Ocularis Recorder Configuration Guide

Version 6.0 R16

January, 2021

Revision History

Revision	Reason for change	Date
00	GA	January 2021

Contents

1 Proprietary and Confidential Information

Copyright

Address

Qognify, Inc.

One Blue Hill Plaza

7th Floor - P.O. Box 1555 Pearl River, NY 10965 Tel: (845)732-7900

Internet: http://www.qognify.com

Subject to alterations, errors and misprints. Rev. code: 0000010312019-1249-5.8.0.785

Version

This manual corresponds to the recorder component software R16 (Version 6.16.1_XX) shipped with Ocularis v6.0.

2 Introduction

Ocularis is Qognify's innovative and cost-effective open platform Video Management Software (VMS) designed to enhance your security while simplifying your daily workload. From convenience stores to city- wide deployments and everything in between, Ocularis can scale up to accommodate an infinite number of cameras to match your growing system needs.

Ocularis is offered in the following models: Professional (PRO), Enterprise (ENT), Ultimate (ULT) to meet the needs of organizations of all sizes and types. RecOn5 NVRs use Ocularis NVR.

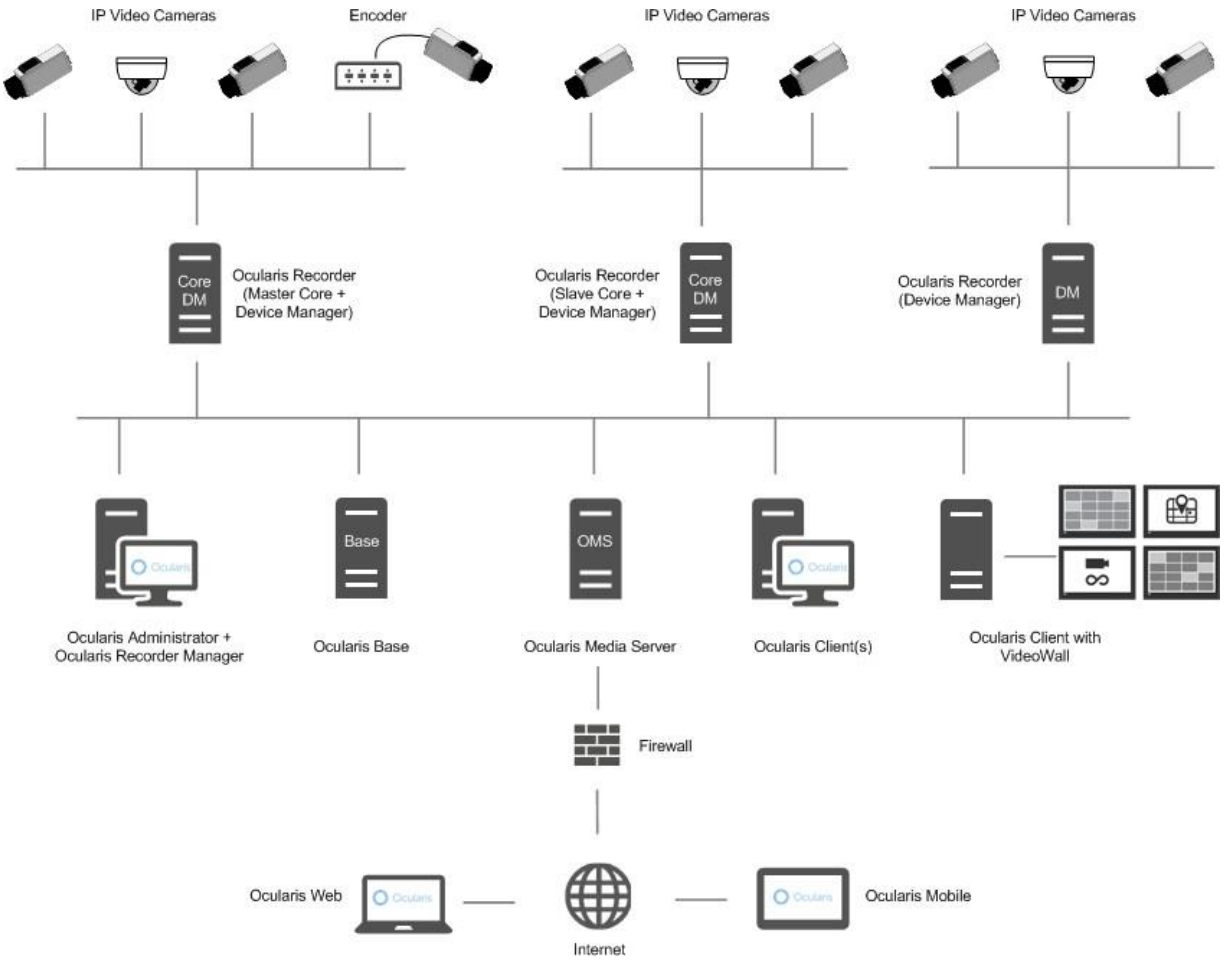
For more information, go to www.qognify.com/

2.1 Functional overview

Ocularis recording components consist of various services that communicate with each other within a closed network and over the Internet. Installations are possible on multiple computers and an unlimited number of servers, clients and devices can be added to the system.

2.2 System Layout

Here is a sample system layout:



It shows components on various servers but in many cases, components may be shared within the same server.

2.3 Recorder Components

Each installation regardless of Ocularis model, has the following components:

- Core Main

When you install the software, the first component installed is the Main Core service. This component is the heart of the recording component and manages the configuration database of the recorder system. It manages system configuration, events, reports, backups and knows about every other component in the system. With smaller systems in Ocularis Enterprise and Ultimate, there is typically just one Main core service in an installation. Multiple main cores may be used in larger, more distributed environments. For Ocularis Professional and RecOn5 NVRs, there is one main core and one Device Manager per server.

- Device Manager

A Device Manager, or DM, is the component that manages the video recordings. Along with its companion service, the MDS or Media Database Service, it controls where video data is stored. Data is stored in one or more Zones. This is the 'recorder' of the installation.

- Zone

A Zone is a volume where video data is stored. Device Managers may be directed to store video data to one or more zones. If multiple zones are configured, video data is load balanced across all available zones. See **Long Term Storage Systems** for information on storing data on long term storage systems.

- Core Secondary

In Ocularis Enterprise or Ocularis Ultimate, an additional core is available to provide redundancy to the master core. This is known as a secondary core. If a main core finds an available secondary core, it will offload much of its work to the secondary. Tasks like user authorization and alarm scenarios will be handled by the secondary core while the main core focuses on maintaining the configuration database. In the event the main core goes down, a secondary core will take over. If a secondary core exists in the root level of the company, users may still log in and view video.

- Ocularis Recorder Manager

This component is the software application used to configure the other components listed above. It may be installed on any number of workstations and it used to log in to the main core to configure settings. The Ocularis Recorder Manager software can be considered a client application.

- Update Service

The Update Service works to update the recorder component software. By default, the system will check daily for updates via the Internet. If found, the updates, which are typically released about once per month, are downloaded and pushed out to each remote recorder component. The default settings may be overridden to manually check or install updates.

2.4 Long Term Storage Systems

When viewing video stored on long term storage systems (e.g. tape), you can now enable a setting to pre- fetch or “fetch in advance” video for a specific time period. The setting is configured in the MDS.conf file for each zone of the DM. This significantly improves the performance of playing video backwards or forwards or for exporting video on systems such as Quantum.

Video stored locally on a hard drive can be played back with little to no delay. The challenge arises with video stored on tape or other long-term storage systems. Video files or .bix files stored on these devices

can take a longer time to load and this delay increases when attempting to simultaneously play video from multiple sources in a single view. Pre-fetching improves performance on such systems.

This new setting will “fetch” the next or previous .bix file(s) based on the configuration.

- Pre-fetching works with Ocularis Client, Ocularis Web and Ocularis Mobile.
- This feature kicks in only during constant playing (forward or backward) of video or when performing a video export or bookmark. Using the Kinetic Timeline to jump ahead or behind will not trigger pre-fetch.
- The default value (if not manually configured) is 300 seconds (5 minutes).
- The flag is set per zone. Therefore, it is possible to have this enhanced mode on one zone but not another. The setting should likely be the same for all zones.

▸ To configure Pre-Fetch for Each Zone

In the mds.conf xml file, add the following (in bold):

<Zones>

<Zone>

<Path> ../data</Path>

<MaxSize>-1</MaxSize>

<Type>standard</Type>

<Prefetch>

<enabled>true</enabled>

<time>10</time>

</Prefetch>

</Zone>

</Zones>

The **<time>** tag represents the number of seconds that should be prefetched in both directions from the current point in time. Files that should be prefetched are based upon this value and will be queued for prefetching until the delta is met or the last/first .bix file is reached.

Contact Qognify Technical Support for questions on how to best configure your system.

2.5 Concept

2.5.1 Administrative rights and user rights

Two types users can be configured in Ocularis Recorder manager:

- **Administrator**. An administrator is installed by default. The administrator is a user with configuration rights and belongs to the administrator group. An administrator inherits the administrator group's rights. The administrative rights of the group and hence the administrators can be restricted to branches, where the administrator may manage only the objects (e.g.

cameras) within the branch without "seeing" other branches. In Ocularis, use of a single administrative user is all that is needed, in most cases. Multiple administrators can be created and assigned at the branch level so that they can administer their own branch.

