarms with medium or high priority are not stopped until they have been confirmed.

1. Activate the **Cameras and layers** to be displayed in the various windows in surveillance mode. The window mode is automatically set to the **normal** view.
2. Choose if the cameras to be displayed as an alarm camera and/or in alarm view.
3. Select **Normal** mode or **Full-image** mode for the **Window mode**.
4. Select the option **Window** to display the camera or layer in the main window or in a secondary window.

   This option is only available when Window mode is not set to "None".

5. Select the option **Digital Preset** to display a digital preset (see "Camera positions / digital presets" on page 249).

   This option is only available when Window mode is not set to "None".

Cameras and layers, and also alarm cameras cannot be displayed in the same window.

Persons involved

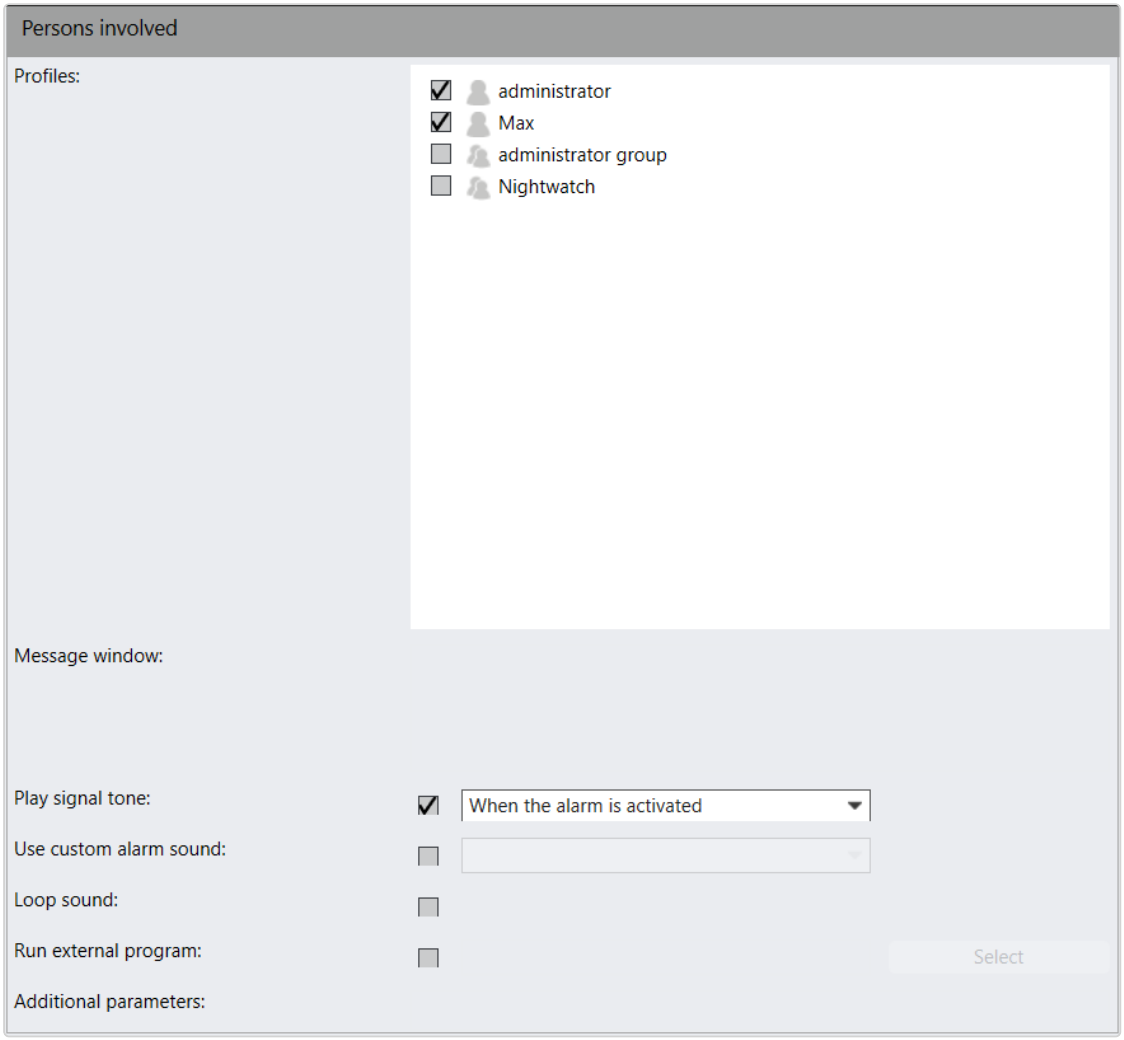


Fig. 214: Alarms - Persons involved

The alarms are only displayed for the selected profiles.

> **For the AlarmWatchDog function (see "The AlarmWatchDog" on page 535), the users defined in the system settings must be activated.**

1. For **Profiles**, select the users or groups allowed to see the alarm.

   > **The visualization of the alarm is also dependent on the user profile of group profiles (see "Profiles" on page 345).**

2. Enter a text for alarms with a medium or high priority level in the message window. This text is displayed in the **Message window**.

3. Select **Play signal tone**, and select if the signal tone is to be played when the alarm is activated by the alarm scenario or triggered manually by the user.

   The alarm tone is in the file system in "<installation folder>/Client/Sound" or "<installation folder>/Client64/Sound" and can be replaced with different *.wav files.

4. Optionally, select a custom alarm sound (see "Managing sound and icon files with custom media" on page 447).
5. Optionally, select to loop the alarm sound.
6. Activate **Run external program** if a program is to be started at the same time as the alarm and select which document is to be opened by the program. The selected program must be installed on the client computer.
7. Enter **Additional parameters** required by the program. A document can be opened using the selected program, for example.

Server

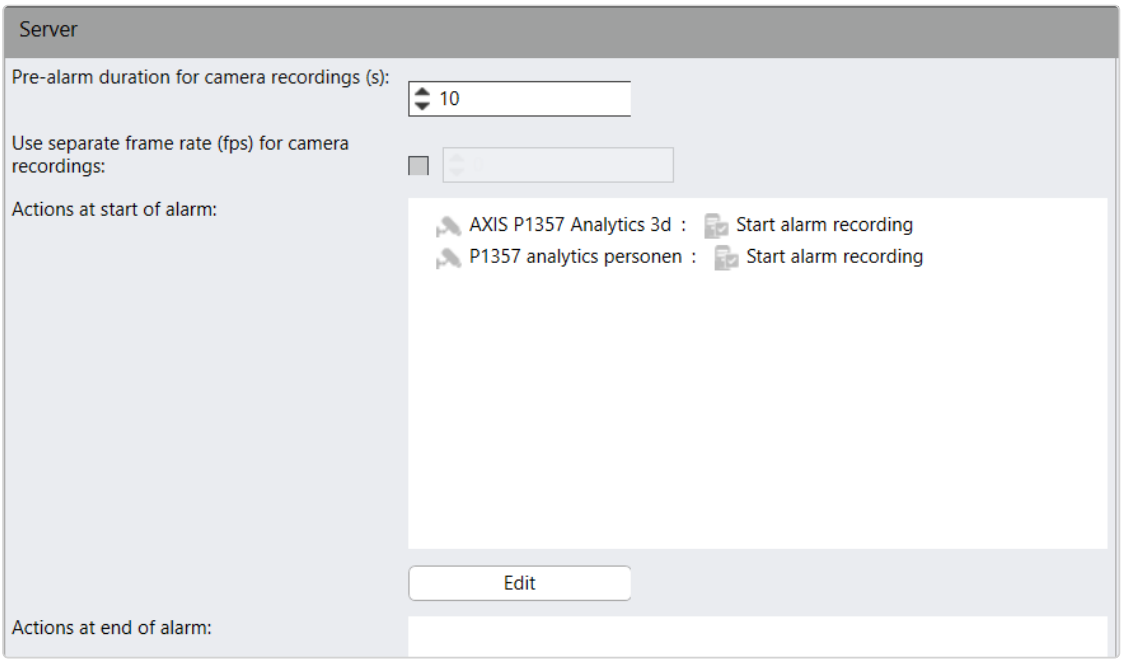
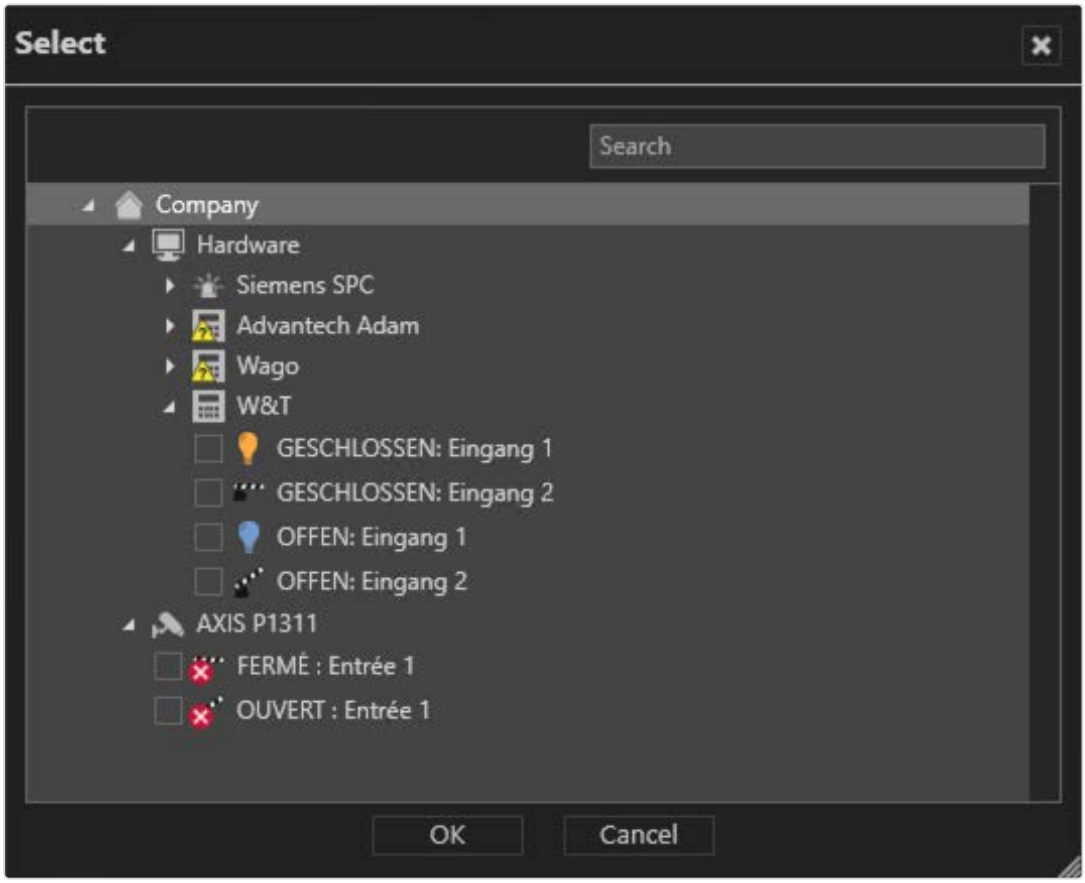


Fig. 215: Alarms - Server

1. Specify the **Pre-alarm duration for camera recordings** (up to a maximum of 3600 seconds) to record a period before the alarm is triggered in alarm recording.

   > **If standard recording is deactivated, the maximum recording duration is limited by the pre-alarm buffer time (see "Multimedia database" on page 469 configuration).**

2. Select **Use separate frame rate (fps) for camera recordings**, and enter the required frame rate. The frame rate can only be changed with M-JPEG.
3. Select **Edit**, and activate the **Actions at start of alarm**. The selected actions are displayed.



4. Select **OK**.
5. Select **Edit**, and activate the **Actions at end of alarm**. The selected actions are displayed.

The following Alarm actions are available:

- **Hardware**
  - Outputs on I/O modules from Adam, Axis, W&T, Wago or Qognify network I/Os etc. can be opened or closed.

    > **The outputs must be activated on the related modules.**

  - License plate recognition can be started on LPR modules
- **Server controlled sequences** can be started or interrupted (see "Sequences" on page 394).
- **Server** On Device Managers Video Data Export can be started (see "Video backup" on page 409).
- **System Manager**
  - A SNMP action can be triggered to a configured SNMP Server (see "Configuring the SNMP server" on page 442).
  - An Alarm Watchdog Action can be triggered to show the alarm in the Alarm Watchdog (see "The AlarmWatchDog" on page 535).
  - A notification can be send to an EBÜS interface.
- **Cameras**
  - Alarm recordings can be started or stopped.
  - Preset positions can be triggered.
  - Outputs can be opened or closed.

Email and FTP

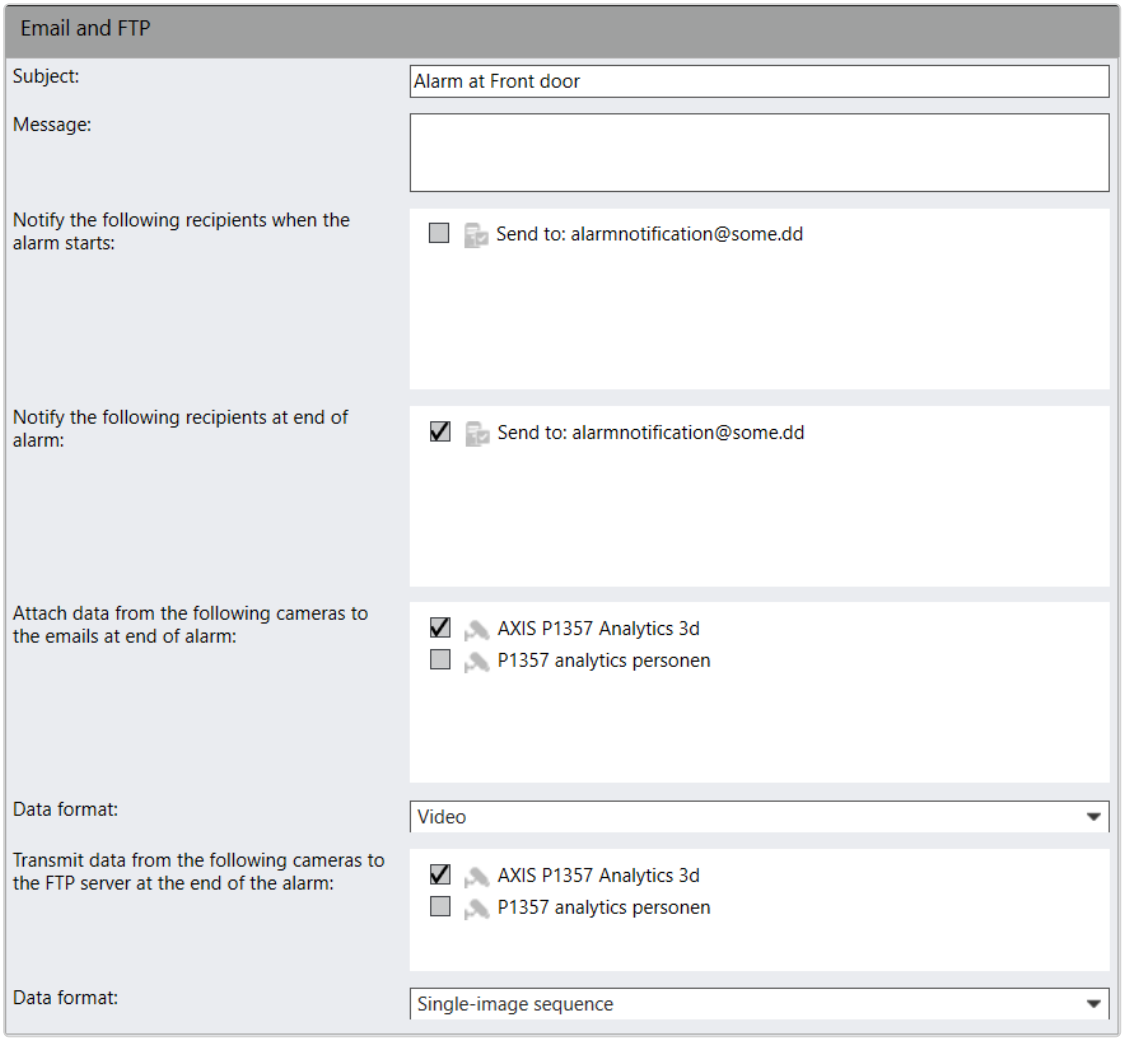


Fig. 216: Alarms - Email and FTP

> **The SMTP server for e-mails and the email addresses must be created in the System control to enable the system to forward the messages (see "Configuring the SMTP server" on page 441).**

In case of an alarm it is possible to send a standard email or specify a data export to an FTP server in addition to the alarm message.

1. Enter the **Subject** and text for the email **Message**.
2. Select the **Recipients** to receive the email at the start and end of the alarm. You can specify the email addresses in the section "Alarm addresses and system addresses" of the system settings (see "Alarm addresses and system addresses" on page 442).

3. Select **Attach data from the following cameras to the emails at end of alarm** to specify which camera data are attached to the email and specify the **Data format**. Two types of file format are possible:
   - Video: the files are sent unencrypted as *.avi (see "Video Backup/Export" on page 252).
   - Single image sequence: the files are sent as image sequence (JPEG).

   > **Note that the email attachments can exceed the permissible size of the email.**
4. Select the cameras whose data is to be stored on an FTP server when there is a large volume of data, and specify the **Data format**. The FTP server is defined in the Qognify VA Administration Tool (see "Qognify VMS VA Administration Tool" on page 476).

   > **If there are problems contacting the FTP server at alarm end, e.g. the FTP server is not available, the program retries sending the data to the FTP server once every minute. After one hour the attempt is canceled and the data are discarded.**
5. **Apply** the set values if you want to make further settings.
6. **Save** the set values to apply the values and conclude input.

Deleting an alarm

1. Select the alarm in the overview.
2. Click **Delete object**.

Duplicating an alarm

1. Select the alarm in the overview.
2. Click **Duplicate object**, and enter a name for the duplicated alarm.
3. If you want to configure the new alarm using the configuration wizard, select **Wizard** in the dialog box (see "Creating an alarm scenario with the wizard" on page 357).
4. Click **OK** to accept the name. The new alarm is displayed in the overview.

Layers

The **Layers** function in the Administration control allows you to adjust the work area to suit your requirements in surveillance mode by dividing it into multiple tiles. This gives the user fixed arrangements and contents of the work area also in multi-installation environments. These layers can be assigned to a user or group profile and are available after the program starts up.

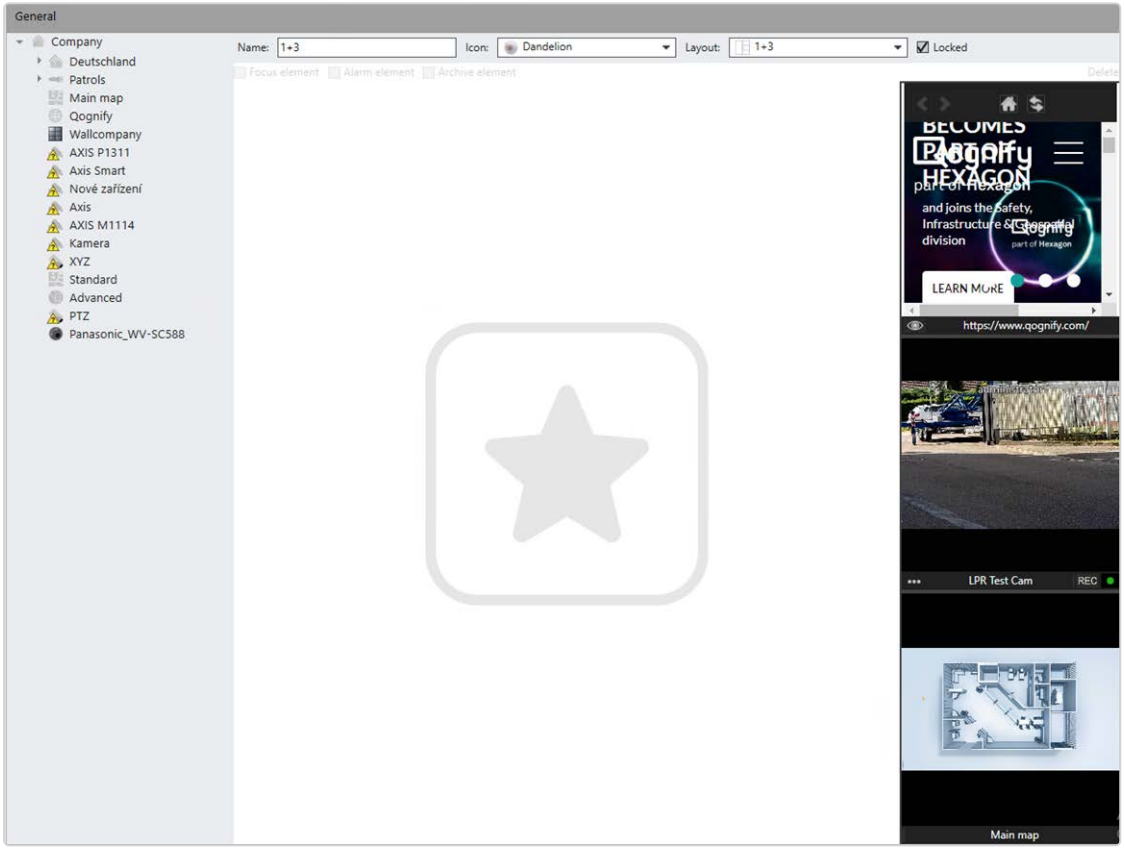


Fig. 217: Layers

1. Select the location in the **Company** control. The selected location is displayed in the title bar of the Administration control.
2. Select **Layers** in the Administration control.

Creating a new layer

1. Click **Create new object** in the layers control bar.
2. Enter the **Name** of the new layer
3. Select the **Type** of layout.
4. To specify the number of tiles yourself, choose **User-defined** from the drop-down list.

5. Click **OK** to apply the setting. The new layer is displayed in the overview.
6. If you have chosen **User-defined**, alter the number of rows and columns in the layer. A maximum of 100 fields is available (64 x 1 or 9 x 7).
7. Drag the mouse cursor over any number of adjacent tiles and click **Connect** to group the selected tiles together as a single tile.
8. Click a group tile and **Disconnect** to separate it into the original number of tiles.
9. Click **OK** to apply the setting. The new layer is displayed in the overview.

Configuring a layer

1. Select the layer in the overview.
2. If necessary, change the **Name** of the layer.
3. Select an **icon** for the layer from the drop-down menu. The selected icon is displayed in the overview in surveillance mode.
4. Select a **layout** from the drop-down-menu. The selected layout is displayed.
5. To unlock a layer, deselect **Locked**. This will unlock the current layer and enable changing the layout. To prevent changes, the layer is locked by default.
6. Drag the cameras, patrols, maps, or web pages to the layer window in accordance with the selected arrangement.

> **All elements of the selected patrol except for camera operations are ignored in the layer.**

Adding audio-only sources

1. To add objects as audio-only sources, drag the source to an empty tile and select  .
2. Select "Audio only". The source view is reduced to a bar at the bottom of the layer.
3. Drag additional audio-only sources directly into the empty bottom bar.

> **Up to four audio-only sources can be minimized.**

7. Click a tile with a camera and select the option **Focus element**. You can mark a tile as a focus tile in every layer. When double-clicking a camera in a layer with a focus tile, the camera image is displayed in the focus tile. When clicking twice on a camera image in a layer without a focus tile, the camera image is displayed in a separate layer.
8. Click a tile with a camera and select the option **Alarm element**. If the layer is visible when an alarm is activated, the alarm cameras will be switched to the alarm tiles in a sequential order.

- For keeping alarm cameras on the alarm tile with the option “Do not close layers automatically at the end of the alarm” even when the alarm is deactivated (see "Configuring an alarm" on page 361.)

> **If there are more alarm cameras in an alarm than visible alarm tiles, the remaining cameras are ignored.**

9. Click a tile with a camera and select the option **Archive element**. When opening a layer with archive element, the camera shows video footage of the previous 30 seconds and an active archive timeline is displayed. When an alarm is configured and active, the camera displays the 30 seconds leading up to the alarm.
10. To remove a camera from the layer, select the camera and click **Delete**.
11. **Apply** the set values if you want to make further settings.
12. **Save** the set values to apply the values and conclude input.

Deleting a layer

1. Select the layer in the overview.
2. Click **Delete object** .

Duplicating a layer

1. Select the layer in the overview.
2. Click **Duplicate object**, and enter a name for the duplicated layer.
3. Click **OK** to accept the name. The new layer is displayed in the overview.

Maps and "Advanced Maps"

The **Maps** function in the Administration control allows you to configure and manage the graphical overview maps of the site or building under surveillance, including the location of the surveillance hardware.

You can place interactive icons, cameras, buttons, digital inputs, layers, websites, alarms and other maps on a map. The geo coordinates of a camera are used for placing the object on a map (refer to "Geo coordinates" on page 230).

The icons are interactive, for example the buttons can be clicked, the cameras can blink if they are defined as alarm cameras (see "Visualization" on page 366) or alarms blink when active and inputs show different icons to visualize their current state (see "Inputs" on page 315).

Advanced maps

Additionally, the maps feature also supports the use of mapping services such as ESRI (Environmental Systems Research Institute) to make all mapping data available without creating multiple static maps as backgrounds.

Using the feature "Advanced Maps" may require an additional license from the mapping service provider that is not included in the software license.

1. Select the location in the **Company** control. The selected location is displayed in the title bar of the Administration control.
2. Select **Maps** in the Administration control.

Creating a new map

1. Click **Create new object**.
2. Select one of the following options:
   - Standard Map
   - Advanced Map
3. Enter the name for the new map.
4. Click **OK** to accept the name. The new map is displayed in the overview.

Configuring a standard map

1. Select the standard map in the overview.

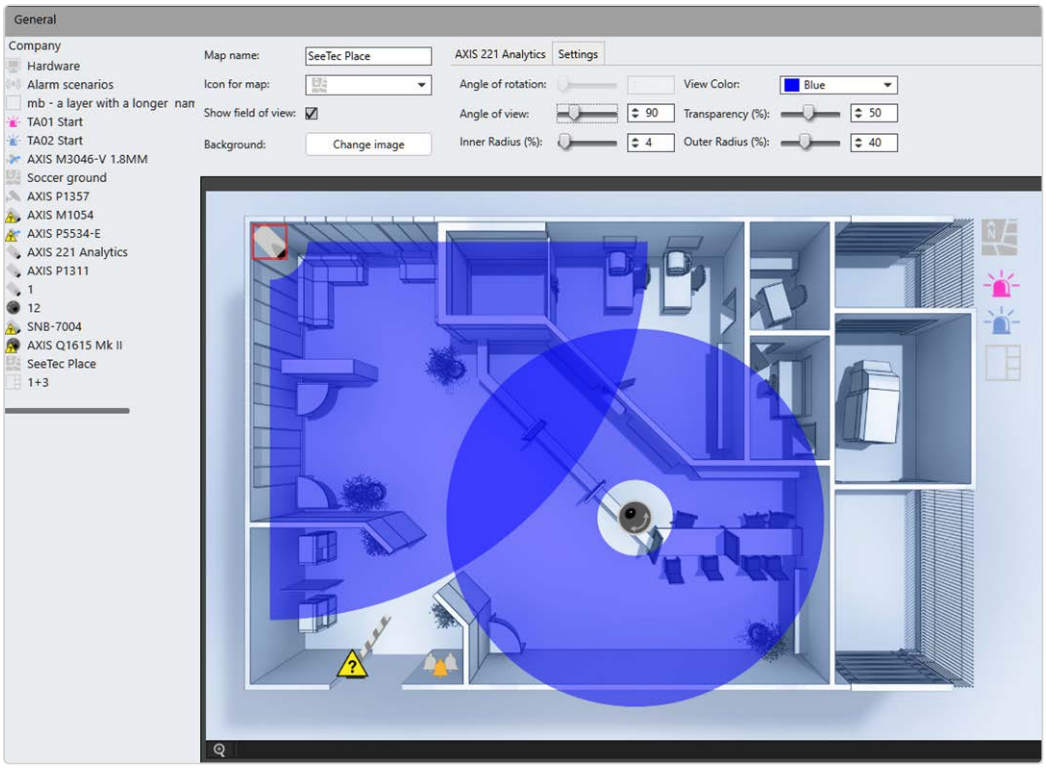


Fig. 218: Standard map - Overview

2. Zoom the map by turning the mouse wheel.
3. Use the scroll bars to move the map to a certain position. Optionally, you can drag the map position while holding the mouse wheel.
4. Drag the available elements from the **Company** tree like cameras, inputs, buttons, alarms etc. required for the desired site from the list to the map background.

General settings

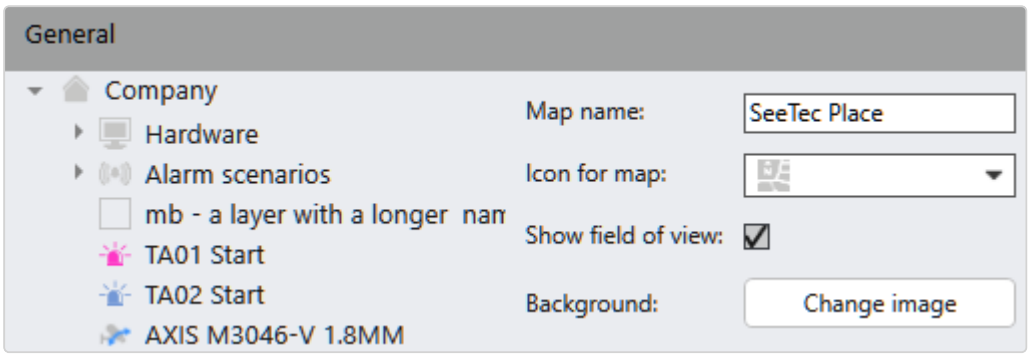


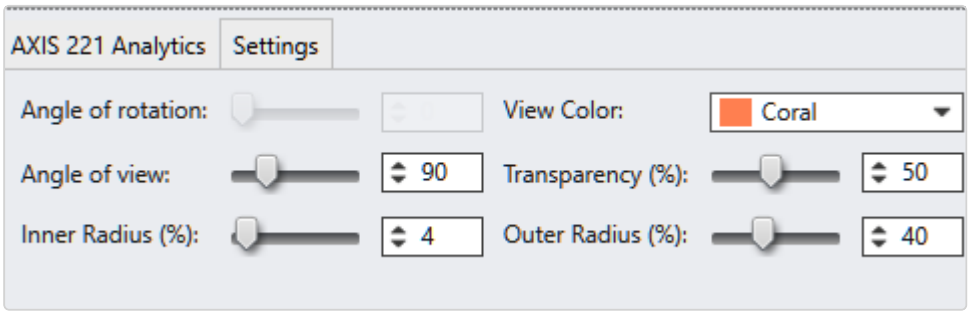
Fig. 219: Maps - General

1. Change the **Map name**, if required.
2. Select a custom **Icon for the map**, if available (see "Managing sound and icon files with custom media" on page 447).
3. Check **Show field of view** to show or hide a graphical field of view for cameras placed on the map.
4. Click **Change image**, and select the desired background image (e.g. building floor plan). The following file formats are possible:

- Images, such as JPG, GIF, PNG, BMP
- Vector graphics (resolution independent): PDF

If an icon on the map is selected while dropping a new icon, the new icon gets the same settings as the selected one.
If there is no icon selected on the map while dropping a new icon, the new icon will get the default settings.

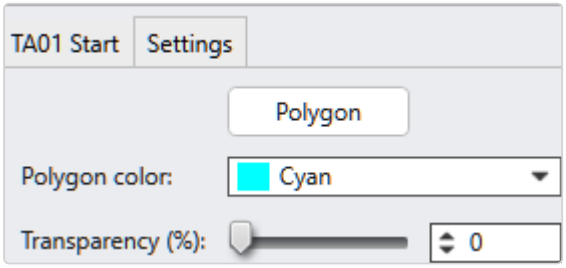
Camera icon settings



1. On the map, click on the icon of the camera to be configured. Optionally, hold down the CTRL key and select multiple elements. Depending on the selection the following camera specific options can be changed:

- **Angle of rotation**: Drag the slider or enter a value to change the icon's angle of rotation. This function is available when the option Lock Angles in the general icon settings is not activated (see General icon settings.)
- **Angle of view**: Drag the slider or enter a value to change the size of the overlay of the camera's angle of view.
- **Inner radius**: Drag the slider or enter a value to change the visualization of the camera's blind spot.
- **View color**: Select a color of the overlay of the camera's angle of view.
- **Transparency**: Drag the slider or enter a value to change the transparency of the overlay of the camera's angle of view.
- **Outer Radius**: Drag the slider or enter a value to change the outer radius of the overlay of the camera's angle of view.

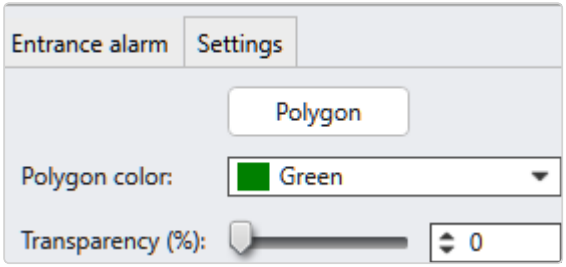
Button icon settings



1. On the map click on the icon of the button to be configured. Optionally hold CTRL and select multiple elements. Depending on the selection the following button specific options can be changed:

- **Polygon**: Click to activate the function. Then draw the active area of the button by clicking the corner points of the polygon on the map.
- **Polygon color**: Select a color for of the overlay of the polygon.
- **Transparency**: Drag the slider or enter a value to change the transparency of the overlay of the polygon.

Alarm icon settings



1. On the map click on the icon of the alarm to be configured. Optionally hold CTRL and select multiple elements. Depending on the selection the following button specific options can be changed:
   - **Polygon**: Click to activate the function. Then draw the active area of the alarm by clicking the corner points of the polygon on the map.
   - **Polygon color**: Select a color for of the overlay of the polygon.
   - **Transparency**: Drag the slider or enter a value to change the transparency of the overlay of the polygon.

Configuring an advanced map

1. Select the advanced map in the overview.

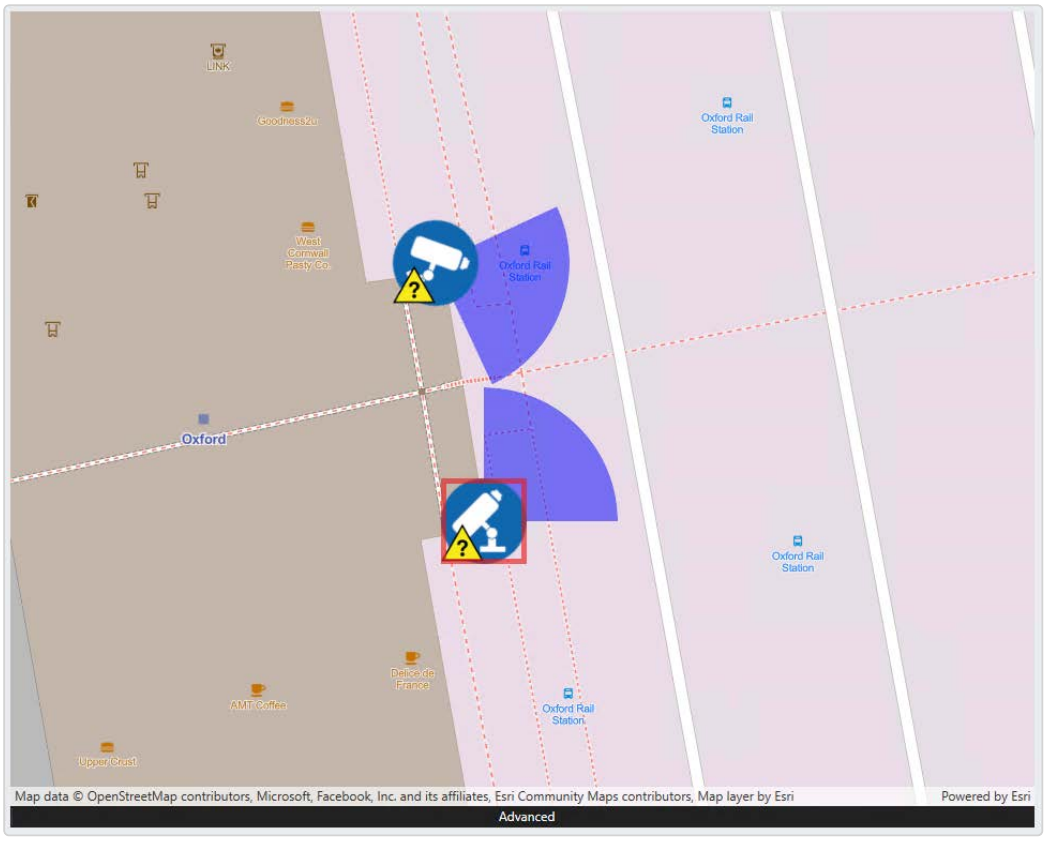


Fig. 220: Advanced map - Overview

2. Enter the geo-coordinates or zoom into the map by turning the mouse wheel for the desired location. When zooming, the coordinates adjust accordingly.
3. Use the scroll bars to move the map to a certain position. Optionally you can drag the map position while holding the mouse wheel.
4. Drag the available elements from the **Company** tree like cameras, inputs, buttons, alarms etc. required for the desired site from the list to the map background.

General settings

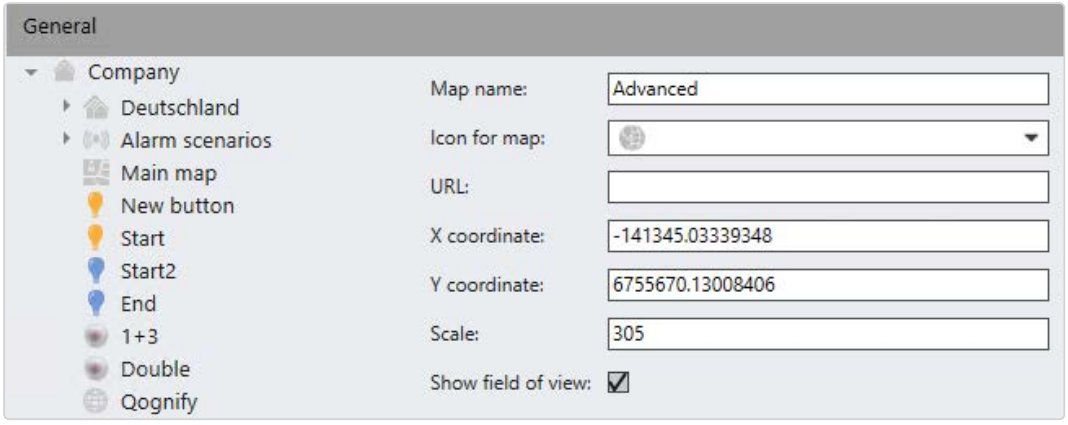
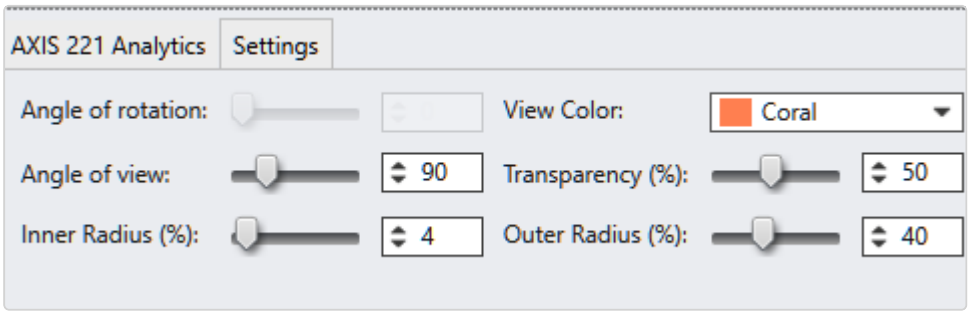


Fig. 221: Maps - General

1. Change the **Map name**, if required.
2. Select a custom **Icon for the map**, if available (see "Managing sound and icon files with custom media" on page 447).
3. Adjust the geo-coordinates.
4. Adjust the scaling factor. The higher the number, the higher "above ground" the view looks.
5. Check **Show field of view** to show or hide a graphical field of view for cameras placed on the map.

> **If an icon on the map is selected while dropping a new icon, the new icon gets the same settings as the selected one.**
> **If there is no icon selected on the map while dropping a new icon, the new icon will get the default settings.**

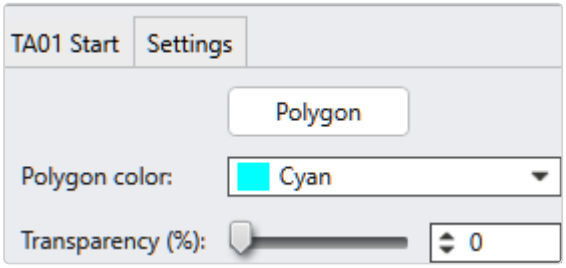
Camera icon settings



1. On the map, click on the icon of the camera to be configured. Optionally, hold down the CTRL key and select multiple elements. Depending on the selection the following camera specific options can be changed:

- **Angle of rotation**: Drag the slider or enter a value to change the icon's angle of rotation. This function is available when the option Lock Angles in the general icon settings is not activated (see General icon settings.)
- **Angle of view**: Drag the slider or enter a value to change the size of the overlay of the camera's angle of view.
- **Inner radius**: Drag the slider or enter a value to change the visualization of the camera's blind spot.
- **View color**: Select a color of the overlay of the camera's angle of view.
- **Transparency**: Drag the slider or enter a value to change the transparency of the overlay of the camera's angle of view.
- **Outer Radius**: Drag the slider or enter a value to change the outer radius of the overlay of the camera's angle of view.

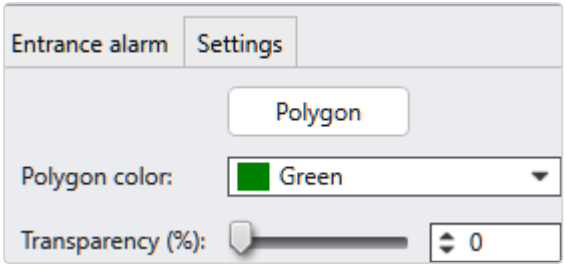
Button icon settings



1. On the map click on the icon of the button to be configured. Optionally hold CTRL and select multiple elements. Depending on the selection the following button specific options can be changed:

- **Polygon**: Click to activate the function. Then draw the active area of the button by clicking the corner points of the polygon on the map.
- **Polygon color**: Select a color for of the overlay of the polygon.
- **Transparency**: Drag the slider or enter a value to change the transparency of the overlay of the polygon.

Alarm icon settings



1. On the map click on the icon of the alarm to be configured. Optionally hold CTRL and select multiple elements. Depending on the selection the following button specific options can be changed:
   - **Polygon**: Click to activate the function. Then draw the active area of the alarm by clicking the corner points of the polygon on the map.
   - **Polygon color**: Select a color for of the overlay of the polygon.
   - **Transparency**: Drag the slider or enter a value to change the transparency of the overlay of the polygon.

Deleting a map

1. Select the map in the overview.
2. Click **Delete object**.

Duplicating a map

1. Select the map in the overview.
2. Click **Duplicate object**, and enter a name for the duplicated map.
3. Click **OK** to accept the name. The new map is displayed in the overview.

Buttons

The **Buttons** function in the Administration control allows you to start specified processes (actions) such as camera recordings or alarm scenarios.

> **To call the configured buttons in surveillance mode, you have to call the Buttons function on the control bar (see "Buttons" on page 153).**

1. Select the location in the **Company** control. The selected location is displayed in the title bar of the Administration control.
2. Select **Buttons** in the Administration control.

Creating a new button

1. Create a new button.
2. Enter the **Name** for the new button.
3. Click **OK** to accept the name. The new button is displayed in the overview.

Configuring a button

1. Select the button in the overview.

General

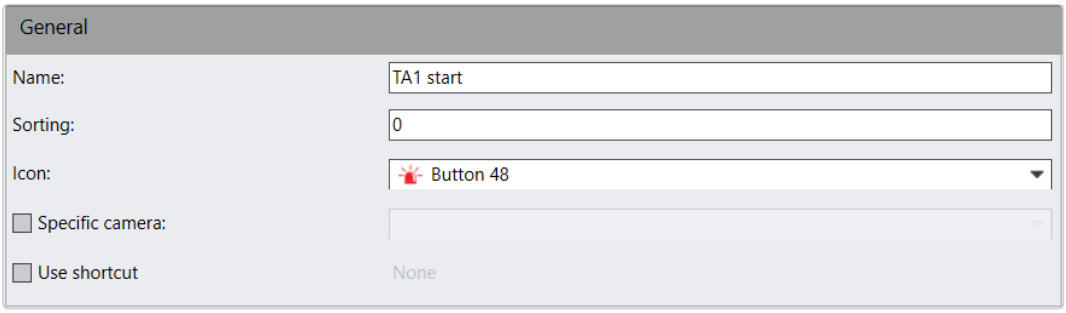


Fig. 222: Buttons - General

1. If necessary, alter the **Name**.
2. Specify the **Sorting** order of the buttons in the controller in surveillance mode (see "Buttons" on page 153). The buttons are automatically sorted in ascending order, i.e. the higher the number of a button, the lower down it appears in the list on the tab.
3. Select an **Icon** to make it easier to recognize.
4. Activate the action for a **Specific camera**, and select the camera. In this case the button is only displayed if the specified camera is selected in surveillance mode.
5. Activate **Use shortcut** and press the desired key combination on the keyboard to trigger the button with a key combination. The key combination is displayed.

   The default keyboard shortcuts cannot be overwritten. Changes by the administrator will be ignored.

Action

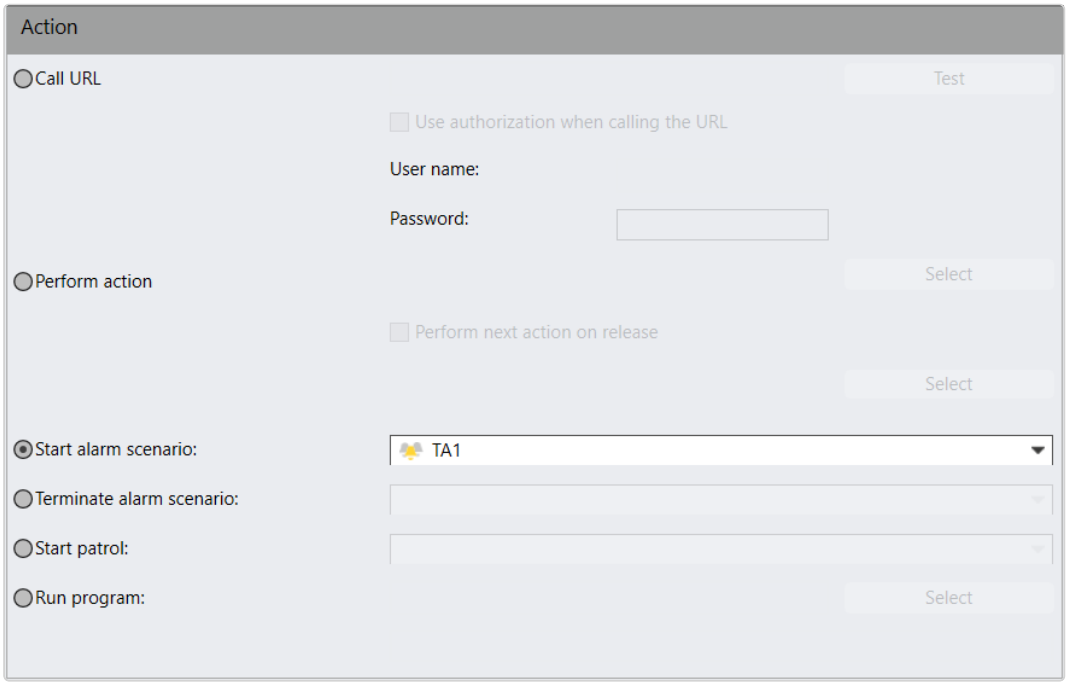


Fig. 223: Buttons - Action

1. Select the **Call URL** option and enter the Internet or intranet address. For example, camera scripts can be started with this address. An Internet or intranet address is not displayed (to embed web pages in the layer, see "Web pages" on the facing page).
2. Select **Test** to check that the specified URL is working.
3. If necessary, activate **Use authorization when calling the URL** and enter the required **User name** and **Password** to get access to the URL.
4. Select the **Perform action** option and select the related action.
5. If a second action is to be performed, select **Perform next action on release** and select the action. In surveillance mode, the action is carried out as soon as you release the button.
6. Select the **Start alarm scenario** option and then the alarm scenario (see "Alarms" on page 356).
7. Select the **Terminate alarm scenario** option and then the alarm scenario (see "Alarms" on page 356).
8. Select the **Start patrol** option and then the patrol (see "Patrols" on page 391).
9. Select the **Run program** option, and click **Select** to select a program that is to be started.

   > **The file path to the selected program must be accessible from the related client computer.**

10. Enter any parameters required by the program. A document can be opened using the selected program, for example.
11. **Apply** the set values if you want to make further settings.
12. **Save** the set values to apply the values and conclude input.

Deleting a button

1. Select the action in the overview.
2. Click **Delete object**.

Duplicating a button

1. Select the action in the overview.
2. Click **Duplicate object**, and enter a name for the duplicated action.
3. Click **OK** to accept the name. The new action is displayed in the overview.

Web pages

The **Web pages** function on the Administration control allows you to embed web pages in the layer (e.g. webcams or intranet pages).

> **The web page feature displays simple structured web pages. Complex or password protected web pages, e. g. configuration surfaces of cameras, might have some functional issues or cannot be displayed at all.**

1. Select the location in the **Company** control. The selected location is displayed in the title bar of the Administration control.
2. Select **Web pages** in the Administration control.

Creating a new web page

1. Create a new web page.
2. Enter the **Name** for the new web page.
3. Select a custom icon for the web page, if available (see "Managing sound and icon files with custom media" on page 447).
4. Click **OK** to accept the name. The new web page is displayed in the overview.

Configuring a web page

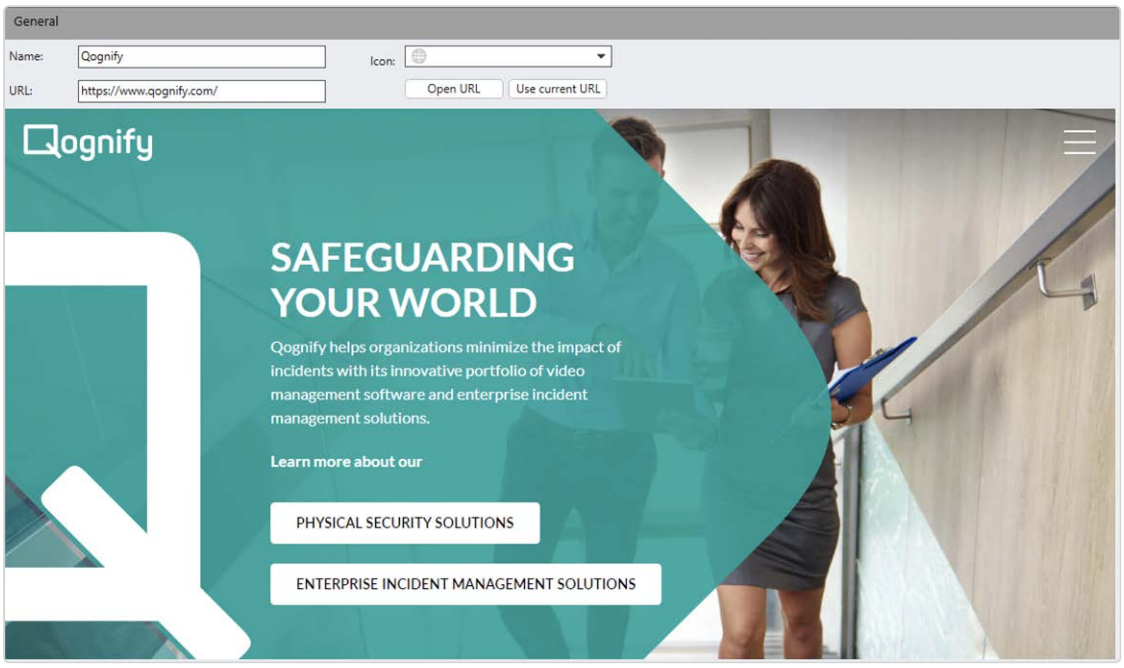


Fig. 224: Configuring a web page - General

1. Select the web page in the overview.
2. If necessary, alter the **Name** of the web page and enter the **URL** (Internet or intranet address).
3. If available, change the icon for the web page (see "Managing sound and icon files with custom media" on page 447).
4. Select **Open URL** to check that the web page can be accessed.
5. **Apply** the set values if you want to make further settings.
6. **Save** the set values to apply the values and conclude input.

Deleting a web page

1. Select the web page in the overview.
2. Click **Delete object**.

Duplicating a web page

1. Select the web page in the overview.
2. Click **Duplicate object**, and then enter the name for the duplicated web page.
3. Click **OK** to accept the name. The new web page is displayed in the overview.

Patrols

The **Patrols** function on the **Administration** control allows you to configure multiple cameras, set positions, maps and layers one after the other for a user-definable time. It is also possible to open or close digital outputs in a patrol and create checkpoints.

1. Select the location in the **Company** control. The selected location is displayed in the title bar of the Administration control.
2. Select **Patrols** in the Administration control.

Creating a new patrol

1. Create a new patrol.
2. Enter the **Name** for the new patrol.
3. Click **OK** to accept the name. The new patrol is displayed in the overview.

> **In order to be able to activate the new patrol in surveillance mode, it must be assigned to a user profile. Switch to the Profile control and activate the patrol for the desired user profile (see Configuring a profile).**

Configuring a patrol

- Patrols can only be triggered on clients that are in surveillance mode.
- When multiple patrols are triggered, the last one triggered will be started. All previously started patrols are stopped.
- During an alarm no patrols can be started. The patrol will be started after the alarm has ended.

General

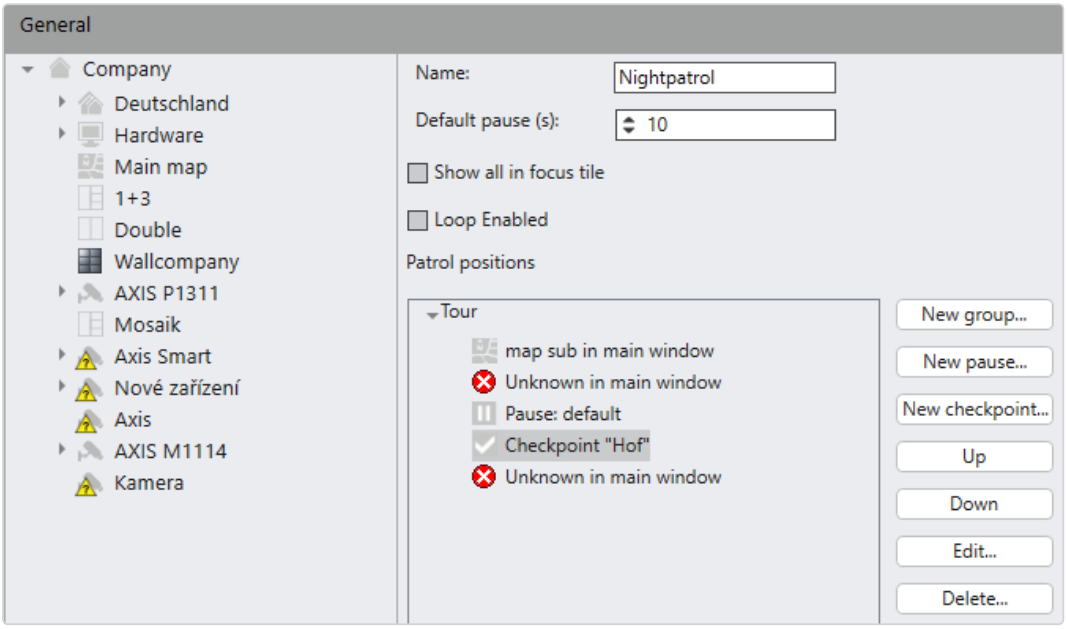


Fig. 225: Patrols - General

1. Select the patrol in the overview.
2. If necessary, alter the **Name** of the patrol.
3. Select the **Default pause** (in seconds) to set the duration for which a layer is to be displayed.
4. Enable **Show all in focus tile** to display all entities (cameras, maps etc.) of the patrol in a single tile instead of covering the complete screen or layers. The entities will “rotate” in the tile in a “carousel” mode.
5. Select **New group** to group together the objects of the patrol.
6. Specify the name of the group, and select **OK**.
7. Drag the objects from the left-hand column to Patrol positions or the group.
8. To add a specific position of a camera to the list, first drag the camera to the group, then the associated preset position.
9. Select a camera, and select **Edit**.
10. If **Show all in focus tile** is disabled, enable the focus tile for each item separately.
11. Select the window in which the camera is to be displayed and click **OK**.
12. If necessary, insert a **New pause** and specify its duration.
13. Insert a **New checkpoint** and enter a name. If a checkpoint is reached, an information window is shown. The user can then decide whether to continue or stop the patrol. Reaching a checkpoint is saved in report mode.

14. To change the sequence of inserted objects, select the objects in patrol positions and move the object **Up** or **Down** in the list by clicking the corresponding button.

    > **For a patrol to be started in surveillance mode, it must first be assigned to a user or group in the Profiles control (see "Profiles" on page 345).**

15. Select the object in Patrol positions, and select **Edit** to adjust the object settings. This enables you to decide in which window the camera image is to be displayed.
16. Select the object in patrol positions, and select **Delete** to delete it.

Start

1. Select the patrol in the overview.
2. Select **Start**.
3. Select **Edit** and select an item from the list that defines the event start or search for the item.
4. Select **OK**. The start event is displayed in the event list.
5. To add another event, select **Edit** and enable another start event.
6. To remove the event, select the item, select **Edit** and disable the item in the list.
7. Select **OK**. The start event is removed from the list.

Stop

1. Select the patrol in the overview.
2. Select **End**.
3. Select **Edit** and select an item from the list that defines the event stop or search for the item.
4. Select **OK**. The stopping event is displayed in the event list.
5. To add another event, select **Edit** and enable another stop event.
6. To remove the event, select the item, select **Edit** and disable the item in the list.
7. Select **OK**. The event is removed from the list.

Persons involved

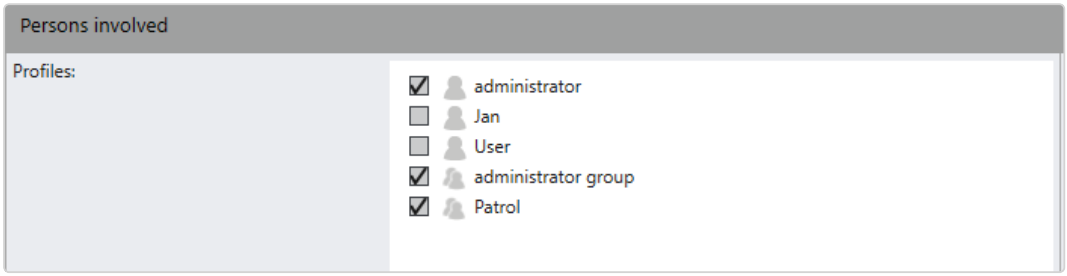


Fig. 226: Configuring the profiles in patrols

1. Select the patrol in the overview.
2. Select **Persons involved**. The available profiles are displayed that have been defined in the profile settings (see Configuring a profile).
3. Select the profiles that are related to the patrol.
4. Save **Apply** the set values if you want to make further settings or **Save** the set values to apply the values and conclude input.

Deleting a patrol

1. Select the patrol in the overview.
2. Click **Delete object**.

Duplicating a patrol

1. Select the patrol in the overview.
2. Click **Duplicate object** and enter a name for the duplicated patrol.
3. Click **OK** to accept the name. The new patrol is displayed in the overview.

Sequences

The **Sequences** function on the **Administration** control allows you to create server side sequences in which configurable actions are triggered.

General information on sequences

- Multiple times and/or time periods can be added to a sequence.
- Multiple sequences can run in parallel.
- A time schedule is not required if the sequence is to be started by an alarm scenario.
- If a sequence is started by an alarm scenario, sequences in progress continue.
- If a sequence is started by an alarm scenario, the sequence is processed in full even if the alarm scenario is stopped earlier.
- If a sequence in progress is stopped by an alarm scenario, the sequence is only interrupted for the configured dead time.
- A recording can only be started in connection with an alarm, not by the sequence directly.
- Sequences do not have exclusive access to the camera positions. If a PTZ camera is controlled during an ongoing sequence, the preset positions are approached with a dead time of one minute not included in the sequence.
- A preset position can also be approached by an alarm scenario, even if the sequence approached a different preset position of the same camera shortly before. The same applies to an additional sequence.

1. Select the location in the **Company** control. The selected location is displayed in the title bar of the Administration control.
2. Select **Sequences** in the Administration control.

Creating a new sequence

1. Create a new sequence.
2. Enter the **Name** for the new sequence.
3. Click **OK** to accept the name. The new sequence is displayed in the overview.

Configuring a sequence

1. Select the sequence in the overview.

General

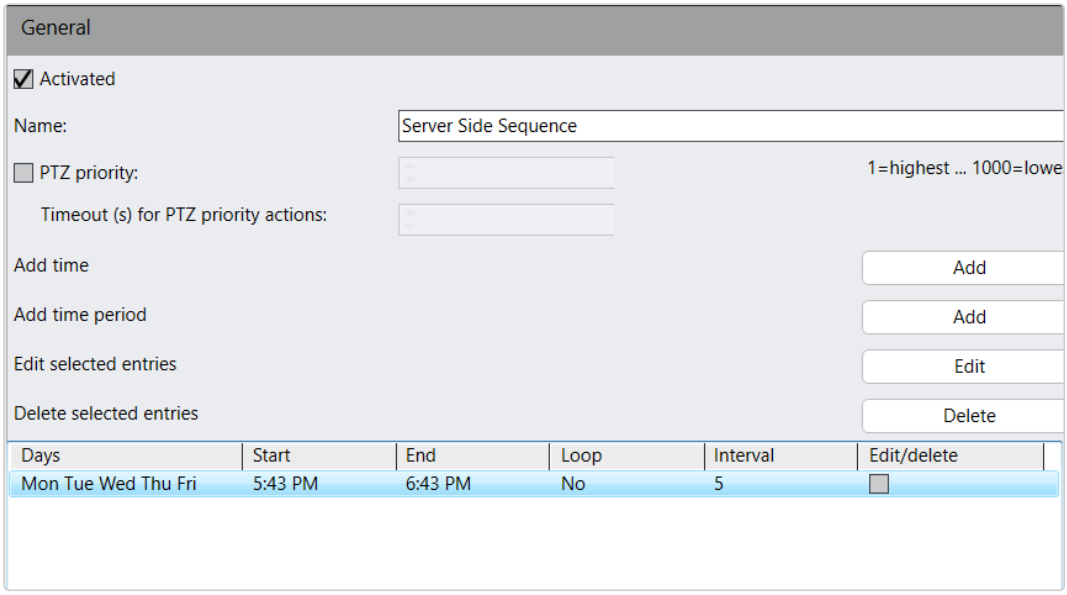


Fig. 227: Sequences - General

1. Select the sequence and, if necessary, alter the **Name**.
2. Enter the **PTZ priority** counter between 1 and 1000 (the higher the number: the lower the priority) and specify the **Timeout for PTZ priority actions** in seconds. If the sequence does not activate any PTZ controls, the camera control is released again after the timeout.

   > **A user (or alarm, or server sequence) with a higher PTZ priority can override another user (or alarm or server sequence) when taking control of the camera.**

3. Use **Add time** and **Add time period** to make additions.
   - **Time**: The sequence is started once at the selected time on every selected day.
   - **Time period**: The sequence is started multiple times depending on the duration of the sequence on every selected day within the time period.
4. Select one or more entries, and select **Edit selected entries** to edit the entries one after the other.
5. Select one or more entries, and select **Delete selected entries** to delete the entries.

Actions

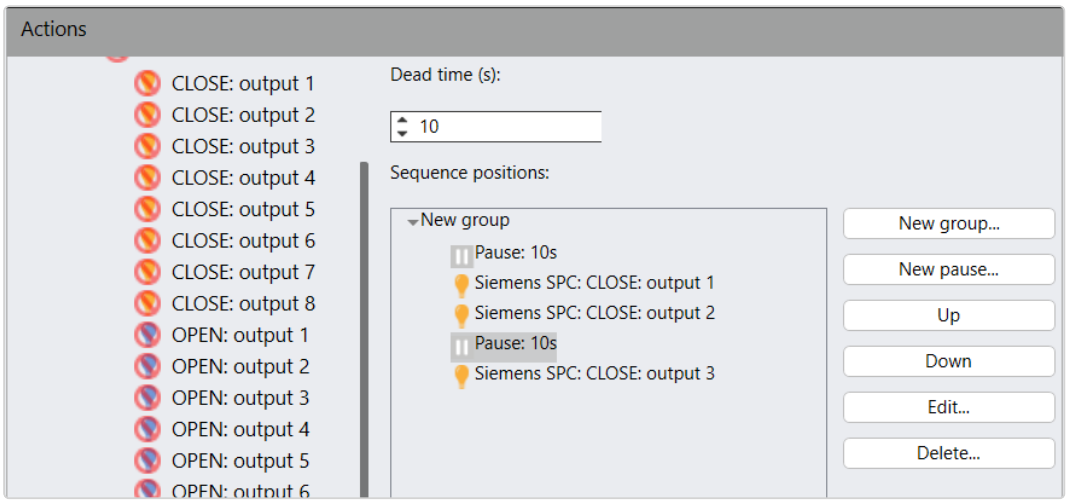


Fig. 228: Sequences - Actions

1. Create a **New group** and enter a name.
2. Specify the **Dead time** (in seconds) to define a time span in which the sequence will be interrupted by an alarm trigger.
3. Drag one or more camera positions or actions to the group.
4. Select a group, and use **New pause** to adjust the pause (in seconds) to specify how long the camera or layer or map is displayed.
5. Select a group or an entry, and use **Up** or **Down** to move it up or down in the list.
6. Select a group or pause, and select **Edit** to edit the name of the group or the duration of the pause.
7. Select a group or an entry, and select **Delete** to delete the group or entry.
8. **Apply** the set values if you want to make further settings.
9. **Save** the set values to apply the values and conclude input.

Deleting a sequence

1. Select the sequence in the overview.
2. Click **Delete object**.

Duplicating a sequence

1. Select the sequence in the overview.
2. Click **Duplicate object**, and enter the name for the duplicated sequence.
3. Click **OK** to accept the name. The new sequence is displayed in the overview.

Video walls

The **Video walls** function in the Administration control allows you to configure the Qognify Dispatcher that controls a DisplayAgent (see "DisplayAgent" on page 87). If defined in the user profile, this allows you to display camera images, layers, maps, alarm scenarios, and web pages on video walls in dispatcher mode.

1. Select the location in the **Company** control. The selected location is displayed in the title bar of the Administration control.
2. Select **Video walls** in the Administration control.

Creating a new video wall

1. Create a new video wall.
2. Enter the **Name** for the new video wall.
3. Click **OK** to accept the name. The new video wall is displayed in the overview.

Configuring a video wall

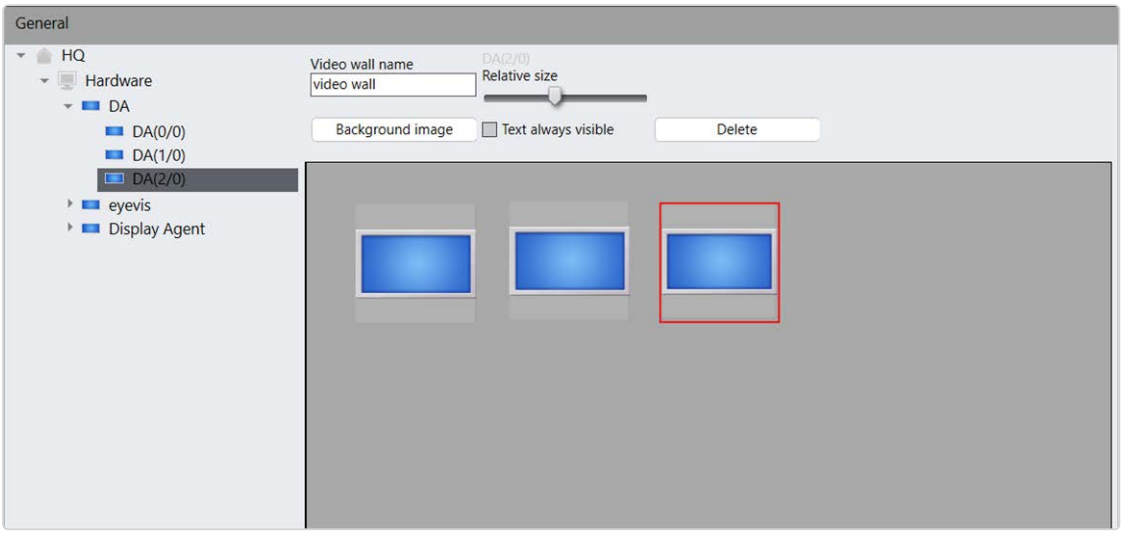


Fig. 229: Video walls - General

1. Select the video wall in the overview.
2. If necessary, alter the **Name** of the video wall.
3. Select the background image to be displayed on the video wall.
4. Drag the monitors that have to be defined as a DisplayAgent to the video wall, and adjust the arrangement of the monitors (see "Other hardware" on page 272).
5. **Apply** the set values if you want to make further settings.
6. **Save** the set values to apply the values and conclude input.

> **Further settings in the user profile are required (see "Video wall module mapping" on page 350).**

Deleting a video wall

1. Select the video wall in the overview.
2. Click **Delete object**.

Duplicating a video wall

1. Select the video wall in the overview.
2. Click **Duplicate object**, and enter the name for the duplicated video wall.

3. Click **OK** to accept the name. The new video wall is displayed in the overview.

License plate groups

In the **License plate groups**, license plates groups for the License Plate Recognition (LPR) can be configured and managed. Depending on the configuration of the LPR process, license plates can be arranged into groups automatically or manually. If for example a license plate from group "suppliers" is recognized, a barrier opens automatically. To add a license plate to a group manually see "LPR master data editor" on page 87.

To restrict the use of the LPR mode (and to prevent possible misuse), at least one LPR group with the corresponding rights must be configured (also refer to "LPR mode" on page 451).

1. Select the location in the **Company** control. The selected location is displayed in the title bar of the Administration control.
2. Select **License plate group** in the Administration control.

Creating a new license plate group

1. Create a new license plate group.
2. Enter the **Name** for the new license plate group.
3. Click **OK** to accept the name. The new license plate group is displayed in the overview.

Configuring a license plate group

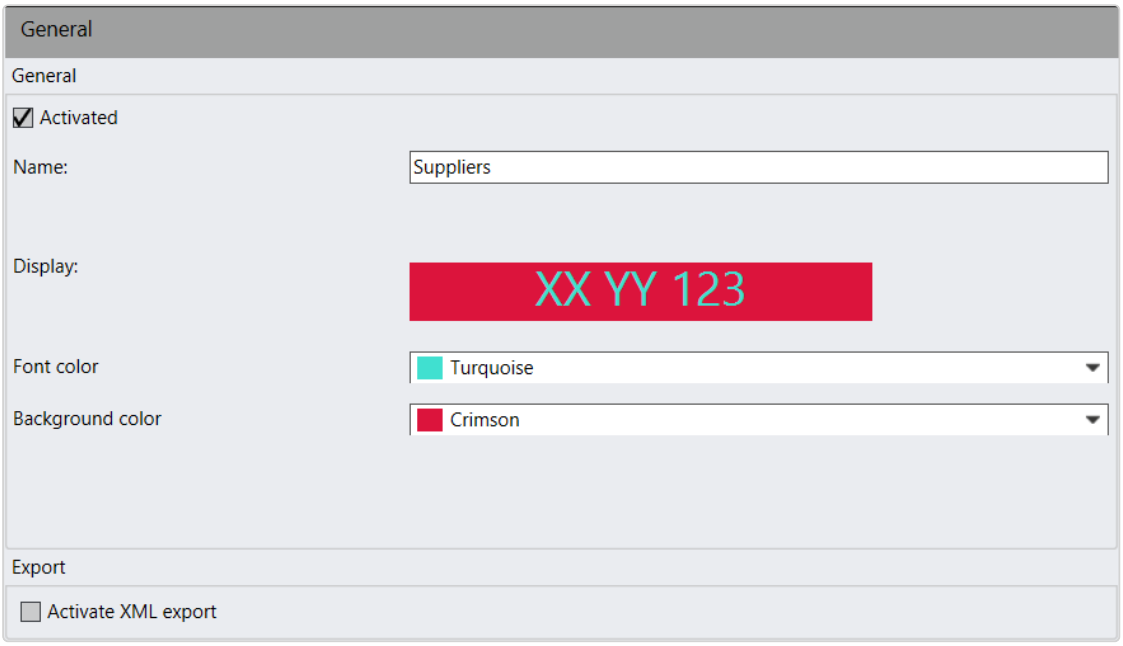


Fig. 230: License plate groups - General

1. Select the license plate group in the overview.
2. **Select** the license plate group.
3. If necessary, alter the **Name** of the license plate group.
4. Adjust the **Font color** and **Background color** in the display of the license plate.
5. Select **XML export** to export the license plate data as an XML file as soon as any license plate from that group is recognized by an LPR event. The XML data is saved in the folder specified during configuration of the "Configuring the LPR module" on page 413.
6. **Apply** the set values if you want to make further settings.
7. **Save** the set values to apply the values and conclude input.

Deleting a license plate group

1. Select the license plate group in the overview.
2. Click **Delete object**.

Duplicating a license plate group

1. Select the license plate group in the overview.
2. Click **Duplicate object**, and enter the name for the duplicated license plate group.
3. Click **OK** to confirm the name. The new license plate group is displayed in the overview.

Server

The **Server** function on the Administration control allows you to configure the server services.
The following services are available after a standard installation:

- Core Service Main
- DeviceManager
- Global OCR settings
- 2 MotionDetection modules
- Generic DVR module

The following modules can be created by a user defined installation (see "Custom installation" on page 41) or with the VA-Administration tool (see "Qognify VMS VA Administration Tool" on page 476):

- License Plate Recognition (LPR)
- Transcoding engine
- Analytics Server module
- Gateway Service
- Analytics Interface
- Server based Motion Detection
- Generic DVR
- Generic Access Control
- Event Interface

> **For further settings, see "Qognify VMS VA Administration Tool" on page 476.**

1. Select the location in the **Company** control. The selected location is displayed in the title bar of the Administration control.

2. Select **Server** in the Administration control.

Configuring the Core Service

The main tasks of the Core Service are:

- Management of system configuration
- Settings of cameras, maps etc.
- Management of all system internal events
- Forwarding to all services and clients
- Management of alarm scenarios
- User management

> **In an distributed installation with multiple core servers, the main branch can contain the Core Service Main (CSM) and one Core Service Sub (CSS) (see "Core Services and branches" on page 22).**

General

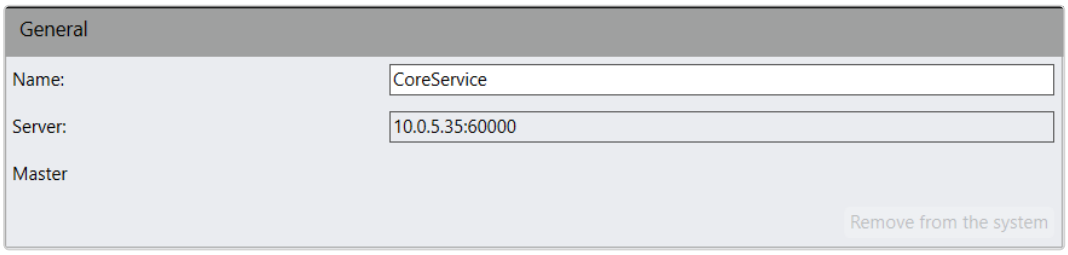


Fig. 231: Core Service - General

1. Select the module in the server function.
2. If necessary, change the **Name** of the **Server**.

   > **The network address and port number of the core server can be changed with the administration tool.**

3. Click **Remove from the system** to remove the core server from the system configuration. Removing from the system is only available for a Core Service Sub (CSS) if the server is not connected to the Core Service Main (CSM).

   > **Always contact Qognify support before deletion.**

4. **Apply** the set values if you want to make further settings.
5. **Save** the set values to apply the values and conclude input.

Configuring the DeviceManager (DM)

The main tasks of the DeviceManager are:

- Management of all connected hardware like cameras, video servers, I/O-modules
- Distribution of image data e. g. to the clients, multimedia database
- Communication with other services
- Event handling

General

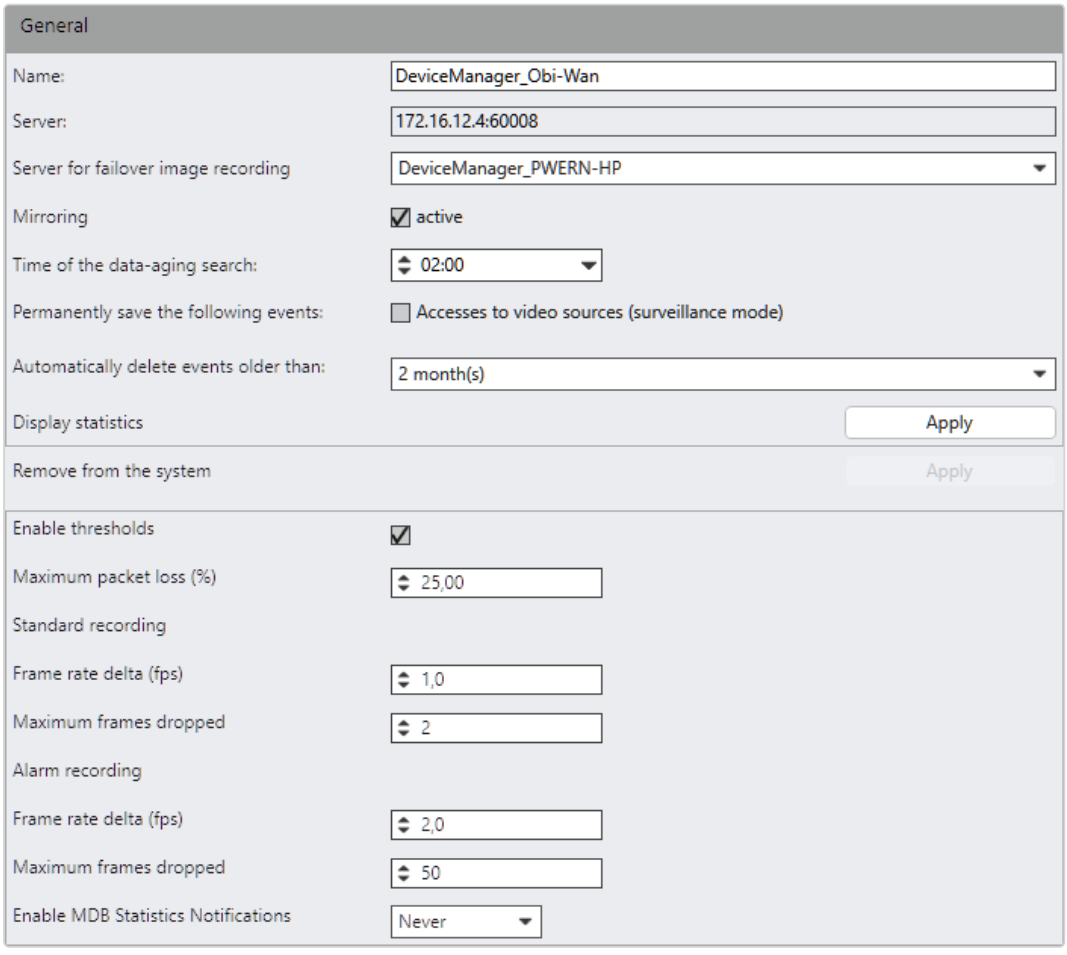


Fig. 232: DeviceManager - General

1. Select the module in the server function.
2. If necessary, alter the **Name** of the image data server.
3. Select the **Server for failover image recording**. In the event of the failure of the image data server, all connected devices are switched to the failover server.

   > **For a failover recording system, a distributed DeviceManager installation is required (see "Installation of a distributed server" on page 38), since the failover server must have sufficient capacity to take over the devices (see "System requirements" on page 31).**

4. Enable **Mirroring**: This option activates the redundant recording of all connected cameras.

   > **This option is only available for an Infinity X license.**

   If activated

   - The productive DM has the lead and multiplexes the data to both MDS if configured.
   - If the productive or redundant server fails, the recordings are continued on the still functioning server.
   - If the productive DM fails, the regular failover scenario takes place and the Core Service switches control of the camera over to the failover server. In this case (as long as not cross-wise configured) recording only takes place on the failover server. As soon as it switches back, there is again a redundant recording.
   - When performing server-side export, each of both servers exports its parts of the recordings.
   - Write protection of recordings will be applied on both servers.
   - Deletion of recordings will be performed on both servers.
   - Edge storage import will be performed on both servers.
5. Specify the **Time of the data-aging search**.
6. Activate **Accesses to video sources** to save these events.
7. Select the period after which the events are automatically deleted.

   > **Due to legal regulations, some events may not be deleted for installations in France.**

8. Activate **Display statistics** to display statistics about the streaming and recording behavior related to the selected DeviceManager. For more detailed statistics, thresholds for a better visualization of critical streaming behaviors can be defined in the "Thresholds" area below.
9. Click **Remove from the system** to remove the DeviceManager from the system configuration.

   Always contact Qognify Support before removing the Device Manager from the system!

Thresholds

To see if the device manager works according to specification, thresholds for certain parameters can be specified. If one of the values is out of the specification, the camera is marked as "limited" in the DeviceManagers statistics and the appropriate values are marked with a colored background .

The DeviceManager statistics need not be open for threshold analysis because it is a background process.

1. Activate **Enable thresholds**.
2. Specify thresholds for the following values:
   - **Maximum packet loss (%)**
   - **Frame rate delta (fps)**: The deviation between the configured frame rate and the recorded frame rate.
   - **Maximum frames dropped**: The maximum number of frames to be dropped by the Multimedia Database (MDB).
3. Select a time range for **Enable MDB Statistics Notifications**.For example, if 1 hour is selected as the time frame, an hourly check is made to see whether certain values from the MDB statistics are on average above or below one of the specified thresholds, system users can be notified. Make sure the option **Threshold values have been exceeded** is activated in the Event Manager.

DeviceManager statistics

The DeviceManager statistics display statistical information about the DeviceManager, e. g. if the recording is performed according to the parameters that have been configured to prevent missing (or insufficient) video documentation.
The statistics can display the following values about the connected cameras:

- Camera ID
- Camera name
- Camera manufacturer
- Model
- Camera firmware
- Camera IP
- Packet loss ratio
- Status of recording
- Sequences
- For each standard and alarm recording:
  - Amount of frames
  - Amount of dropped frames
  - First image
  - Last image
  - Age of first timestamp in recording range
  - Percentage filled in recording range
  - Size (GB)
  - Width
  - Height
  - Expected height
  - Codec
  - Expected codec
  - Video frame rate (fps)
  - Video bit rate (kbps)

The granularity is set to one hour by default, i.e. only data of the last hour is considered.

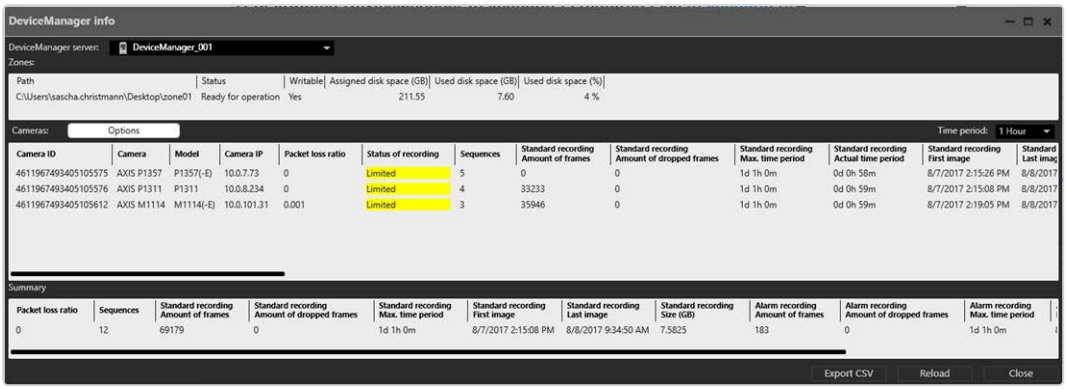


Fig. 233: DeviceManager statistics

The following options are available:

- **DeviceManager Server**: The DeviceManager can be changed quickly.
- **Zones**: Displays an overview on the zones that are configured with the selected DeviceManager.
- **Cameras**: Displays detailed information about the connected cameras.
- By selecting **Options** details can be specified. All columns can be displayed or hidden.
- The **columns** of the statistics can be sorted manually by dragging the column header to the left or to the right.
- The values of the statistics can be re-ordered by clicking on the related column header.
- **Time period**: Selected time period on which the statistic is based. The default value is 1 hour.
- **Summary**: Displays the summery values of all cameras connected to the selected DeviceManager.
- **Export CSV**: The displayed statistics can be exported as CSV file.
- **Reload**: Reloads the statistics to display the most recent values.
- **Close**: Closes the statistics window.

Options

Fig. 234: DeviceManager - Options

1. If necessary, alter the **Port for SIP messages** (see "VoIP and SIP" on page 72).

Video backup

In this section the settings of the DeviceManager for automated backup and manual video data export can be configured.

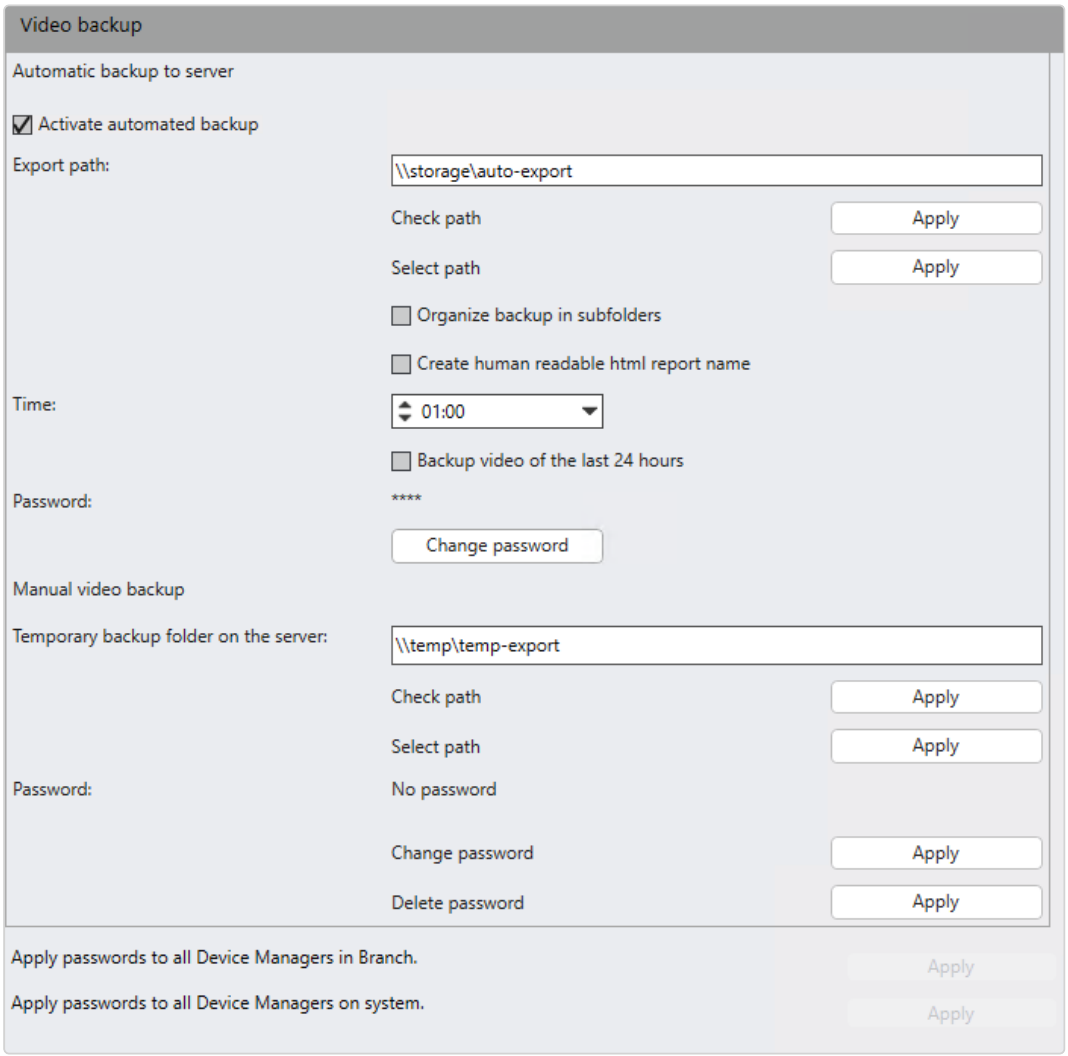


Fig. 235: DeviceManager - Video backup

Automatic backup to server

Automatic video backup to the server depends on the camera settings where the camera-specific export needs to be activated (see "Video Backup/Export" on page 252).