- **Users**. The user has restricted rights and can be member of one or more user groups. This type of user has no function most Ocularis environments. It is useful when using Ocularis OpenSight.

2.5.2 Multi-level administration

The video management system has multi-level administration, which 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**. For defining user group rights, see **Managing user rights**, for defining specific user rights, see **Managing user rights**.

The system allows subdivision of the administrative rights levels and division into a control center and as many branches as required. The branches are defined as logical subunits with their own configuration con- text and cannot be nested.

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

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

2.5.3 Relationship between the CoreServices - main and secondary

The Core Service server of the company is installed, configured and managed as "CoreService Main" (CSM) in the main branch. The CoreServices of the branches cannot manage or configure the CSM or a CoreService within another sub-branch. The CoreServices of the sub-branches are regarded as "CoreSer- vice Secondary" services, CSS. All CSS are configured by the CSM.

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.

2.5.4 Relationship between the main branch and its sub-branches

2.5.4.1 Changing the branch name

For changing the name of the main branch from the default name ("company"), see **Editing the name of the "company"**.

2.5.4.2 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.

2.5.4.3 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".

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 either configured with the CoreServiceMain (CSM) of the main branch for all CoreServices. 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 **Relationship between the CoreServices - main and secondary**.

NOTE: 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.

2.5.5 Branches

2.5.5.1 General

The recording engine in Ocularis is broken into several components, each with its own purpose. Cores deal with configuration data, events, alarms and authorization, while a Device Manager, along with its corresponding MDS (Media Database Service) manages the storage of recorded video data. An additional component, called a branch, may also be used in certain circumstances to effectively manage the system.

2.5.5.2 Branches in Ocularis

In Ocularis, a branch may be used to logically organize the components of the recording system. Viewing and configuring branches is done via the Ocularis Recorder Manager. There is a top level main 'branch', defaulted to Company, and other branches may be created. In some cases, branches are optional and provide for visual ease of use of the product. In other cases, branches are required.

When the software is installed, one Company or main branch is created. You can rename this branch as your own company name or the company name for the customer. For installations where multiple people will be administering recording components, creating a user account at a branch level will isolate that user's ability to configure the system solely for their branch (similar to a Group Administrator in Ocularis Administrator). They will not have visibility to other branches. The administrator at the top level will always have visibility down all branches.

Branches may also be organized into a Branch Group to facilitate navigation. Branch groups are displayed as folders and serve no other function than for cosmetic display and organization.

2.5.5.3 Branches and Secondary Cores

As a review, the heart of an Ocularis recorder system is the main core. This component manages the configuration database of the system. The main core is always in the top level main branch. In Ocularis ENT

and ULT, additional cores called 'secondary cores' may be added to help distribute the work load from the main core and provide redundancy. If an Ocularis ULT or ENT installation has a main core but no secondary core(s) and the main goes down, operators will not be able to see video or log in to the system, events will not be transmitted to the Base and the system cannot be configured. With a secondary core installed, operators already logged in will still be able to see video although new log ins will not be successful nor will events be received. Therefore, it is important to take advantage of secondary cores in these models of Ocularis and always install at least one.

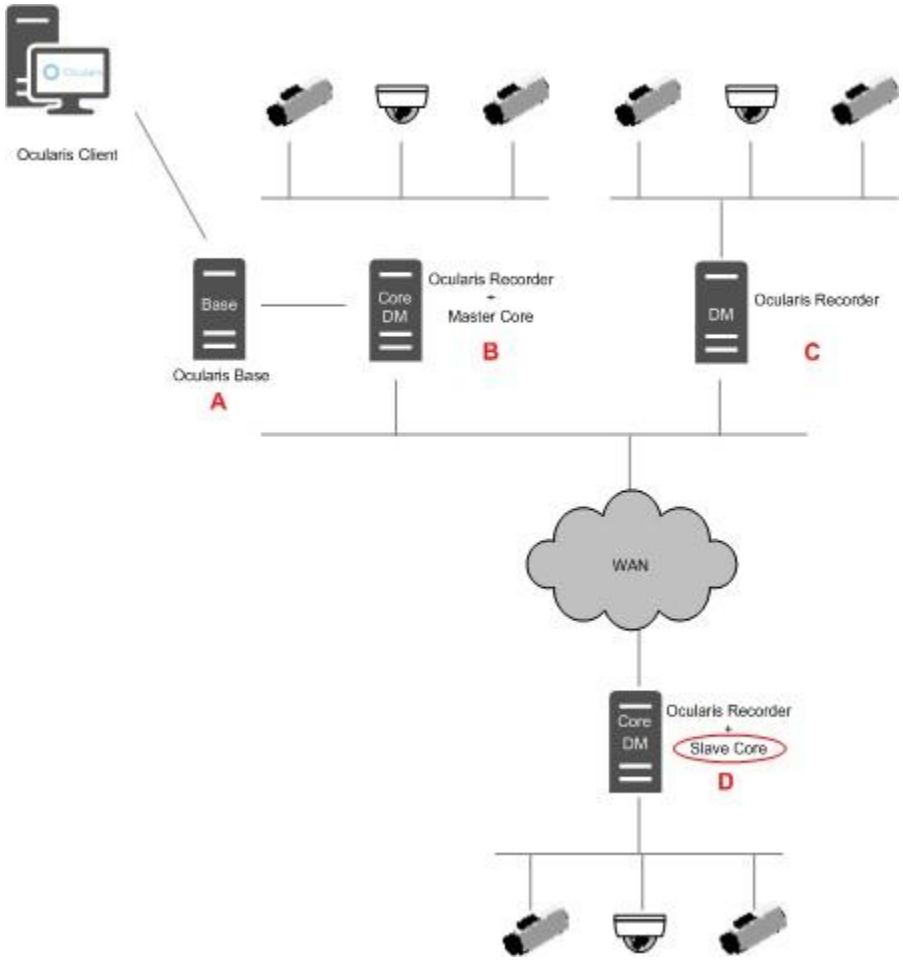
In Ocularis, there are some things about secondary cores and branches that are worth looking at closely. To start, there are some general rules about the two:

- There can be only one secondary core at the company (top) main level
- More than one secondary core at this level is useless, non-functional and displayed with a '+' symbol
- There is a maximum number of secondary cores or DMs in an installation of 250
- Secondary cores in branches are needed to shift the load away from the main, especially when using slower connections
- We recommend installing secondary core at the company (top) main level, even if there are no DMs there for redundancy.

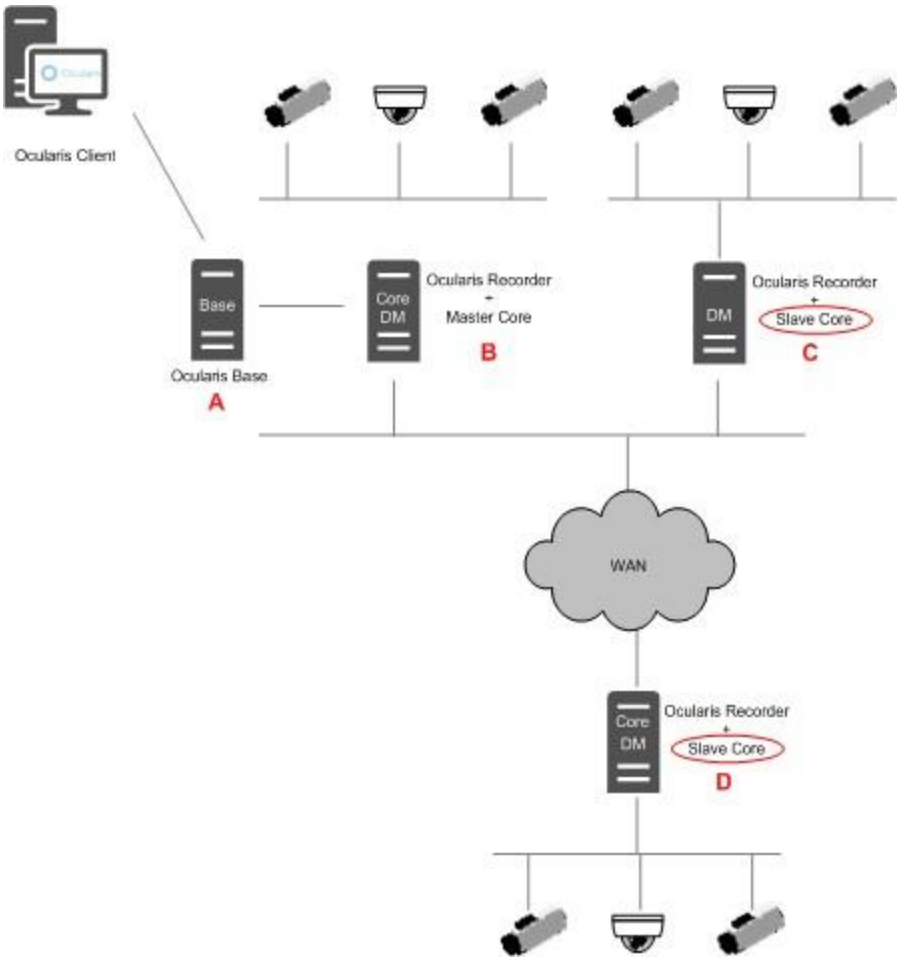
2.5.5.4 The Main – Secondary Core Relationship

When there is an available secondary core in an installation it will synchronize with the main core configuration. The main core will offload much of its work to that secondary (hence the name) so that the main core can concentrate on more important things. The secondary core takes care of handling authorization of clients as well as alarm scenarios. The main core manages the configuration database and handles things like backup, events, and report mode. Once the main core receives events from the secondary core, the events will be deleted from the secondary core. It is important, therefore, to be aware of where a secondary core is installed since its location can actually be a detriment to the system.

In the sample layout shown below, when the operator logs in with Ocularis Client, if there is an available secondary core, it will take over for the main core for user authentication. Since the secondary in this example (on server D) is not on a local network, performance is dependent on the bandwidth across the WAN. This will likely cause sluggish performance for the operator at best.



In this case, you should add a secondary core to Server C alongside the DM.



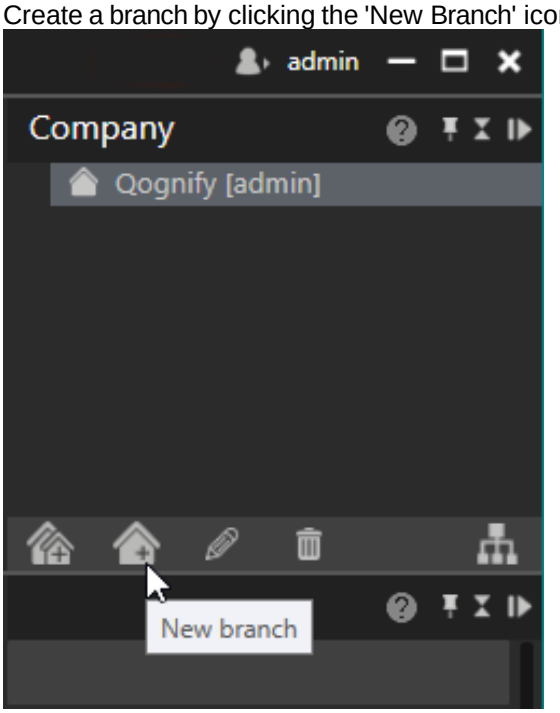
Having a secondary here makes more sense. However, we now just broke the first general rule about not having more than one secondary at the company level. Therefore, we need to add a branch to accommodate the remote secondary core.

With Ocularis v5.6, you can now also assign a specific branch to a user group. This forces Ocularis Client to use a local secondary core which maximizes efficiencies. For more details, refer to the *Ocularis Administrator User Manual*.

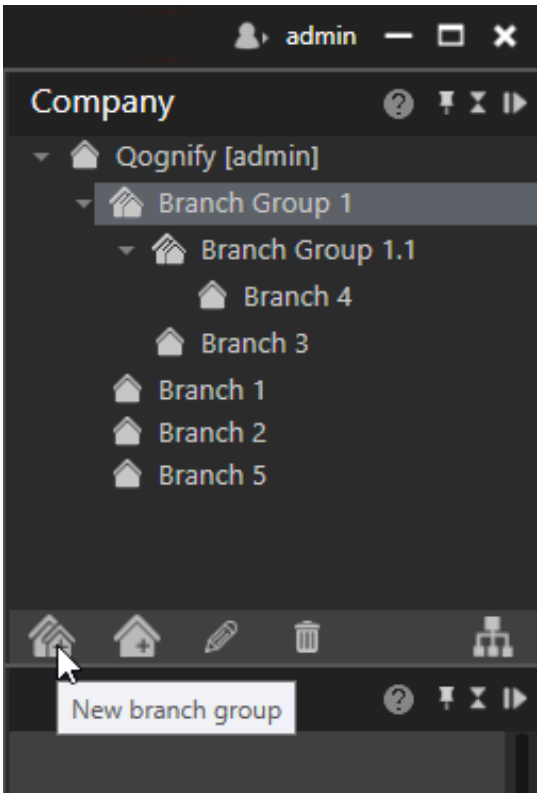
2.5.5.5 Creating Branches

Branches in the Ocularis Recorder Manager are used to organize a structure within the recording components. They also serve the purpose of providing a means to allow multiple secondary cores to function. If there is more than one secondary core at the company top level, only one is functional. All others will be displayed with a '+' symbol. If you see this, it means the secondary core is non-working.

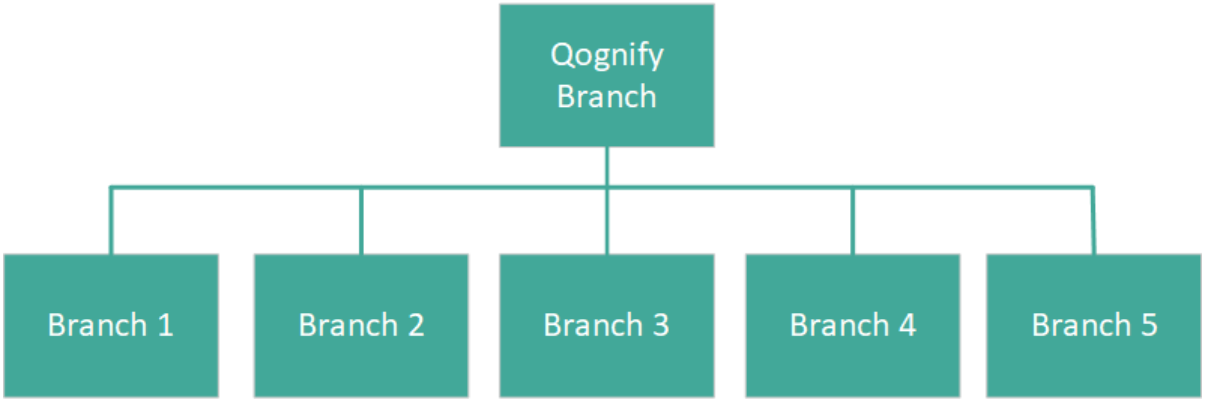
Create a branch by clicking the 'New Branch' icon in the uppermost portion of the control bar as shown below.

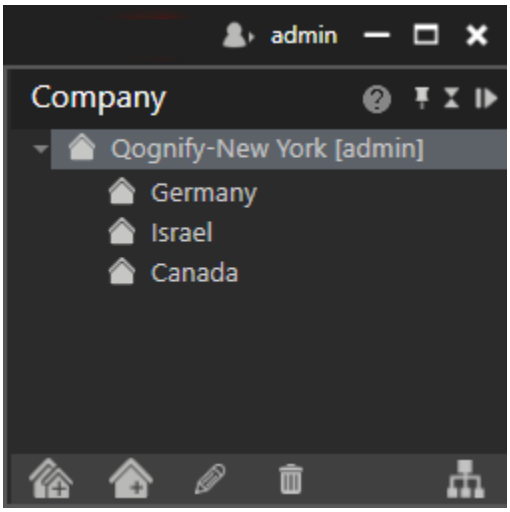


There can only be one true level of branches. Branches cannot have sub-branches. However, a branch group may be created to create the illusion of a hierarchy. Use the 'New branch group' icon to create one. For example: in the figure below there are five branches. All branches technically stem from the Company top level despite the appearance that Branch 4 is somehow a sub branch of Branch 3. Branch folders are simply used to organize the screen.



The actual layout is shown here:

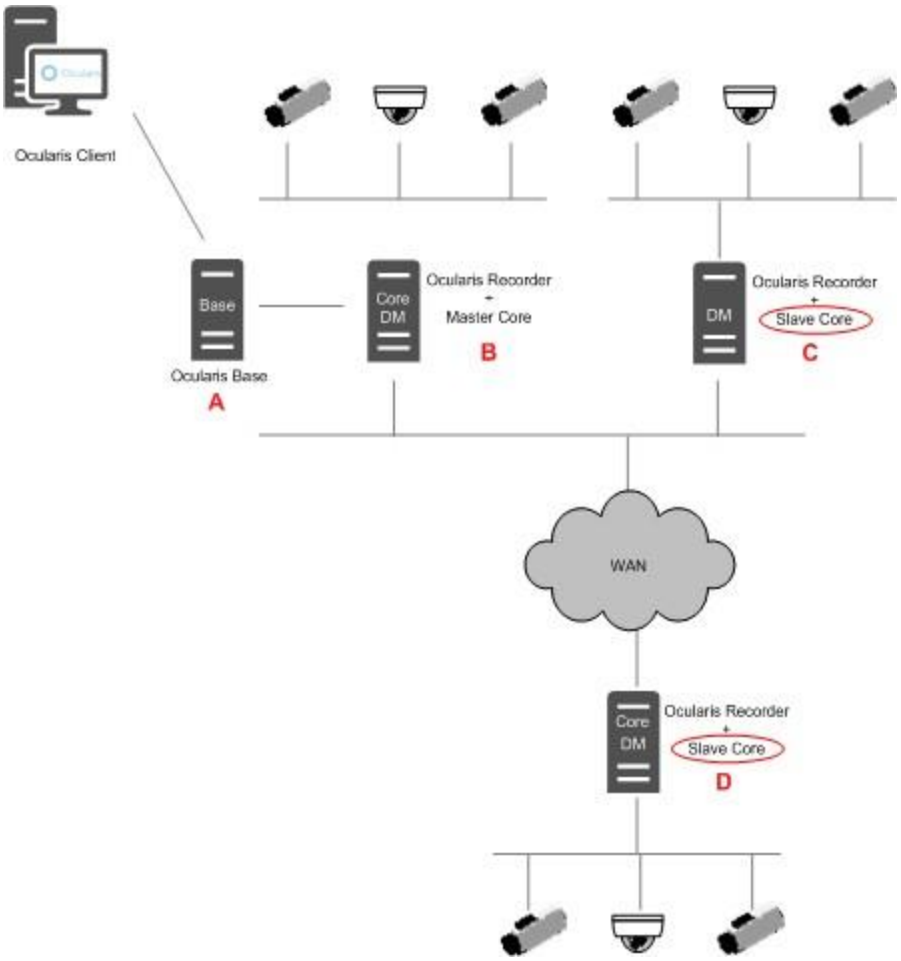




Branches can be organized in many different ways. You may, for instance, want to organize branches geographically.