1. Enable the automated export.
2. Create the **Export path** for the automatic storage of the image data, or click **Select path** to select the folder directly in Windows Explorer (the path can only be selected if the Qognify VMS Client is running on the same Windows system as the DeviceManager).

   > **The export path must be accessible by the DeviceManager server.**

3. Select **Check path** to check the availability of the specified path.
4. Enable **Organize video export in subfolders** if you want the exported recordings to be stored in folders named after camera names. Otherwise the exported recording will not be organized in folders.
5. Enable **Create human readable html report name**. Otherwise the computer timestamp is used as file name of the report.
6. Define the **Time** at which the export is to start.
7. Activate **Export image data of the last 24 hours** to export the image data of the last 24 hours before the specified export time. If this option is not to be activated, the image data of the previous day (midnight to midnight) are exported.
8. Specify a **Password**, with which the image data is encrypted.
9. To apply the password to all image data encryption in a branch, select **Apply**.
10. To apply the password to all image data encryption in a company, select **Apply**.

Manual image data export

For manual image data export to the client, a temporary folder on the server is required (see "Video Backup/Export" on page 252). There the export data are stored temporarily before they are sent to the client.

1. Create the **Temporary export folder on the server** for the manual storage of the image data, or click **Select path** to select the folder directly in Windows Explorer.

   > **The temporary export path must be accessible by the DeviceManager server.**

2. Select **Check path** to ensure that the Qognify server services can write to the folder and read from it.

   > **Make sure that there is sufficient storage space for large export files on the partition on which the temporary folder is created.**

3. Specify a **Password** to be used to encrypt the image data. The password will be required to export the image data (see "Multiple export of image data" on page 104).
4. Remove the stored password with **Delete password**.
5. **Apply** the set values if you want to make further settings or **Save** the set values to apply the values and conclude input.

Setting the expiration date for overwrite protection

The desired time to expire overwrite protections can be configured. If operating days are configured, they are also considered and the time span before removal is adjusted accordingly.

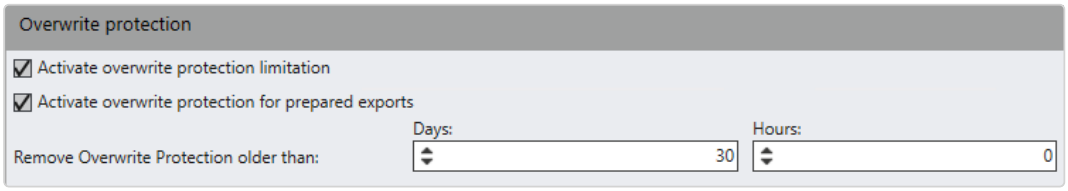


Fig. 236: Setting the expiration date for overwriting protection

1. Enable **Activate overwrite protection limitation**.
2. Enable **Activate overwrite protection for prepared exports** to protect all saved export designer sequence ranges against overwriting.

   > **This feature can only be enabled when "Activate overwrite protection limitation" is also enabled.**

3. Specify the expiration time by setting the days and hours. The default setting is 30 days.

Configuring the global OCR settings

The server on which the LPR service is to be executed is displayed.

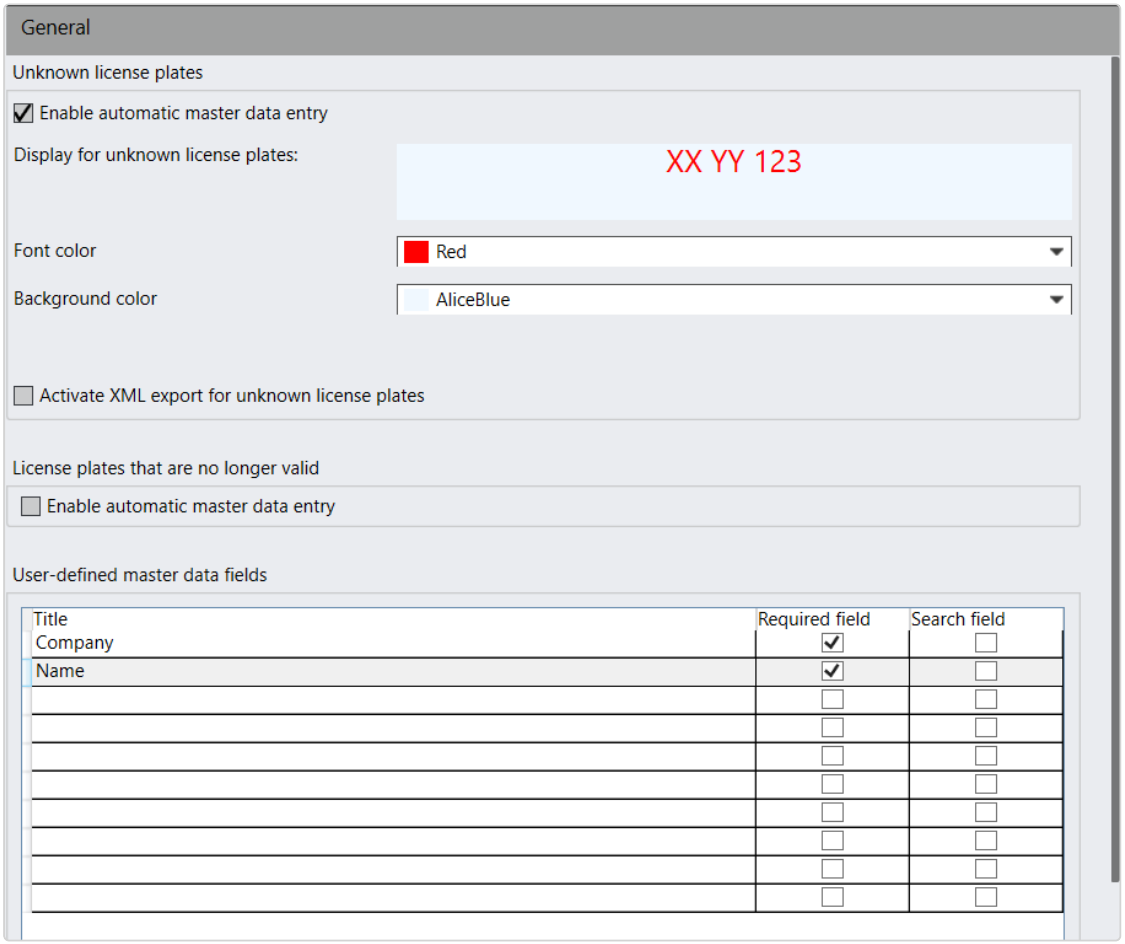


Fig. 237: Global OCR settings - General

1. 1. Select the module in the server function.
2. Select **Enable automatic master data entry** for unknown license plates. This displays the LPR master data editor as soon as the camera detects an unknown license plate.

   For the master data editor, the user must have permission to edit at least one license plate group (i.e. there must be at least one license plate group available), and "view live" permission on the camera that detected the license plate.
3. Change the **Font color** for unknown license plates and the **Background color** in the display of the license plate. Known license plates can be changed in the License plate groups control (see "License plate groups" on page 400).
4. Select **XML export** to export the license plate data as an XML file.
5. Select **Enable automatic master data entry** for no longer valid license plates e.g. because of an expired ticket.
6. Define up to 10 **User-defined master data fields**. These fields are displayed when adding or editing a license plate.
7. Select **Required field** to specify that an entry must be made in this field.
8. Select **Search field** to specify that it is possible to search for the data in this field in the LPR master data editor.
9. **Apply** the set values if you want to make further settings.
10. **Save** the set values to apply the values and conclude input.

Configuring the LPR module

> **To configure an LPR module, you first have to create it in the Qognify VA administration tool (see "Qognify VMS VA Administration Tool" on page 476).**

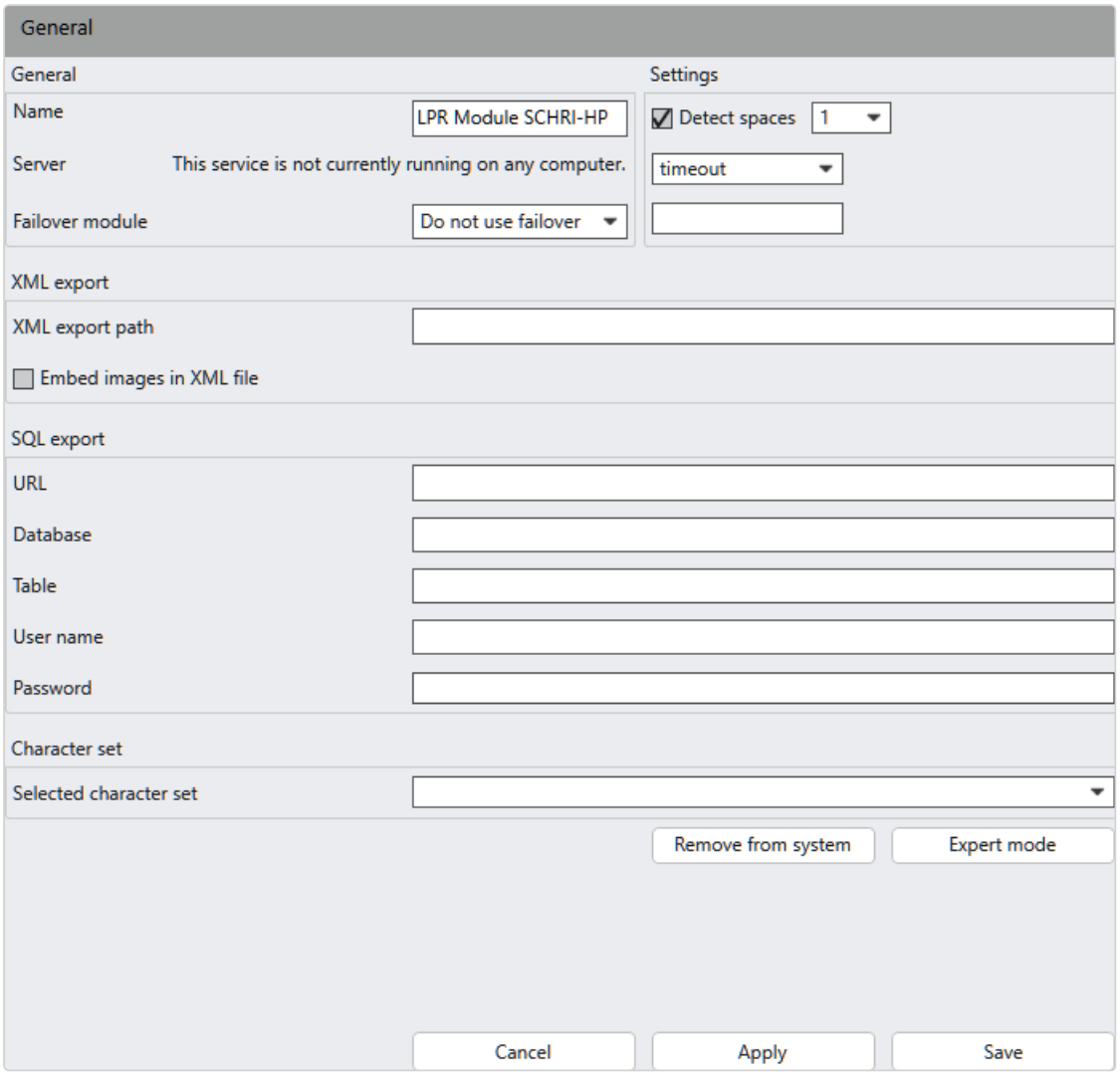


Fig. 238: LPR module - General

1. 1. Select the module in the server function.
2. If necessary, alter the **Name** of the module.
3. Select the **Failover module** in order to be able to switch to a different server in the event of the failure of the server.
4. Select **Detect spaces** to include spaces in the license plate.
   - Set the value to “1” to process maximum on single space between the detected characters of the license plate.
   - Set the value to “2” in order to activate the recognition of new German E-number plate (XX XXX E) which are made for electric cars.

     The detection of German E-number plates requires an ARH Dongle with the new LPR engine version 9 (cmanpr-7.3.9.97:latin)

5. Specify the **XML export path** for the storage of the exported XML files. The export path must be available on the LPR module server. Each recognized license plate is saved as a separate XML file, including the license plate, license plate group, time and lane name.
6. Select **Embed images in XML file** to save an image as a JPEG in Base64 of the recognized license plate in the XML file.
7. If you like, you can specify an export path for the SQL export. Specify the corresponding information for this (**URL**, **Database**, **Table** and **User name** and **Password** for accessing the database). The export contains the license plate, country code, date and time. In the SQL table, three columns must be created:
   - "NumberPlate" (char), approx. 20 characters
   - "LastSeen" (varchar) or (string), size 20 characters
   - "Country" (char) with at least 30 characters. The size depends on the recognized country codes. Most country codes have only 3 letters, such as GER, FRA. However, there are also longer country codes, such as GER_Oldtimer_old.

     > **Only Microsoft SQL-Database are supported.**

   > *Example*
   > *NumberPlate, LastSeen, Country*
   > *KA LH 0001, 10.02.2011 16:27:25, GER*
8. If multiple character sets have been installed, select which character set will be used for the recognition of the license plate.
   - The character set cmanpr-7.2.7:99: default does not have an integrated country code.
   - The character set cmanpr-7.2.7:99: latin also recognizes the country but requires more time for recognition.
   - You can get character sets for non-European license plates on request.
9. Click **Remove from system** to completely delete the LPR module from the Qognify VMS system.
10. Click **Expert mode** to modify special parameters to increase the image quality for the LPR process (see "LPR module expert mode" on the next page).
11. After configuration, add at least one LPR group to prevent misuse of the license plate recognition (see "License plate groups" on page 400).

LPR module expert mode

Before changing any values in the expert mode consult the Qognify support team and ask for the reference manual for the CMANPR software module.

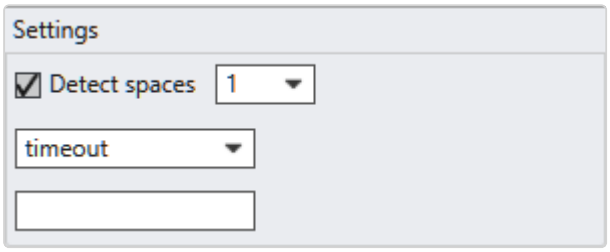


Fig. 239: LPR modules - Expert mode

In the LPR modules expert mode the following values can be edited to improve the quality of the detected license plates:

- timeout
- contrast_min
- size
- nchar_min
- nchar_max
- size_min
- size_max
- slope
- slope_min
- slope_max
- slant
- slant_min
- slant_max
- xtoyres
- colortype
- unicode_in_text

Configuring the Qognify Analytics Server 3D module

> **To configure an Analytics Server module, you first have to create it in the Qognify VA administration tool (see "Adding an Analytics Server module" on page 479).**

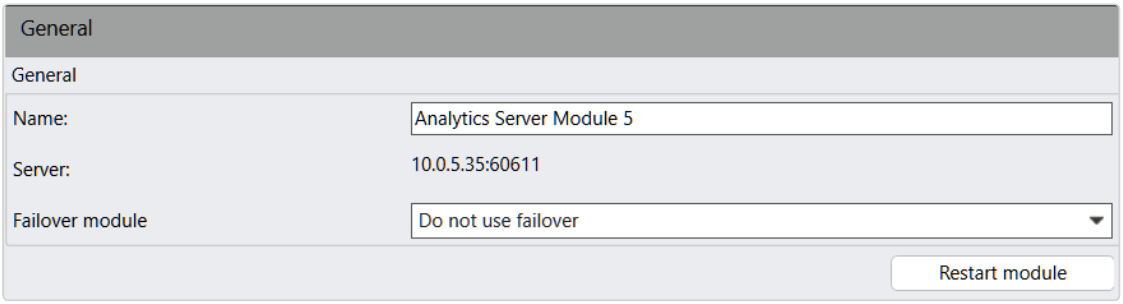


Fig. 240: Qognify Analytics Server 3D module - General

1. 1. Select the module in the server function.
2. If necessary, change the **Name** of the module.
3. Select the **Failover module** to be able to switch to a different analytics server in the event of the failure of the current analytics server.
4. If required, restart the module.

   > **Restarting the module is not necessary after changing the configuration. It is recommended to restart modules only if they are not running correctly.**

5. **Apply** the set values if you want to make further settings.
6. **Save** the set values to apply the values and conclude input.

> **For settings see "Qognify Analytics Server" on page 309.**

Configuring the Analytics Interface module

> **To configure an Analytics Interface, you first have to create it in the Qognify VA administration tool (see "Adding an Analytics Interface module" on page 483).**

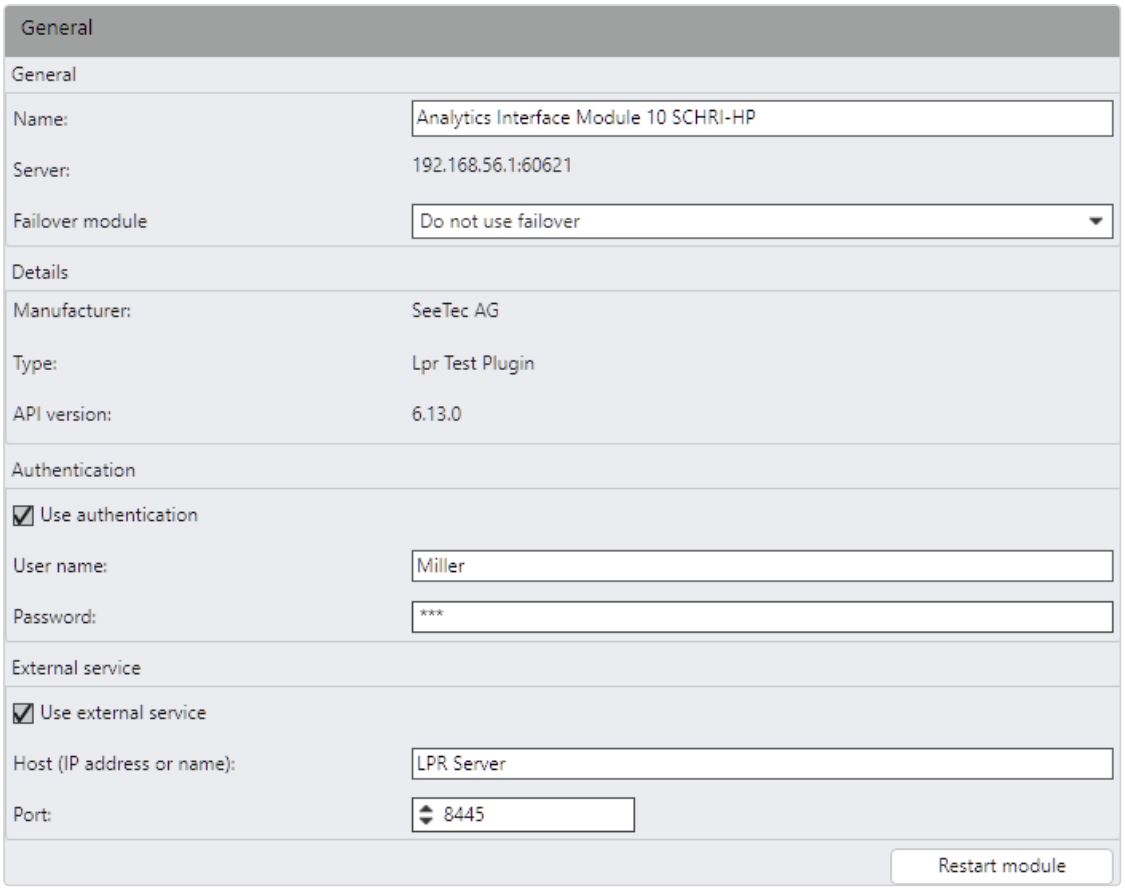


Fig. 241: Analytics interface module - General

1. Select the module in the server function.
2. If necessary, change the **Name** of the module.
3. Select the **Failover module** to be able to switch to a different analytics server in the event of the failure of the current analytics server.
4. If required enter **User name** and Password to access the module.
5. If configured **enter Host name** or **IP Address** of the external LPR service
6. If required, restart the module.

> **Restarting the module is not necessary after changing the configuration. It is recommended to restart modules only if they are not running correctly.**

7. **Apply** the set values if you want to make further settings.
8. **Save** the set values to apply the values and conclude input.

Configuring the Gateway-Service (SGS) module

To configure an Gateway-Service module, you first have to create it in the Qognify VA administration tool (see "Adding a Gateway Service module (SGS)" on page 482).

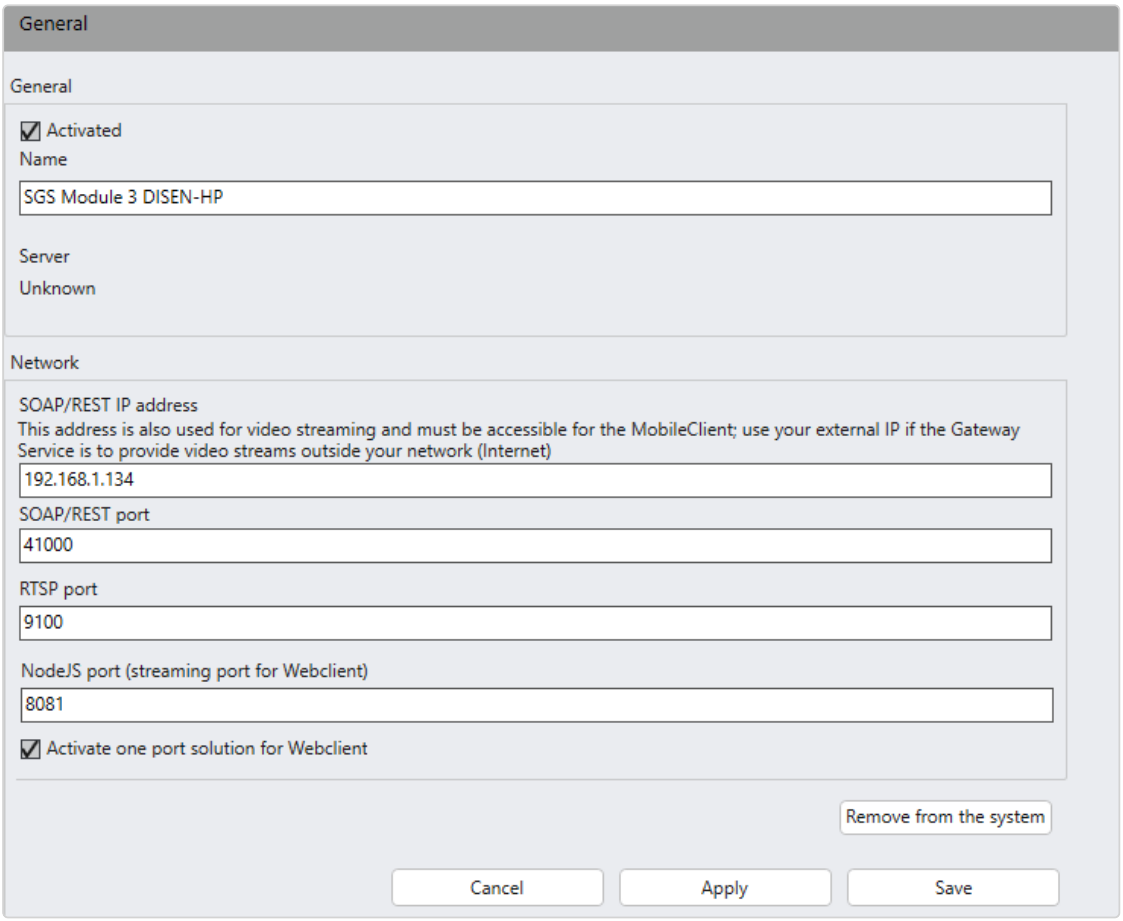


Fig. 242: Qognify Gateway-Service module - General

1. Select the module in the server function.
2. If necessary, change the **Name** of the module.
3. If required change the **SOAP/REST IP address**. This address is also used for video streaming and must be accessible for the MobileClient; use your external IP if the Gateway Service is to provide video streams outside your network (internet).
   - If accessing the network from the intranet (internal access), enter the local IP of the server.
   - If accessing the network from the internet (external access), enter the public IP of the router or firewall. Additionally, transparent port forwarding must be activated at the router or firewall.

4. If required change the **SOAP/REST port**.
5. If required change the **RTSP port**.
6. If required change the **NodeJS port** (streaming port for the WebClient).
7. **Activate one port solution for WebClient** if you want all videos to be streamed over port 443.

   This option is not backwards compatible. If you upgraded to Qognify VMS 7.5 from an older where, you have activated the one port solution manually in the configuration file, you also need to activate it here in configuration mode to force the Webclient to use the one port solution again.

8. **Activate DisplayAgent TCP port** to enable sending simple text commands over a TCP connection (only IPv4) (for entity numbering, see "Configuring the entity numbering" on page 444).

   Enabling this feature is a potential security risk. There is no authentication, authorization or encryption. If this feature is enabled, make sure that no unauthorized access is possible.

9. If required, restart the module.

   > **Restarting the module is not necessary after changing the configuration. It is recommended to restart modules only if they are not running correctly.**

10. **Apply** the set values if you want to make further settings.
11. **Save** the set values to apply the values and conclude input.

> **After saving the configuration, an information about a possible decrease of performance in video streaming is displayed.**

Configuring the transcoding module

The transcoding module is required to optimize video images to be displayed in the web client (see "Qognify VMS web client" on page 509) and mobile client (see "The Qognify VMS mobile client" on page 515).

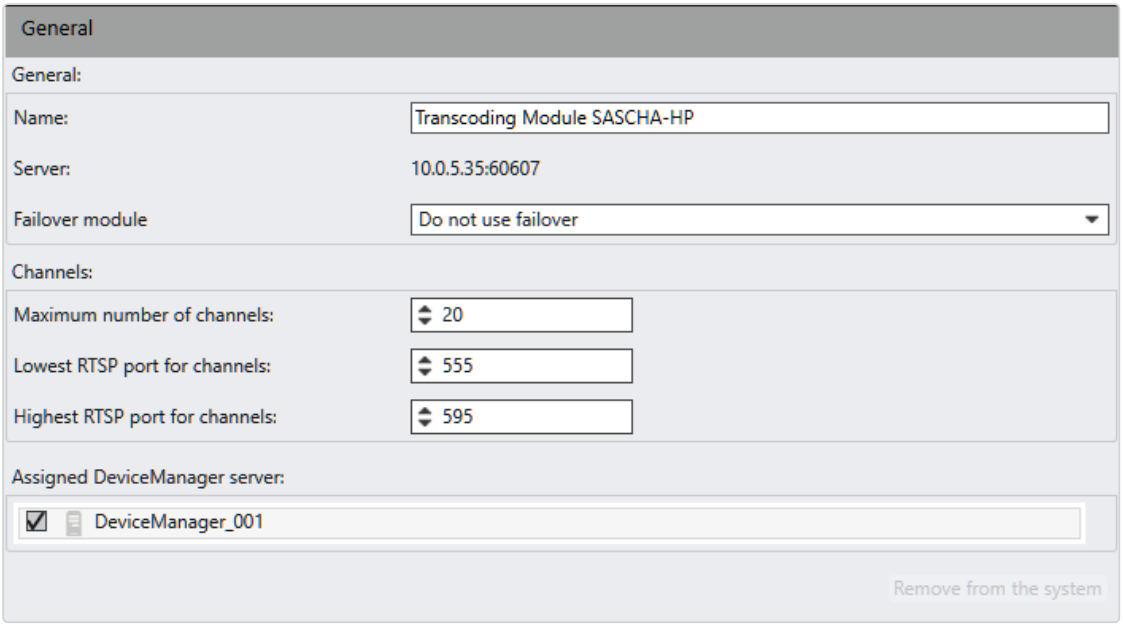


Fig. 243: Transcoding module - General

1. Select the module in the server function.
2. If necessary, alter the **Name** of the module.
3. Select the **Failover module** to be able to switch to a different transcoding module in the event of the failure of the current transcoding module.
4. Specify the **Maximum number of channels** (default number: 20). For each image requested by the web client or mobile client, one channel is needed.

   > **To reduce the network load and the load on the transcoding module, it is recommended to limit the number of channels per transcoding module.**

5. Specify the **Lowest RTSP port** and the **Highest RTSP port** number for channels. The number of ports must correspond to or exceed the number of channels. The default port range contains 40 ports (port 555 to port 595).
6. Activate the **Assigned DeviceManager server** from which the transcoding module receives the video images to transcode.
7. **Apply** the set values if you want to make further settings.
8. **Save** the set values to apply the values and conclude input.

Configuring the Motion Detection module

Two Motion Detection modules are available per default.

Prerequisite

To configure a Motion Detection module, you first have to create it in the Qognify VA administration tool (see "Adding an Analytics Server module" on page 479).

Configuration

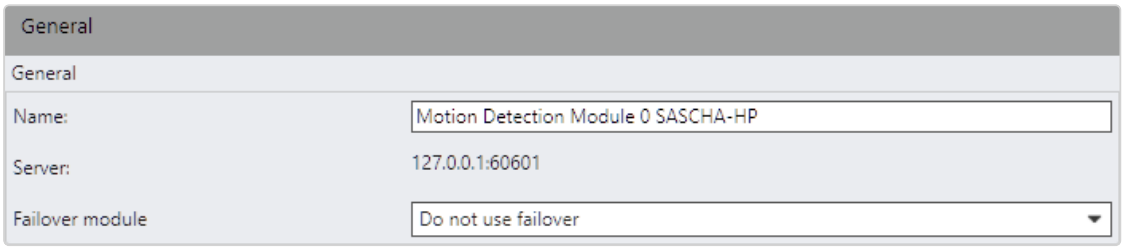


Fig. 244: Motion Detection module - General

1. Select the module in the server function.
2. If necessary, change the **Name** of the module.
3. Select the **Failover module** to be able to switch to a different Motion Detection module in the event of the failure of the current module.
4. **Apply** the set values if you want to make further settings.
5. **Save** the set values to apply the values and conclude input.

For further settings see "Motion detection" on page 255.

Configuring the QMM server module

Prerequisites

- A QognifyMetadataManager (QMM) server must be installed (see "Installation and upgrade" on page 519).
- The IP address of VMS Core service must be applied so it registers to the Qognify VMS Core.

Configuration

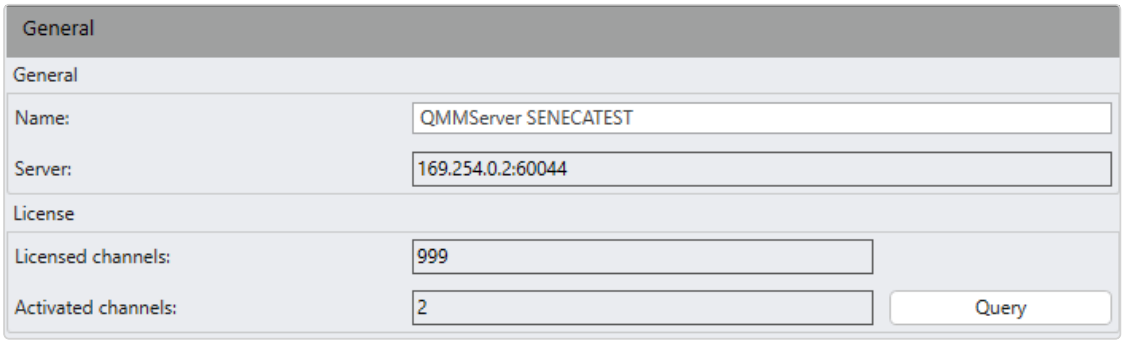


Fig. 245: Configuring the QMM server module

1. Select the module in the server function.
2. If necessary, change the **Name** of the module.
3. **Save** the set values to apply the values and conclude input.

Configuring the generic DVR module

Make sure that the module is added and preconfigured properly in the VA Administration Tool.

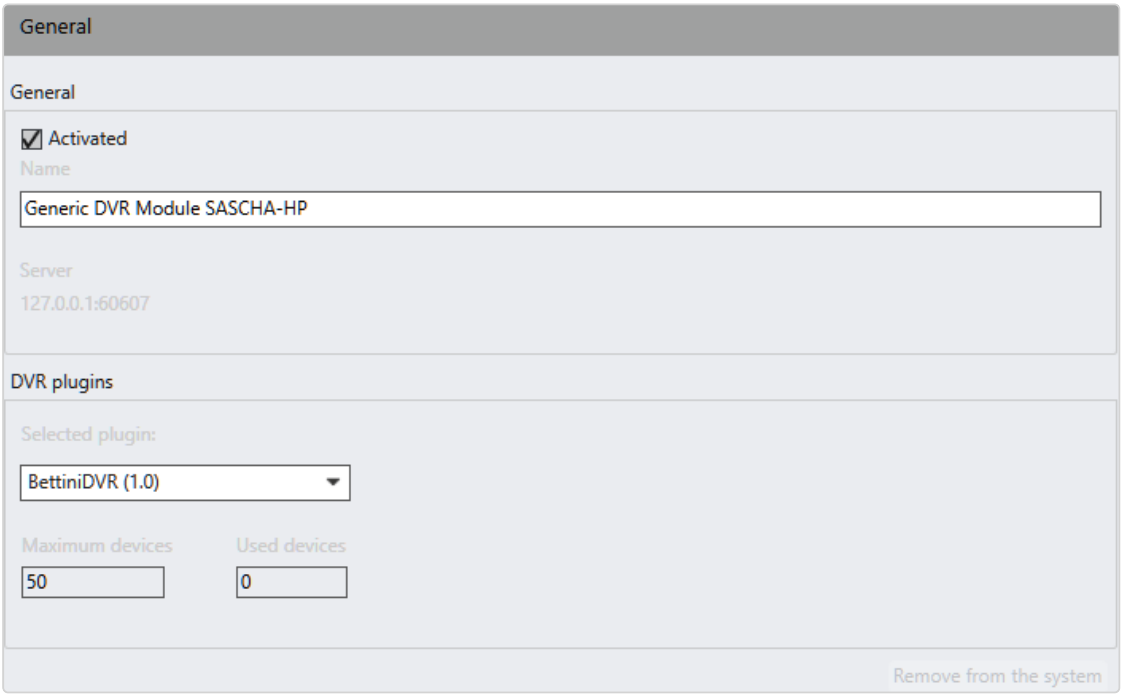


Fig. 246: Generic DVR module - General

1. Select the module in the server function.
2. If necessary, change the **Name** of the module.
3. Select a **DVR plug-in**.
4. Specify the **Maximum number of devices**.
5. **Apply** the set values if you want to make further settings.
6. **Save** the set values to apply the values and conclude input.

Configuring a generic access control module

To configure a generic access control module, you first have to create it in the Qognify VA administration tool (see "Qognify VMS VA Administration Tool" on page 476).

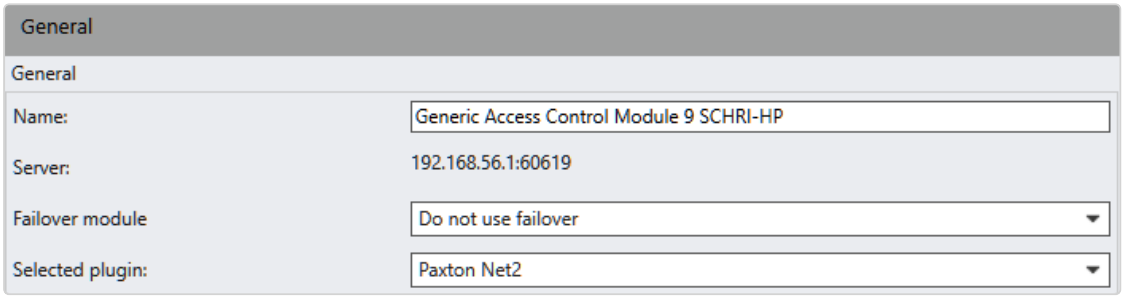


Fig. 247: Generic access control module - General

1. Select the module in the server function.
2. If necessary, change the **Name** of the module.
3. Select a **Failover module** (Qognify VMS Infinity X license required).
4. Select the **Selected plug-in**.
5. **Apply** the set values if you want to make further settings.
6. **Save** the set values to apply the values and conclude input.

For further settings see "Event Interfaces" on page 322.

Configuring a Qognify event interface (QEI) module

To configure an event interface module, you first have to create it in the Qognify VA administration tool (see "Qognify VMS VA Administration Tool" on page 476).

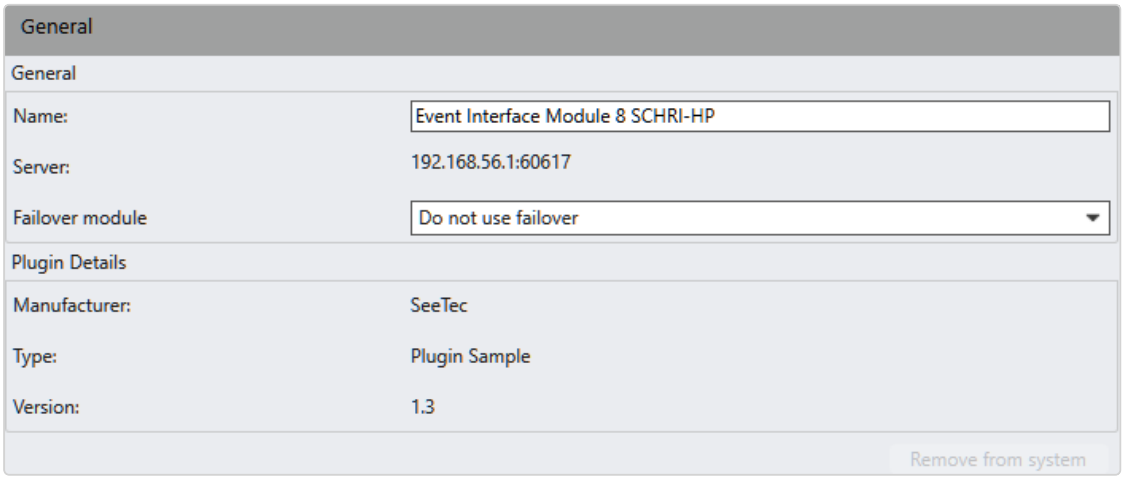


Fig. 248: Event interface module - General

1. Select the module in the server function.
2. If necessary, change the **Name** of the module.
3. Select a **Failover module** (Qognify VMS Infinity X license required).
4. **Apply** the set values if you want to make further settings.
5. **Save** the set values to apply the values and conclude input.

For further settings see "Event Interfaces" on page 322.

Configuring a body-worn camera connector module

To configure a body-worn camera connector module, you first have to create it in the Qognify VA administration tool (see "Adding a body-worn camera connector module" on page 492).

When moving the AXIS Body Worn System from a different VMS to Qognify VMS make sure to export existing users from the system controller before resetting the system and uploading the connection file. You can import the users after the Body Worn System is set up.

1. Reset the system controller to factory settings.

   The system controller must be reset to its factory default setting before importing the connection file created by Qognify VMS. Also, if you want to change the content destination where the system controller pushes the video to a factory reset of the system controller is required.

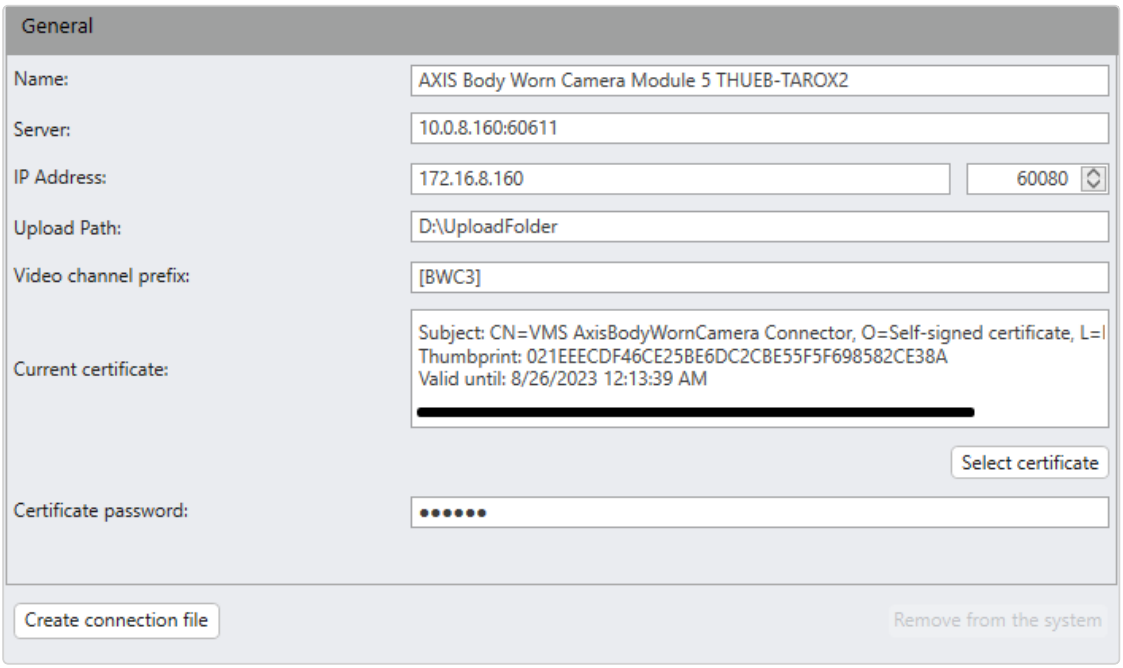


Fig. 249: Body-worn camera connector module

1. Select the module in the server function.
2. If necessary, change the **Name** of the module.
3. Enter the server and the IP address of the machine where the VA module is running.
4. Enter the path to the temporary upload folder where the body cam video files are stored (see "Configuring the body-worn camera connector" on page 221).
5. Specify the video channel prefix to be displayed. This helps to differentiate body-worn camera channels from regular IP camera channels.
6. Select a P12 certificate (for creating a self-signed P12 certificate, refer to "Creating a self-signed P12 certificate" below). A web server will be started on the IP address and port that is specified.

   > **The port used must be allowed for incoming packets by the firewall.**

7. Enter the password for the certificate.
8. Select **Create connection file**. A JSON File will be saved into the folder which was specified.

   This file must be manually imported into the AXIS Body Worn Camera System Controller in factory default state or after a full reset.

9. **Save** the set values to apply the values and conclude input.

Creating a self-signed P12 certificate

Define a configuration file for the certificate creation

1. Create a new .txt file by opening the app “Editor” and adding the following content into the .txt file.

```
[req]
default_bits  = 2048
distinguished_name = req_distinguished_name
req_extensions = req_ext
x509_extensions = v3_req
prompt = no

[req_distinguished_name]
countryName = XX
stateOrProvinceName = N/A
```

```
localityName = N/A
organizationName = Self-signed certificate
commonName = VMS AxisBodyWornCamera Connector

[req_ext]
subjectAltName = @alt_names

[v3_req]
subjectAltName = @alt_names

[alt_names]
IP.1 = xxx.xxx.xxx.xxx
```

2. Change the IP address in the file “certificate.conf” to the IP of the VA module which will communicate with the Axis W800 system controller. **Only the configured IP address will be allowed to communicate with the W800 system controller.**

   > **Make sure to include the IP address of the computer where the AXIS Body Worn Camera VA Module is running.**

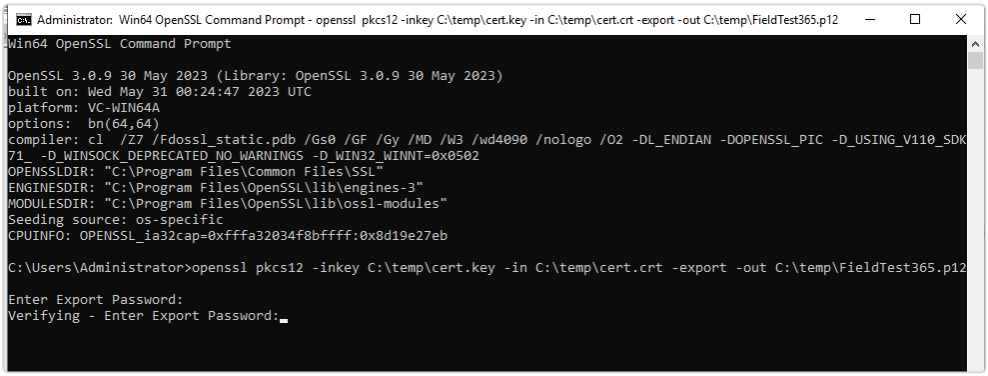
3. Save the file as “certificate.conf”.

Certificate creation

1. Download and install OpenSSL-Win64 or OpenSSL-Win32 (e.g: https://www.heise.de/download/product/win32-openssl-47316).
2. Install the OpenSSL-Win64 and run the “win64openssl-3_0_9.exe”.
3. Select the option “Windows system directory” to install it.
4. Open OpenSSL as a command console “Win64 OpenSSL Command Prompt”.
5. Run OpenSSL-Win64 via command line with the following parameters (adjust the parameters <full path> and the validity time to your needs):
   `openssl req -x509 -newkey rsa:2048 -keyout <full path>\cert.key -out <full path>\cert.crt -days 365 -nodes -config <full path>\certificate.conf`
   Example:openssl req -x509 -newkey rsa:2048 -keyout C:\temp\cert.key -out C:\temp\cert.crt -days 365 -nodes -config C:\temp\certificate.conf
   Two files will be created (cert.key and cert.crt).

Certificate conversion into P12 format

1. Open OpenSSL as a command console “Win64 OpenSSL Command Prompt”.
2. Run OpenSSL-Win64 via command line with the following parameters and adjust the parameters <full path>:
   `openssl pkcs12 -inkey <full path>\cert.key -in <full path>\cert.crt -export -out <full path>\QVMS_certificate.p12`
   Example:openssl pkcs12 -inkey C:\temp\cert.key -in C:\temp\cert.crt -export -out C:\temp\FieldTest365.p12
3. Set a password for the certificate. You will need to enter the password in a later step once you import the P12 certificate into the VA module.



A certification file QVMS_certificate.p12 will be created in the specified folder.

System

The **System** function on the **Administration** control allows you, for example, to configure and manage system-wide settings for the network, automatic backups as well as communication settings and event management settings.

> **The system manager is valid for all locations.**

1. Select the main location in the **Company** control. The selected location is displayed in the title bar of the Administration control.
2. Select **System** in the Administration control.

Configuring the video classification

General

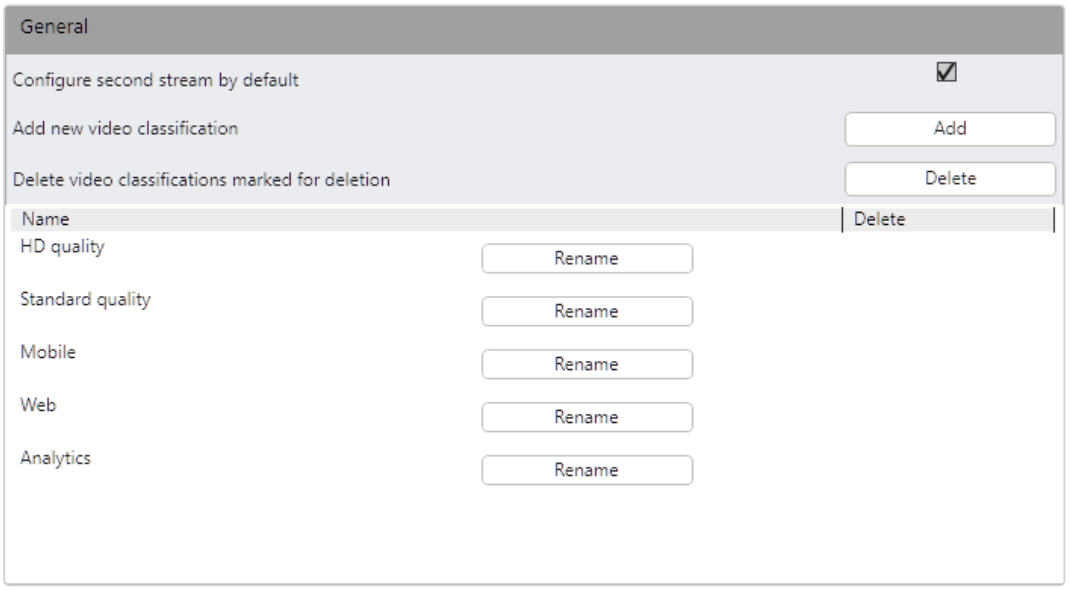


Fig. 250: Video classification - General

1. Disable **Configure second stream by default**, then new cameras are integrated with one configured stream only. Additional stream have to be configured manually (see Creating a new video stream).
2. To add a new video classification, select **Add**, and specify the **Name** of the video classification.
3. Click **OK** to confirm. The new video classification is displayed in the list.
4. To delete video classifications marked for deletion, select the video classifications you want to delete, and click **Delete**.

   > **The standard video classifications ("HD quality", "Standard quality", "Mobile", "Web", "Analytics") cannot be deleted; they can only be renamed.**

5. **Apply** the set values if you want to make further settings.
6. **Save** the set values to apply the values and conclude input.

Bandwidth optimization

Depending on the license a bandwidth optimized video stream can be selected in Archive mode (see "Archive player" on page 164).

A transcoding channel is required to get a bandwidth optimized stream from the archived recordings (see "Adding a Transcoding engine module" on page 481).

When using a multi-installation login, all connected installations need to have the feature enabled, otherwise bandwidth optimized playback will not be enabled at all (see "Installation manager" on page 82).

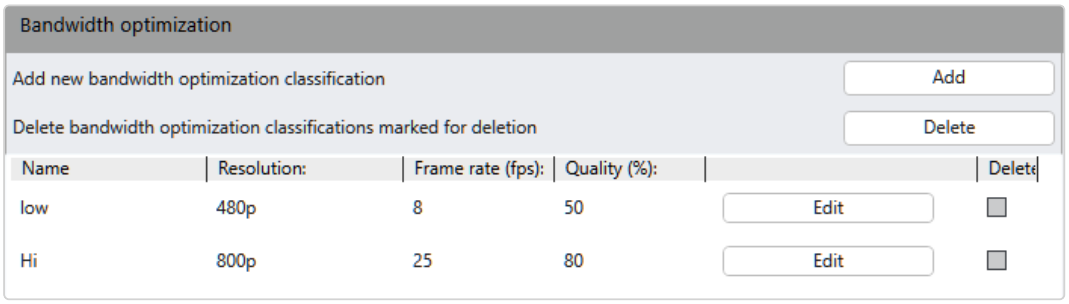
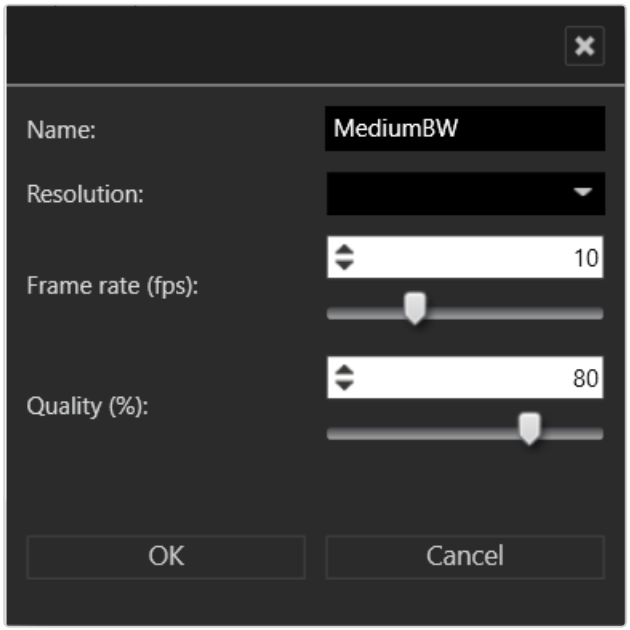


Fig. 251: Video classification - Bandwidth optimization

Add a bandwidth optimized video classification

1. Select **Add**. The window for configuration of the video classification is displayed.



2. Specify the **Name** of the video classification.
3. Specify the **Resolution**, **Frame-rate (fps)** and **Quality (%)**.
4. Select **OK** to confirm. The new video classification is displayed in the list

Edit a bandwidth optimized video classification

1. Select the related video classification and select **Edit**. The window for configuration of the video classification is displayed.
2. Edit the required settings.
3. Select **OK** to confirm.

Delete a bandwidth optimized video classification

1. Select the related video classification and select **Delete**.

Configuring the alarm classifications

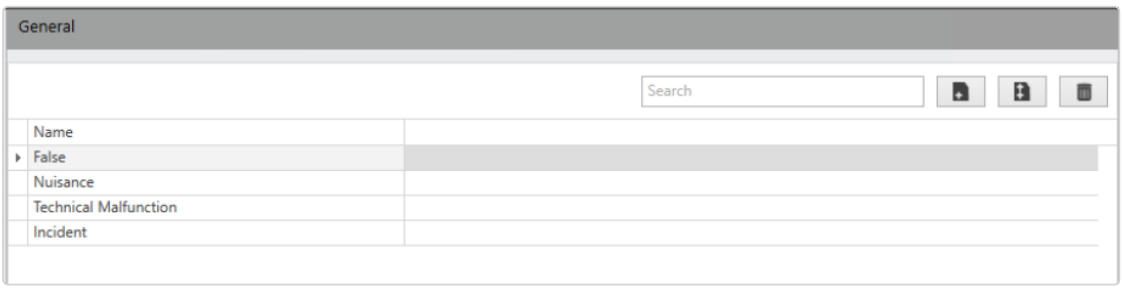


Fig. 252: Alarm classifications

The alarm categories are defined in the **System** function using the Alarm classifications. By default, four classifications are provided: "False", "Nuisance", "Technical Malfunction", "Incident".

1. Select Alarm classifications.
2. Double-click a existing entry a alter the name, if required.
3. Select **Add** to add a single item and edit its name.
4. Select **Add multiple** to add ten new items to the list and edit their names.

5. Select an existing item in the list and select **Delete** to remove the classification from the list.

   The classification will also be removed from the correspondingly classified alarms.

6. **Apply** the set values if you want to make further settings or **Save** the set values to apply the values and conclude input.

Configuring the backup

The default setting of the automatic backup of the management database is 1 a.m. every night. To restore a backup the Administration Tool is required (see "Qognify Administration Tool" on page 465).

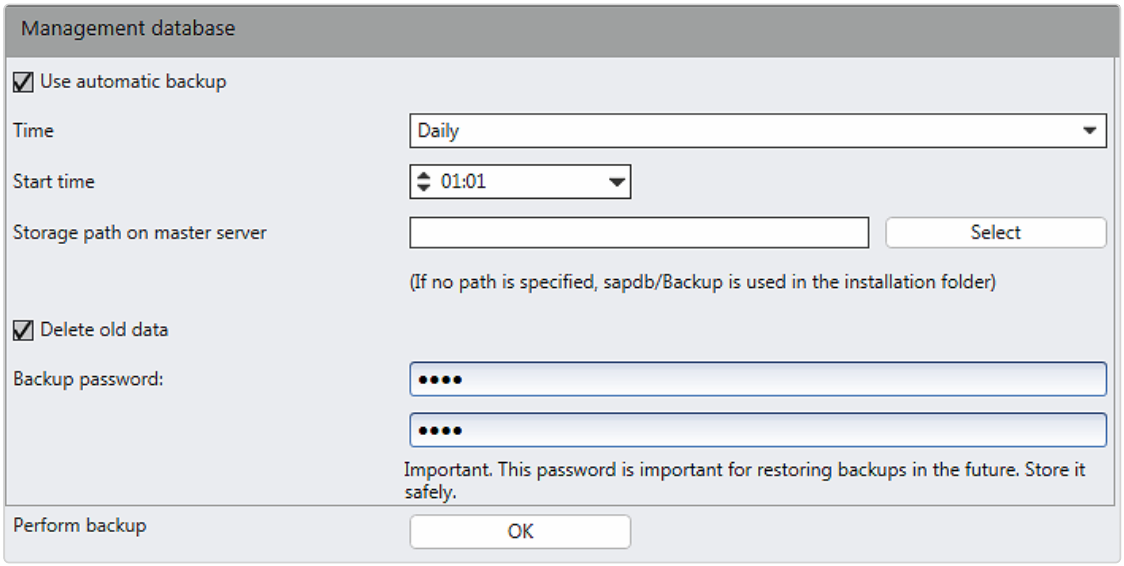


Fig. 253: Configuring the backup

1. Select **Use automatic backup** to schedule automatic backups.
2. Select the **Time** and **Start time** of the backup.
3. If necessary, edit the **Storage path** for data backup or click **Select** to select the folder directly in Windows Explorer.

   The export folder can only be selected if the client is installed on the Core Service Main server. Otherwise, the storage path to the export folder on the server has to be entered manually.

4. Select **Delete old data** to delete existing backups before the data is backed up. This setting is only applicable for automatic backup. There are up to eight backups.

   The backup folder should be backed up to a tape drive or other backup medium at regular intervals to ensure that the data backups are still available in the event of a hard drive crash.

5. Enter the **Backup password**. The backups are encrypted with AES-256 to prevent misuse of backups.

   The backup password must not be blank.

6. Click **Perform backup** to carry out the data backup immediately. The backup is started. The backup file is named as follows: "Qognify_M_20yymmdd.hhmm.zip", where "yy" is the decade, "mm" the month.

   Example "Qognify_M_20130725.1145.zip" for a manual backup performed on July 25, 2013, at 11:45 am.
   "Qognify_A_20130725.1145.zip" for an automatic backup performed on July 25, 2013, at 11:45 am.

7. **Apply** the set values if you want to make further settings.
8. **Save** the set values to apply the values and conclude input.

Configuring the Event Manager

During operation, various system events occur that are managed in the system database. The Event Manager administers the event database and the notification settings for email and SNMP.
Events are separated into the categories error, warning, and info.

The access to video sources in surveillance mode is stored in the corresponding DeviceManager (see "Configuring the DeviceManager (DM)" on page 404).

Legislation in France requires that events are never deleted in installations in France. Make sure that the management database (MAXDB) has sufficient storage space at its disposal. The capacity of the management database is configured with the Qognify Administration Tool.

General

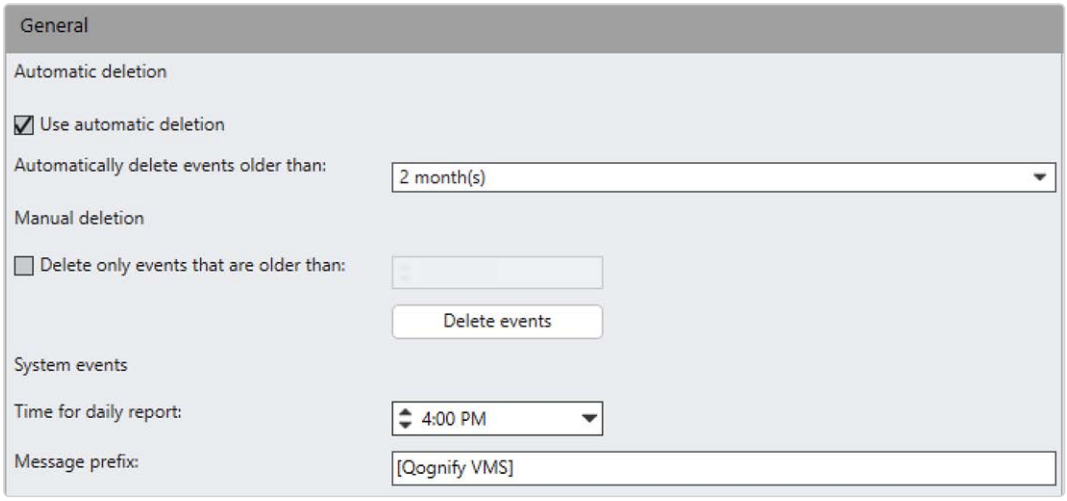


Fig. 254: Event Manager - General

Automatic deletion

1. Select **Use automatic deletion**, and select the period after which the event database is to be deleted (default: active, period: 2 months).
2. To tidy up the database manually, select **Delete only events that are older than**, and then specify the period.
3. Click **Delete events** to delete the events in the selected period from the database.

System events

The software can send a daily report about the system status by email. For this, the configuration of an SMTP server is required (see "Configuring the SMTP server" on page 441), as well as the configuration of email addresses (see "Configuring the Email Manager" on page 442).

1. Specify the **Time for daily report** on the system events. The email with the report of the events of the last 24 hours is sent to all email addresses stored as system addresses in the email manager.
2. If required, add a **Message prefix** that will be attached to the message to make it discernible.

Notifications

Events are grouped according to their prevalence and classified by the following criteria:

- Errors : Errors are serious events that impair the operation of the software. Administrative measures are required (see "Errors" below).
- Warnings  : Warnings are system-relevant events that can affect the function of the whole system or parts of the system. Usually, prompt administrative actions are required (see "Warnings" on page 437).
- Info  : Infos are system-relevant events that do not affect the function of the whole system or parts of the system. Usually, no administrative actions are required (see "Info" on page 439).

The individual notifications are editable (see "Editing Notifications" on page 440).

Errors

The following errors trigger a notification:

- **Error changing the license file**: The license file in the conf-directory cannot be changed. Possible reasons are an invalid license file or changed user rights.
- **FlatFileLogging: Cannot write alarm file**: The flat-file logging can be set in the configuration of the Core Service Main. Possible reasons for errors are changed user rights on the share-volume or insufficient storage space.
- **FlatFileLogging: Cannot write summary file**: The flat-file logging can be set in the configuration of the Core Service Main. Possible reasons for errors are changed user rights on the share-volume or insufficient storage space.
- **Service monitoring check failed**: The user is informed when a service fails due to network issues, e.g. the DeviceManager, the MDS, or the Video Analytics service.
- **Service monitoring not available**: The module monitoring the services fails to load and cannot inform about failing services.

- **The configuration and event database is full:** The data volume of the MaxDB is 4 GB after standard installation. The size can be adjusted with the administration tool (see "Qognify Administration Tool" on page 465).
- **Cannot mount multimedia database zone**: Without zone, video data cannot be recorded. Possible reason can be a wrong server path or missing permissions. The zone settings have to be checked (see "Management database (MaxDB)" on page 467).
- **Cannot start multimedia database**: The MDS cannot be started. Possible reason can be a lack of disc space (zone is full).
- **Multimedia database statistics are not available**: The statistics cannot be generated. Contact Qognify service for support.
- **Multimedia database zone is full**: The available storage space has reached 95%. The edge storage deletes the oldest recordings (see "Image storage" on page 231
- **A service is reporting a memory overflow**: This concerns the services VMS_Core, VMS_DM, or VMS_MDS. Contact Qognify service for support.
- **A service was unexpectedly terminated**: Contact Qognify service for support.
- **Cannot find LPR dongle**: The license plate recognition does not work, because the LPR dongle is missing (see "LPR mode" on page 451).
- **Failure of image analysis due to poor light** :This error concerns the video analysis (see "Qognify Video Analytics" on page 290). If not enough details can be discerned in the image, the image analysis fails.
- **Image analysis failure due to distortion**: This error concerns the video analysis (see "Qognify Analytics" on page 301). If the image is distorted due to a camera manipulation, the image cannot be analyzed.
- **No additional threads available**: The system resources are full. Contact Qognify service for support.
- **VA communication with third party system lost**: The VA module probably lost the network connection. Check the third party system, the network setting or the VA configuration (see "Qognify VMS VA Administration Tool" on page 476).

- **VA service has lost video signal**: The VA service requires a reliable video stream, e.g. for motion-based detection. Possible reasons are lost network connections or camera issued.
- **AV export failed**: The AV export does not work. Possible reason is a setting in the AV configuration (see "Qognify VMS VA Administration Tool" on page 476).
- **Cannot establish image stream**: The DeviceManager cannot establish an image stream from the camera. Possible reasons can be network or camera issues.
- **Device cannot be started**: A camera or other hardware device is unavailable. Possible reason is defective hardware.
- **Initialization of the VMS_DM service failed**: The DM service cannot be started. See the log file for further information or contact Qognify for support (see "Support" on page 13).
- **User deactivated**: The user is deactivated after a preset number of failed login attempts (see "Configuring the user security settings" on page 448).

Warnings

The following warnings trigger a notification:

- **Cyclic backup of configuration and event database failed**: The cyclic backup of the system databases has failed (see "Configuring the backup" on page 432).
- **Sub Core unreachable**: When multiple Core Service servers are installed, the Core Service Sub cannot be reached (see "Core Services and branches" on page 22).
- **The configuration and event database is almost full**: The data volume of the MaxDB is 4 GB after standard installation. The size can be adjusted with the administration tool (see "Qognify Administration Tool" on page 465).

- **MDB automated video backup interrupted**: The automatic video data backup was interrupted (see "Video Backup/Export" on page 252 and "Video backup" on page 409).
- **The last archive image is older than the configured value**: A configuration error has occurred (see "Multimedia database" on page 232).
- **Thresholds values of DM statistics have been exceeded**: If certain thresholds of the DeviceManager statistics have been exceeded, a notification can be sent (see "General" on page 404).
- **Zone almost full**: Only 15% of the available video storage space are remaining. The ring storage system will delete the oldest recordings when 95% storage space is reached (see "Image storage" on page 231).
- **System time changed**: The system time change impacts the archive time stamps or the client behavior if they are not synchronous with the Core Service server.
- **AV export more than two hours old**: The configuration at the camera has to be adapted (see "Video Backup/Export" on page 252) and must be activated in the alarm settings (see "Email and FTP" on page 372).
- **AV export older than four hours**: The configuration at the camera has to be adapted (see "Video Backup/Export" on page 252) and must be activated in the alarm settings (see "Email and FTP" on page 372).
- **Edge storage import was interrupted**: A notification is triggered when an edge storage import process has failed (see "General" on page 404).
- **Loss of video signal at encoder detected**: This feature has to be enabled in the camera configuration (see "Tampering detection" on page 260). Additionally, this event can be used as alarm trigger (see "Configuring an alarm" on page 361).
- **Services have been stopped**: Check the Qognify services (see "Qognify ServiceManager" on page 474
- **Tampering alarm**: This feature has to be enabled in the camera configuration (see "Tampering detection" on page 260). Additionally, this event can be used as alarm trigger (see "Configuring an alarm" on page 361).

Info

The following information trigger a notification:

- **License file changed successfully**: A license file has been successfully registered at the Core Service server.
- **MDB automated video backup completed**: The automatic video data export is completed (see "Video Backup/Export" on page 252 and "Video backup" on page 409).
- **MDB automated video backup started**: The automatic video data export has started (see "Video Backup/Export" on page 252 and "Video backup" on page 409).
- **Restoration of failed image analysis**: In some cases an interrupted calibration of video analytics could be recovered.
- **VA video signal recovered**: A lost video signal could be reestablished.
- **Edge storage import was successful**: The edge storage import process was finished successfully.
- **Services have been restarted**: If a service stops e.g . due to an update it automatically restarts.
- **Manual export started**: The manual export of image data has started successfully.
- **Manual export completed**: The manual export of image data has completed successfully.
- **Manual export failed**: the manual export of image data did not succeed or the export has been canceled by the user.

Manual exports that trigger a notification are:

- Native server-side export
- Delayed native server-side export
- Native client-side export
- AVI export
- JPEG export
- Export with the ExportDesigner (refer to "The Export Designer" on page 96)

When connecting a new client to an old server prior to version 7.5, only the event "Manual export started" is generated.

Editing Notifications

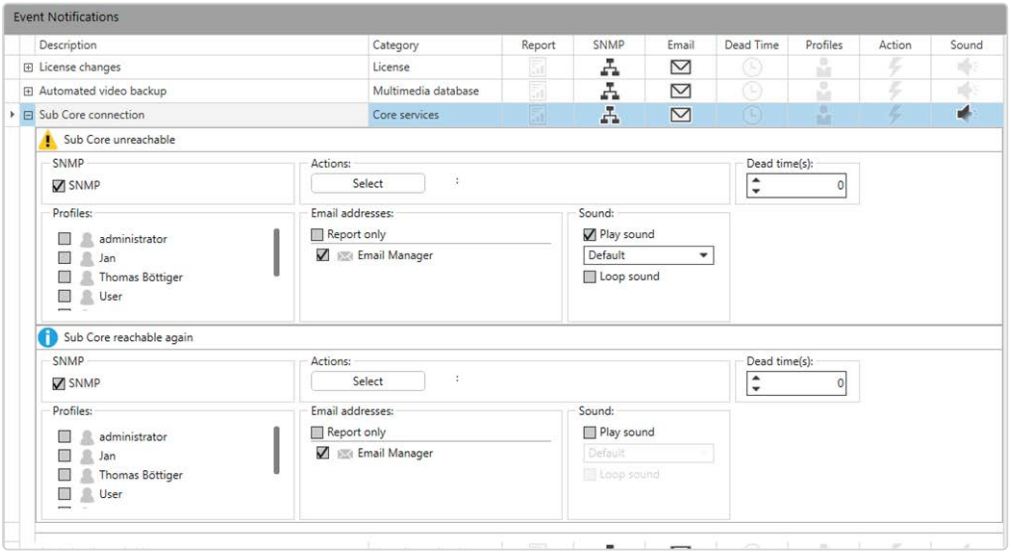


Fig. 255: Editing notifications

1. Select the event in the list, and specify:
   - If the event is displayed only in the daily report of the system events that is sent by email (see "Configuring the SMTP server" on the facing page, and "Configuring the Email Manager" on page 442).
   - If an SNMP trap is sent to a management host when the event occurs (see also "Configuring the SNMP server" on page 442).

2. To edit one or more events, select it in the **Edit** column and click **Edit selected objects**.
3. Specify whether an **Action** is to be performed:
   - to which recipient an email is to be sent,
   - for which **Profiles** a message is to be displayed in surveillance mode.
   - if a sound is played when the event occurs, what sound should be played and if it is repeated. For custom sounds, see "Managing sound and icon files with custom media" on page 447.
4. Click **Back to overview** to go back to the list of events.
5. **Apply** the set values if you want to make further settings.
6. **Save** the set values to apply the values and conclude input.

Configuring the SMTP server

To enable the Qognify services to report the malfunctioning or failure of a camera, the software requires the data of an accessible SMTP server.

1. Activate the SMTP server.
2. Specify the network address of the SMTP server and the SMTP port number.
3. Enter the **User name** and **Password** for the user account.
4. If necessary, select the encryption method with which the e-mails are to be sent. The following encryption methods are available: SSL and TSL.
5. Enter the **Sender address**.
6. Click **Send test** email to check the settings.
7. **Apply** the set values if you want to make further settings.
8. **Save** the set values to apply the values and conclude input.

> **Internet services like Google might block sign-in attempts. If this is the case you need to configure your corresponding Google account and "allow less secure apps to access your account".**

Configuring the Email Manager

The email lists are used to send system messages (see "Configuring the Event Manager" on page 433). The email addresses are also used send to the report (see "Configuring the SNMP server" below).

1. Click **Add new email list**, and specify the name of the new list.
2. Click **OK** to confirm. The new list is displayed.
3. To remove the list, activate it and click **Delete list marked for deletion**. All activated lists (except for alarm addresses and system addresses) are deleted.

Alarm addresses and system addresses

The lists of alarm addresses and system addresses are already created. The system messages are sent by default to all email addresses in system addresses.

1. Select the desired list.
2. Click **Add new email address**, and enter the new email address.
3. Click **OK** to confirm. The new email is displayed in the list.
4. To change the email address, click **Rename**.
5. To remove the email address, activate the email and click **Delete email addresses marked for deletion**. All activated email addresses are deleted.

Configuring the SNMP server

It is possible to send SNMP v1, v2 and v3 traps.

1. Activate the SNMP server to report system errors by means of SNMP messages.
2. Enter the **ManagementHost**.
3. Enter the **ManagementHostTrapListenPort**, the **LocalTrapSendPort** and the **CommunityString** in accordance with the settings required for the SNMP server.

> **If the SNMP component (Simple Network Management Protocol) is installed in the Control Panel > Software > Add / Remove Windows Components > Management and Monitoring Programs, a different port for LocalTrapSendPort must be set, because transmission is not possible via port 161. If port 161 is set as the default, it will not work.**

MIB (Management Information Base)

To monitor the current status of Qognify VMS in a 3rd party monitoring solution, a MIB file (Management Information Base) "vms.mib" is installed together with the Core Service in the installation directory "/tools/MIB". As soon as the MIB file is read in into the PRTG software the descriptions for SNMP v1 and SNMP v2 traps are available.

> **PRTG is network-monitoring software that can run on a Windows machine within the network and collect statistics from designated hosts such as routers, servers, switches and other important devices or applications.**

SNMP v1/v2

1. Activate **SNMP v1** or **SNMP v2**. SNMP v2 adds simple security features, whereas SNMP v1 has none.
2. Enter the **CommunityString** to enable correct responses from the host.

SNMP v3

SNMP v3 is currently the most secure protocol version.

1. Activate **SNMP v3**.
2. Enter the **Security Name**, **Authentication Type**, **Authentication Password**, **Encryption Type**, and the **Encryption Password**.
3. To test the settings, click **Send SNMP test message** to check the settings.
4. **Apply** the set values if you want to make further settings.
5. **Save** the set values to apply the values and conclude input.

Configuring the NAT list

The NAT feature is only available for the client in the Qognify software over the Internet without requiring a VPN tunnel; port forwarding must be activated on your router or firewall. Ports 60000-60008 are required by default for NAT.

These ports have to be open on all distributed servers.

1. Click **Add new NAT entry**.
2. Enter the internal and public address.
3. To remove an entry, select list, select **Delete** at the end of each line, and click **Delete NAT entries marked for deletion**.

4. **Apply** the set values if you want to make further settings.
5. **Save** the set values to apply the values and conclude input.

Configuring the entity numbering

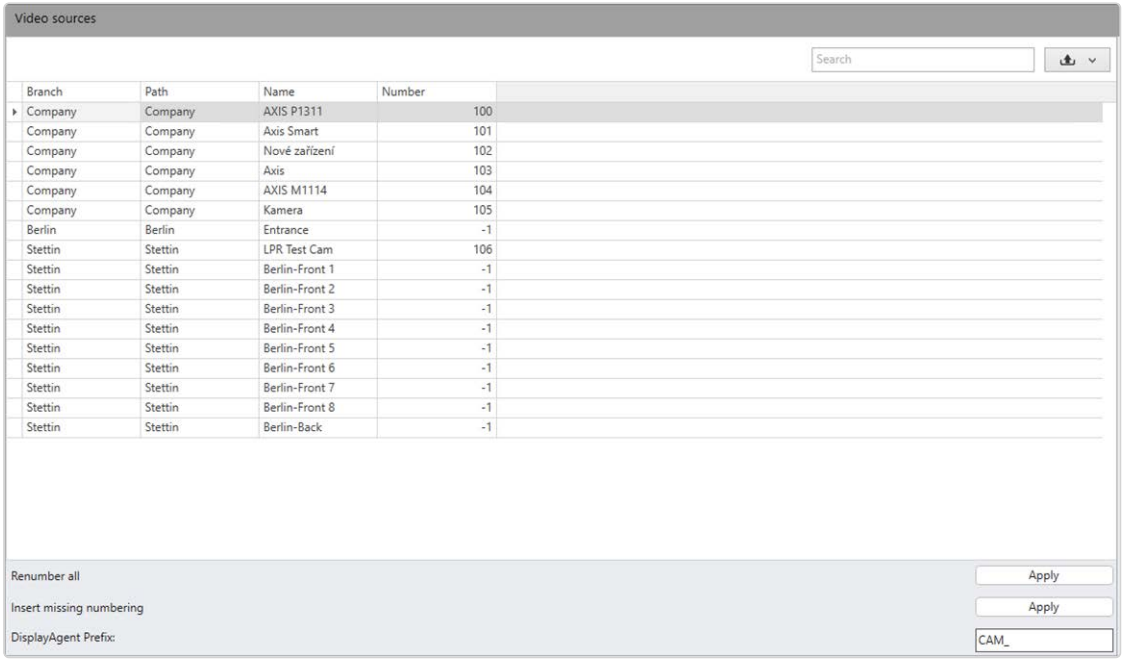


Fig. 256: Entity numbering

The ID entity number is **not** assigned by the system. If entity numbers are used, the numbers must be configured manually. The number serves as a reference point for the SDK or the keypad assignment with virtual sequences (see "Input devices" on page 73). The number can also be changed later.
The maximum entity number is 99.999.999.

1. If necessary, change the entity number of the device by entering the new ID directly into the text box or changing the numbers up or down step by step with the arrow keys.

   > **Only change the entity numbering if necessary during configuration of the software by third-party vendors.**

2. Select **Renumber all** to assign a unique entity number to every device by selecting a starting number. After specifying the start number, Qognify VMS will automatically increment the numbers in steps of "1".

   > **Only visible entries are renumbered.**

3. Select **Insert missing numbering** to assign a unique entity number to devices without entity numbers. Qognify VMS will automatically use the highest number in the list and increment by “1”.
4. Define the **DisplayAgent prefix**. Four configurable prefixes for cameras, layers, windows, and tiles are available (see "Working with the DisplayAgent prefix" on the next page). Valid combinations are:
   - Camera on window
   - Camera on tile
   - Layer on window
   - Patrol sequences (see "Changing cameras sequentially" below)
5. **Apply** the set values if you want to make further settings.
6. **Save** the set values to apply the values and conclude input.

Exporting the entity numbers

The list of entity numbers can be exported as a PDF file or as a comma-separated document that can be imported with any spreadsheet editor.

1. Select **Export** ( ).
2. Select the export file format (PDF or CSV).
3. Select the folder and click **Save**.

Changing cameras sequentially

The camera sequence can be set so that they are displayed in a tile one after another, e.g. for patrols. The camera sequence loops until something else is displayed in the same tile.

> **It is possible to have different camera sequences in different tiles running at the same time in the same DisplayAgent.**

1. Select **Patrols**.
2. Change the entity number of the patrol to define a sequence.
3. Define the **DisplayAgent prefix**.

Working with the DisplayAgent prefix

When the DisplayAgent prefix is activated, the sender can open a new connection for each command or can separate different commands by a line break (CR, LF or CRLF). The parser searches for the prefixes and a directly following number, all other characters are ignored.

The simplest command has the form “CAM_1 WINDOW_1” but is also valid to send something like “DUMMY_HEADER CAM_1 SOME_TEXTWINDOW_1”.[1]

Configuring the AlarmWatchDog

The AlarmWatchDog monitors the alarms of multiple Qognify installed systems at once. If an alarm occurs on any of the monitored systems, the user can establish a connection to the system and see the alarm. To activate the respective alarm transmission, set the AlarmWatchDog option in the server-settings of the related alarm scenario (see "Alarms" on page 356).

> **Each system can only be connected to one AlarmWatchDog.**

1. To configure the AlarmWatchDog, select **AlarmWatchDog** in the System control bar.
2. Activate the AlarmWatchDog and specify the IP address and port number (default: 12000) of the client with the AlarmWatchDog installed. For obtaining the correct IP address, see the section on the AlarmWatchDog configuration (see "Configuring the AlarmWatchDog" on page 535).
3. Specify the IP address and port number of the VMS server. All clients to be watched must be connected to this server.
4. Set the **User name** and **Password** of the user who will be logged into the server in case of an alarm.
5. Specify the user profile (default: user name).
6. Enter a description of the server.
7. Activate **NAT** if the client can reach the server only via NAT (network address translation), e.g. through a router.
8. **Apply** the set values if you want to make further settings.
9. **Save** the set values to apply the values and conclude input.

[1] Both messages are parsed to "Show Camera 1 on Window 1".

Managing sound and icon files with custom media

With the custom media feature you can manage your own sound and icon-files. Custom icons and sounds are stored in the management database. The sounds and icon files can be applied to the appropriate items, e.g. as custom icons for cameras.

Uploading and deleting image files

For best quality, we recommend image files with low complexity (when displayed as icons) and 512x512 px (when used for maps and larger sizes.

1. Click **Add** to add a custom image file from the file system. The following image formats are supported: png, jpg, gif.
2. Click **Save** to upload the images to the server. They will be stored in the local cache for improved performance. The file icon is visible after the images have bee uploaded successfully.
3. Click **Edit** to rename the file.
4. To remove the image, click **Delete**. All assigned items will be displayed with their default icons after restarting the client.

Uploading and deleting sound files

1. Click **Add** to add a custom sound file from the file system. The following sound formats are supported: mp3, wav.
2. Click **Save** to upload the sound files to the server. They will be stored in the local cache for improved performance.
3. Click **Edit** to rename the file or play the selected sound.
4. To remove the sound file, click **Delete**. All assigned items will be reset to their default sounds after restarting the client.

Assigning custom media

1. To assign the custom files to items, open the following settings in configuration mode:
   - Camera - General. When the custom icon is assigned to a camera, it is displayed throughout the system for this camera.
   - Hardware settings
   - Maps
   - Video wall
   - Views

Configuring the user security settings

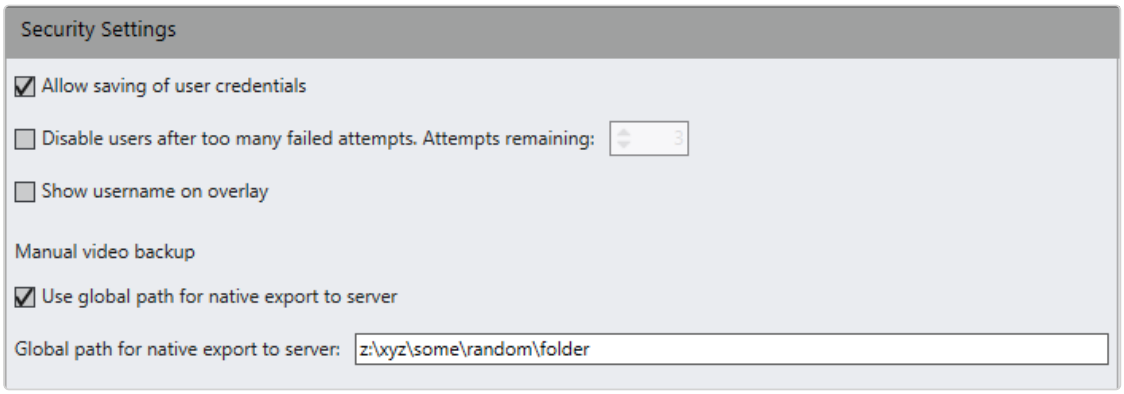


Fig. 257: Security settings

For compliance with the GDPR regulations under EU law, the automatic saving of user credentials can be disabled. It is enabled by default for all users and can only be enabled or disabled per installation. Additionally, the number of login attempts can be limited.

1. Select **Security settings** in the System control bar.
2. Disable the saving of user credentials. When disabled, the user credentials have to be entered at log in.
3. Enable **Show username on overlay** to display the current user of the camera in the top part of the image as overlay.

   > **This feature increases the CPU usage by 10% and may impact responsiveness.**

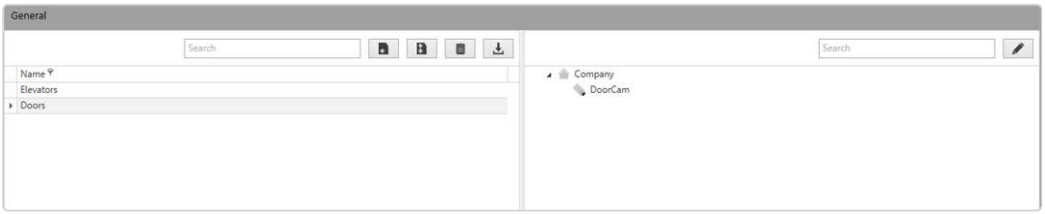
4. Enable the setting for the number of failed login attempts and define the number to a reasonable amount (default is three attempts). When the user exceeds the number of allowed login attempts, a notification can be triggered (see "Notifications" on page 435).
5. To prevent users from exporting their files in deliberately selected locations on the server, activate **Use global path for native export to server** and specify the path where all native exports are placed. When activated, the location option in the export settings is disabled (refer to "Exporting native image data to the server" on page 109).
6. **Apply** the set values if you want to make further settings or **Save** the set values to apply the values and conclude input.

Creating entity labels

Labels can be attributed to any entity such as cameras and help finding the results with pre-configured filters. The labels can be used for searching in surveillance mode, archive mode and LPR mode. The labels work as filters that are combined as Boolean OR parameters, so that searching with multiple labels will display the results to which all labels apply. The search however, uses the Boolean AND parameter.

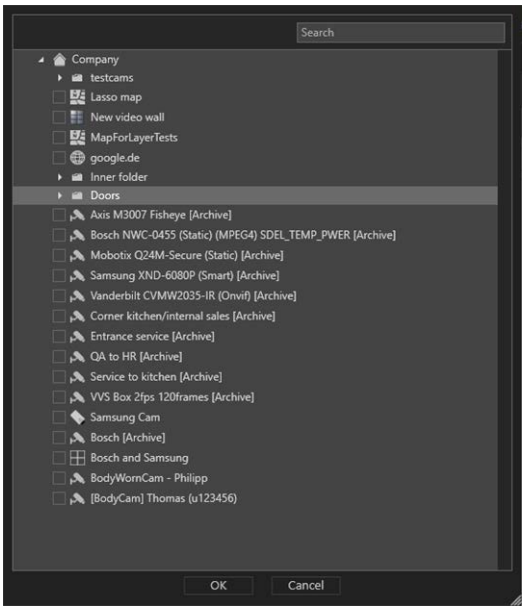
> **Only labels corresponding to the respective user rights will be displayed to the user.**

1. Select **Entity labels** in the System control bar.



2. Select **Add** or **Add multiple** to add one or more labels to the list and name the labels.
3. To add predefined labels, select **Import** and navigate to the text file that contains the labels (see "Preparing the label file" on the next page). After importing, the list is populated with the labels from the file.

4. Select a label on the left side and click **Edit** .



5. Assign one or multiple entities to the selected label and click **OK**. The assigned entities are now displayed at the right of the respective label.
6. **Apply** the set values if you want to make further settings or **Save** the set values to apply the values and conclude input.

Preparing the label file

Labels can be prepared in a simple text file (e.g. by using the Editor) by adding names for labels separated by line breaks.

1. Create a new file with the Editor.
2. Enter a label name and press the return key.
3. Add as many labels as required, each in a new paragraph.
4. Save the document as a *.txt file.

11

LPR mode

The automatic license plate recognition (LPR) in the video image and comparison with a license-plate database allows items such as entry checks and barrier control, parking and loading area administration and triggering of alarms.

LPR mode is for analyzing the LPR events and displaying the information associated with the event (including master data, if available). In addition, statistics can be kept.