Here you can organize local resources such as secondary cores, DMs, cameras, etc. within each branch. You can create a user account at the branch level for local administrators to configure only their branch.

Another common use of branches is to create a branch for each server. For example: the layout shown here:



might look like this:

Creating one branch will allow the secondary core on Server D to concentrate on local tasks while the secondary core on Server C can deal with tasks on that side of the firewall.

Alternately, you can also set up a branch for Server C.

Then, you can place resources within a given branch.

- The main core will always be in the top level.
- One or more Device Managers can also be at the top level.
- The secondary core on Server C can be at the top level or in the Server C branch.
- Server D should be in a branch and have its own secondary core and DM.

NOTE: branches and branch groups are not visible in Ocularis Administrator.

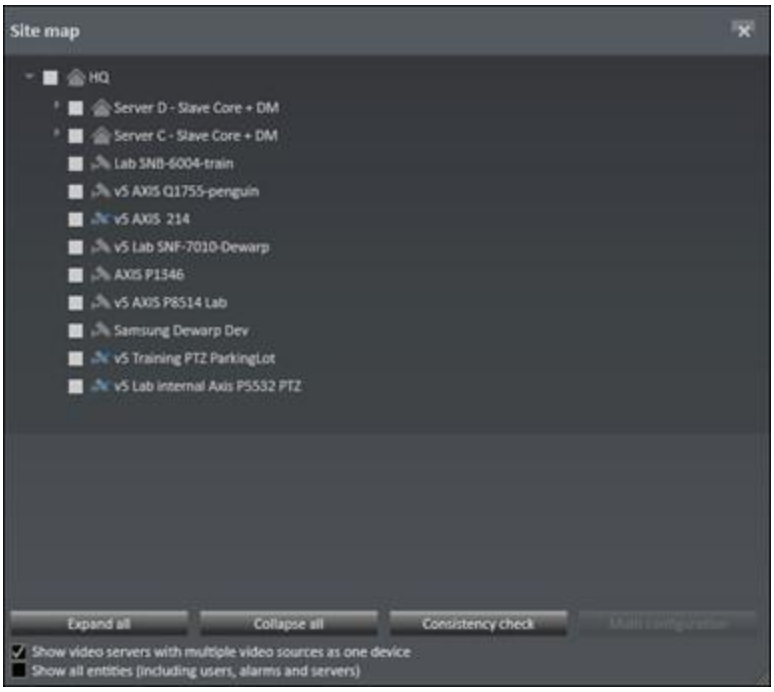
To Place a Resource in a Branch

Among other things, the Site Map is used to move objects to or between branches.

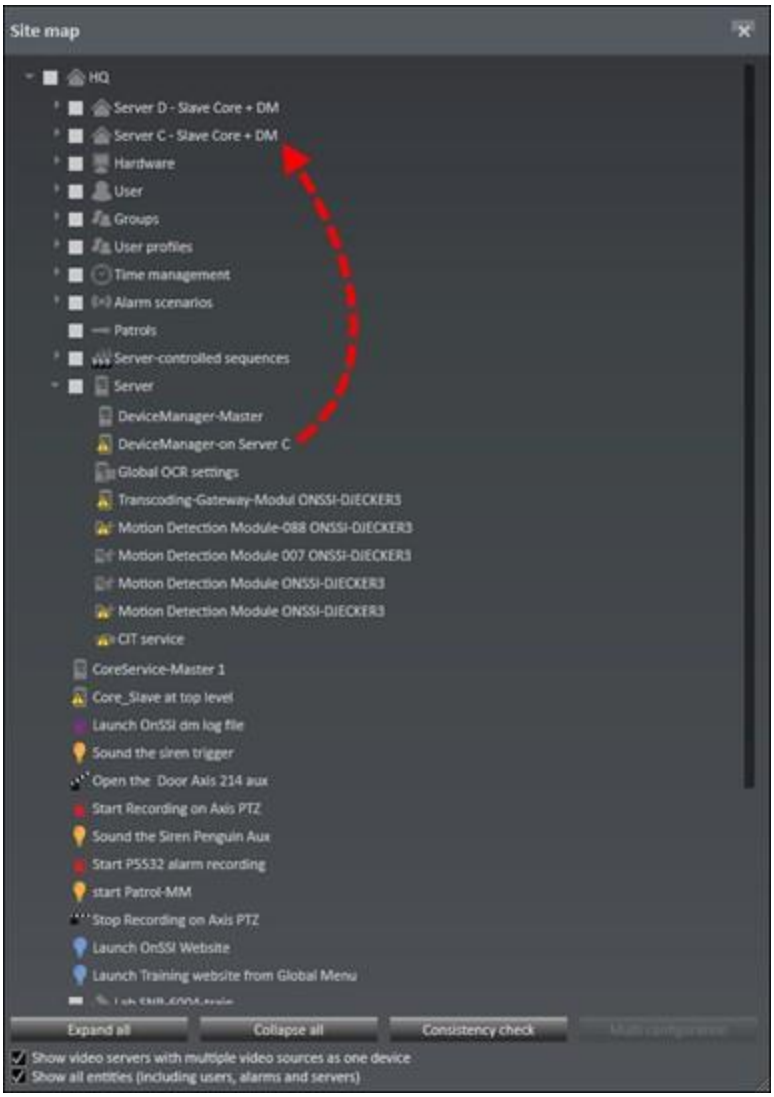
1. First, create the resource (e.g. camera, user, device manager, etc.) in the main/top-level branch[1].
2. Create the branch (if not already done).
3. Click the 'Site Map' icon located in the upper right portion of the Control Bar.

A pop-up appears displaying branches and video sources.

[1] If you are using multiple secondary cores, it is recommended to have one installed at the top level before installing secondary cores intended for branches. When you first install a secondary core, it is located at the top level until you associate it with a branch. If there is no secondary core already at the top level, the secondary intended for the branch will be given tasks to perform before you have a chance to associate it with a given branch. This can cause it to potentially overload due to poor bandwidth.



- Click 'Expand all' to be sure all levels are visible.
- To see all objects, click the box for 'Show all entities (including users, alarms and servers)'.



4. Drag and drop the resource from the list to the desired branch.
5. Repeat for each resource.
6. Click the branch name to see resources associated with that branch.

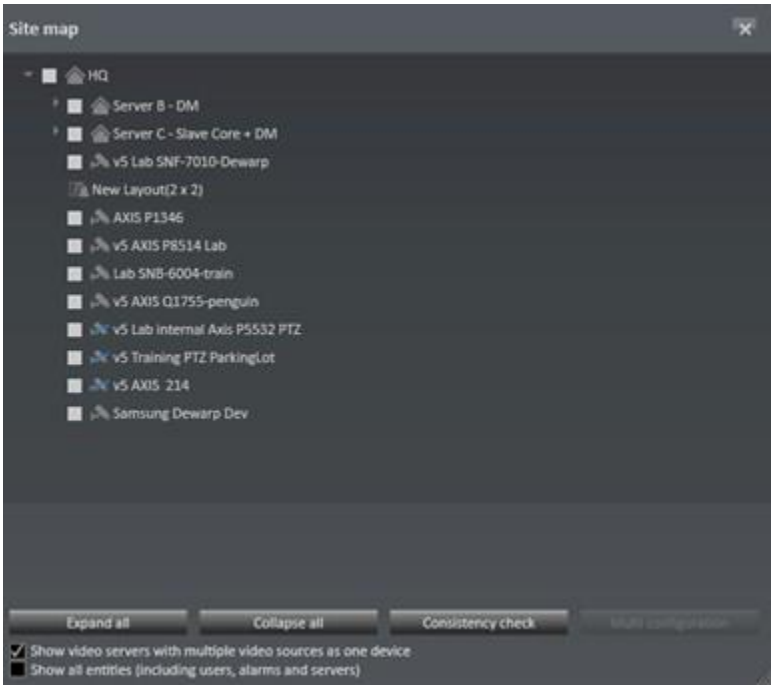
Resources may only be moved between branches by an administrator at the top level branch. It is recommended to move the following resources to the branch level including:

- Secondary cores on the branch
- Device Managers and corresponding cameras
- Alarm scenarios associated with the device manager
- VA Motion Detection (MD) modules related to the cameras

Also, moving objects between branches may cause inconsistent references. Therefore, it is important to perform a consistency check.

To Perform a Consistency Check using Site Map

1. Open the 'Site Map' icon in the upper right portion of the Control Bar.
2. A pop-up appears displaying branches and video sources.



   - Click 'Expand all' to be sure all levels are visible.
   - To see all objects, click the box for 'Show all entities (including users, alarms and servers)'.
3. Click the **Consistency check** button to perform a check. A 'No problems found.' message should appear if everything is ok.

If there are inconsistencies, you will see a pop-up identifying them.

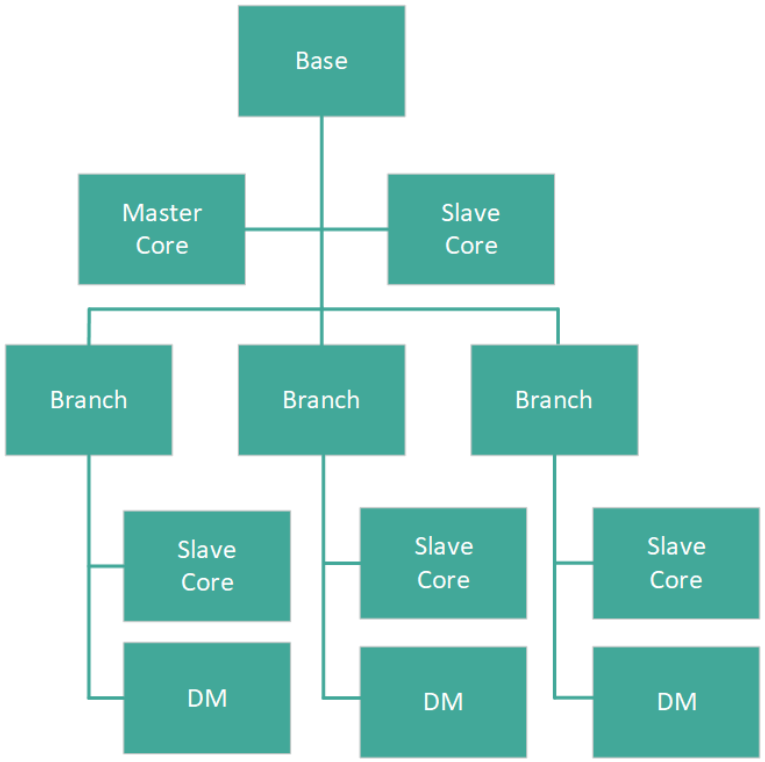
Lastly, you may use the Site Map as another way to configure multiple devices. Check the devices you want to configure as a group and then click 'Multi configuration'. It will launch the Multiple IP camera con- figuration screen and allow you to configure shared parameters as a group.

2.5.5.6 Best Practices with Branches

These items apply to Ocularis ENT and ULT:

- For installations in a single physical location, the recommendation is to use one main core and one secondary core.
- For multiple locations connected over a WAN:
  - If there is a good connection between each site, the recommendation is to use one main core and DM. Additional physical locations should have one secondary core installed along with one or more DMs in branches.

  - If there is poor connection between each site, the recommendation is to use one main core on each Device Manager (DM) server. Additional main core licenses are available at no charge.
- In *Ocularis Administrator*, assign each user group to its local branch.
- In situations where NAT is used between sites, it is recommended to install separate main cores at each remote site.
- If there is no connectivity between sites, each site is an independent system requiring its own Ocularis Base and recorder (and corresponding SLCs).
- NAT is not supported between a core and a DM.
- If you distribute administration of the system to multiple people, create a user account in their branch. Be sure to grant them access rights to the devices and objects in the branch.
- For maximum redundancy and performance, for each physical location, install a branch with a secondary core alongside one or more Device Managers.
- You should also associate Device Manager (DM) cameras with the DM branch. This will help with understanding the configuration layout and is useful if you are using multiple administrators to configure individual branches.
- If you are using server side motion detection, for each branch with a DM, associate corresponding VA MD modules with thatbranch.
- For cameras, folders may be used as another level of organization. Folders help you organize your objects further especially if you have a long list of items. Folders only serve the purpose to help you visually. For instance: for each branch you may decide to organize cameras by Indoor vs. Outdoor, PTZ vs. Fixed.
- Install a secondary core at the top level.



2.6 Licensing model

Each IP address requires one license, e.g. an encoder with four IP addresses requires four licenses.

3 Installation

3.1 Information on installation

- Ocularis Recorder must not be installed on a compressed drive, since this can result in problems with the database. A drive on which Ocularis Recorder 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.
- The Ocularis AutoUpdater (Update Service) is always installed by default.

3.2 Virus scanning

Web guard and internet security features must not be installed.

- To run the 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 Ocularis Recorder 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\Ocularis Recorder*.* (including all sub folders) - do this on a Core Server and/or DM
  - c:\inetpub\wwwroot\OcularisService*.* (including all sub folders) - do this on Ocularis Base server
  - c:\Program Files\Qognify*.* (including all sub folders) - do this on Ocularis Base server
  - c:\Program Files\Common Files\OnSSI*.*
  - Path to Multimedia Database Zone(s)
- Exclude these Windows Services:
  - MAXDB:SEETEC
  - VMS_CORE
  - VMS_DM
  - VMS_MDS
  - VMS_UPDATER
  - VMS_UPDATESVR
  - VMS_VA
- Exclude these Windows Processes:
  - VMS_VAS.exe

  - VMS_VA.exe
  - VMS_UpdateService.exe
  - VMS_UpdateAgent.exe
  - VMS_MDS.exe
  - VMS_DM.exe
  - VMS-CORE.exe
- Exclude real time network scanning on TCP ports
- Exclude network scanning of the processes starting with VMS_* (e.g. VMS_Client.exe)

3.3 Firewalls

Multiple ports on the server computer must be available by default to allow the Ocularis Recorder software to function correctly in a network environment with a firewall.

These are in the range from 60000 to 60008 (TCP communication), 63000 (TCP, AutoUpdate) and 60007 (UDP, image transmission).

The client must also be accessible at ports 60000-60008, 63000 (TCP) and 60007 (UDP).

The TCP alarm ports of the camera must also be accessible on the server computer that administers a cam- era to guarantee alarm processing.

Some cameras use the RTSP over RTP over UDP standard for MPEG4 image transmission. In this case, the server sends the requirements (e.g. frame rate and resolution) to the camera via TCP port 554. The cam- era sends the image data to the server via a UDP port.

The corresponding ports must therefore not be blocked between the camera and the server.

3.4 Setup types

- **Manager & Server**. This installation type installs the main core server, device manager and Ocularis Recorder Manager on the computer.
- **Manager**. This installation type installs only the Ocularis Recorder Manager software.
- **Device Manager**. This installation type installs only the device manager (recorder) services for the cameras (DM/MDB) on the selected computer.
- **Custom**. In a Custom or user-defined installation, it is possible to install only specific components on a computer. Use this option when installing a secondary core.

  For detailed instructions on software installation, refer to the document *Ocularis Installation & Licensing Guide* on the Qognify website.

3.5 System requirements

3.5.1 Known limitations

The performance requirements of the 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.

Note that the hardware requirements depend very greatly on the configuration. Ocularis Recorder is based on an advanced software architecture in response to technological progress. Qognify recommends a 64-bit operating system in order to enable the use of the Ocularis 64-bit Client.

3.5.2 Requirements for the Help system

- Current browser (e.g. Mozilla Firefox, Internet Explorer, Google Chrome) with JavaScript activated
- For the PDF-based help file Adobe Reader is recommended

3.5.3 Hardware Requirements

For detailed up-to-date hardware requirements for each component, go to the Qognify website at: https://www.qognify.com/support-training/hardware-recommendations/

3.5.4 Installing the Windows 'Desktop Experience'

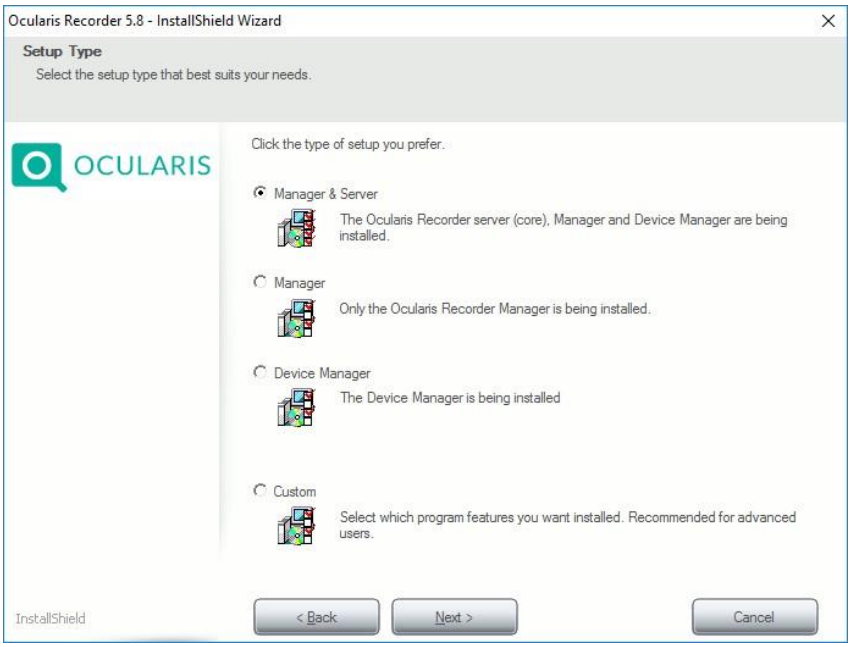
For servers which include a VA module (which is typically the same server as the corresponding device manager), a component of Windows Media Player is required for Server Side Motion Detection to properly function. This component is not normally installed by default on a Server level operating system. Install the 'Desktop Experience' feature available within the 'Programs and Features - Add Windows Features' section in the Windows Control Panel.

1. Open the Server manager.
2. Select **Manage**.
3. Select Add Roles and Features.
4. Select **Features**.
5. **Select** User Interfaces and Infrastructure (Installed)**.**
6. Select Desktop Experience.
7. Click **Add Features** and then click **Next**.
8. Click **Install**.