> - LPR functionality requires a license key.
> - LPR functions are not supported if the client and server do not have the same version (e.g. LPR does not work on a client running version 7.5 if the server does not have the same version 7.5).

User rights in LPR mode

- The user rights and permissions required for using LPR mode are defined by the LPR user groups. Only groups with the permissions “View” or “Change” are allowed to use the LPR mode.
- If no LPR groups are available, any user can use and view the LPR mode.

To restrict the use of the LPR mode (and to prevent possible misuse), at least one LPR group with the corresponding rights must be configured (see "License plate groups" on page 400).

Editing LPR master data

LPR master data are all information that is assigned to a specific license plate (such as group, validity). The master data are created and managed with the LPR master data editor (see "LPR master data editor" on page 87).

Displaying license plate recognition details

When a license plate is recognized, the master data and alarm messages belonging to that license plate are displayed.

1. Click a column header in the main window to sort the column (alarm, layer/camera, start, stop) in ascending or descending order.
2. Select the required layer or camera (or start or end of recording). The selected object is displayed in the player.

Player

The player is operated in LPR mode in the same way as in archive mode (see "Archive mode" on page 163).

Query for license plates

In the Administration control, the stored events for a license plate or a container code in the master data set can be searched for in the LPR database.

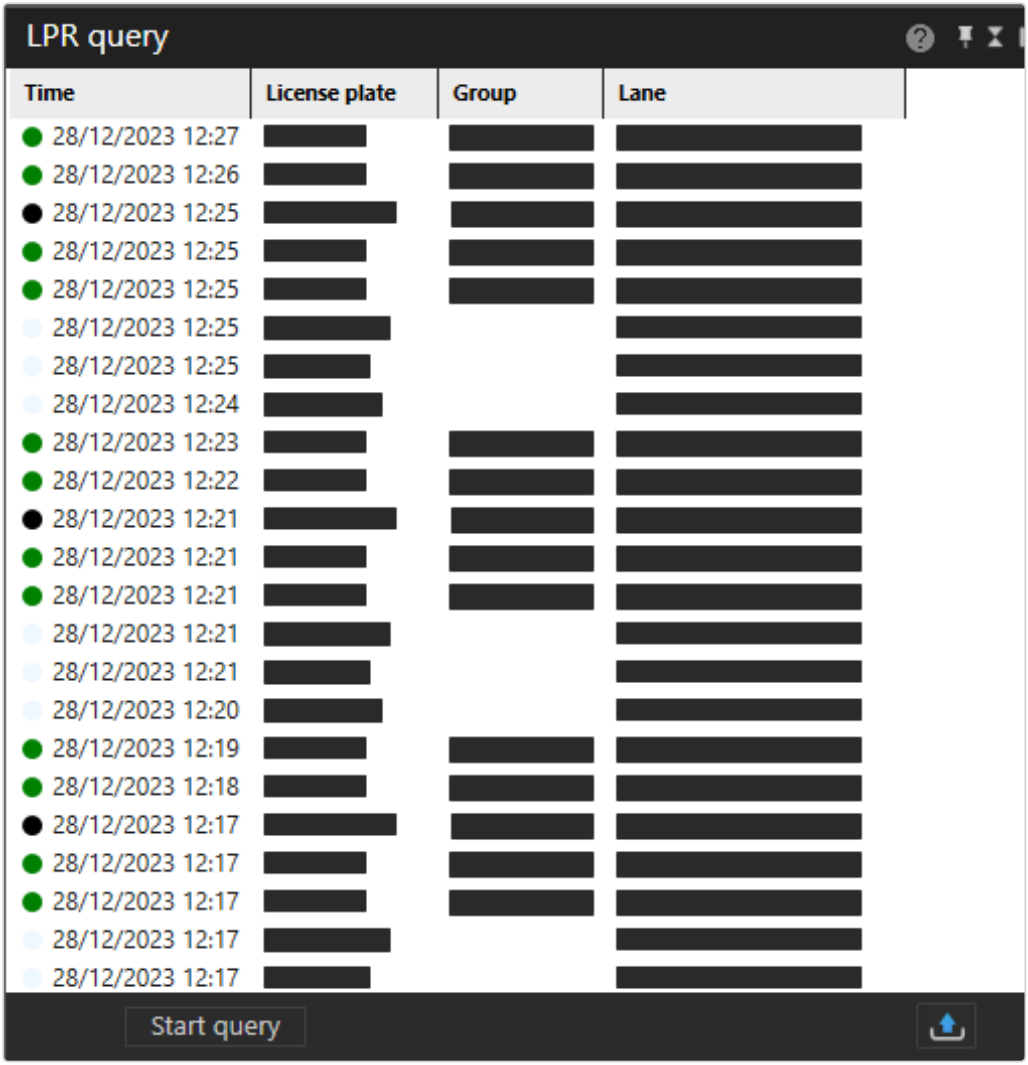
1. Select a column header in the main window to sort the license plates in ascending or descending order on the basis of the column's category (time, license plate, group).

2. Select **Start query** to display all stored events for the selected license plate or to search for a specific license plate.

Fig. 258: Query for license plates in LPR mode

3. Limit the search filter by selecting the **License plate group** and, if appropriate, entering information on the **license plate**, selecting the **lane**, and specifying the **Time period**.

4. If only the statistics are to be searched through, select **Query statistics only** and the type of the statistics.
5. Select **Start query** to search the database for e.g. license plate, group, country, or lane.
6. The search results are displayed in the **License plate recognition details** window.



7. Select the event found or sort the results using the column "Time". The player opens the selected item and skips automatically to the selected point in time.
8. To export the results as a CSV file, select **Export** .

12

Admintools

The Qognify admintools contain a suite of administration tools required to manage the servers, clients and additional modules such as the UpdateService and the AlarmWatchDog (see "The AlarmWatchDog" on page 535).

- **VA Administration Tool**: The VA Administration tool is used to configure the settings for the core server and installing the "Versatile Application" extension. The extension parameters are then configured from within the client (see "Qognify VMS VA Administration Tool" on page 476).
- **Administration Tool**: The Administration Tool is used to configure the image database and the administration database of the servers (see "Qognify Administration Tool" on page 465).
- **ServiceManager**: The ServiceManager is used for starting and stopping services (see "Qognify ServiceManager" on page 474).
- **UpdateService Configuration Tool**: The UpdateService Configuration Tool manages the configuration of the UpdateService on the Core Service Main (CSM) and the UpdateAgents on the clients (see "UpdateService Configuration Tool" on the next page).

UpdateService Configuration Tool

The UpdateService Configuration Tool manages the configuration of the UpdateService and the connected UpdateAgents (i.e. distributed server, modules and clients). The configuration tool will be installed automatically with the UpdateService (see "Configuring and updating the UpdateAgent" on page 47).

The UpdateService looks for available updates and patches immediately after installation, and downloads them before distributing the updates and patches (see "Editing the server configuration" on page 463).

The UpdateService Configuration Tool supports the following features:

- Displaying all connected UpdateAgents, their hardware specification, their installed feature, and the applied patches of each UpdateAgent
- Displaying status information of all UpdateAgents in a group
- Creating groups of UpdateAgents to configure
- Renaming and deleting groups and old UpdateAgents from the configuration
- Import and export of download packages and patch files for the UpdateService (no directories necessary)
- Export of patches and updates and import them with the help of a small tool to the UpdateAgents
- Configuration for getting updates/patches and how they should be deployed to the UpdateAgents
- Checking for updates or patches at the server

> **The UpdateService can be used to update software without an installed Qognify VMS client, as it keeps the configuration and log data in a separate folder.**

1. Start the UpdateService configuration tool in the Qognify VMS installation folder. If required, confirm the systems administration rights. The information tab is displayed.

Information on rollbacks

Rolling back to a previously installed update may be necessary to assure system operation with a minimum of interruption. In case of an update error all steps will be reverted to the backup that has been kept before updating.

Configuring the UpdateService

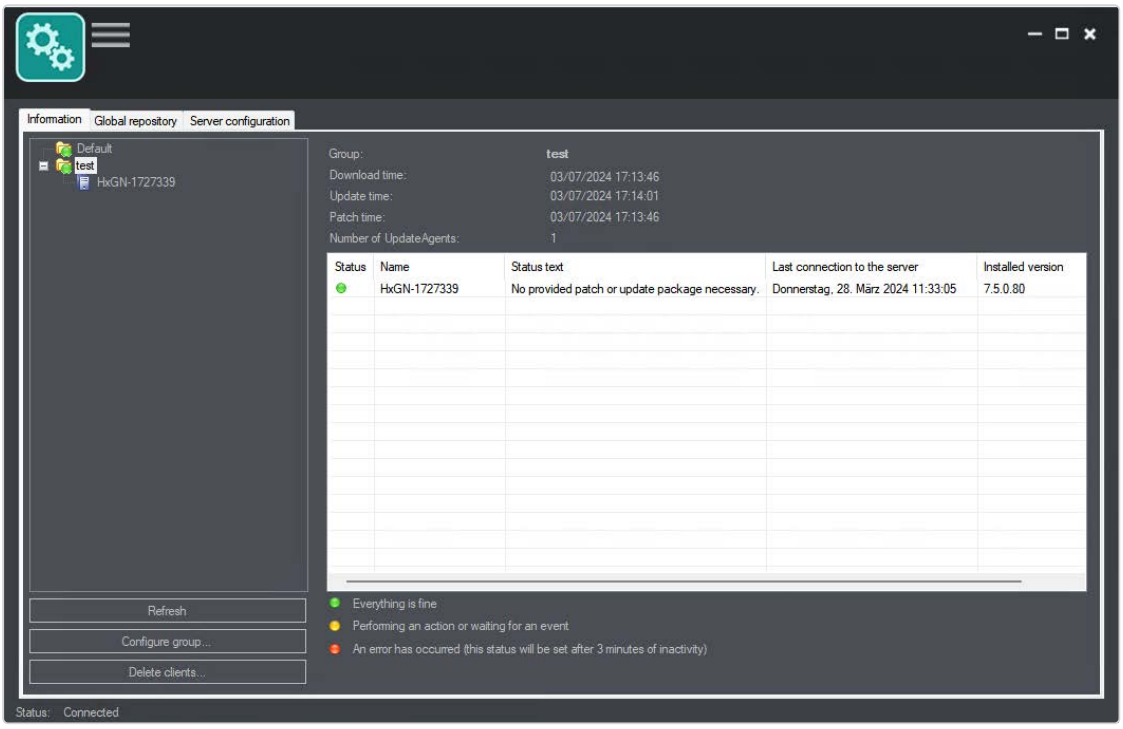


Fig. 259: Configuring the UpdateService

The panel on the left displays all groups managed by the UpdateService alphabetically. The group "Default" contains all UpdateAgents (clients) not assigned to a group. Additionally, the update status, the connection status, and the version to the server are displayed in the right panel.

> **Clients in the default group are updated automatically. Clients that should not receive updates or patches have to be located in a separate group (see "Configuring a group" on page 459).**

1. Click on a group folder to display the status overview of all clients within the group. A colored bullet point on the folder icon shows the worst status of any item in the group and another colored bullet point shows the current status of each client:
   - **Red**: An error occurred at the client or the UpdateAgent of the client is offline for more than 3 minutes.
   - **Yellow**: UpdateAgent is currently busy (patching, downloading, etc.) or waiting for an event triggered by the UpdateService (e.g. manual distribution of patches).
   - **Green**: The client's UpdateAgent is up-to-date.
2. Click on a client name to display the installed components (e.g. the system software, the software version, the status, and the installed patches).

3. Click **Refresh list** to see a more current status.
4. Click **Configure group** to create, rename or delete a group and specify the group's update and patch settings (see "Configuring a group" on the facing page).
5. Click **Delete clients** to remove clients that do not connect to the UpdateService anymore. The clients will not be deleted automatically.

Manually starting the update or patch process

If a group is configured to be updated or patched manually, **Start patch/update at the UpdateAgents** is displayed in the group's status pane.

1. Click **Start patch/update at the UpdateAgent** to start the update. It will require up to 60 seconds before the update process is started.

Proceeding after a rollback

1. Check the log to find out what the problem was.
2. Resolve the problem.
3. Stop the services.
4. On the update server, delete the update files in the updates folder and adjust upd64.xml /upd.xml by deleting the md5 sums and also the version tag.
5. On the UpdateAgent, delete the already downloaded update files in the updates folder and delete the rollback file in the updates folder.
6. Adjust upd64.xml /upd.xml by deleting the md5 sums and also the version tag.
7. Restart the services.

Configuring a group

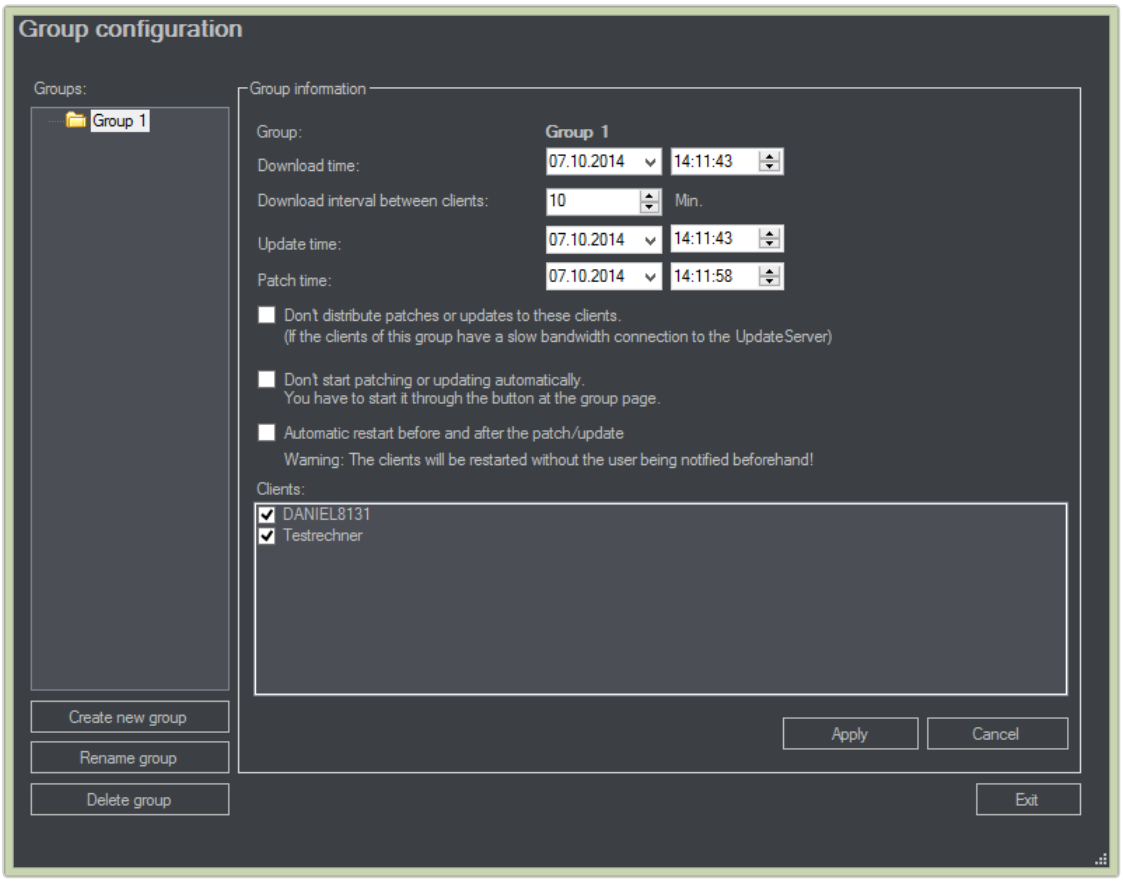


Fig. 260: Configuring a group

The group configuration allows the configuration of:

- Specific download date and time of the update package or the patch files.

  > **If the time is in the past, downloads and patches will start immediately.**

- Download interval between each UpdateAgent in minutes (e.g. the first UpdateAgent starts the download at 10:00, the second UpdateAgent starts the download at 10:10, the third at 10:20, etc).
- Update and patch date and time.
- Specific update and patch behavior for the UpdateAgents in the current group.

1. Specify the required update and patch settings for the group.
2. Select **Don't distribute patches or updates to these clients** to prevent automatic distribution at low bandwidth. If this option is activated, the patches have to be distributed manually.

3. Select **Don't start patching or updating automatically** to prevent automatic installation of patches and updates. Patching and updating has to be performed manually if this option is selected.
4. Select **Automatic restart before and after the patch or update** to shut down the Windows systems on the UpdateAgents before and after applying the patch. The clients will be restarted automatically.
5. If required, deselect clients from the groups list. Only the selected clients will be affected by the group settings.

Creating a group

1. Click **Create new group**.
2. Enter a **name** for the new group and click **OK**. The new group will be displayed in the group's column.

Renaming a group

1. Click **Rename group**.
2. Change the name of the group and click **OK**. All assigned UpdateAgents will remain in the group and adhere to the group's settings.

Deleting a group

1. Select a group in the Groups column.
2. Click **Delete group**. All clients in the group will be moved into the default group and will be exempted from the update settings. UpdateAgents in the default group will get updates and patches as soon as they are available.

> **The default group cannot be deleted.**

Global repository

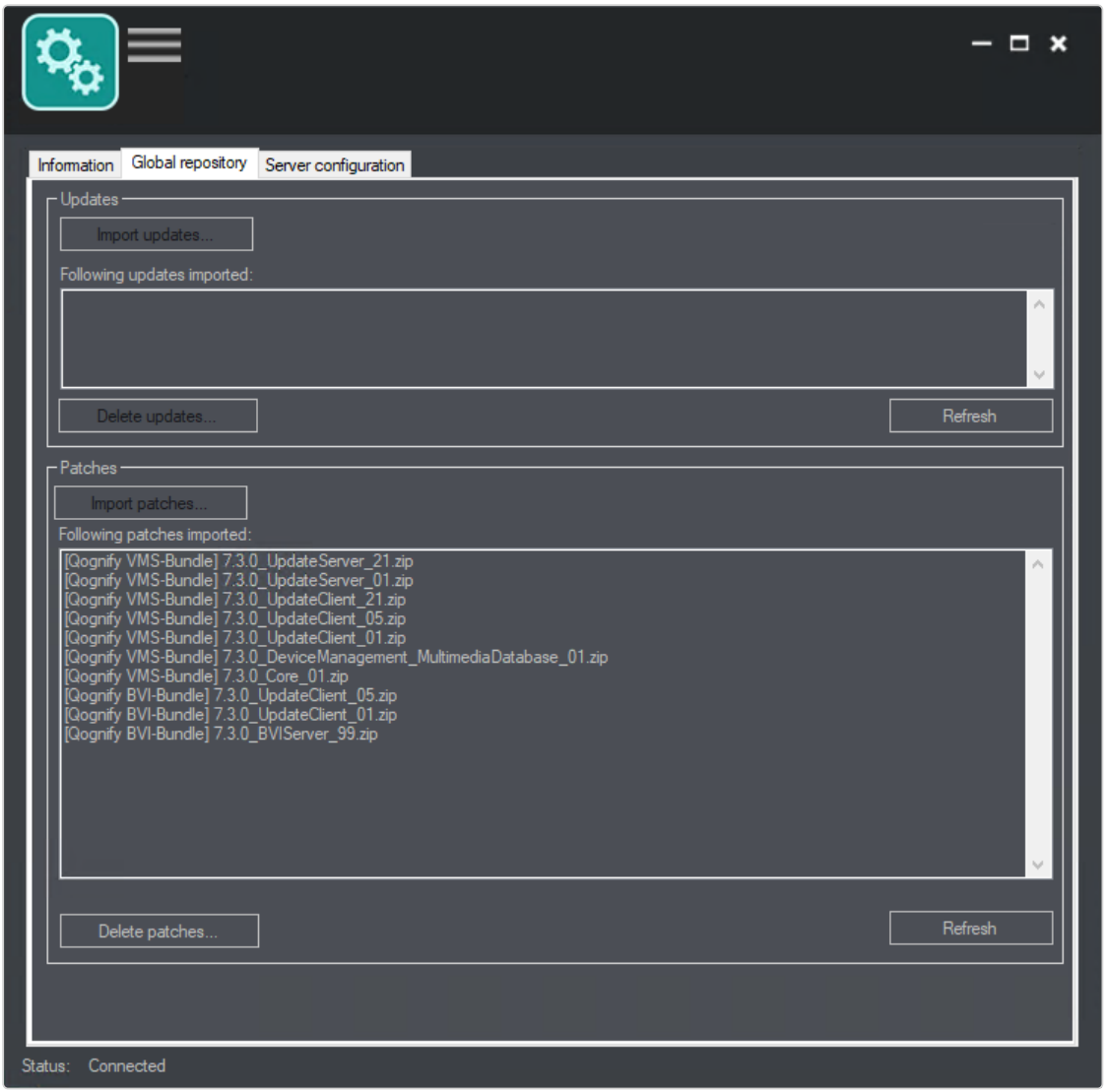


Fig. 261: Global repository

The tab displays the available updates and patches. If the UpdateService has been configured for manual distribution in the server configuration tab, all updates and patches can be imported from the server and exported to a directory on the server or an attached media (see "Editing the server configuration" on page 463).

- Updates can be imported only one at a time.
- Patches can be imported several at a time.

1. Select **Import updates** to download the available updates from a directory that is available in the local network.
2. Click **Refresh** to check at the server for updates not yet displayed.

3. Click **Export** to copy the updates and a "Qognify.UpdatePatchImport.exe" to a directory that can be copied to any media such as a USB stick. The "Qognify.UpdatePatchImport.exe" updates and patches can be installed at each client separately (see "Import of updates and patches at the UpdateAgent" on page 465).
4. Click **Import patches** to download the available patches from a directory that is available in the local network. The available patches are displayed.
5. Click **Export** to copy the patches and a "Qognify.UpdatePatchImport.exe" to a directory that can be copied to any media such as a USB stick. The "Qognify.UpdatePatchImport.exe" updates and patches can be installed at each client separately (see "Import of updates and patches at the UpdateAgent" on page 465).
6. Click **Refresh** to check at the server for patches not yet displayed.

Removing patches / updates from the list

1. If patches are not required, select the patches from the list. Pressing the shift key selects multiple objects at once.
2. Select **Delete patches** before exporting them. Only the patches listed will be distributed.

Editing the server configuration

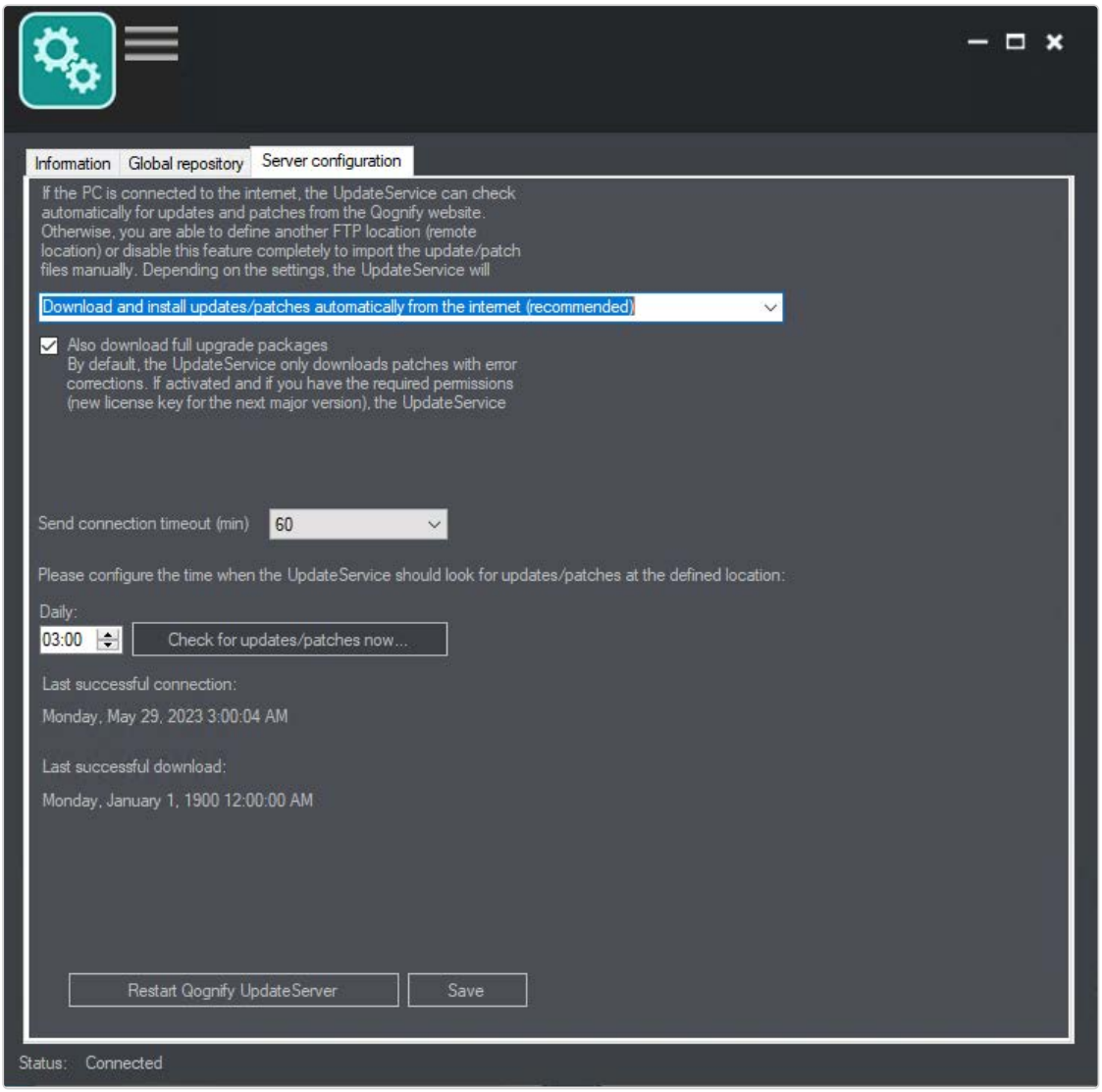


Fig. 262: Editing the server configuration

With the Server configuration tab, the basic settings for the communication between the Update server and the clients are managed. By default, the UpdateService connects to the server providing the updates, downloads and distributes the updates and patches to the UpdateAgents. However, if manual distribution or a different server for downloads is preferred, the automatic setting can be changed.

1. Select an option from the menu:
   - **Download and install updates/patches automatically from the internet**. This is the recommended setting for automatic updates and distribution of patches.
   - **Download and install updates/patches automatically from a defined remote location**. The updates and patches will be downloaded from an FTP server that has to be configured and automatically installed at the UpdateAgents (see "Configuring the FTP server" below).
   - **Don't look for updates from the internet or any remote location**. The option is not recommended, as no updates or patches will be downloaded or distributed automatically. The updates and patches will have to be downloaded and exported manually (see "Global repository" on page 461).
2. Select **Also download full upgrade packages**, to download all downloads and distribute also packages including version upgrades, if the appropriate permission (new license key for a next major version) is available. All UpdateAgents will be upgraded to the new version according to your group settings. (By default, the UpdateService downloads only patches including error corrections.)
3. Specify the time of the day when updates and patches will be downloaded and installed.
4. Click **Check for updates/patches now** to manually check for available downloads. Currently active downloads are displayed.
5. Click **Restart UpdateServer** to restart the UpdateServer with the applied settings.
6. Click **Save** to apply the settings.

Configuring the FTP server

1. After selecting the option **Download and install updates/patches automatically from a defined remote location**, enter the IP address and **port** number of the **FTP server.**
2. **Provide** the **user** name and **password** for the FTP server.
3. To establish a secure connection, activate **Use FTP via SSL**, if the server supports SFTP. (Contact the network administrator for the correct settings.)

Import of updates and patches at the UpdateAgent

1. After successfully exporting patches or updates (see "Global repository" on page 461) copy the directory to an USB stick, and plug it into the computer where the UpdateAgent is running.
2. Start the application "Qognify.UpdatePatchImport.exe" and click **Yes**.
3. Click **OK** and start the update and patching process. The UpdateAgent will be stopped for the update/patch process. After the process, the UpdateAgent will be restarted automatically.

Qognify Administration Tool

The Qognify Administration Tool is used to configure the administration database (MaxDB) and the image database (MDB) of the servers.

> **Note that incorrect settings in the administration tool may result in a non-operational system.**

1. Start the Administration Tool in the Qognify VMS installation folder.

> **All settings in the administration tool are not valid until the services or the complete computer have been restarted (to start the services see "Qognify ServiceManager" on page 474)**

General settings

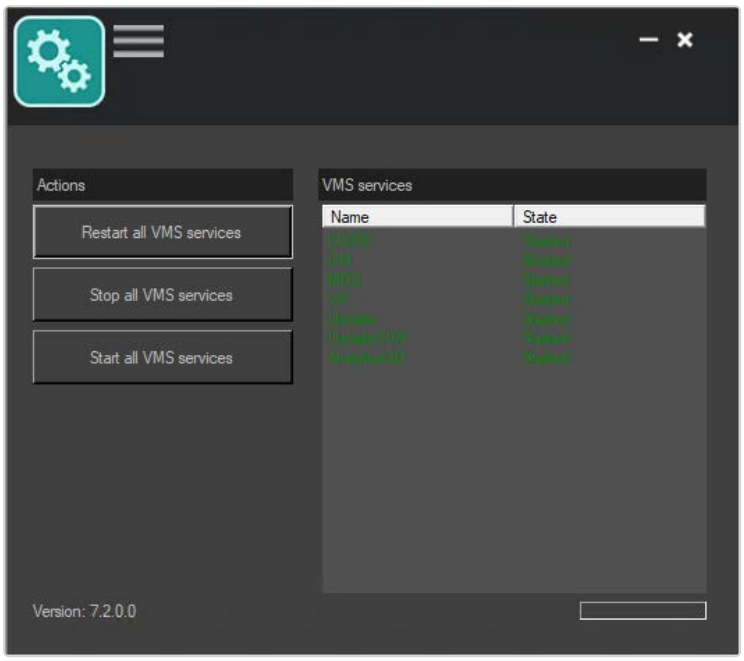


Fig. 263: General settings

1. Configure the **server** and **port** of the Core Service server if administration was started on a distributed server. If administration was started on the main server, leave these settings unchanged (default: server: localhost, port: 60000).
2. Enter the IP address of the **server** and the **host name** for the services to connect to in the "IP address/host name for server communication" area.
3. Enter the **network password**.
4. Select **Settings** ( ), and select **Save** from the **File** menu to save the changes.
5. Restart the services (see "Qognify ServiceManager" on page 474).

Management database (MaxDB)

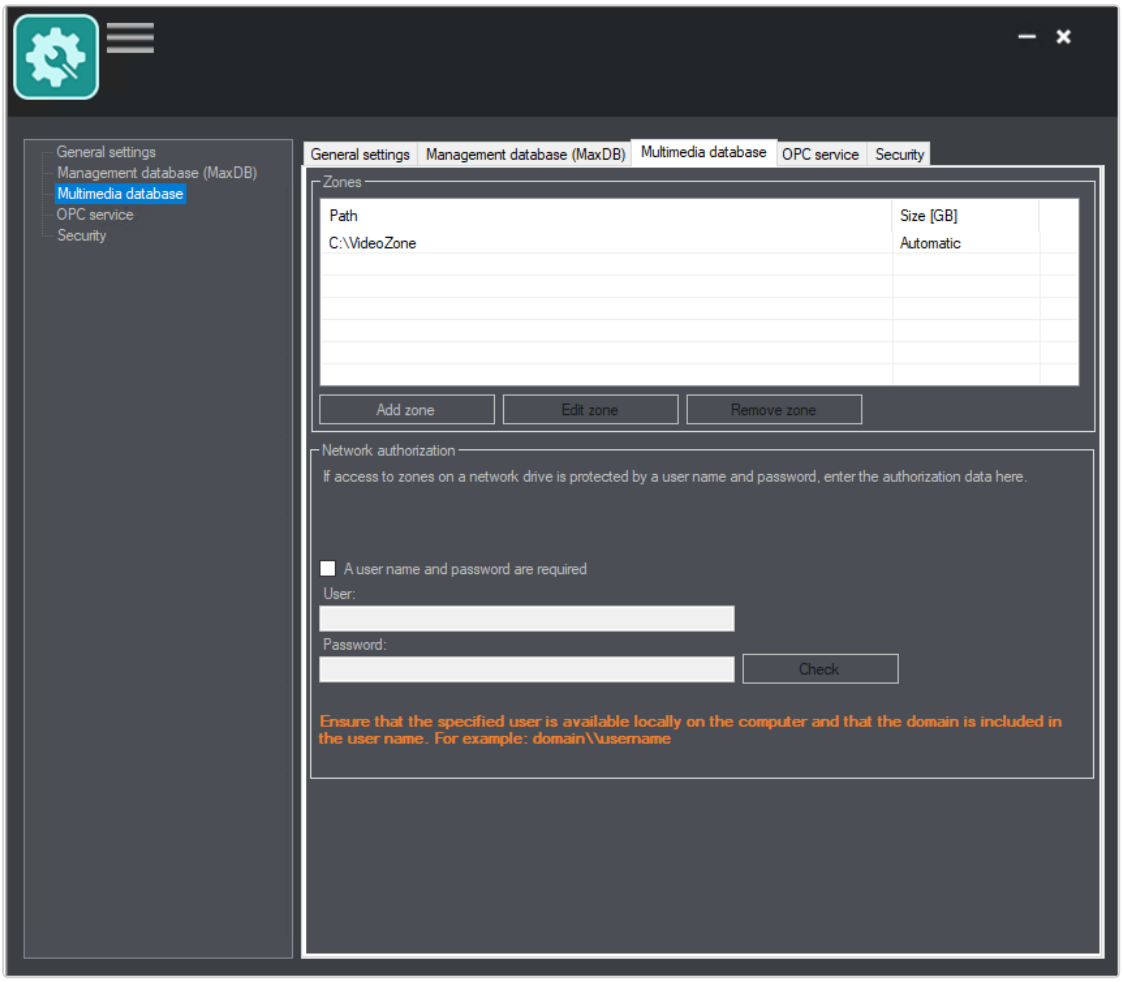


Fig. 264: Management database (MaxDB)

Backup and restore

For a secure backup (AES-256 encrypted) in the file format *.7z, a password is required. The password is also required for restoring backups in the file format *.7z (see "Configuring the backup" on page 432).

1. To create a backup of the management database, click **Backup**. The database is backed up in the "\Qognify\sapdb\backup" folder.
2. Enter the **user name** and **password**.
3. Add a (different) **Second password**, if required.
4. Click **OK**. The management database is backed up. This may take some time depending on the size of the database.

Do not interrupt the process.

5. For restoring a backup, click **Restore** and enter the password.

Increase storage space (and volume)

If more storage space has to be made available to the administration database (MaxDB) because, for example, the event data is to remain available for an extended period, an additional volume can be added to the MaxDB. The default size of the MaxDB is 4 GB.
A maximum of four volumes can be added to the MaxDB.

> **This extension has no influence on the actual multimedia database (MaxDB).**

1. Enter the **size [MB]** of the additional storage space for the expansion of the MaxDB (minimum: 512 MB, maximum: 8000 MB).
2. Click **Add new volume**. The additional storage space is available immediately under DISK000X in the MaxDB installation folder.
3. Click **Refresh** (↺) for an estimate of how long (in days) the space in the MaxDB will last at the current alarm rate. A reliable estimate can only be made if the system is running under normal load with reference to the alarm occurrence.

Cache

If a large number of events occurs with resulting high loading times, the MaxDB cache size can be increased.
However, this value should be selected carefully. Enlarging the cache is not useful if the computer does not actually have enough free RAM available.
The current cache size of the RAM reserved for the MaxDB is displayed. The actual size of the MaxDB is shown under “Current capacity utilization of the management database”.

> **The cache size of the MaxDB is an extremely system-critical parameter that should not be changed unless there are good reasons for it. The throughput is optimal if the complete database is kept in the cache.**

1. Enter a value in MB for the desired **size**, and click **Adjust cache size**.

Multimedia database

The multimedia database tab is used for maintenance and editing of zones of the multimedia database. The zones are paths in which the multimedia database stores its image data. Both local drives and network drives can be addressed. The specified zone size is not reserved immediately but only used as required.

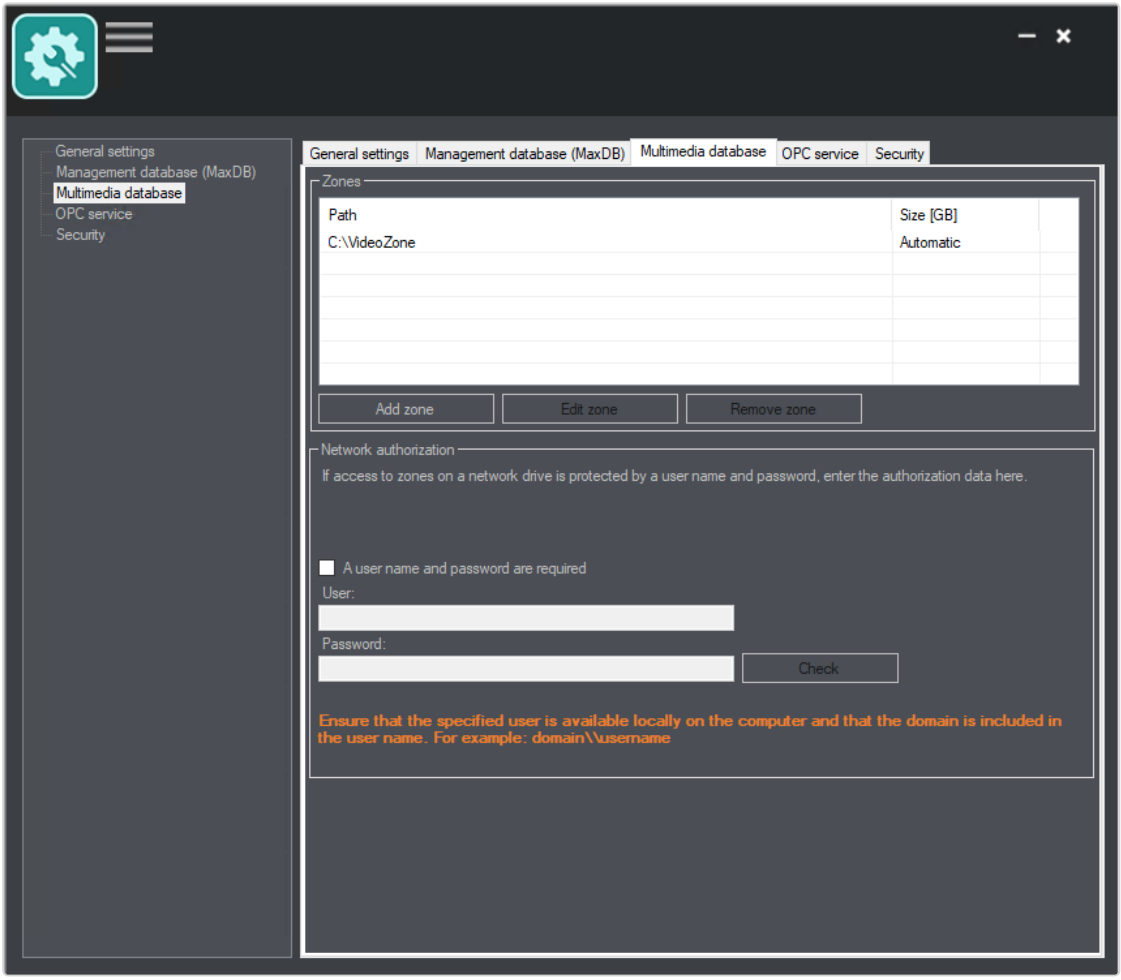


Fig. 265: Multimedia database

About zones

Zones specify the maximum storage depth of the multimedia database and thus of the software. By default, the software does not set any limits on the zone of the multimedia database. The default zone is placed in the following folder in a new installation: "Qognify VMS installation folder\re\md\mds\data\.

However, we recommend replacing it with a zone on a dedicated partition.

If the volume of the existing zone is not sufficient, another zone can be added. A maximum of ten zones should be created. A larger number has a negative effect

on the performance of the multimedia database. It is also better to have a few large zones than a larger number of small zones.

If more storage space than is available on the zones or on the hard disk is assigned to the connected cameras, the database stops recording.

> **Do not use an external hard disk drive connected by USB or FireWire as a multimedia database zone, because this will have a very negative effect on the performance. The multimedia database should be placed on another hard disk or a RAID system to ensure satisfactory performance.**

Add a zone

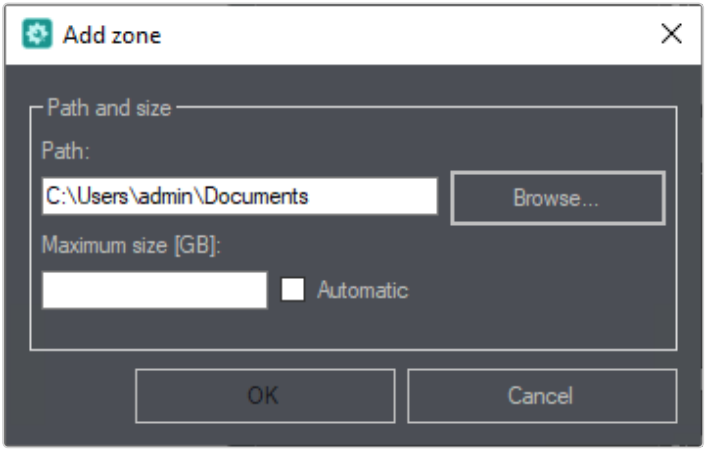


Fig. 266: Add zone

1. Create a folder on a dedicated partition as a zone to store the image data.
   The cluster size should be 64 KB.
2. Click **Add zone**.
3. Enter or **Browse** the **path** to the zone directory.
4. Enter the maximum size (in GB).
5. Enable **Automatic** to use all the physical space in the partition.

   > **It is recommended to use Automatic, so the multimedia database efficiently manages the available disk space. If a fixed maximum size has to be defined, make sure that no more than 95% of the physical space on a partition is used, because any more will adversely affect the performance of the operating system.**

6. Click **OK** to confirm.

Add a zone on network drive

1. Create a folder on a server in the network to store the image data.
2. Click **Add zone**.
3. Enter the **UNC path** and the **maximum size** (in GB) (e.g. "\\192.168.2.20\Path\To\Accept").
4. Activate **Unlimited** to use all the physical space in the partition.
5. Activate **A user name and password are required** in the network authorization area, and enter the authorization data of the network drive, i.e. the server login information.
6. Enter the **User name** and **Password**. Note that the user must also be available locally on the computer and the domain is also required, e.g.: DOMAIN\firstname.lastname
7. Click **Test** to check the availability and authorization on the network drive.

Edit a zone

1. Select the desired multimedia database in the zones field.
2. Click **Edit zone** to change the path and/or size. We recommend using no more than 95% of the physical space on a partition, because any more will adversely affect the performance of the operating system.
3. Click **OK** to confirm.