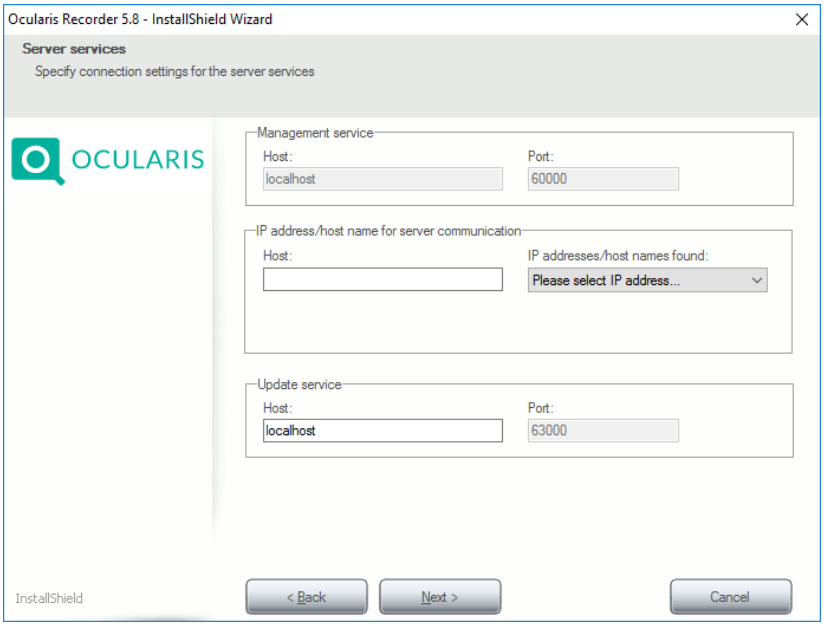
3.6 Standard installation

The standard installation installs the system with the configuration application (called the 'Ocularis Recorder Manager'), and device manager and main core on a single system ('Manager & Server').

1. From the ‘Ocularis Component Downloads’ web page, click the **Download** button next to Ocularis Recorder.
2. Choose to **Run** the application to launch the installer.
3. Select the installation language. You can configure the language of the user interface after installation.
4. Click **OK** to start installation.
5. At the Welcome screen, click **Next**.
6. Read the software license agreement, accept the terms and then click **Next**.
7. Change the destination folder if desired. Click **Next**.



8. Select 'Manager & Server' as the Setup Type and click **Next**.



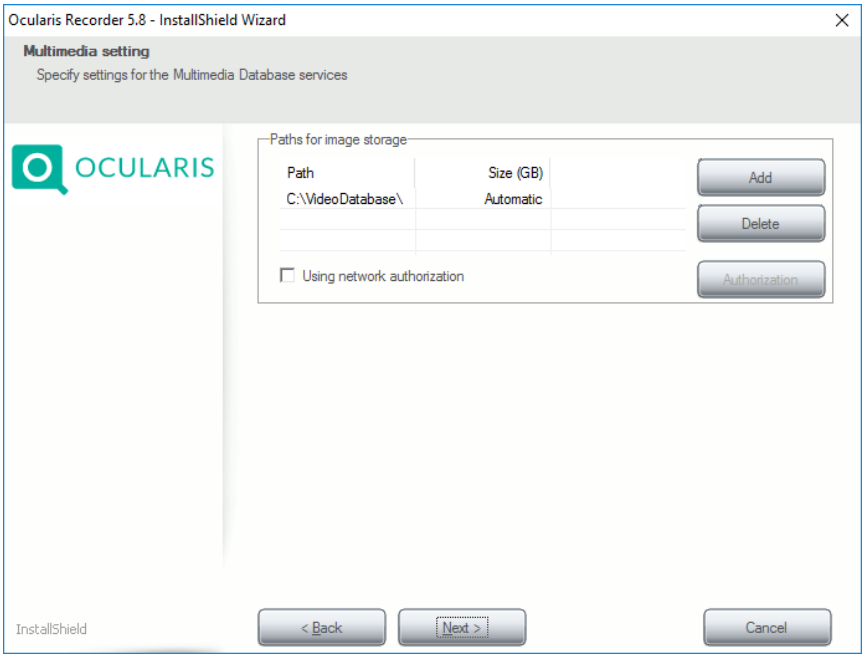
The port number of the Management service (Main Core) is set at '60000'. If the port number must be changed, contact Tech Support.

9. In the Host field under 'IP address/hostname for server communication', enter the IP Address for the Device Manager. Select it from the drop-down list labeled 'IP addresses/host names found'. This should be the IP Address of the computer you are running the installation on.

NOTE: Neither the IP 127.0.0.1 nor the host name ‘localhost’ may be used in this field.

In the *Update service* section, 'localhost' is acceptable if you are installing the UpdateService SVR on the Main Core Server. This is the default value and is recommended. See Update Service for more information on the Update Service.

10. Click **Next.**



11. Recommended – change the default location (or 'Zone') for video storage to a drive other than the C: drive. You can add one or more additional locations or 'zones' for video storage now or after the software has been installed. Use a sub-folder and not the root of a drive for a zone.

If the folder is created on a network drive, enter the complete UNC path.

NOTE: Example: \\IP Address\Release name\path

If the network drive is protected with a user name and password, select Using network authorization and click Authorization.

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").

Notes About Zones:

- A zone should never be as large as the available maximum storage space on the hard disk.
- The hard drive's cluster size should be 64KB.
- You can use a maximum of 10 zones per DM; each zone should be on its own dedicated partition; it is better to have few larger zones than many smaller zones that this impacts performance
- It is recommended to store video data on a separate hard disk or RAID system. Do NOT use a hard disk connected via USB or firewire.
- Zones on the network may be identified with a UNC path. You also need to provide network username and password.
- Always use a sub-folder for a zone and not the root directory.

12. Click **Next**.
13. Click **Install**.

When asked, accept the EULA (End User License Agreement) for installing the Microsoft DirectX 9 component. This window may appear behind the R16 installation window.

You may be asked to restart the computer.

The Ocularis Recorder components: Core Service Main, Device Manager and Ocularis Recorder Manager are now installed on your computer.

3.7 Ocularis Recorder Manager installation

The 'Manager' refers to the software used to configure the Ocularis Recorder (Core and Device Managers). This is called 'Ocularis Recorder Manager'. This application is installed when you choose the 'Manager & Server' option from the prior section. However, you may want to also install this application on remote computers, allowing you access to configure the recorder from anywhere on the network.

From the main recorder installation on the Ocularis Component Downloads page:

1. From the 'Ocularis Component Downloads' web page, click the **Download** button next to Ocularis Recorder.
2. Choose to **Run** the application to launch the installer.
3. Select the installation language. You can configure the language of the user interface after the installation.
4. Click **OK** to start installation.
5. At the Welcome screen, click **Next**.
6. Read the software license agreement, accept the terms and then click **Next**.
7. Change the destination folder if desired. Click **Next**.
8. Select 'Manager' as the Setup Type and click **Next**.
9. Click **Install** to begin the installation.

3.8 Installation of a Device Manager

In the Device Manager only installation, the database modules for the video database are installed together with the Ocularis Recorder Manager on a different computer from the already installed Ocularis Recorder Manager and Core server (Main). The Device Manager reduces the utilization of the core server because the image database is located partially or entirely on another server.

NOTE: In order to configure the Device Manager server, you need an installed and configured Ocularis Recorder Manager and Primary Core server.

1. From the 'Ocularis Component Downloads' web page, click the **Download** button next to Ocularis Recorder.
2. Choose to **Run** the application to launch the installer.
3. Select the installation language. You can configure the language of the user interface after installation.
4. Click **OK** to start installation. You may be asked to install Microsoft Visual C++.
5. At the Welcome screen, click **Next**.
6. Read the software license agreement, accept the terms and then click **Next**.

7. Change the destination folder if desired. Click **Next**.
8. Select 'Device Manager' as the setup type and click **Next**.
9. In the Management service area, specify the IP address of the Main Core in the Host field. Leave the port number unchanged at'60000'.

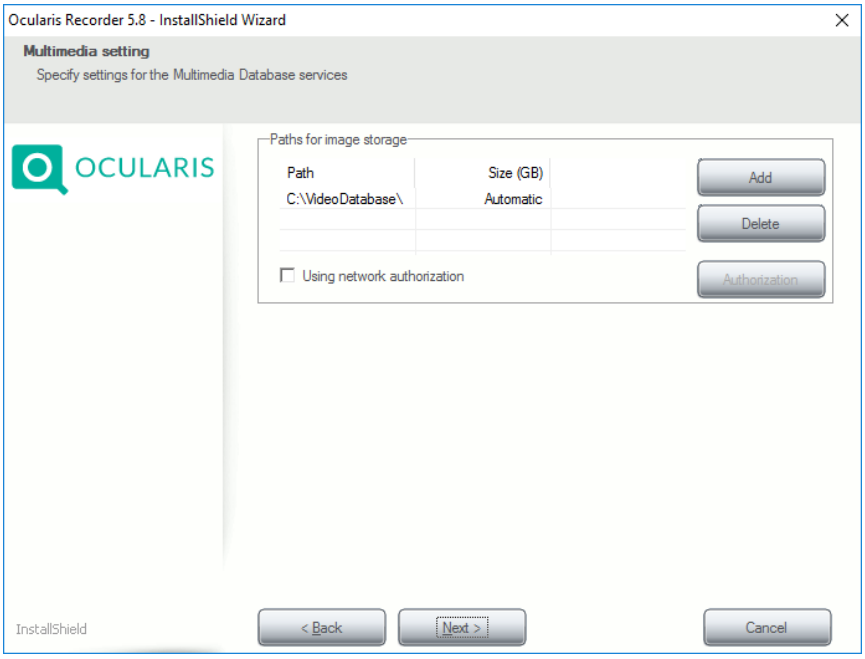
NOTE: It is important to enter the IP address of the Primary Core in the Host field of the Management ser- vice area in order for the system to function properly. Leave the port as 60000.

In the IP address/host name for server communication section, the IP address of the Device Manager should be placed in the Host field. This can be done by selecting it from the IP address/host names found in the drop-down list. The list shows you all of the existing network addresses and host names of the PC or server. If there is more than one network adapter on this computer, be sure to select the correct one.

NOTE: Neither the IP 127.0.0.1 nor the host name ‘localhost’ may be used in this field.

In the Update service section, enter the IP address where the UpdateService SVR (Server module) is installed. This is most likely the IP address of the Main Core Server since this is the default. See Update Service for more information on the Update Service.

10. Click **Next**.



11. Recommended - change the default location (or 'Zone') for video storage to a drive other than the C: drive. You can add one or more additional locations or ’zones’ for video storage now or after the software has been installed. Use a sub-folder and not the root of a drive for a zone.

If the folder is created on a network drive, enter the complete UNC path.

NOTE: Example: \\IP Address\Release name\path

If the network drive is protected with a user name and password, select Using network authorization and click Authorization.

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").

Notes about Zones:

- A zone should never be as large as the available maximum storage space on the hard disk.
- The hard drive's cluster size should be 64KB.
- You can use a maximum of 10 zones per DM; each zone should be on its own dedicated partition; it is better to have few larger zones than many smaller zones that this impacts performance
- It is recommended to store video data on a separate hard disk or RAID system. Do NOT use a hard disk connected via USB or firewire.
- Zones on the network may be identified with a UNC path. You'll also need to provide network username and password.
- Always use a sub-folder for a zone and not the root directory.

12. Click **Next**.
13. Click **Install**.

When asked, accept the EULA (End User License Agreement) for installing the Microsoft DirectX 9 component. This window may appear behind the R16 installation window.

You may be asked to restart the computer.

The Ocularis Recorder components: Device Manager and Ocularis Recorder Manager are now installed on your computer.

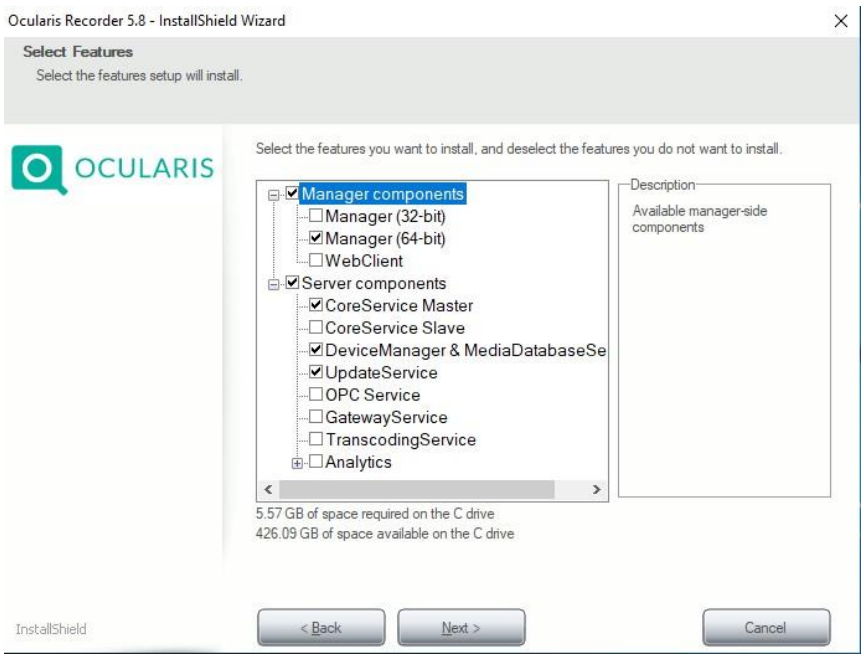
3.9 Custom installation

In a Custom installation you can install selected modules. For Ocularis Enterprise and Ultimate, use the Custom option when you want to install a secondary core that serves as a redundant server and thus increases the reliability of the main core server.

For a description of the components for the user-defined installation, see **Components for the Custom installation**.

3.9.1 Procedure

1. From the 'Ocularis Component Downloads' web page, click the **Download** button next to Ocularis Recorder.
2. Choose to **Run** the application to launch the installer.
3. Select the installation language. You can configure the language of the user interface after installation.
4. Click **OK** to start installation. You may be asked to install Microsoft Visual C++.
5. At the Welcome screen, click **Next**.
6. Read the software license agreement, accept the terms and then click **Next**.
7. Change the destination folder if desired. Click **Next**.
8. Select 'Custom' as the setup type and click **Next**.



9. 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.
   If in doubt, contact Tech Support for advice on which component to select.
10. Click **Next**.
11. Click **Install**.
12. When asked, accept the EULA (end user license agreement) for installing the DirectX 9 component.

The modules and services are now installed on your computer.

3.9.2 Components for the Custom installation

The following components are available.

3.9.2.1 Manager components

- **Manager (32-bit)**: The Ocularis Recorder Manager for 32-bit and 64-bit operating systems
- **Manager (64-bit)**: The Ocularis Recorder Manager only for 64-bit operating systems
- **Web client**: This component is not used with Ocularis

3.9.2.2 Server components

- **CoreService Main**: The main core services and management database
- **CoreService Secondary**: The secondary core services and management database for redundant system management. Secondary and main 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 recorder component system (see Installing and configuring the UpdateService and the UpdateAgent)
- **OPC Service**: The "Open Platform Communications" interface provides a standardized data exchange between applications and devices in real time. This component is not currently used with Ocularis.
- **GatewayService**: The GatewayService is required to use mobile and Web clients. This component is not currently used with Ocularis.
- **TranscodingService**: The TranscodingService is required to use mobile and Web clients for the recorder web client. This component is not currently used with Ocularis.
- **Analytics**: The server side components for VideoAnalytics features (e. g. Analytics, License plate recognition); This is for third party analytics.

3.10 Updating the system with the Auto Updater (Update Service)

With the AutoUpdater you can keep all recorder 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 AutoUpdater system consists of two components, the UpdateService and the UpdateAgent(s):

- The UpdateService (SVR): Immediately after the installation and then periodically, the Update Service (SVR) checks if there are new patches or updates available and distributes them to the connected UpdateAgents. By default, the UpdateService is installed on the Core Service Main server. Optionally the Update Service can be installed on another server.
- The UpdateAgent(s): An UpdateAgent is automatically installed with any recorder component (DM, Ocularis Recorder Manager, 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.

3.10.1 Installing the UpdateService

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

NOTE:	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 Customization and repair). Before installing updates with the UpdateService (e.g. from R9 to R10), update all UpdateAgents

with the current UpdateService.

NOTE:	Always check the current version's Release Notes for any specific instructions on using the Update Service that may be unique to a particular software version

1. Select the server that runs the 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.

3.10.2 Configuring the UpdateService

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

For configuration settings, see **UpdateServer Configuration Tool**.

3.10.3 Configuring and updating the UpdateAgent

The UpdateAgent is a service that is installed automatically on each computer where a recorder component (e.g. Core Service, Ocularis Recorder Manager, DeviceManager, VA-Service etc.) is installed. During the installation process the IP address of the UpdateService server component must be provided. 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.

3.10.4 Manually changing the IP settings for the UpdateAgent

1. Stop the UpdateAgent with the Ocularis Recorder ServiceManager (see **Starting and stopping the services**).
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 Ocularis Recorder ServiceManger (see **Starting and stopping the ser- vices**).

Example

updateclient.conf.xml

```
<?xml version="1.0"?>

<ServerInformation xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd-d="h- ttp://www.w3.org/2001/XMLSchema">

<ip>10.0.8.131</ip> <port>63000</port>

</ServerInformation>
```

3.10.5 Manual updating

Generally, the Ocularis Recorder system can be patched or updated automatically by the AutoUpdater. If the AutoUpdater is configured correctly, uninstalling the previous version of Ocularis Recorder is not required before updating to a newer version.

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

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

NOTE: Always check the latest Release Notes for any specific instructions that may apply to a particular upgrade

3.10.6 Modify, repair and remove

1. Open the Windows Control Panel and select **Programs**.
2. Select Programs and Features.
3. Select Ocularis Recorder 5.x.
4. Click Change or Repair.
5. Select one of the following options:
   - To install or uninstall additional components select "Modify" and then click **Next**. This allows you to carry out a custom installation, in which you can install and uninstall the modules and services you choose.
   - To repair the program, select "Repair" and then click **Next**. The system tries to repair and reinstall any damaged program components itself.
   - To remove the program from the hard disk, select "Remove" and then click **Next**. All components of the program 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\Ocularis Recorder folder in "C:\Program Files" manually.