Remove a zone

1. Select the desired multimedia database in the zones field.
2. Click **Remove zone**.

> **The image data in the deleted zone are no longer available in Qognify VMS, but are not automatically deleted.**

OPC Service

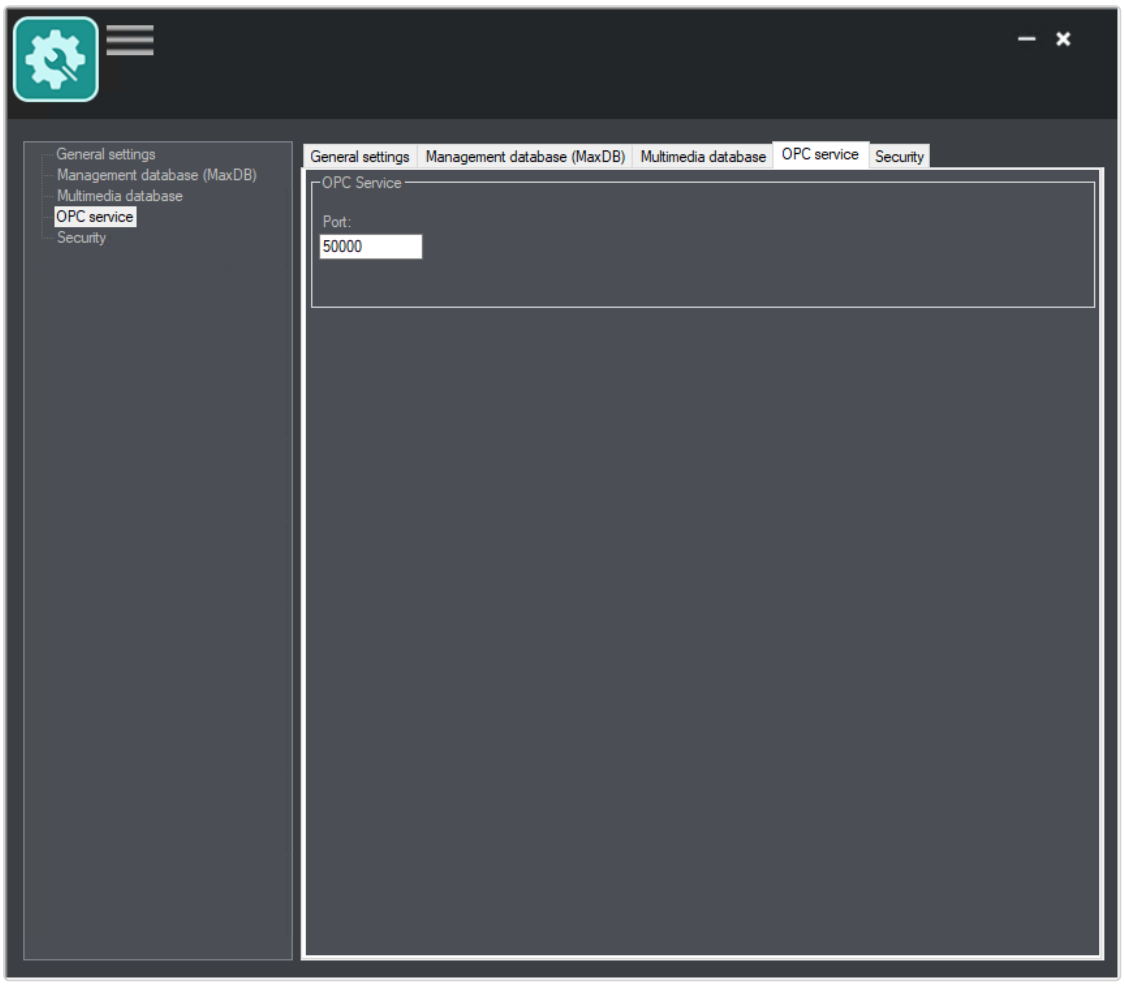


Fig. 267: OPC Service

The OPC service supports defines the port number for the communication between Qognify VMS and the software service.

> **The OPC service is optional. The setting is only available when the UpdateAgent is activated.**

1. Enter the port number.

Security

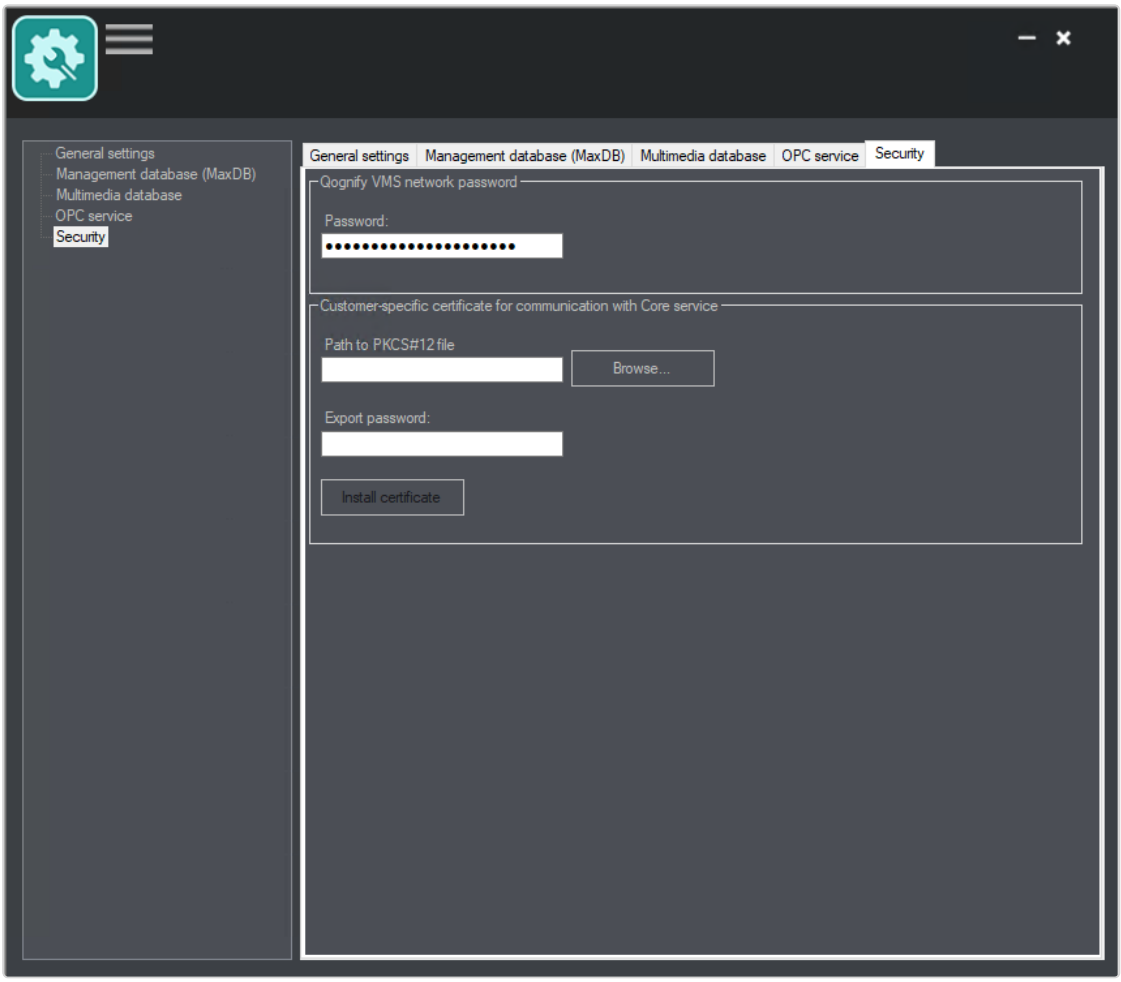


Fig. 268: Security

The security settings support defining a network password and customer-specific certificate for the communication between Qognify VMS and the server.

> **To use the network password, the password on the computer with the core service must be replaced.**

1. Enter a network password. The password is used for the communication between the Qognify VMS services. **For security reasons, adhere to the required safety standards of the company.**
2. Create or download a PKCS#12-encrypted certificate file.
3. Select “Browse” and navigate to the file.
4. Enter the “Qognify VMS network password” and select **Install certificate**.
5. Restart the Core Service (see "Starting and stopping the services" on page 475).
6. Repeat the certificate installation for every core service using the same certificate.

7. Install the corresponding public key certificate on every computer attached to the core services into the following directory:
   - %SeeTecINSTALL%\conf\
8. Rename the file to “cayugaCore.crt”.

Qognify ServiceManager

The ServiceManager is used for starting and stopping services. The following functions are available in the ServiceManager:

- Restart all services
- Stop all services
- Start all services

The ServiceManager is automatically installed when a server service is installed.
To start the ServiceManager automatically at login, add "-autostart" as the command line parameter (see "Command line parameters" on page 497).

1. Start the ServiceManager in the installation folder or the Windows Start menu.

Switching the display language

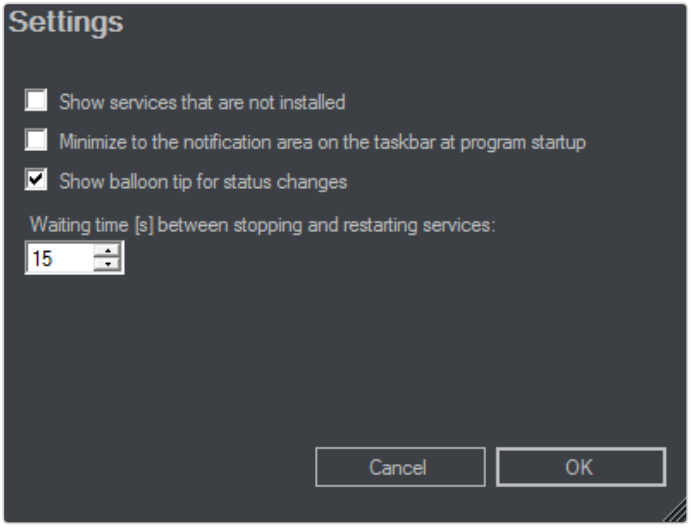
1. Exit the ServiceManager.
2. Start the command prompt as the administrator and enter "VMS_ServiceManager.exe -l:<code_for_the_display_language>".

   > *Example For English: "VMS_ServiceManager.exe -l:en-us", or for French: "VMS_ServiceManager.exe -l:fr-fr"*

3. Start the ServiceManager.

Editing the settings

1. Select **Settings** (☰).



2. Activate **Show services that are not installed** to show all available services in the list. By default, services not installed are not displayed.
3. Activate **Minimize to the notification area on the taskbar at program startup** for faster access to the ServiceManager.
4. Activate **Show balloon tip for status changes** to see an immediate notification on the screen in the event of changes to the services.
5. Define the **Wait time between stopping and restarting services** (default 15 seconds). Increase the interval to allow the services to start and terminate correctly with large installations.
6. Click **OK** to confirm.

Starting and stopping the services

The state of the services is displayed and color-coded:

- Green = service is started
- Red = service is stopped
- Yellow = service is started or stopped
- Black = service is not installed

1. Click **Restart all services** to stop all services regardless of the state of the services and to restart them.
2. Click **Stop all services** to stop all services regardless of the state of the services.
3. Click **Start all services** to start all services regardless of the state of the services.

Optionally, specific service are started, stopped, or restarted by clicking the service with the right mouse button.

Qognify VMS VA Administration Tool

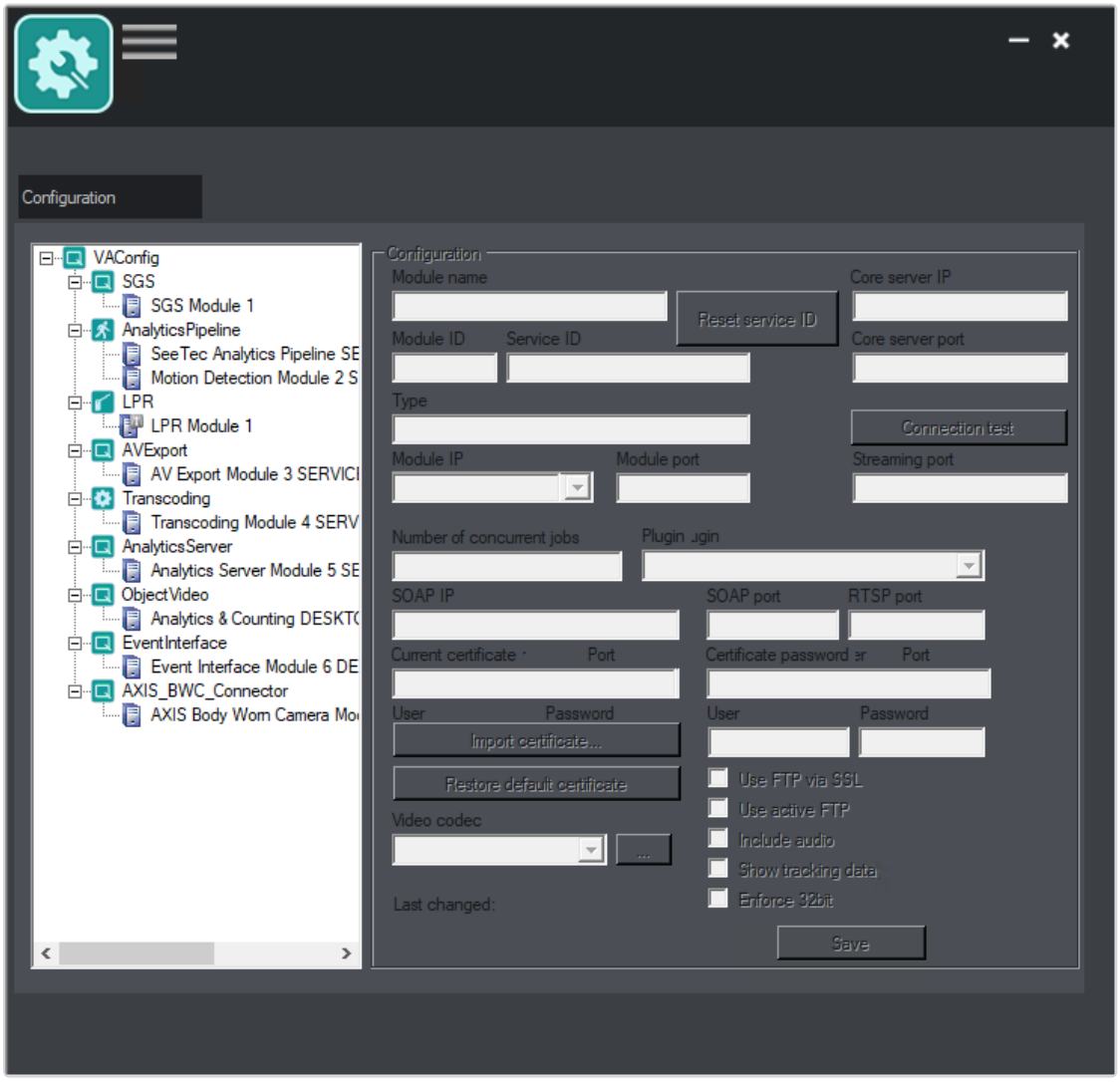


Fig. 269: The Qognify VMS VA Administration Tool

With the Qognify VMS VA Administration Tool the following modules (services) can be managed:

- **License Plate Recognition (LPR)**, see "Adding an LPR module" on the next page
- **Analytics Server**, see "Adding an Analytics Server module" on page 479
- **Transcoding engine**, see "Adding a Transcoding engine module" on page 481
- **Gateway service**, see "Adding a Gateway Service module (SGS)" on page 482
- **Analytics Interface**, see "Adding an Analytics Interface module" on page 483
- **Server based motion detection**, see "Adding a server-based motion detection module" on page 485
- **Generic Access Control**, see "Adding a generic Access Control module" on page 487
- **Event Interface**, see "Adding a Qognify Event Interface module" on page 490
- **AV Export Module**, see "Configuring the AV export module" on page 488

The Qognify VMS VA administration tool is started from the Windows® Start menu or from the Qognify VMS installation directory.

Switching the display language

1. Exit the Qognify VA administration tool.
2. Start the command prompt as the administrator and enter "VMS_VA_ConfigurationTool.exe -l:<code_for_the_display_language>".

   > *Example For English: "VMS_VA_ConfigurationTool.exe" -l:en-gb or "VMS_VA_ConfigurationTool.exe" -l:en-us*
   > *or for French: "VMS_VA_ConfigurationTool.exe" -l:fr-fr*

3. Start the Qognify VA administration tool.

Creating a new configuration file

1. Click **Settings** (1), and select **Create new configuration file** from the **File** menu.

Adding an LPR module

The Qognify LPR-Module is an interface to connect to a **L**icense **P**late **R**ecognition engine by ARH.

> **You may only operate one LPR-Module per server at the same time. You may however install multiple LPR modules on multiple servers if only one server is activated.**

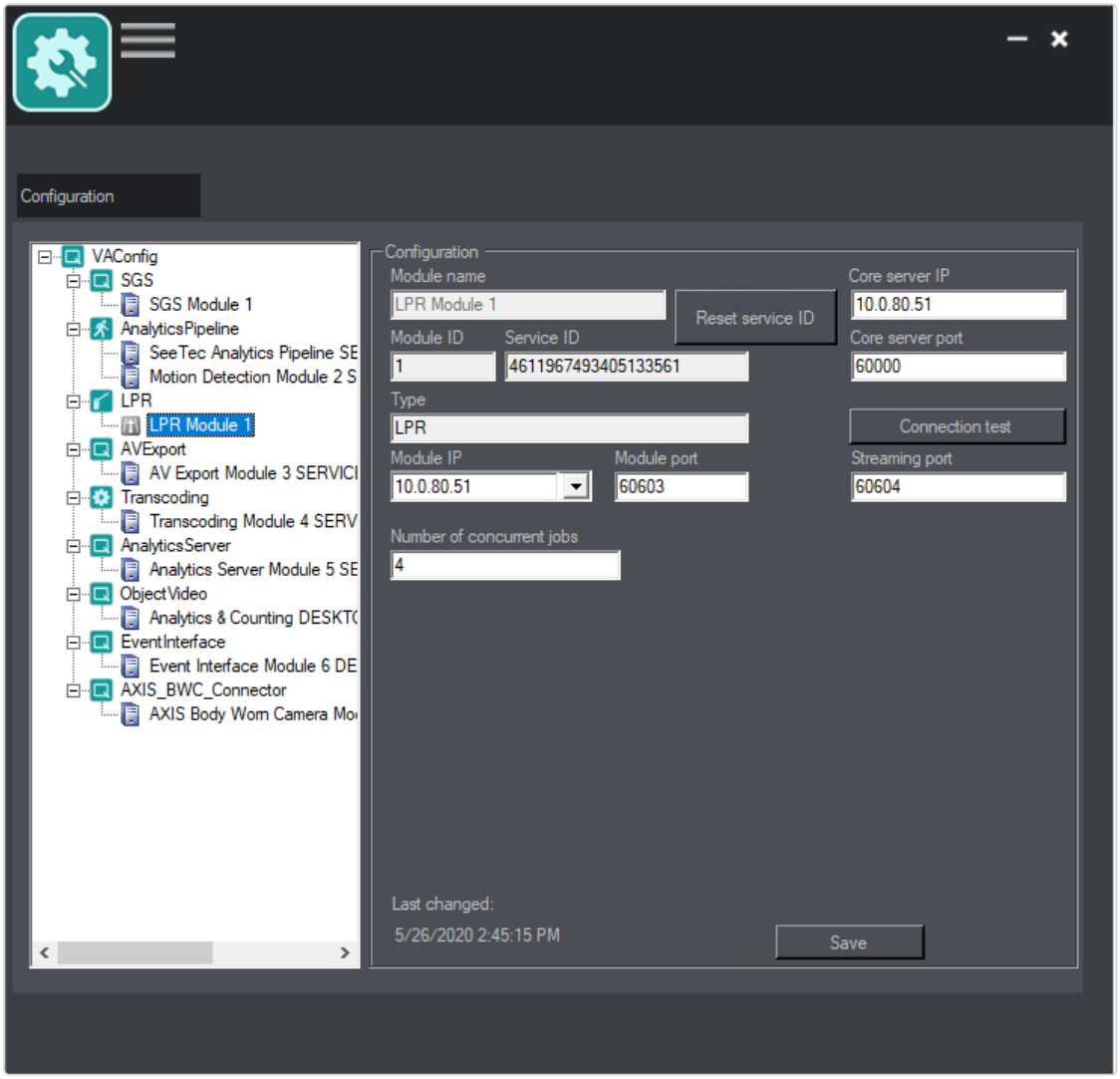


Fig. 270: Adding an LPR module

1. On top of the module tree right-click on **VAConfig**.
2. Select **Add new module**.
3. Select **License plate recognition**. A new entry is created.
4. Change the **Module name**.
5. Enter the **IP address** of the core server.

> **Do not use localhost or 127.0.0.1 as the entry as other services must communicate via these IP addresses.**

The service ID changes after the first connection to the Qognify server.

Do not reset the service ID without talking to Qognify Support first.

6. Click **Connection test** to check the connection between the module and the main server. If the module does not connect, check and configure the network and the firewall settings.
7. Select the **Module IP**.
8. Enter the **Module port** used by the LPR module.
9. Specify the **number of concurrent jobs** that are to be transferred. This number should exceed the number of lanes to be monitored.

   > *Example For each lane, more than one vehicle may be waiting. Hence, multiple concurrent jobs may be present per lane. The jobs will then be set on a "waiting list" where the queue is processed one after the other. Do not change to 32-bit mode without talking to Qognify support first (see "Support" on page 13).*

Do not change to 32-bit mode without talking to Support first.

10. Click **Save**.
11. Restart the services with the service manager (see "Qognify ServiceManager" on page 474) or add further modules.

    > **Further configuration steps are required in configuration mode (see "Configuring the LPR module" on page 413).**

Adding an Analytics Server module

The Qognify Analytics Server Module is required for **3D Analytics** and **2D intelligent Motion Detection**. For more details see "Qognify Analytics Server" on page 309.

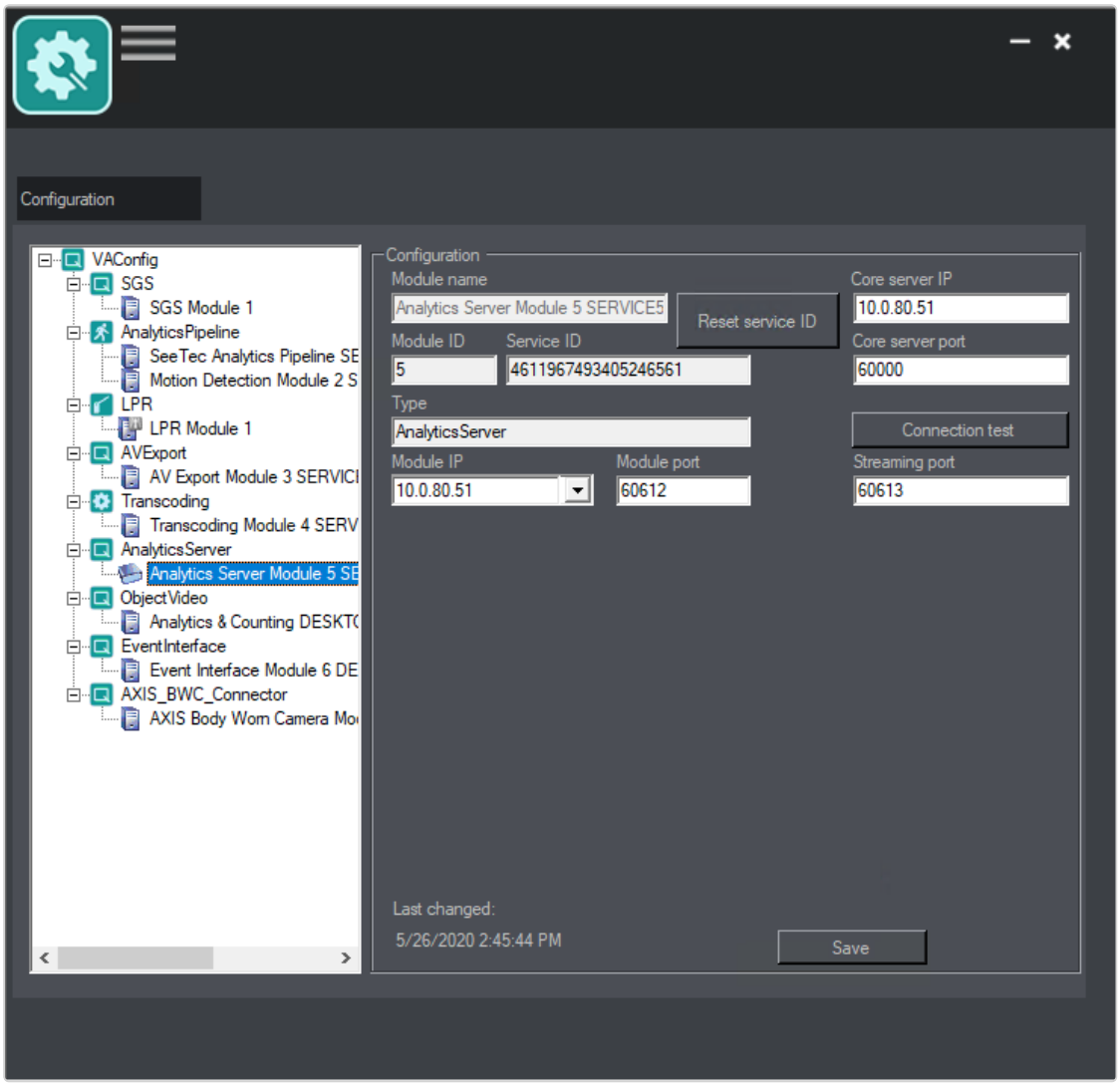


Fig. 271: Adding an Analytics Server module

1. Right-click the configuration file in the column on the left and select **Analytics Server** from the **Add new module** context menu. A new entry is created in the configuration file in the menu tree (see "Configuring the transcoding module" on page 420).
2. Change the module **name**.
3. Enter the **IP address** of the core server.

   Do not use "localhost" or "127.0.0.1" as other services must communicate via these IP addresses. The service ID changes after the first connection to the Qognify server. Do not reset the service ID without talking to Qognify support first (see "Support" on page 13).

4. Click **Connection test** to check the connection between the module and the main server.

   If the module does not connect, check and configure the network and the firewall settings.

5. Select the module IP.
6. Enter the module **port** used by the Analytics Server module.
7. Click **Save**.
8. Add further modules or restart the services (see "Qognify ServiceManager" on page 474).

Adding a Transcoding engine module

1. Right-click the configuration file in the column on the left and choose **Transcoding engine** from the **Add new module** context menu. A new item is created under the configuration file in the menu tree (see "Configuring the transcoding module" on page 420).
2. Change the **module name**.
3. Enter the **IP address** of the core server.

   Do not use localhost or 127.0.0.1 as the entry as other services must communicate via these IP addresses.

The service ID changes after the first connection to the Qognify server.

Do not reset the service ID without talking to Qognify Support first (see "Support" on page 13).

4. Click **Connection test** to check the connection between the module and the main server. If the module does not connect, check and configure the network and the firewall settings.
5. Select the **module IP**.
6. Enter the **module port** used by the transcoding module.
7. Select **Enforce 32-bit** if the devices are not 64-bit capable. This setting only applies to devices that have not yet been released for 64-bit.

Do not change to 32-bit mode without talking to Qognify Support first (see "Support" on page 13).

8. Click **Save**.

9. Restart the services (see "Qognify ServiceManager" on page 474), or add further modules.

Adding a Gateway Service module (SGS)

The Qognify Gateway Service module network based interface which provides certain functionality to services like Qognify WebClient or Mobile client or SDK.

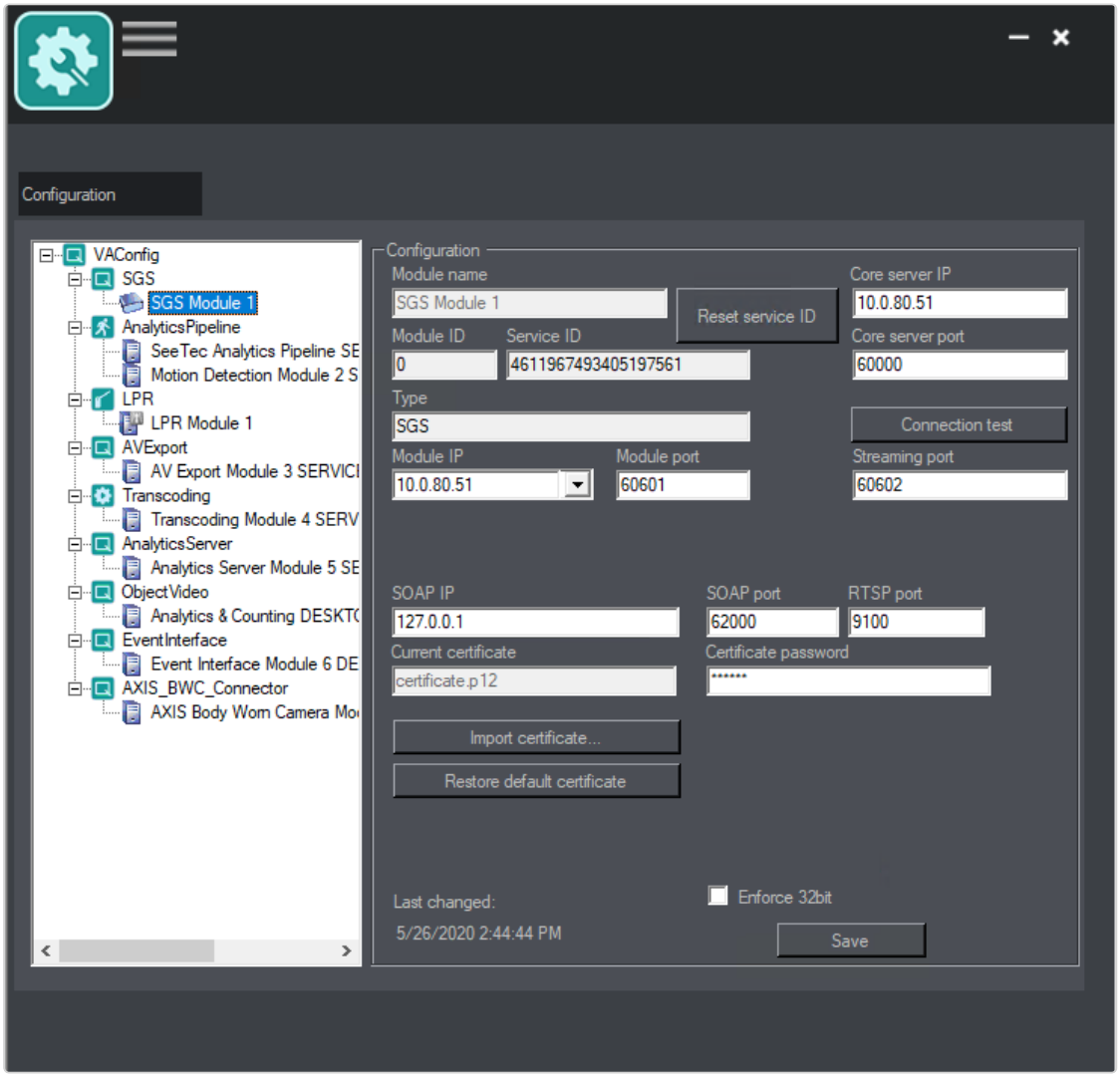


Fig. 272: Adding a Gateway Service module

1. Right-click in the column on the left, and choose **Gateway Service** from the **Add new module** context menu. A new entry is created under the configuration file in the menu tree (see "Server" on page 402).
2. Change the **module name**.
3. Enter the **IP address** of the core server.

Do not use localhost or 127.0.0.1 as the entry as other services must communicate via these IP addresses.

The service ID changes after the first connection to the Qognify server.

Do not reset the service ID without talking to Qognify Support first.

4. Click **Connection test** to check the connection between the module and the main server. If the module does not connect, check and configure the network and the firewall settings.
5. Select the **module IP**.
6. Enter the **module port** used by the SGS module.
7. Enter the **SOAP IP** and the **SOAP port**.
8. If accessing the network from the intranet (internal access), enter the local IP of the server.
9. If accessing the network from the internet (external access), enter the public IP of the router or firewall. Additionally, transparent port forwarding must be activated at the router or firewall.
10. Optionally, import your own certificate. Make sure that the certificate is a PKCS#12 (X509) certificate that includes the private key.
11. Select **Enforce 32-bit** if the devices are not 64-bit capable. This setting only applies to devices that have not yet been released for 64-bit.

Do not change to 32-bit mode without talking to Qognify Support first.

12. Click **Save**.
13. Restart the services (see "Qognify ServiceManager" on page 474) or add further modules.

> **Further configuration steps are required in configuration mode (see "Configuring the Gateway-Service (SGS) module" on page 419).**

Adding an Analytics Interface module

With the standardized Qognify Analytics Interface (SAI), server-based or camera-based analysis applications from other manufacturers can be integrated into the Qognify VMS environment.
SAI-Plugins are available from several manufacturers, e.g. Axis, Forlan, NumberOk, etc.

> **The available SAI-Plugins are listed on and can be downloaded from the Qognify PartnerWeb.**

Note that third-party (non-certified) plug-ins must first be tested and certified by Qognify. Non-certified plug-ins will be automatically deactivated after 12 hours.

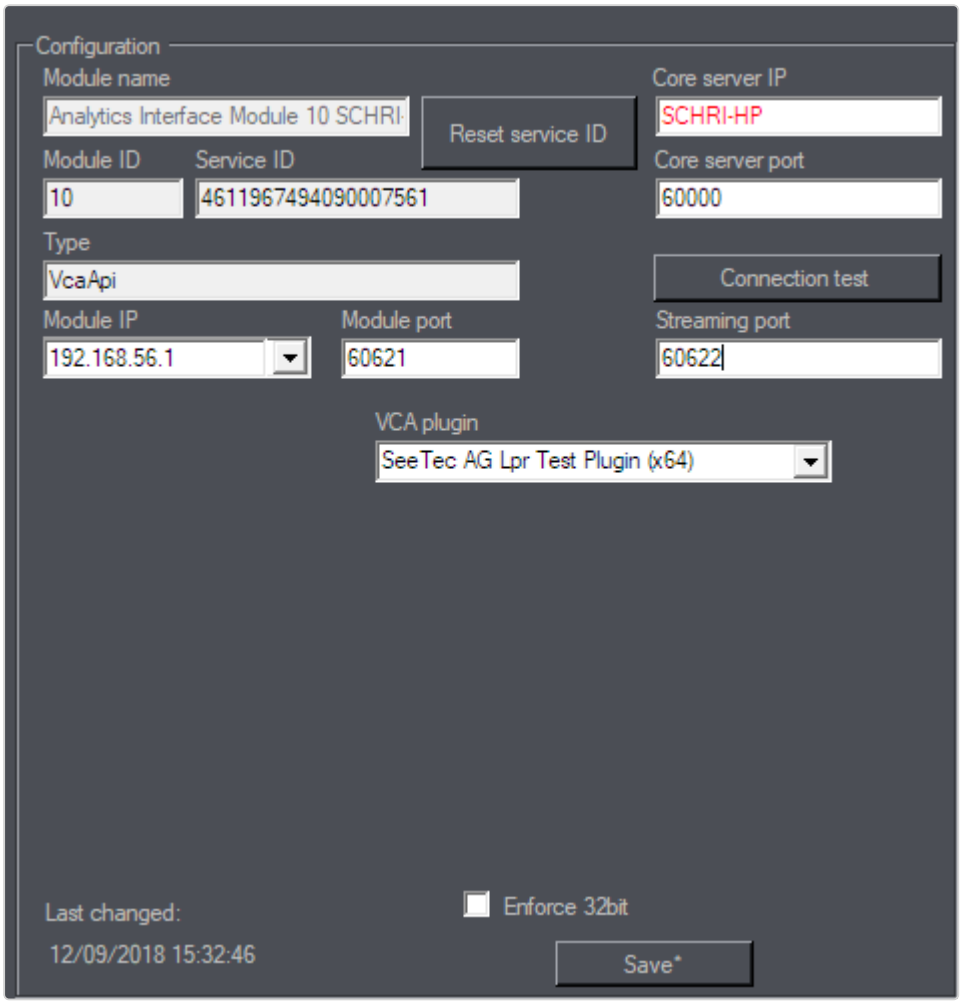


Fig. 273: Adding an Analytics Interface module

1. Copy the VCA plug-in DLL files into the Qognify plug-in directory (C:\Program Files\Qognify\VersatileApplications64\VcaPlugin\).
2. Restart the VA-services with the service manager (see"Qognify ServiceManager" on page 474).
3. On top of the module tree right-click on **VAConfig**. The **Add new module** menu appears
4. Click on **Analytics interface**. A new entry is created.
5. Change the **Module name**.
6. Enter the **IP address** of the core server.

Do not use localhost or 127.0.0.1 as the entry as other services must communicate via these IP addresses.

The service ID changes after the first connection to the Qognify core server.

Do not reset the service ID without talking to Qognify Support first.

7. Click **Connection test** to check the connection between the module and the main server. If the module does not connect, check and configure the network and the firewall settings.
8. Select the **Module IP**.
9. Enter the **Module port** used by the VCA module.
10. Enter the **Streaming port** used by the VCA module.
11. Select the **VCA plug-in**. The Qognify supplied plug-in must have been installed in the plug-in folder before (C:\Program Files\Qognify\plug-ins).
12. Select **Enforce 32-bit** if the devices are not 64-bit capable. This setting only applies to devices that have not yet been released for 64-bit.

Do not change to 32-bit mode without talking to Qognify Support first.

13. Click **Save**.
14. Restart the services (see "Qognify ServiceManager" on page 474) or add further modules.

Removing a SAI channel for a CogVis Forlan camera requires removing the channel on the manufacturer's system.

Adding a server-based motion detection module

Two server based motion detection modules are preconfigured by default. They are needed for the server side functions (see "Server side functions" on page 253) like motion detection, reference image comparison, and tampering detection. Further configuration is available in the server settings of the configuration mode (see "Server" on page 402).

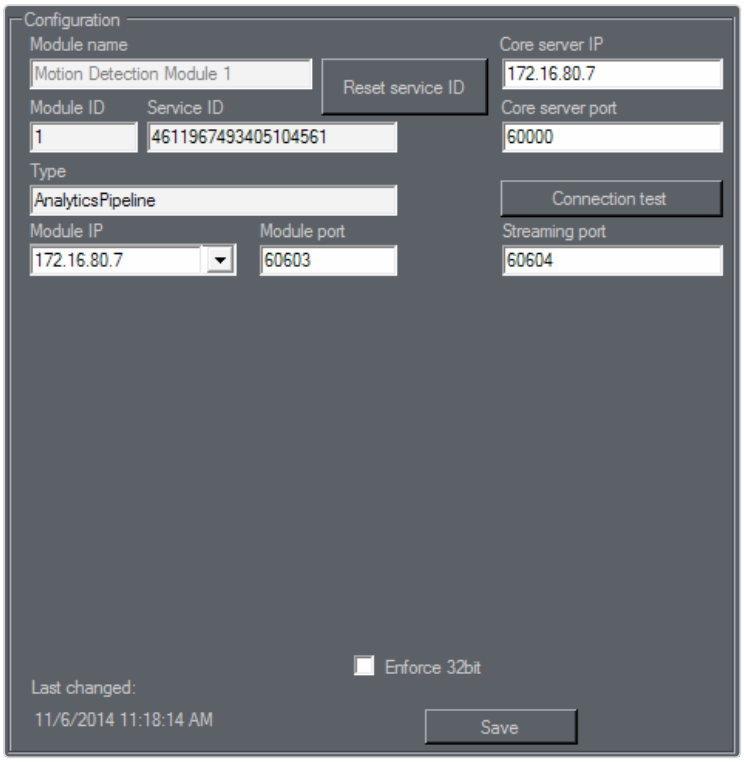


Fig. 274: Adding a server-based motion detection module

1. Right-click the configuration file in the column on the left and choose **Server-based motion detection** from the **Add new module** context menu. A new entry is created under the configuration file in the menu tree (see "Server" on page 402).
2. Change the **module name**.
3. Enter the **IP address** of the core server.

> **Do not use localhost or 127.0.0.1 as the entry as other services must communicate via these IP addresses.**

The service ID changes on the first connection to the Qognify server.

Do not reset the service ID without talking to Qognify support first.

4. Click **Connection test** to check the connection between the module and the main server. If the module does not connect, check and configure the network and the firewall settings.
5. Select the **module IP**.
6. Enter the **module port** used by the motion detection module.
7. Select **Enforce 32-bit** if the devices are not 64-bit capable. This setting only applies to devices that have not yet been released for 64-bit.

Do not change to 32-bit mode without talking to Qognify support first.

8. Click **Save**.

9. Restart the services (see "Qognify ServiceManager" on page 474) or add further modules.

Adding a generic Access Control module

With a generic Access control module the Qognify system is connected to third-party access control devices.

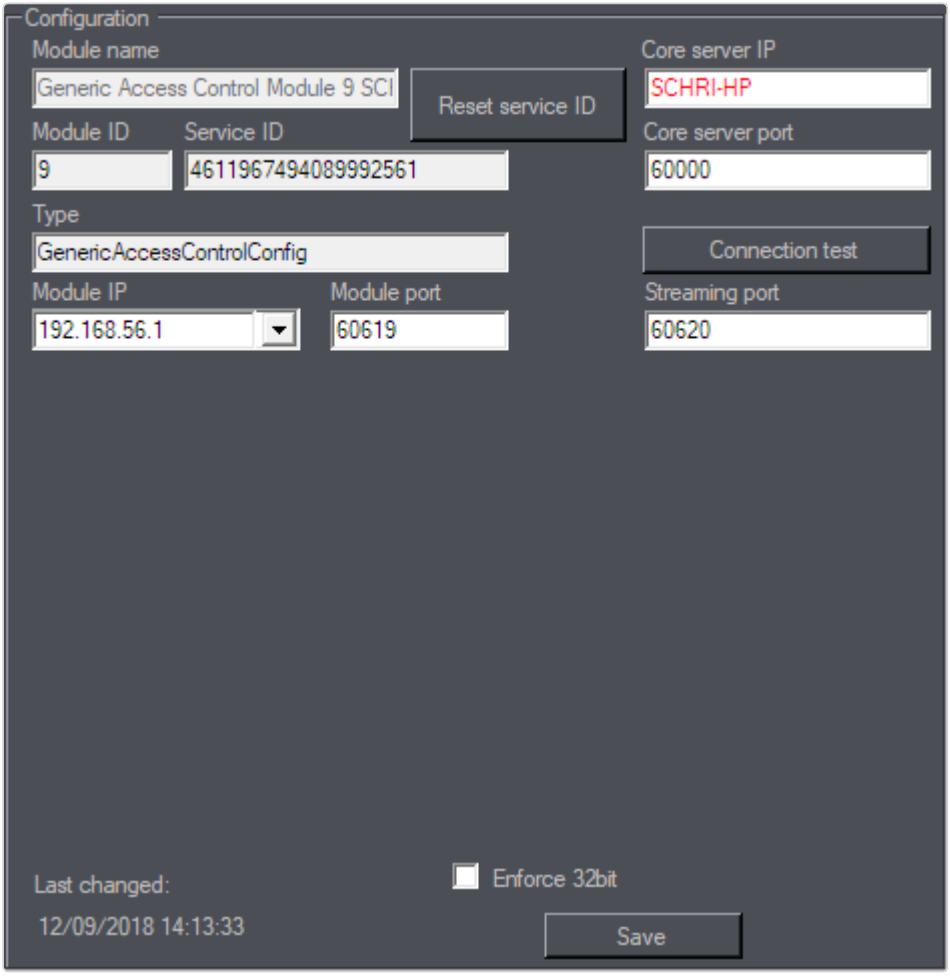


Fig. 275: Generic access control module

1. Right-click the configuration file in the column on the left and choose **Generic Access Control** from the **Add new module context menu**. A new entry is created under the configuration file in the menu tree (see "Configuring a generic access control module" on page 424).
2. Change the **module name**.
3. Enter the **IP address** of the core server.

Do not use localhost or 127.0.0.1 as the entry as other services must communicate via these IP addresses.

The service ID changes after the first connection to the server.

Do not reset the service ID without talking to Qognify support first.

4. Click **Connection test** to check the connection between the module and the main server. If the module does not connect, check and configure the network and the firewall settings.
5. Select the module IP.
6. Enter the **module port** used by the module.
7. Select **Enforce 32-bit** if the devices are not 64-bit capable. This setting only applies to devices that have not yet been released for 64-bit.

   Do not change to 32-bit mode without talking to Qognify support first.
8. Click **Save**.
9. Restart the services (see "Qognify ServiceManager" on page 474) or add further modules.

Configuring the AV export module

The AV export module is installed per default and cannot be deleted. It is required to transcode video recordings based on a video codec and transfer the results to a FTP server or to a SMTP server. Further settings are required in the camera configuration (see "Video Backup/Export" on page 252) or in the alarm configuration (see "Email and FTP" on page 372).

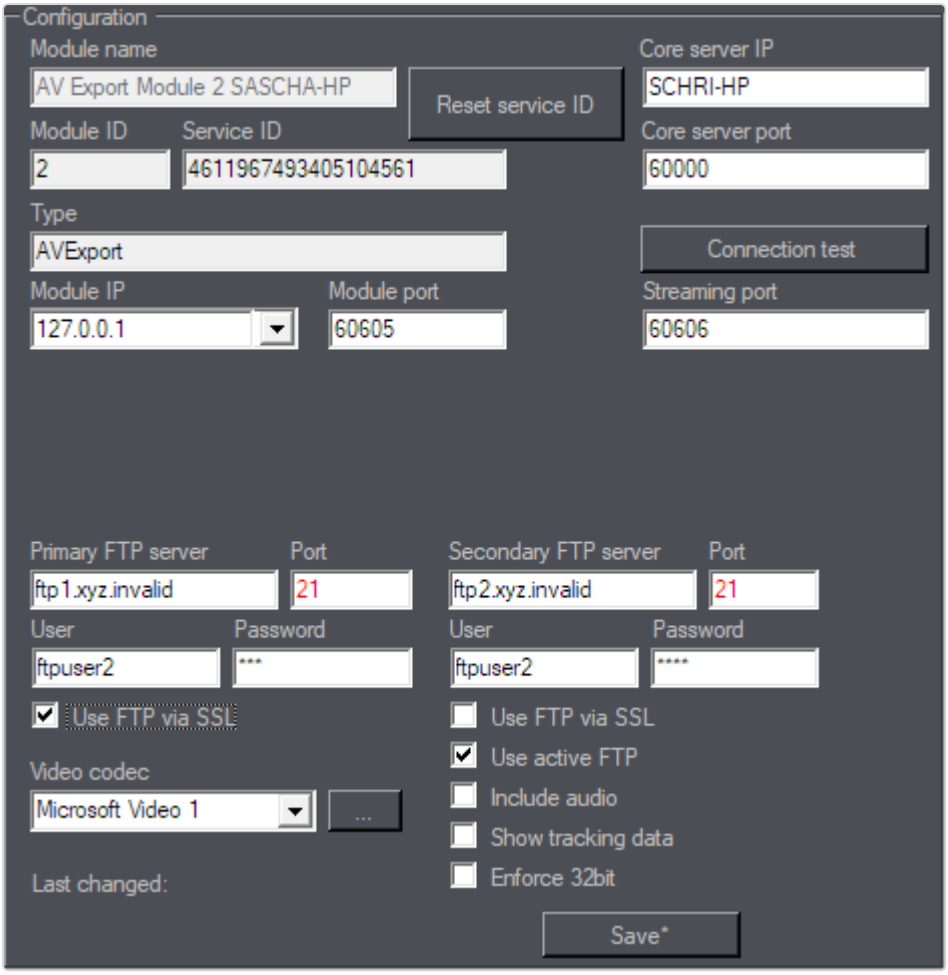


Fig. 276: Configuring the AV export module

1. Click on the **AV Export Module**.
2. Enter the **IP address** of the core server if it has changed.

> **Do not use localhost or 127.0.0.1 as the entry as other services must communicate via these IP addresses.**

The service ID changes on the first connection to the Qognify server.

Do not reset the service ID without talking to Qognify Support first.

3. Click **Connection test** to check the connection between the module and the main server. If the module does not connect, check and configure the network and the firewall settings.
4. Select the **Module IP**.
5. Enter the **Module port** used by the AV Export module.
6. Enter the **Streaming port** used by the AV Export module.
7. Enter the IP address and **Port** of the **Primary FTP Server** and if required for the **Secondary FTP Server**.
8. Enter the required **User** and **Password** to access the FTP Servers.

9. Check **Use FTP via SSL** for a secure connection with the FTP Servers.
10. Check **Use active FTP**. Otherwise passive FTP (default) is used.

> **When active FTP (also "active mode") is used, the client opens a random port and informs the server of this port and its own IP address using the PORT or EPRT command.**
> **In passive FTP (also called "passive mode"), the client sends a PASV or EPSV command and the server opens a port and transmits it together with the IP address to the client. This technique is used if the server cannot establish a connection to the client.**

11. Check **Include audio** to integrate recorded audio into the exported video.
12. Check **Show tracking data** to render tracking data from video analytics into the exported video.
13. Select **Enforce 32-bit** if the devices are not 64-bit capable. This setting only applies to devices that have not yet been released for 64-bit.

Do not change to 32-bit mode without talking to Qognify Support first.

14. Click **Save**.
15. Restart the services (see "Qognify ServiceManager" on page 474) or add further modules.

Adding a Qognify Event Interface module

The Qognify Event Interface (QEI) is an open interface to connect to third party safety systems, such as burglar alarm, fire panel, access control etc. The Qognify Event Interface is not limited to certain manufacturers or systems.
For a third-party developer it is possible to provide a plug-in for the interface. For details contact the Qognify Support (see "Support" on page 13).

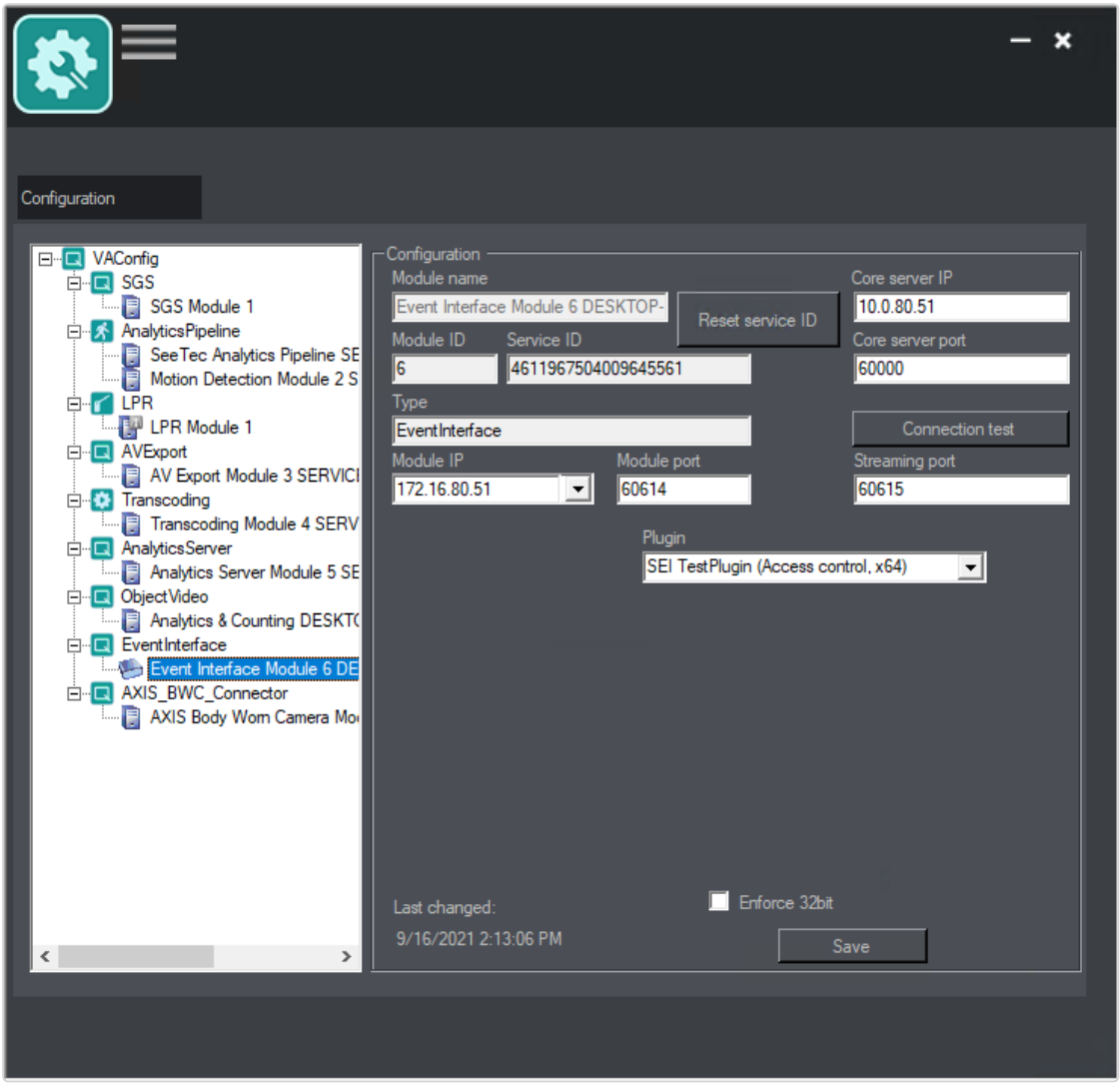


Fig. 277: Adding a Qognify Event Interface module (QEI)

1. Copy the QEI plug-in DLL files into the Qognify plug-in directory (C:\Program Files\Qognify\VersatileApplications64\EventPlugins\"plug-in name").
2. Restart the VA-services with the service manager (see "Qognify ServiceManager" on page 474).
3. On top of the module tree right-click on **VAConfig**. The **Add new module** menu appears.
4. Click on **Event Interface**. A new entry is created.
5. Change the **Module name**.
6. Enter the **IP address** of the core server.

> **Do not use localhost or 127.0.0.1 as the entry as other services must communicate via these IP addresses.**

The service ID changes after the first connection to the Qognify core server.

Do not reset the service ID without talking to support first.

7. Click **Connection test** to check the connection between the module and the main server. If the module does not connect, check and configure the network and the firewall settings.
8. Select the **Module IP**.
9. Enter the **Module port** used by the Qognify Event Interface module.
10. Enter **Streaming port** used by the Qognify Event Interface module.
11. Select the **QEI plug-in**.
12. Select **Enforce 32-bit** if the devices are not 64-bit capable. This setting only applies to devices that have not yet been released for 64-bit.

Do not change to 32-bit mode without talking to support first.

13. Click **Save**.
14. Restart the services with the service manager (see "Qognify ServiceManager" on page 474) or add further modules.

For further configuration see "Event Interfaces" on page 322.

Adding a body-worn camera connector module

The body-worn camera connector module is required for transferring the correct information between the controller and Qognify VMS.

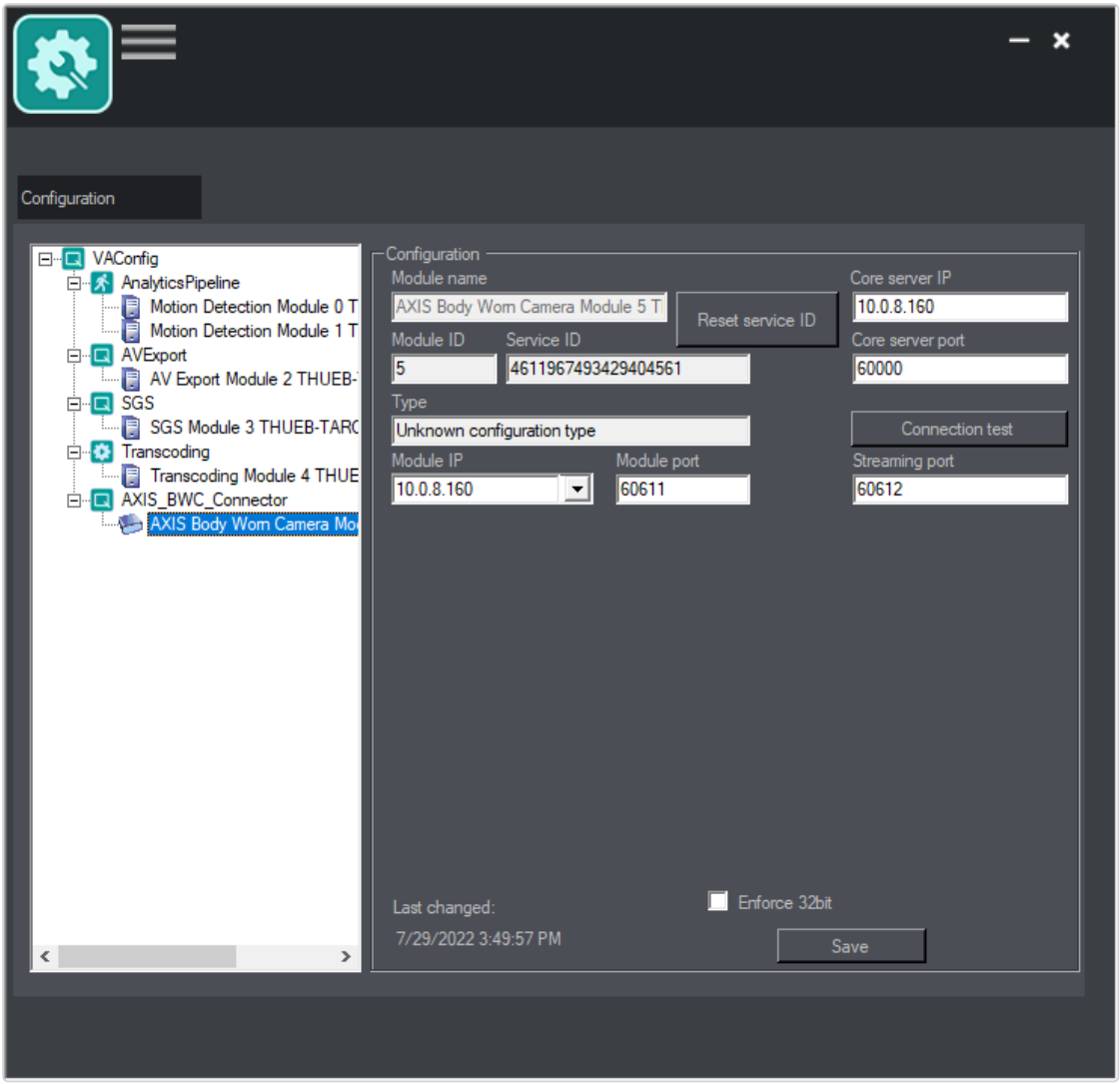


Fig. 278: Adding a AXIS body-worn camera connector module

1. On top of the module tree right-click on **VAConfig**.
2. Select **Add new module** in the context menu.
3. Select **AXIS Body Worn Camera Connector** in the context menu. A new entry is created.
4. If necessary, enter the **IP address** of the core server.

> **Do not use localhost or 127.0.0.1 as the entry as other services must communicate via these IP addresses.**

The service ID changes after the first connection to the Qognify core server.

Do not reset the service ID without talking to Support first.

5. Click **Connection test** to check the connection between the module and the main server. If the module does not connect, check and configure the network and the firewall settings.
6. Select the **Module IP**.

7. Enter the **Module port**.
8. Enter **Streaming port**.
9. Select **Enforce 32-bit** if the devices are not 64-bit capable. This setting only applies to devices that have not yet been released for 64-bit.

Do not change to 32-bit mode without talking to Support first.

10. Click **Save**.
11. Restart the services with the service manager (see "Qognify ServiceManager" on page 474) or add further modules.

For further configuration of the body-worn cameras, see "The AXIS body-worn camera controller" on page 220.

Exporting the configuration settings

The configured settings in Qognify VMS can be exported as *.xlsx file, including the camera settings, the user and group settings, and the alarm settings.

1. Navigate to the folder “tools/Configuration export” in the Qognify VMS installation folder.
2. Start “VMS_ConfigurationExport.exe”.

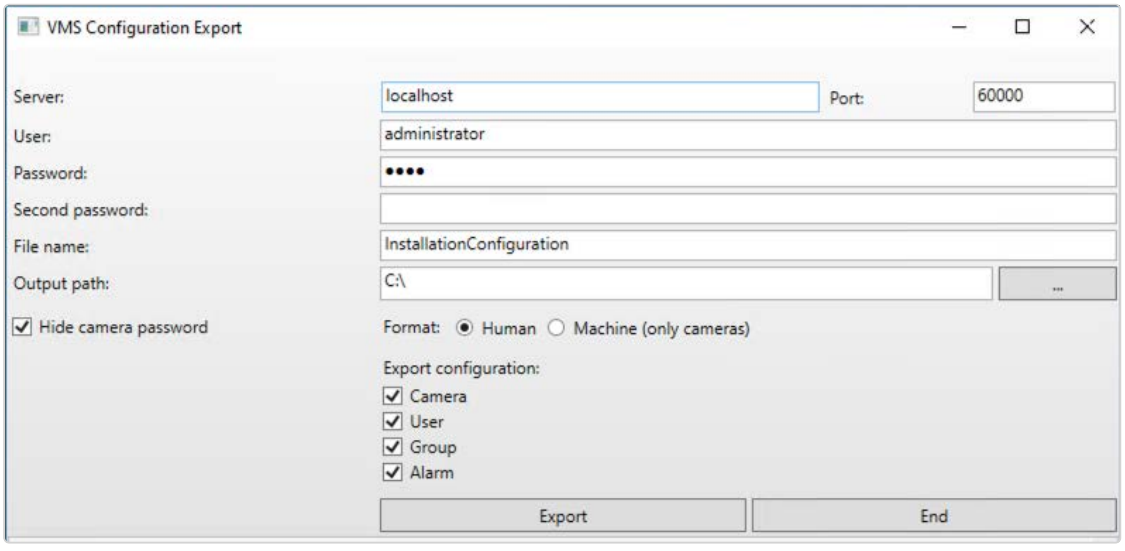


Fig. 279: Exporting the configuration settings

3. Define the IP of the **Server** where Qognify VMS is hosted. Alternatively, enter “localhost” for a local installation.
4. Specify the **Port** number (default: 60000).

5. Enter **User** name and **Password** for the administrator that is configured in the Qognify VMS settings (see "Login" on page 55)
6. If required, provide the second password.
7. Enter the **File name** for the exported data and select the file path to the output folder.
8. To prevent the camera passwords from being displayed in the output file, enable **Hide camera password**.
9. If the output file should be comprehensible to a human operator as a legible file, select **Human** and activate the settings that are included in the export.
10. If the output file should only be comprehensible to the computer, select **Machine**.

    Only the camera settings will be exported.

11. Enable the settings that will be exported.
12. Click **Export**. The export progress is displayed.
13. Quit the application when finished.
14. Open the exported file with an appropriate spreadsheet application.

13

Command line parameters

Overview

Command line parameters	Application	Meaning
alarmid:<AlarmEventID>	AlarmWatchdog	Open the alarm event with the specified ID
camerano:<CameraID>	■ Qognify VMS native client ■ Qognify Viewer	Open the camera with the specified ID
config:<directory>		set the path for the client configuration
host:<IP/hostname>		IP address or name of the Qognify server
-l:<language> (only ServiceManager and VA		Change language: The client can be started in a dif-

Command line parameters	Application	Meaning
Administration Tool) lang:<language>		ferent language with this command line parameter. The following languages are supported: en-us (English), de-de (German), fr-fr (French), ru-ru (Russian), tr-tr (Turkish), nl-nl (Dutch), sv-sv (Swedish), da-da (Danish), no-no (Norwegian), it-it (Italian), es-es (Spanish), pl-pl (Polish), pt-pt (Portuguese), cs-cs (Czech), gr-gr (Greek), ja-JP (Japanese), ro-RO (Romanian), th-TH (Thai)
log:<directory>		set the path for the client log
nat:<true/false>		Login by means of NAT yes (true)/no (false)
nolayers		Start client without layers
nosecondinstancecheck		Suppresses warning on client start if another client instance is already running.
noserverip		If set, the label and the textbox of the login screen are invisible. The "Switch installation" item in the menu is not affected.
nosip		Start client with deactivated SIP protocol
pass:<password>		Password
pass2:<password>		Second password (if required)
port:<port>		Port for login, default: 60000
profile:<profile>		Profile (user or group profile)
user:<user name>		User name
viewer	Qognify VMS cli-	The Qognify VMS client starts dir-

Command line parameters	Application	Meaning
	ent	ectly in offline mode (Archive mode). Can be used together with the language settings command “lang”.

Procedure

1. Open the application shortcut in the folder "Start Menu > Programs".
2. Right-click the application icon and select **Properties**.
3. Navigate to the **Shortcut** tab, and add the required parameters to the text in the **Target** text box.
4. Add the required command line parameters to the properties of the client. The command line parameters are entered in the form <key>:<value>.

   > *Example To start the Qognify client in English at the server with the IP address 192.168.0.10, right-click the link and append the command line parameter "lang:en-us" at the end of the line.*
   > *The line is then displayed as follows (for a default installation path):*
   > `"C:\Program Files\Qognify\Qognify VMS\VersatileApplications64\VMS_VA_ConfigurationTool.exe" -l:de-DE`
   > ***Note that no spaces are allowed after the colons.***

5. Click **OK** to confirm and start the program. The client is started with the specified parameters.

14

Shortcut keys

The following keyboard shortcuts are available for users in the client to speed up function calls.

> **More shortcuts are available and configurable in the client configuration (see "Keyboard shortcuts" on page 79).**

Shortcut key	Meaning
CTRL+1	Switch to surveillance mode
CTRL+2	Switch to archive mode
CTRL+3	Switch to report mode
CTRL+4	Switch to configuration mode **(only possible as administrator)**
CTRL+5	Switch to LPR mode
CTRL-Y	Display statistics in video image in Surveillance and Archive mode
F10	Switch full-image mode on or off

Shortcut key	Meaning
F1	Show Qognify User's Guide
F2	Moves all windows to primary display (only when multiple displays are connected)
ESC	Hide all controls
+/-	When digital zoom is active, pressing + or - zooms in or out

15

Anywhere Viewer

The Anywhere Viewer can be used to access exported image data that are in the Qognify image format without connection to the database.

> **The Viewer displays recorded data only in Archive mode. All other modes are not accessible as they require database access.**

- The Viewer is automatically installed as a subset of the Qognify VMS client installation. It can also be installed separately in a user-defined installation (see "Custom installation" on page 41).
- The Viewer is exported to the export folder with any video data export.
- The Viewer manual is installed in the manual folder during installation.

When viewing files that are exported to the local hard drive of the client with the Viewer, any local installation of the Qognify VMS client must be quit to prevent conflicts.

1. Quit Qognify VMS if running as a normal client connected to a database.
2. Start the Viewer from within the export folder.

Switching the interface language

Without a Qognify VMS client installed on the local hard drive, the language can only be changed using command line parameters.

1. Exit the Qognify Viewer and start the Qognify VMS client.
2. Change the interface language in the **File** menu of the function bar in the Qognify VMS client (see "Changing the language" on page 79).
3. Exit the Qognify VMS client and start either the Qognify VMS client in Viewer mode or the Qognify Viewer.

Import and play recording

Import recording into the Viewer

1. Start the Qognify Viewer (see "Login" on page 55). The overview panel with the available recordings is displayed.
2. To add additional exported camera sequences, select **Add exported cameras** in the overview panel.
3. Optionally, navigate to the export folder of the recording and start the Qognify Viewer in the folder.
4. Navigate to the folder where the files are located.

5. Click **OK** to import the selected data into the viewer.

> **When opening a folder that contains multiple exported camera sequences (even in subfolders), all files will be imported.**

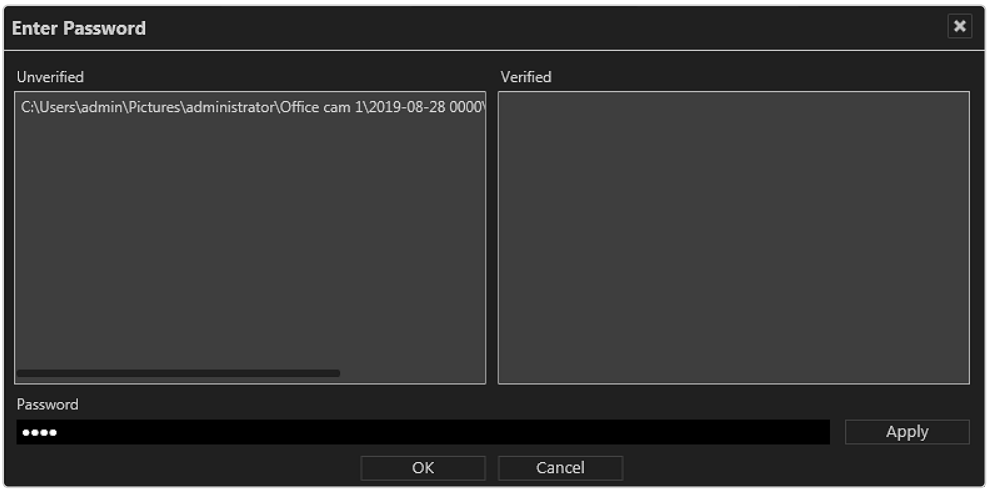


Fig. 280: File selection for importing into the Viewer in offline mode

6. Enter the **password** specified during export.
7. **Apply** the password and click **OK**. Any exported video sequence that matches the password moves to the "Verified" section on the right. You can enter and apply further passwords for additional video sequences.
8. Enter the **password** specified during export.
9. **Apply** the password and click **OK**. Any exported video sequence that matches the password moves to the "Verified" section on the right. You can enter and apply further passwords for additional video sequences.

> **Importing data into the Qognify Viewer may take some time.**

10. Click the exported camera that you wish to view. Alternatively, you can drag the desired camera to the previously occupied tile. If you imported multiple sequences from the same camera they will be shown as one camera in the tree. If you open this camera all the sequences of this camera can be found in the same timeline.

Play recording

Fig. 281: The Qognify Viewer controls

The Viewer allows limited control of the playback from one or multiple exported recordings in a single timeline. In Viewer Mode or in the Viewer you can use layers to simultaneously display multiple cameras in a grid. Multiple timelines are displayed just as in the regular Qognify VMS client.
The Viewer has the following functions:

- **Bandwidth optimization options** ( ): Depending on the license and configuration an optimized video stream can be selected to reduce client and network load (see "Bandwidth optimization" on page 430).
- **Previous frame** ( ): Jumps to the recordings previous video frame.
- **Play backward** (3): Plays the archived video stream in reverse chronological order.
- **Pause** ( ): Pauses the playback.
- **Play** ( ): Plays the recorded video in the correct chronological order.
- **Next frame** ( ): Jumps to the recordings next video frame.
- **Real time** (1:1): Plays the event in real time.
- **Next alarm recording** ( ): Jumps to the selected camera's next alarm recording.
- **Skip pause** ( ): Skips the pause between two recordings in playback mode.
- **Calendar** ( ): Opens a calendar window in order to navigate to a specific calendar time (date and time).
- **Zoom out from timeline** ( ) or **Zoom in to timeline** ( ): Enlarges or reduces the size of the display of the timeline. You can also zoom within the recording period by clicking the timeline and then turning the scroll wheel on the mouse.

- **Update timeline** ( ): Updates the camera's timeline. For manual synchronization with edge storage recordings (see "Full import" on page 238), hold down the CTRL key when clicking the icon.
- **Add bookmark** ( ): Adds a bookmark to the current frame (see).
- **Bookmark overview** ( ): Displays the overview of all bookmarks (see "Working with bookmarks" on page 177).
- **Multiselection mode** ( ): Sets a marker across multiple time streams.
- **Set marker** ( ): Sets the start and end markers for a selected area of the timeline (see "Editing an area" on page 166).

  Bookmarks are not supported in Viewer Mode / Qognify Viewer.
- **Delete marking** ( ): Deletes the selected marking.
- **QogniFinder** ( ): Starts the forensic search when the appropriate usage rights are provided (see "Using the QogniFinder" on page 168).
- **Synchronized mode** ( ): All visible cameras are synchronized to the time of the selected camera by default. If the synchronized mode is deactivated, each camera can show a different point in time.
- **Write protection** (/): Sets write protection for the marked area of the timeline. See "Write protection" on page 173
- **Delete area** ( ): Deletes the marked area from the timeline.
- **Export area** ( ): Starts the AVI export or the Qognify video data export (see "Exporting recordings" on page 171).

  Exporting in Qognify file format is not supported.
- **Jog dial**: Plays the sequence forward and backward. The further you turn the jog dial to the right or left, the faster the sequence is played forward or backward. The playback speed is displayed below the jog wheel.
- **Timeline / time stream**: See "Timeline / time stream" on page 166.

Export a recording

For information on exporting the recordings, refer to "The Export Designer" on page 96.

16

Qognify VMS web client

With the Qognify VMS web client, the Qognify system displays a web based interface within a browser. The image quality of the video stream transmitted to the web client is identical to the settings of a standard stream. The maximum frame rate is 12 fps. The maximum resolution may be limited by the size of the tile, in which the video image is displayed.

In surveillance mode, the web interface provides basic functions of the client, such as:

- Accessing cameras
- Accessing predefined layers
- Accessing maps
- Accessing web pages (i.e. "https://...")
- Receiving alarms and confirm them
- Controlling PTZ cameras and activating PTZ preset positions
- Displaying buttons and triggering their actions
- Displaying the same entity tree as in Windows®

In archive mode, the web client provides the following features:

- Stepping forward/backward in single image steps in the archive
- Playing the archive forward in real time (without speed choice and rewind)

Configuration mode and report mode are not available.

Installing the web client services on the Qognify server

1. Perform a custom installation of the Qognify system (see "Custom installation" on page 41) and additionally add the web client feature.
2. Switch to the native Qognify client and open the server menu in the configuration mode.
3. In configuration mode select **Server Transcoding Module** and configure the required settings (see "Configuring the transcoding module" on page 420).
4. In configuration mode select **Server Gateway Service** and configure the required settings (see "Configuring the Gateway-Service (SGS) module" on page 419).

The Gateway service should be automatically configured by the installer, if you have chosen the correct IP of the core server (for looking up the IP address, see "Configuring the Core Service" on page 403).

Connecting with the Qognify web client

1. Start a current web browser and enter the IP-address of the client in the URL bar: "https://<your-client-ip>. The web clients website is displayed.

   Make sure the URL starts with "https".

2. When asked to trust some security exceptions, confirm the request.
3. In the login screen enter the **user name** and **password**.
4. Click **Login**.

Remarks, limitations and known issues

- The resolution and quality streamed to the Mobile Client is configurable in the user profile (see "Image settings" on page 348):
  - For Single Image (Motion JPEG, MxPEg): **Normal** quality.
  - For configured video classifications: **Normal** or **Medium** squalid.
- Upload speed of at least 2 MB/s is required (for 2-3 simultaneous camera views). For a higher number of connections and camera views, more bandwidth is required.
- The following ports must be routed transparently if you are using a firewall:
  - Port 62000 (SGS)
  - Port 9100 (RTSP proxy)
  - Port 443 (webserver)
  - Port 8081 (NodeJS, which is delivering the images)
- Grandeye IPC fish-eye cameras are currently not supported; there is no live stream possible.
- It is recommended to use a current browser version.
- Upload speed of at least 2 MB/s is required (for 2-3 simultaneous camera views). For a higher number of connections and camera views, more bandwidth is required.
- The following ports must be routed transparently if you are using a firewall:
  - Port 62000 (SGS)
  - Port 9100 (RTSP proxy)
  - Port 443 (webserver)
  - Port 8081 (NodeJS, which is delivering the images)
- User profiles which are configured in the Qognify system are not supported. Assigned start layers to the user profile will not be displayed automatically in the web client. The user and group rights are not affected.
- Newly added or deleted cameras only show after reloading the web client in the browser. There is no restriction of the number of cameras displayed simultaneously, but beware that the web browser has to render all images AND the images have to be delivered through the transcoding service which is only serving the number of channels configured. The image rendering also depends on the hardware.

- Grandeye IPC fish-eye cameras are currently not supported; there is no live stream possible.
- Mobotix (MxPEG) cameras have a mirrored image if exporting a single image.
- If a layer contains an insecure (non-HTTPS) web page or a predefined insecure (non-HTTPS) web page in the web client is displayed, the browser may not display the web page because it is blocked automatically as "unsafe" by the browser or system settings. You can deactivate these checks permanently or for the current session, depending on the browser.
- Objects like cameras, layers, maps etc. have to be dragged into the view area (they are not displayed by clicking like in the native Qognify VMS client).

Harden IIS

On port 443 used by IIS several issues were discovered that can be resolved by hardening the IIS server with a configuration adjustment such as "forbid SSL v3".

TLS 1.0 and TLS 1.1 should remain unused, if possible.

SSL 3.0 is not considered as secure enough anymore so it should be disabled on the server if not done already.
If possible, the TLS versions 1.0 and 1.1 should also be disabled for server side applications.

1. Follow the instructions below to disable each of the protocols.
2. Restart the server to apply the changes.

SSL 3.0

1. go to HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server.
2. Create the key if it does not exist.
3. Make sure that DWORD value Enabled exists and is set it to 0.
4. Make sure that DWORD value DisabledByDefault (if exists) is set it to 1.

5. It is also advisable to disable SSLv3 for client authentication by repeating the above steps for the key HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client).

TLS 1.0

1. go to HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server.
2. Create the key if it does not exist.
3. Make sure that DWORD value Enabled exists and is set it to 0.
4. Make sure that DWORD value DisabledByDefault (if exists) is set it to 1.

TLS 1.1

1. go to HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server.
2. Create the key if it does not exist.
3. Make sure that DWORD value Enabled exists and is set it to 0.
4. Make sure that DWORD value DisabledByDefault (if exists) is set it to 1.

17

The Qognify VMS mobile client

> **The mobile client app is available for iOS 7 or later and Android 2.3 or later.**

In surveillance mode, the mobile interface provides basic functions of the client, such as:

- Accessing cameras
- Accessing predefined layers
- Receiving alarms and confirm them
- Controlling PTZ cameras and activating PTZ preset positions
- Displaying buttons and triggering their actions
- Sending selected frame by email

In archive mode, the mobile client provides the following features:

- Stepping forward/backward in single image steps in the archive
- Playing the archive forward in real time (without speed choice and rewind)
- Sending selected frame by email

> **Configuration mode and report mode are not available.**

Installing the mobile client services on the Qognify server

1. Perform a user-defined installation of the Qognify system (see "Custom installation" on page 41) and additionally add the mobile client feature.
2. Switch to the native Qognify client and open the server menu in the configuration mode.
3. In configuration mode select **Server Transcoding Module** and configure the required settings (see "Configuring the transcoding module" on page 420).
4. In configuration mode select **Server Gateway Service** and configure the required settings (see "Configuring the Gateway-Service (SGS) module" on page 419).

The Gateway service should be automatically configured by the installer, if you have selected the correct IP of the core server (for looking up the IP address, see "Configuring the Core Service" on page 403).

Installing the mobile client on a mobile device

1. Before downloading, verify that your device meets the necessary requirements. The client is available on "Google Play" for Android OS version 2.3 or later, and on the iTunes App Store for iOS 7 or later.
2. Download the application from the appropriate app store.

Configuring the Qognify mobile client on the mobile device

1. Start the app on the mobile device.
2. Tap **Add Server** and enter the **user name**.
3. Enter a **description** to identify the server.
4. Enter the SOAP **IP** or **URL** of the server.
5. Enter the **port** number of the server.

6. For iOS devices: Specify the **FPS** (frames per second) and the horizontal **resolution** when connecting via 3G network. The default settings are: 3 fps and a resolution of 200 px.
7. Select the server type (SeeTec 5 or Qognify VMS).
8. Tap **Save**.

Remarks, limitations and known issues

- The resolution and quality streamed to the Mobile Client is:
  - Android tablet and smartphone: 480 x 320px, 12 fps (WLAN & 3G)
  - iOS iPad and iPhone (low resolution): width 480 px, 24 fps
  - iOS iPad and iPhone (high resolution): 703 x 512px, 24 fps
- Upload speed of at least 2 MB/s is required (for 2-3 simultaneous camera views). For a higher number of connections and camera views, more bandwidth is required.
- The following ports must be routed transparently if you are using a firewall:
  - Port 62000 (SGS)
  - Port 9100 (RTSP proxy)
  - Port 443 (webserver)
  - Port 8081 (NodeJS, which is delivering the images)

Connecting with the Qognify mobile client

1. Start the app on the mobile device.
2. Select a preconfigured server.
3. Enter the password.
4. Tap **Login**.

Installing the Qognify Metadata Manager (QMM)

Introduction

The Qognify Metadata Manager (QMM) is a module that ingests and stores object metadata provided by external video analytics sources with the purpose of offering these metadata to QogniFinder. QogniFinder is a user interface within the Qognify VMS client that can search recorded video footage for specific object types and other object characteristics.

> **Object metadata are generated and stored in real time.**

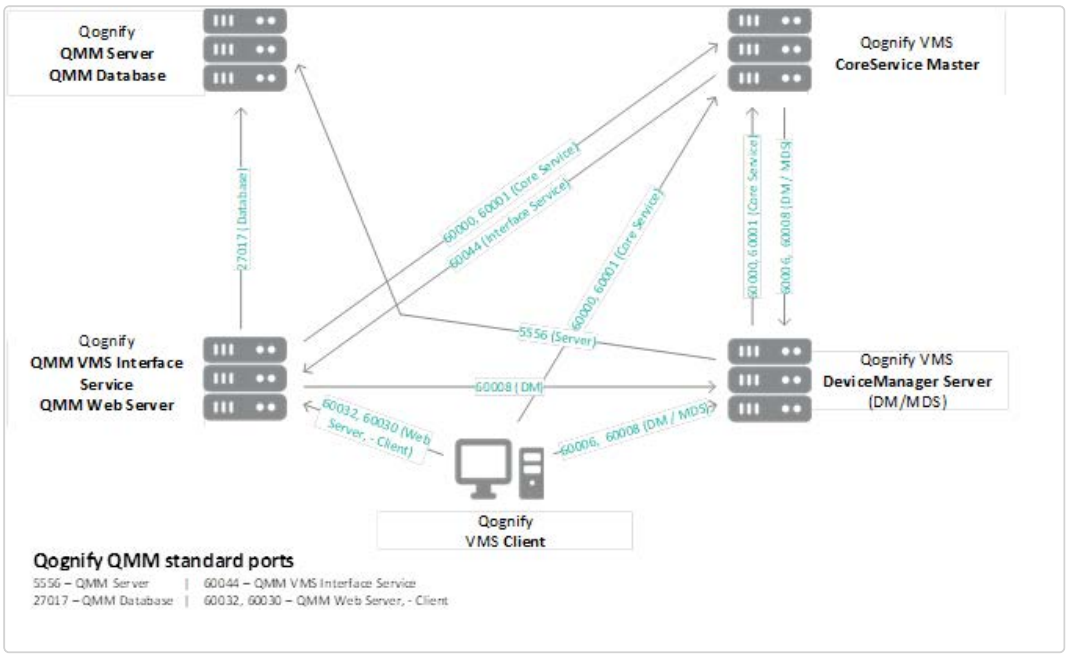
Prerequisites

This guide describes the installation process of the Qognify Metadata Manager.

> **An installed Qognify VMS is required.**

During the installation .Net Framework and Microsoft Visual C++ Redistributable will be installed automatically as soon as the installation process is started. During the installation a restart of the operating system may be required. Make sure to close all open programs before executing the setup file. After the reboot the installation process will be continued automatically.

Architecture and used default ports



Component name	Description
QMM database	MongoDB which stores all collected metadata
QMM Server	Service running on the same machine as the MonogDB which receives the metadata and writes them to the database
QMM VMS Interface service	Communication service between QMM and Qognify VMS
QMM WebServer	IIS which requests metadata from the QMM database and delivers it to the Qognify VMS Client.

Installation and upgrade **519**
Camera settings **531**
Troubleshooting **533**

Installation and upgrade

The QMM Installer is provided as a zip file.

1. Unzip the installer.
2. Run the installation file as administrator and follow the Installation wizard. As soon as the installation process is started the following components will be installed on the server:

- .Net Framework 4.8
- Microsoft Visual C++ Redistributable 2015-2019

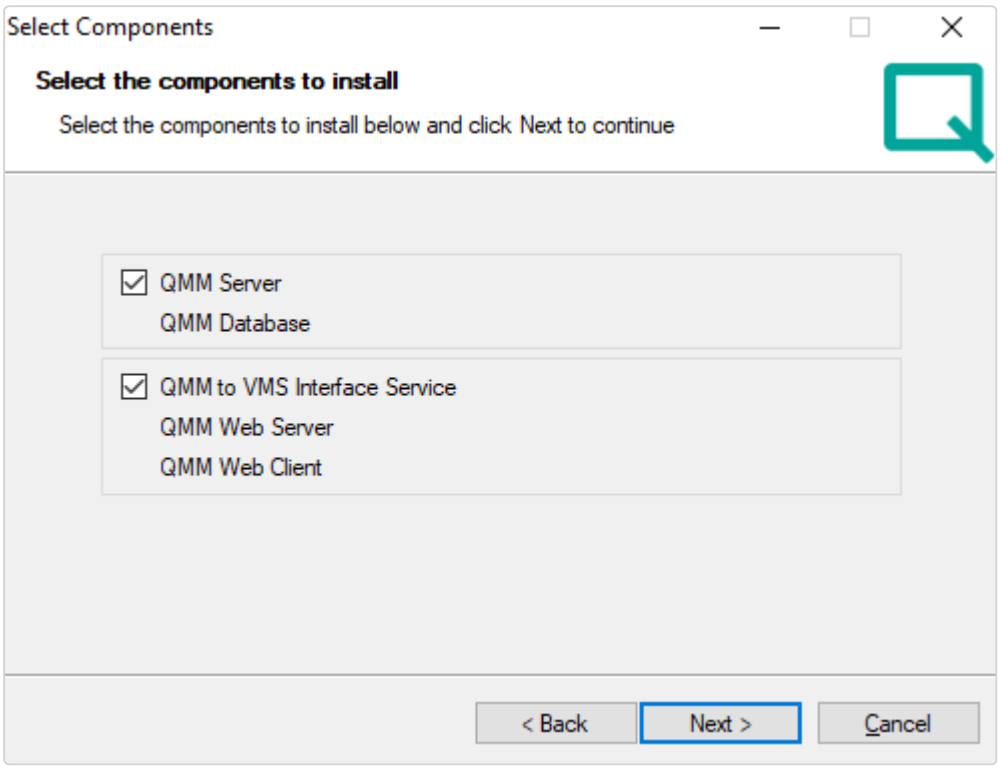
To continue the installation a restart of the operating system is mandatory.

After the reboot the installation will start immediately, and you will see the Welcome screen.

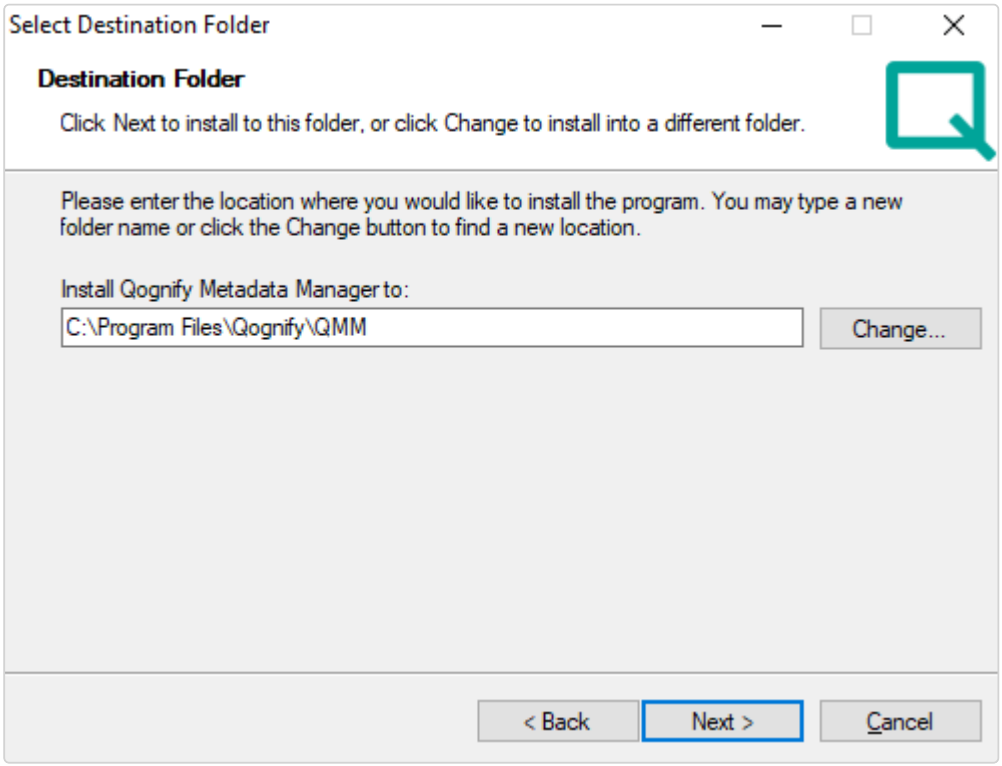
3. Read and accept the End-User License Agreement.
4. Select **Next**.

In the next section you select components you want to install on the PC.

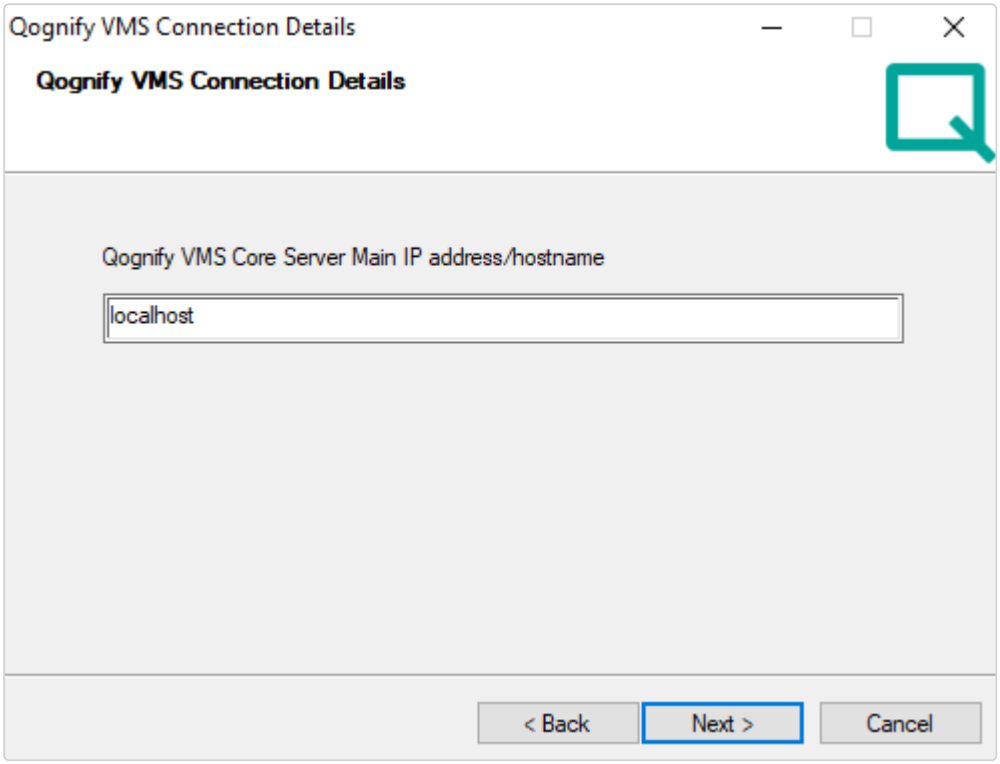
Option 1 (Default): Select all components



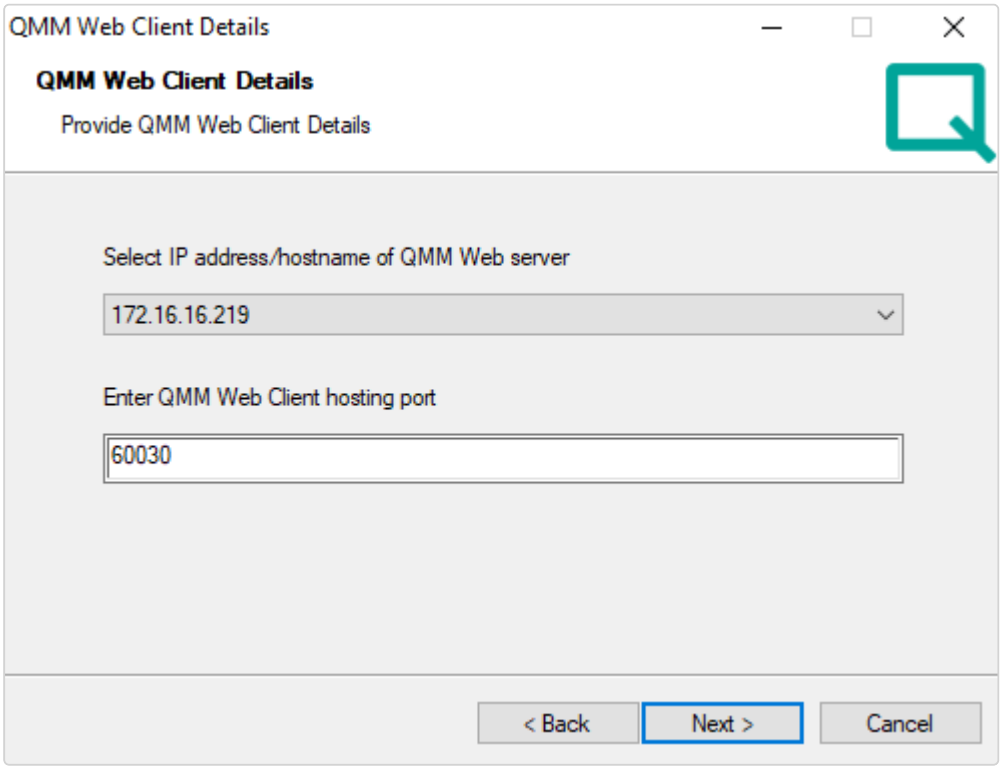
1. Enable the check boxes for all components and select **Next**.



2. Specify the installation folder on the next page and select **Next**.

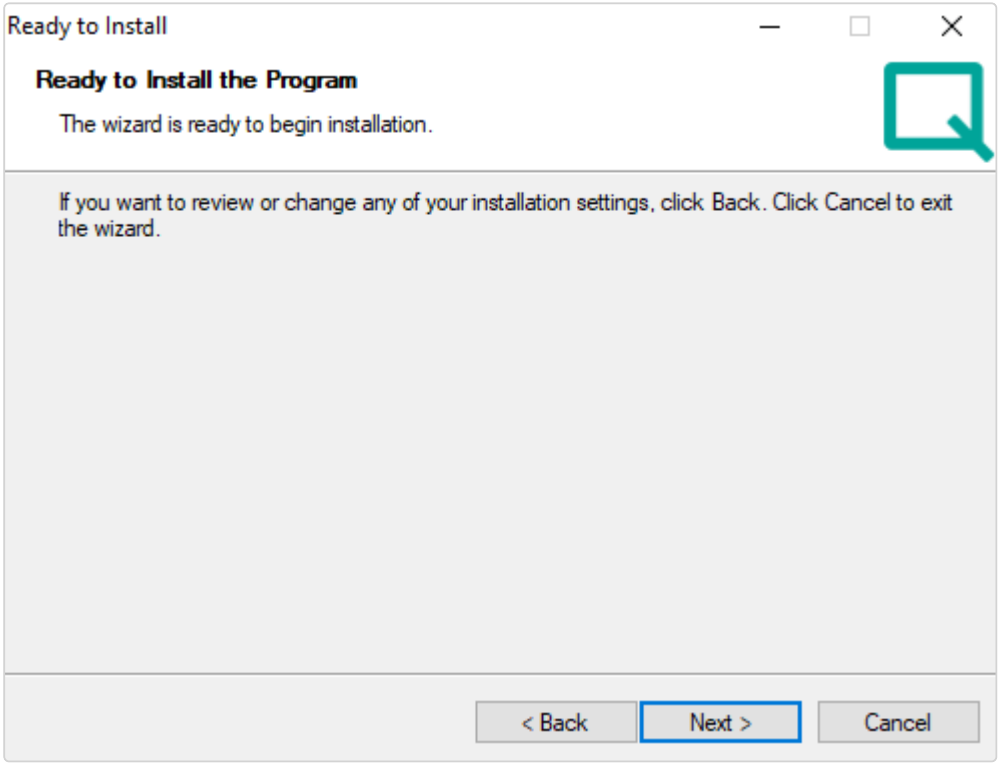


3. Enter the IP address or host name of the Qognify VMS Core Server Main. The communication port is set to "60000" by default and cannot be changed during the installation process.



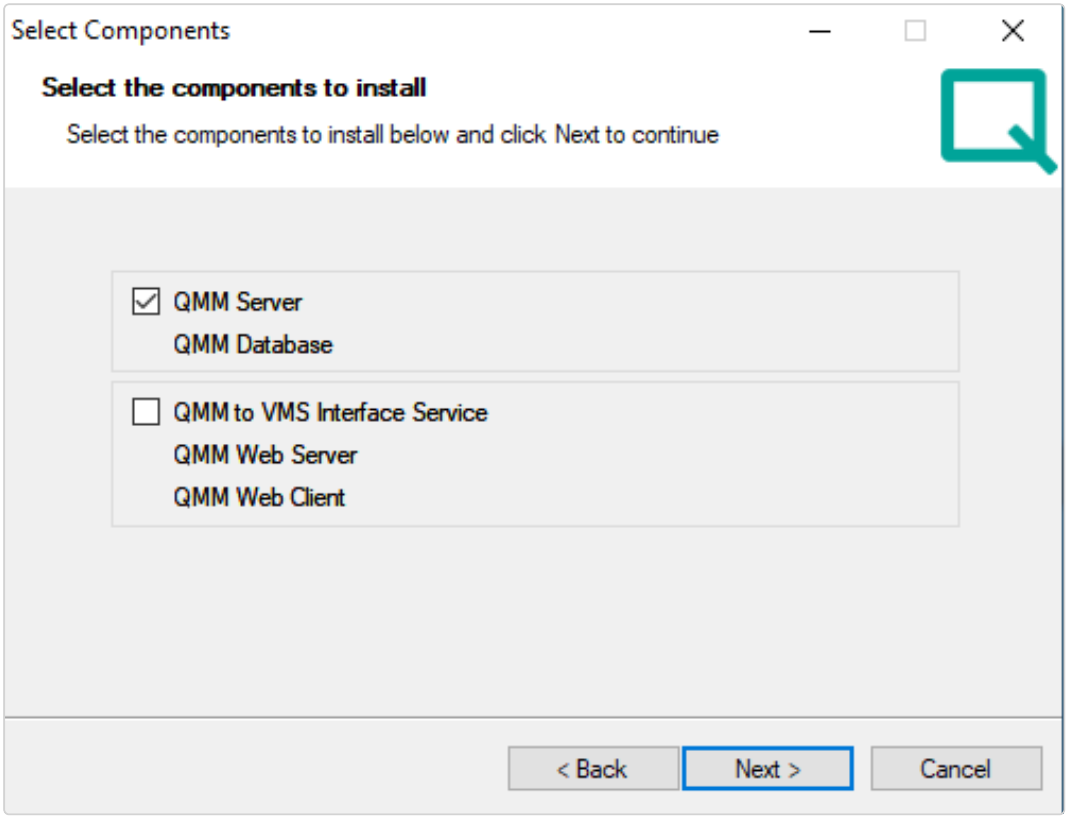
4. Select the IP address or host name on which the web server should be accessible. Also specify a port (Default: 60030) for the communication.

> **Remember to open the port in your firewall settings after the installation has been finished.**

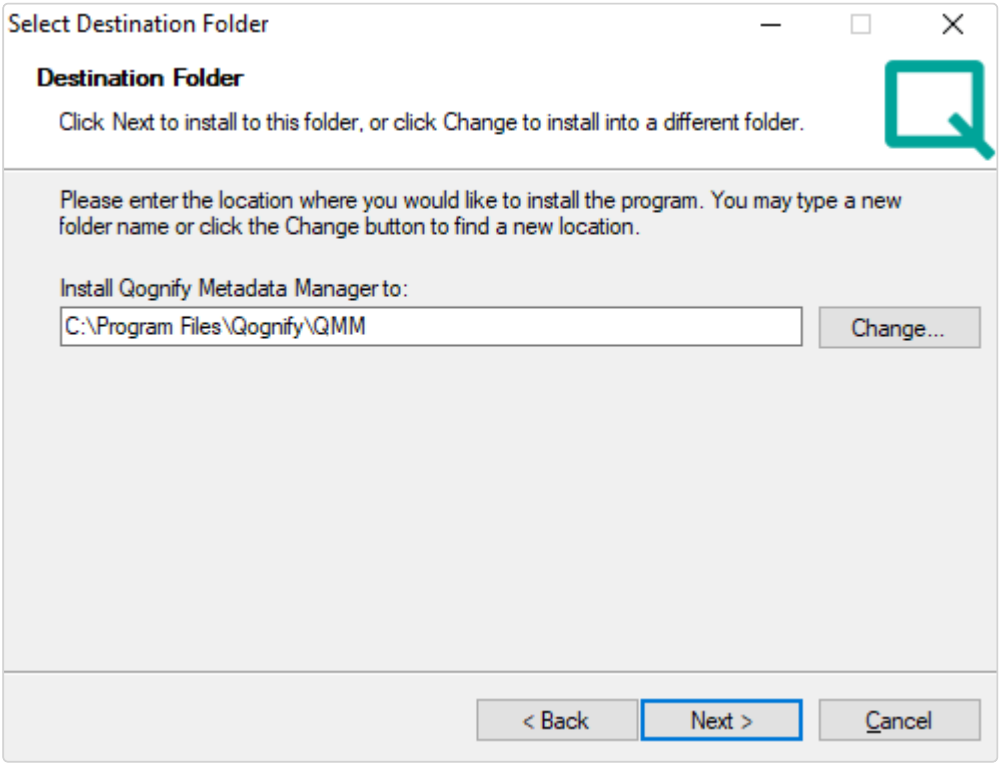


5. Select **Next** to start the installation.
6. After the installation select **Finish** to close the Setup Wizard.

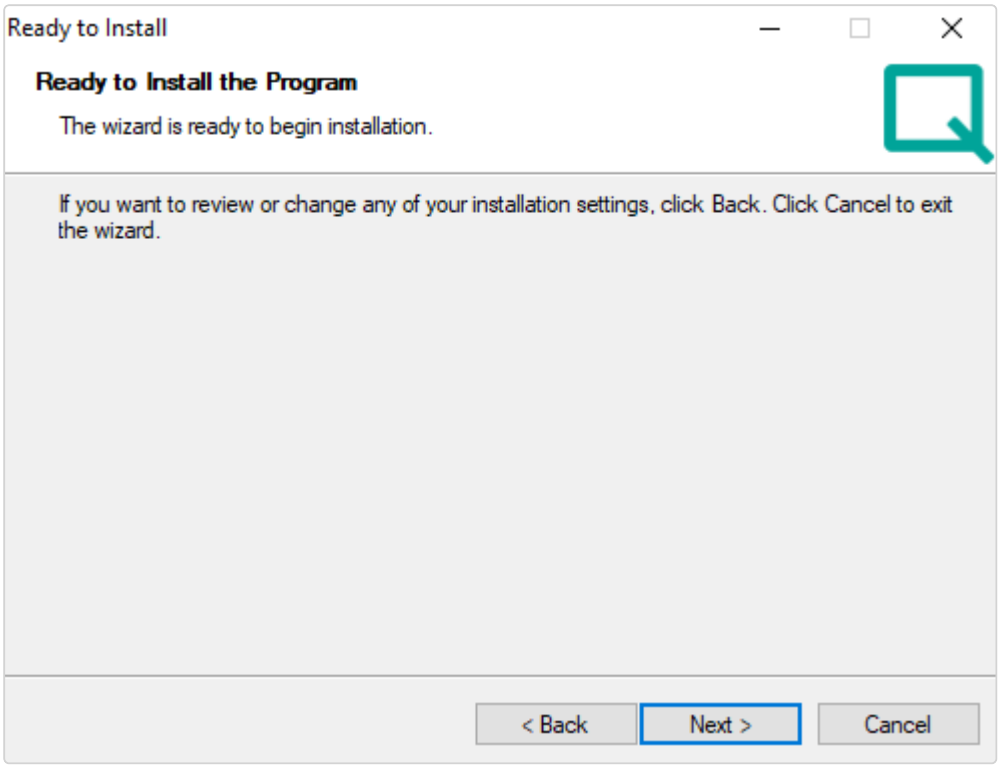
Option 2: Select QMM Server & QMM database



1. Enable QMM Server and QMM Database and select **Next**.



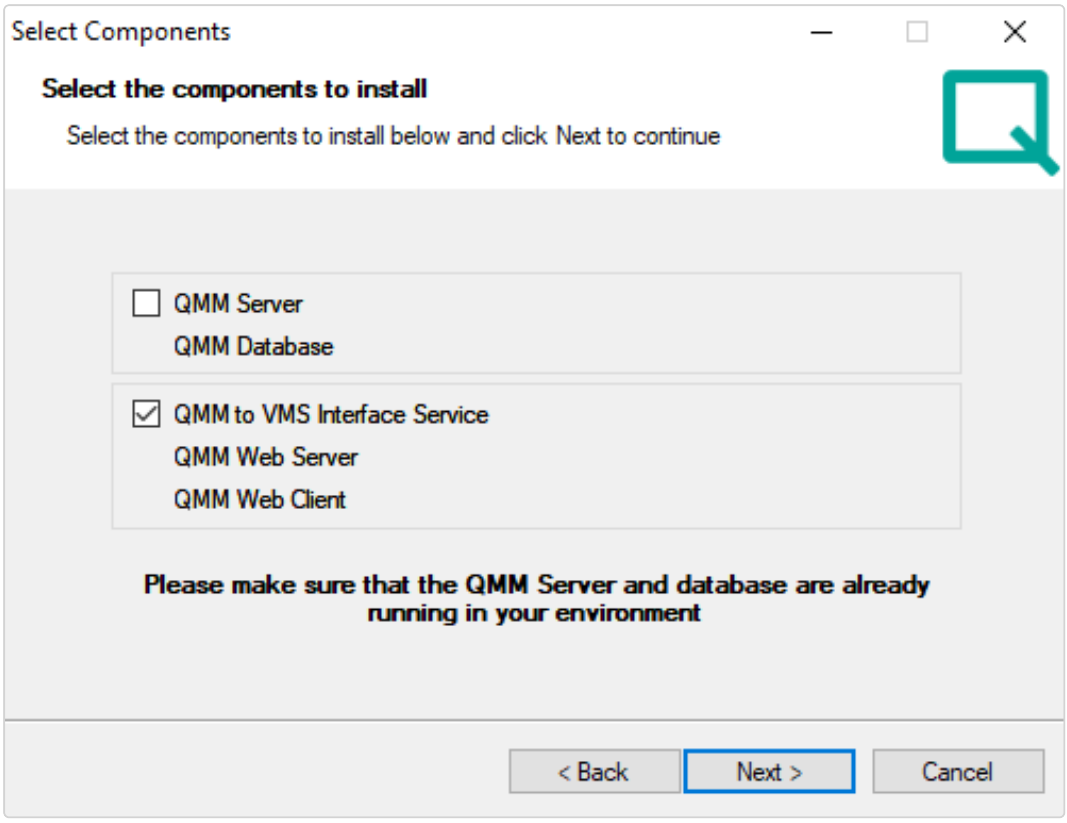
2. Specify the installation folder and select **Next**.



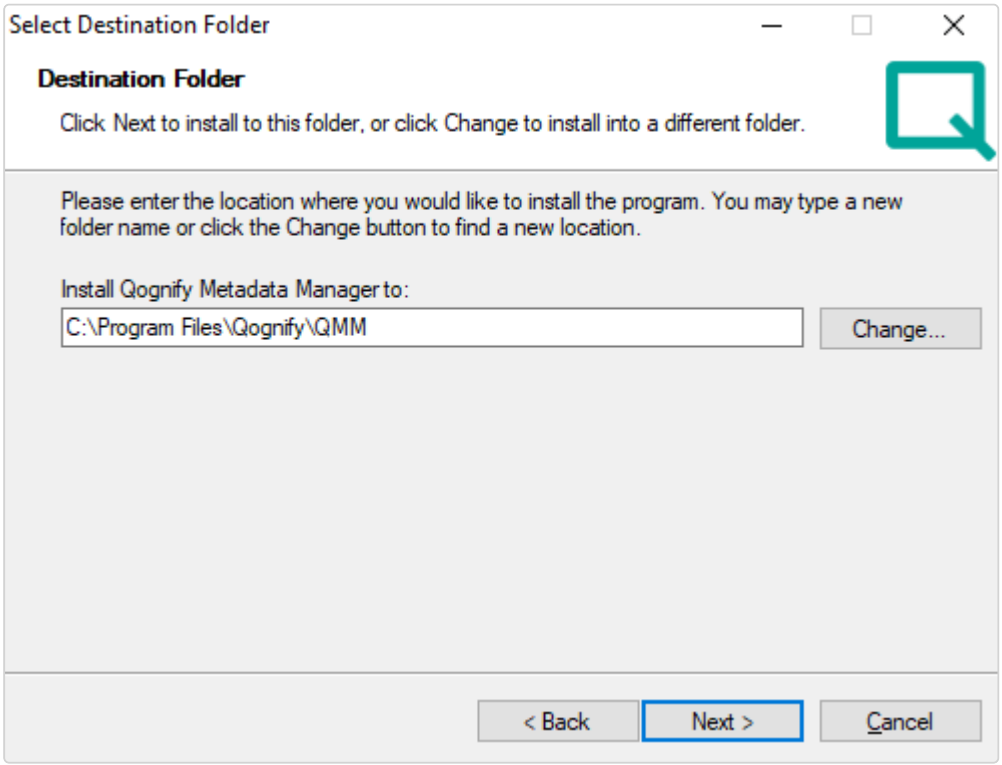
3. Select **Next** to start the installation.
4. After the installation select **Finish** to close the Setup Wizard.

Option 3: Select QMM to VMS Interface Service & QMM WebServer

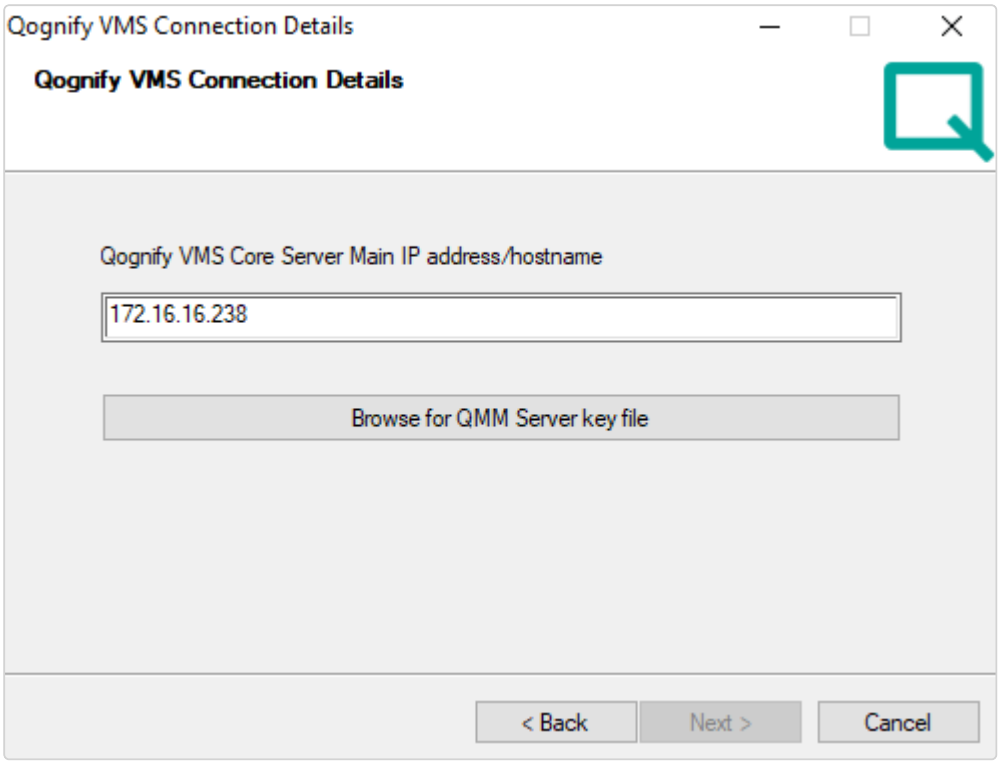
> **For this type of installation, you need an existing QMM Server and QMM Database in your environment.**



1. Enable for QMM to VMS Interface Service and select **Next**.

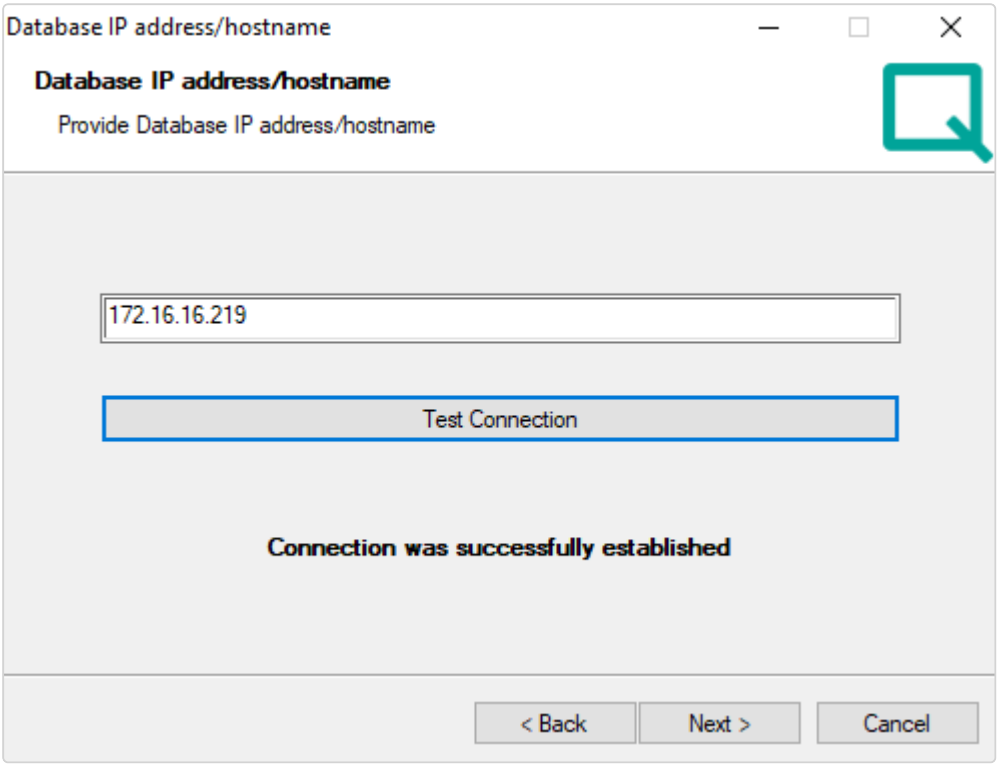


2. Specify the installation folder and select **Next**.



3. Enter the IP address for the Public QMM Server key that is stored on the PC where the QMM Server and QMM Database are installed. You can find the key file
4. Select Browse for QMM Server key file and select the key file *QVAServer-Public.key* in the installation folder: *%InstallDir%\Qognify\QMM\QMM Server*

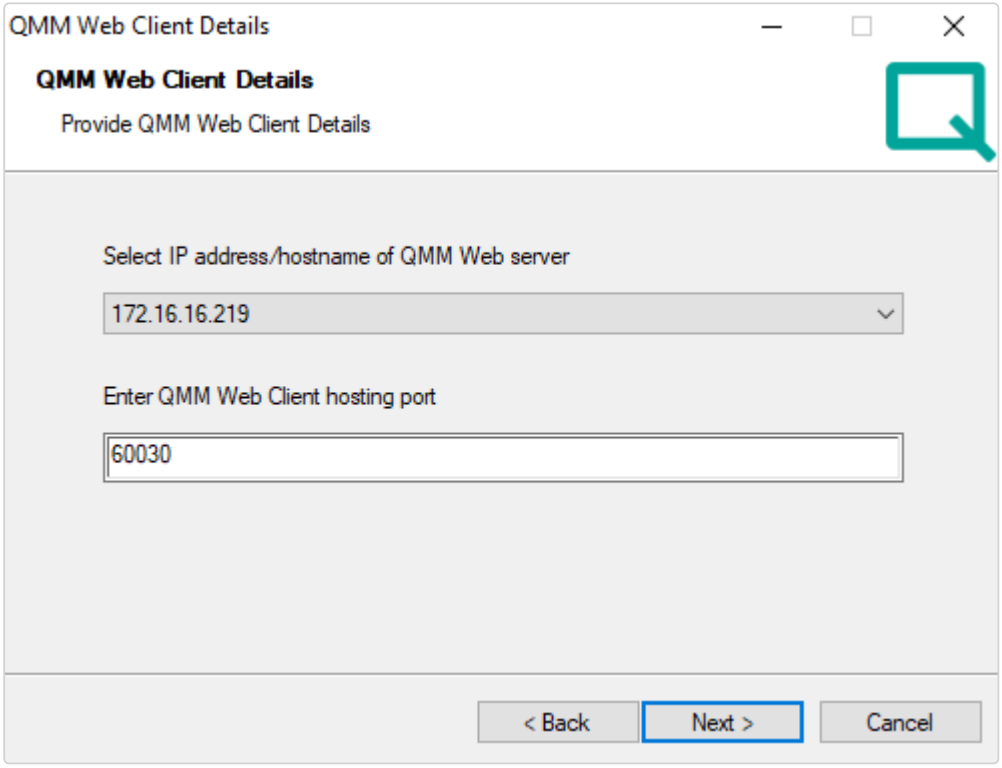
5. Specify the IP address or hostname of the Qognify VMS Core Main Server and select **Next**.



6. Set the IP address of the QMM database.

7. Select **Test Connection** and wait until a connection is established. Once the connection was established successfully, select **Next**.

> **Make sure the QMM database is running and accessible from remote.**



8. Select the IP address or host name on which the web server should be accessible
9. Specify a port (Default: 60030) for the communication.

> **Remember to open the port in your firewall settings after the installation has been finished.**

10. Select **Next** to start the installation.
11. After the installation select **Finish** to close the Setup Wizard.

Upgrading and uninstalling

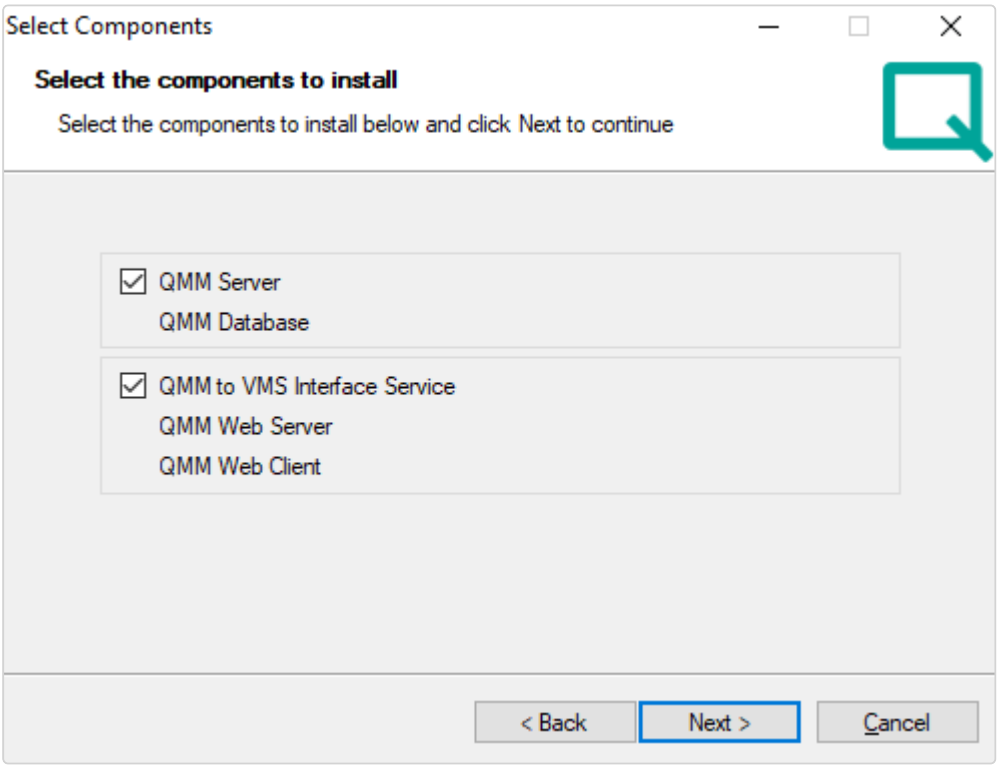
Upgrading

The software can be upgraded without uninstalling the previous version.

> **An automatic restart of the operating system can be required. Make sure to close all open applications before running the installer.**

After the reboot the installation will start immediately.

1. Read and accept the End-User License Agreement and click **Next**.

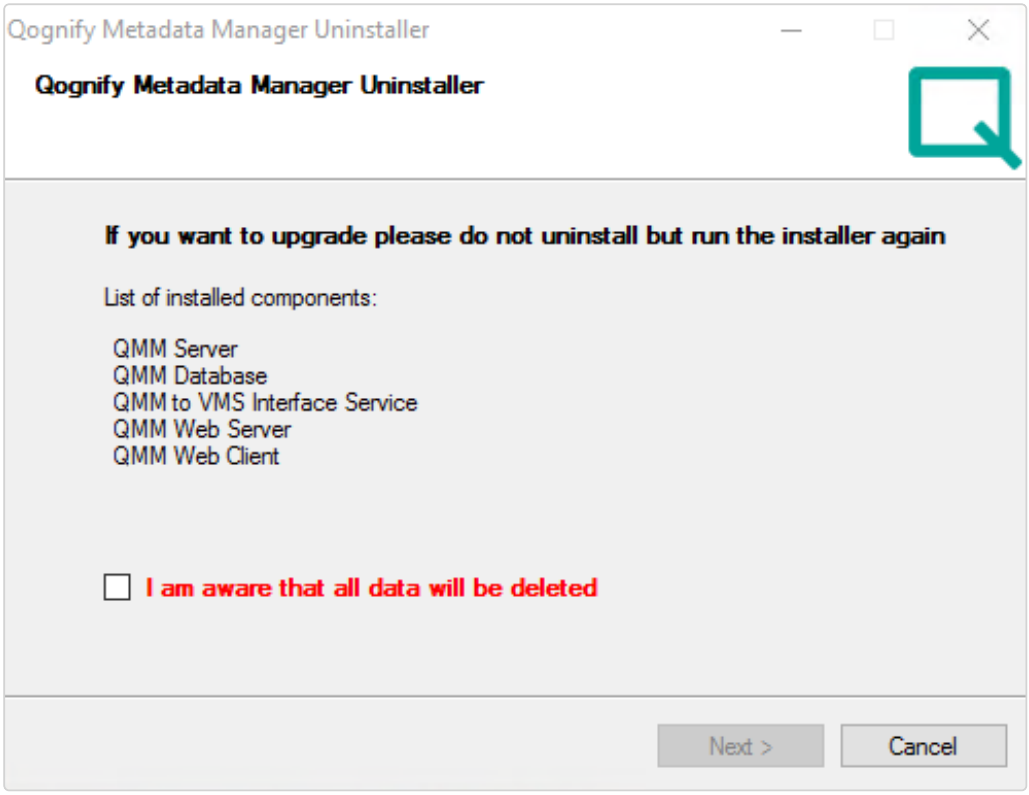


2. Select the components you want to update. Only the previous installed components are selected.
3. Select **Next** to start the installation.
4. After the installation select **Finish** to close the Setup Wizard.

Uninstalling

> **Note that all components and their configuration are deleted when uninstalling. Any stored object metadata will be deleted.**

1. To completely uninstall the software open **Control Panel > Programs and Features** and select "Qognfiy Metadata Manager".
2. Select **Uninstall**. The uninstall process will be started.



3. To continue select the check box and click **Next**.

Camera settings

> **To get metadata from a camera you have to add the device to your Qognify VMS installation first. For more information how to add a new camera entity to the Qognify VMS system, see "Cameras" on page 211.**

To get the recognized metadata from the camera with the most accurate timestamp, activate the time synchronization and the object detection on camera side.

> **Time synchronization is essential for the QogniFinder to work as the metadata require the correct timestamp.**

Supported devices

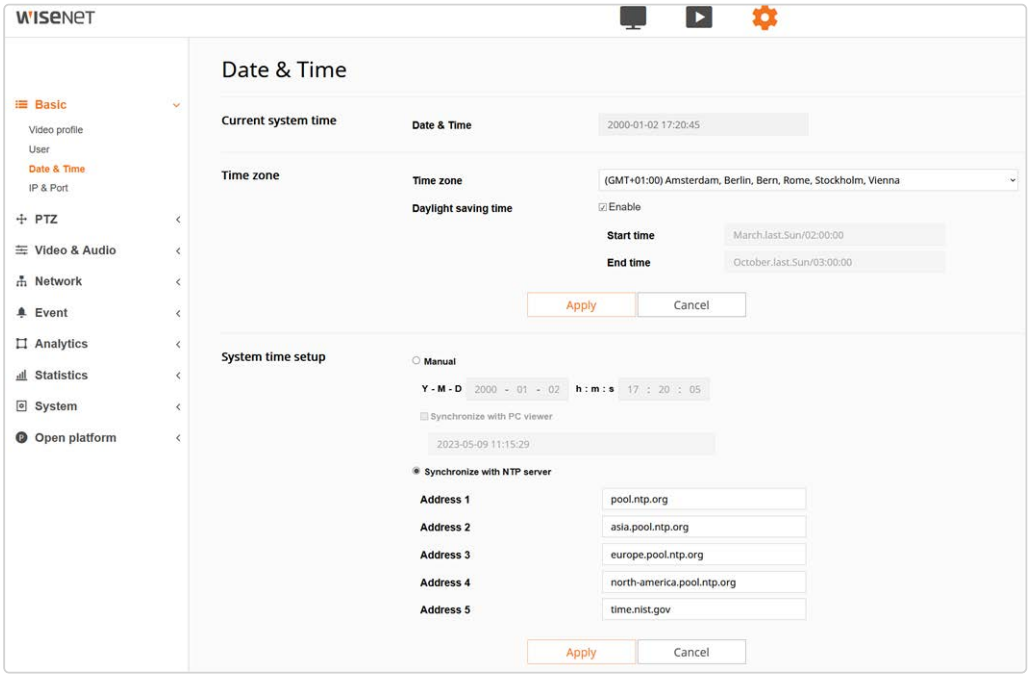
The following camera series from Hanwha are supported:

- P-Series AI – provides object classification and further attributes
- X-Series AI – provides object classification only
- Multi-AI – provides object classification only

Time synchronization

> **To get the most accurate timestamp for each event it is required to synchronize all Qognify VMS components, cameras, operating systems etc. with the same time server.**

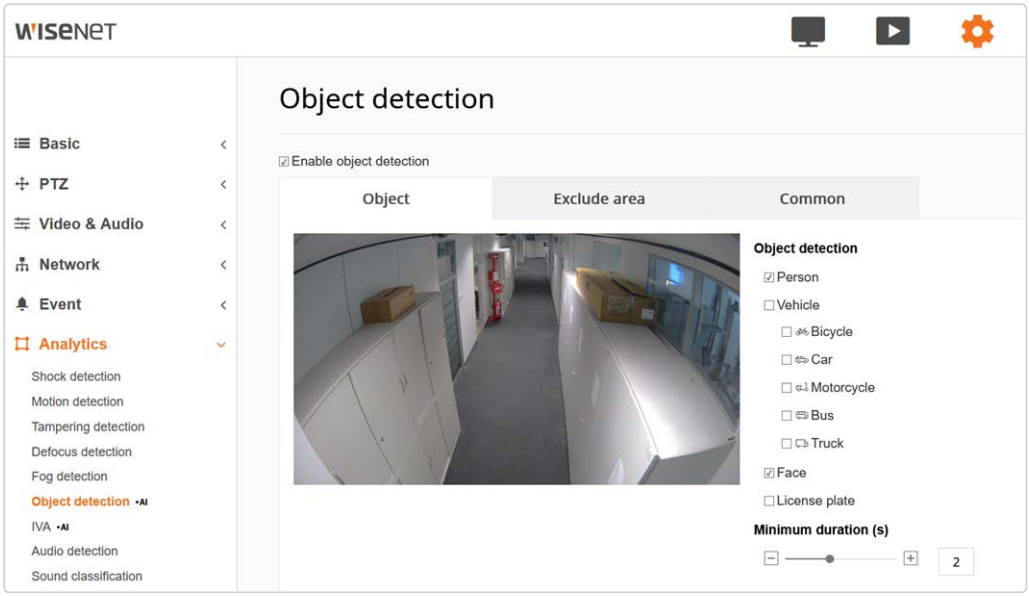
1. Open the web interface of the camera in your browser and select **Settings** .
2. Select **Basic** in the configuration and select **Date & Time**.



3. Select your time zone and enable the option for **Daylight saving time**.
4. In section **System time setup** enable the option **Synchronize with NTP server**.
5. Define the NTP servers that should be used to synchronize the camera time. Metadata and archive footage are synchronized by the timestamp.

Object detection

1. Select **Analytics** in the camera **Settings** .
2. Select **Object detection**.



3. Select **Enable object detection** and define the relevant option on the right side of the camera image which should be detected by the camera.

> **The available options vary according to the camera type used.**

Troubleshooting

Problem	Possible reason
There is no object shown in the results which are visualized by QogniFinder.	Check the system time of the camera and the operating systems where the Qognify VMS components are installed. It's important to use the same time server for time synchronization to get the most accurate result.

18

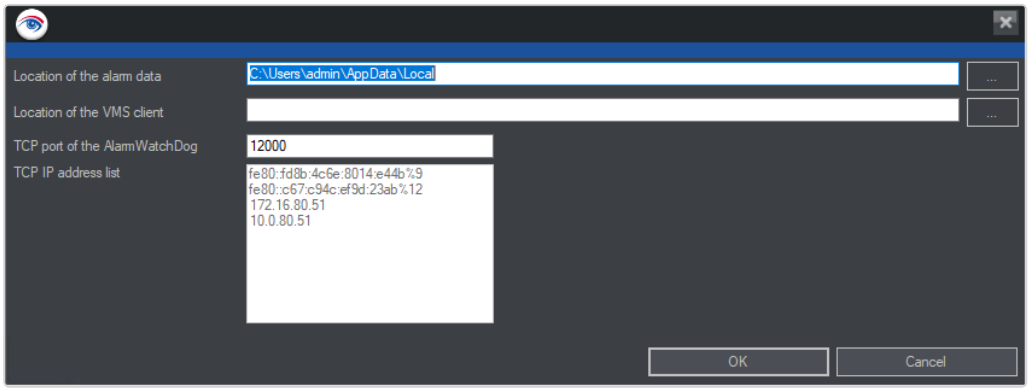
The AlarmWatchDog

The AlarmWatchDog service displays all alarms on all clients connected to the AlarmWatchDog server that are defined as an AlarmWatchDog-Alarm. For setup and configuration of the service, see "Configuring the AlarmWatchDog" on page 446.

1. Start the **AlarmWatchDog** service from the tools folder in the installation directory.

Configuring the AlarmWatchDog

1. Open the settings menu .



2. Specify the **Location of the alarm data** by setting the file path to the storage directory.

   > **Read and write permissions must be enabled.**

3. For **Location of the VMS client**, specify the installation directory of the client (e.g. "C:\Program Files\...").
4. For **TCP port of the AlarmWatchDog**, specify the port number that has been set in the server configuration of the AlarmWatchDog.
5. The available TCP IP addresses of the client are displayed.
6. Select one IP address from the **TCP IP address list** and copy it to the clipboard.
7. Paste the IP address in the AlarmWatchDog settings in the System menu (see "Configuring the AlarmWatchDog" on page 446).
8. Select **OK**.

Using the AlarmWatchDog

1. Start the **AlarmWatchDog** service from the tools folder in the installation directory. All occurring alarms on all connected clients are displayed in the list according to their
   - Alarm scenario name
   - The date and time of the occurrence
   - The name of the client where the alarm occurs
   - The status of the alarm
2. Double click on the alarm to open it. The client will be started and a connection to the respective server is established.
3. After responding to the alarm, close the client. The alarm is displayed as "finished" in the AlarmWatchDog window.
4. To remove all finished alarms from the list, click **Remove finished alarms**.