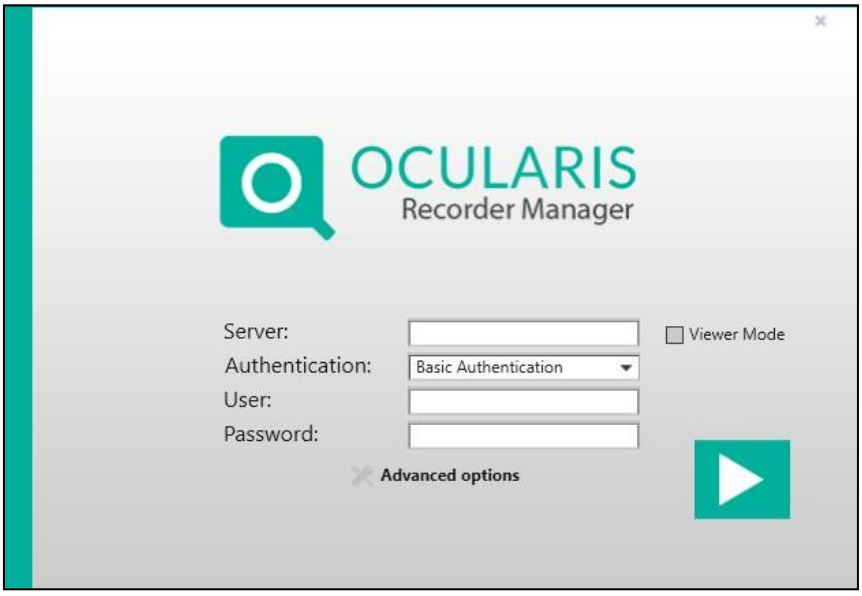
4 Login

Once the system is installed, you must log in to the main core service using the Ocularis Recorder Manager.

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

4.1 Procedure

1. Start the Ocularis Recorder Manager from the desktop icon.



2. Enter the IP address of the server with the Main Core installed. You may use 'localhost' if you are located on the same computer.
3. Select Authentication type. Basic Authentication is most often used unless using Windows Active Directory.
4. Enter the name of the **user** and the **password**. Make sure the user name and password are entered correctly, because the system distinguishes between upper and lower case (case-sensitive). If this is the first time you are logging in use: User: **admin** Password: **admin**.
5. Apply your entry by clicking green triangle.

NOTE: 'Viewer Mode' is not used.

4.2 Logging in for the first time

1. When you log in for the first time, you must modify the default user password.
2. By default, "Enforce secure password" is selected. The rules for secure passwords are: minimum of 8 characters, at least one number, one upper-case letter and one lower-case letter.
3. Enter the new password twice.

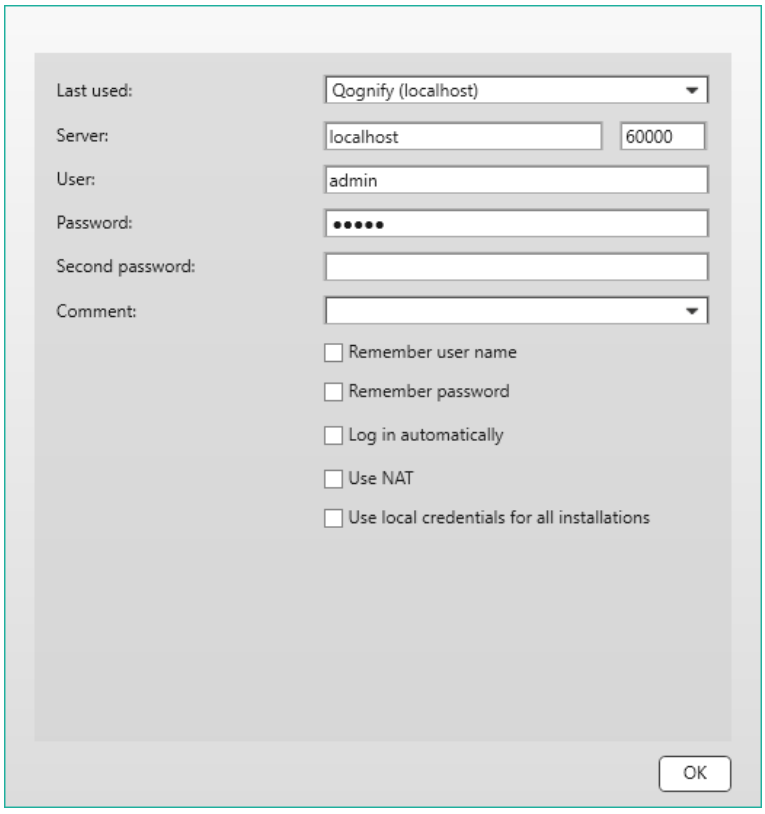
4. Bypass the entry of a second password as it is not used with Ocularis.
5. Click **OK**.

NOTE: Important: DO NOT FORGET THE ADMIN PASSWORD. If you forget the admin password and no additional users have been created in the administrator group, it will no longer be possible to access the system configuration setting.

4.3 Advanced options

In the advanced options you can configure additional user management functions.

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

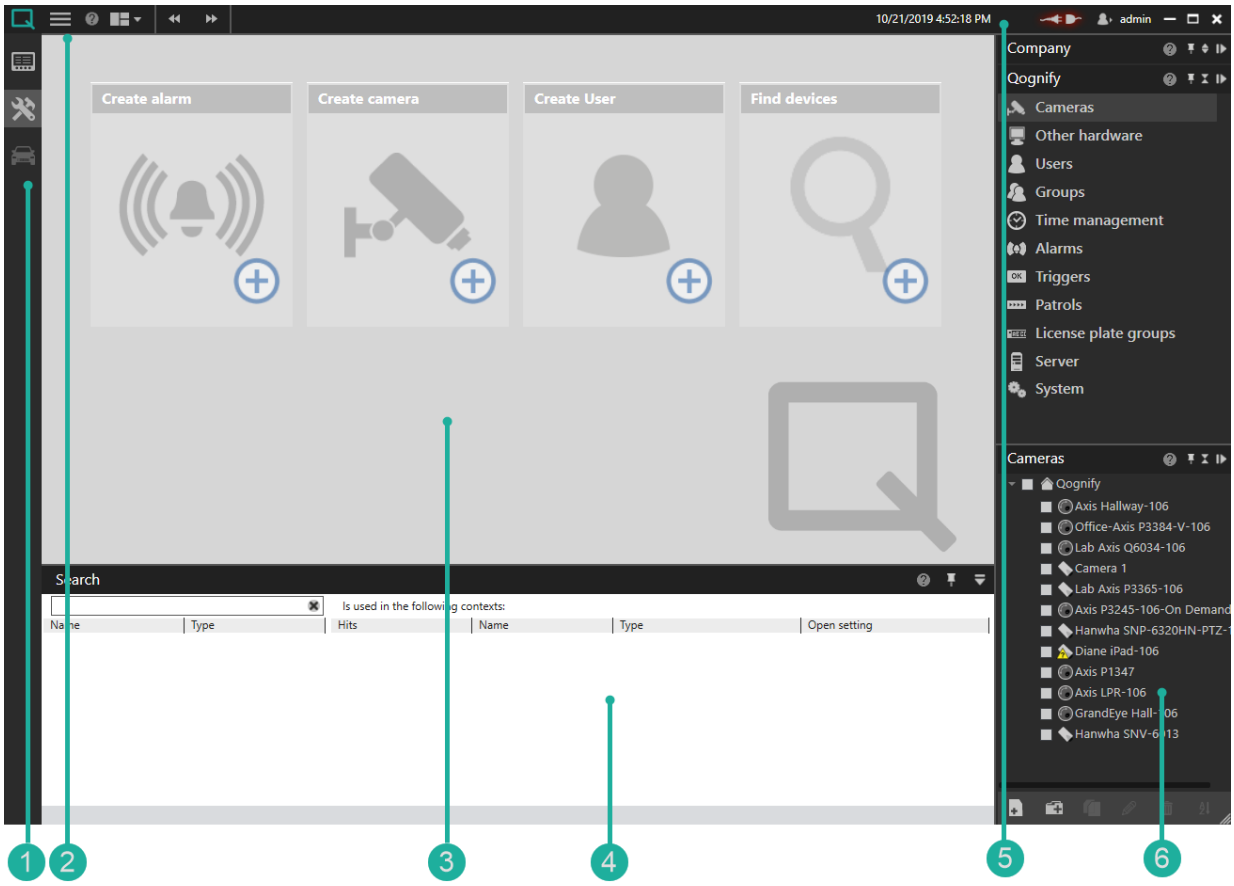


2. From the drop-down list, you can select a different server from previously connected servers with the **Last used** drop-down list.
3. Enter the hostname or IP address for the main core you are logging into under **Server**. Localhost is supported. Modify the port number if necessary but 60000 is the default.
4. Enter the **User** and **Password** for the log in account.
5. Ignore the **Second password**field.
6. Optional: In the drop-down **Comment** list, select a comment or enter a new comment. Commenting can be used to store additional information for the selected login.
7. Select **Remember user name** and **Remember password** in order to avoid having to specify the user data. The system enters the specified user name and password in the login window. **Note: due to legal regulations, in France the user name and password may not be saved for install- ations.**
8. Select **Log user in automatically** to go straight to the user interface when the program starts up.(not recommended).
9. Select **Use NAT** to use the Ocularis Recorder Manager to configure a different core over the Internet. Deselect this option if no internet connection is required. This option requires NAT-settings in configuration mode.
10. Ignore the Use local credentials for all installations checkbox.

NOTE: 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.

DO NOT FORGET THE ADMIN PASSWORD!

5 The user interface



The user interface is subdivided into different sections:

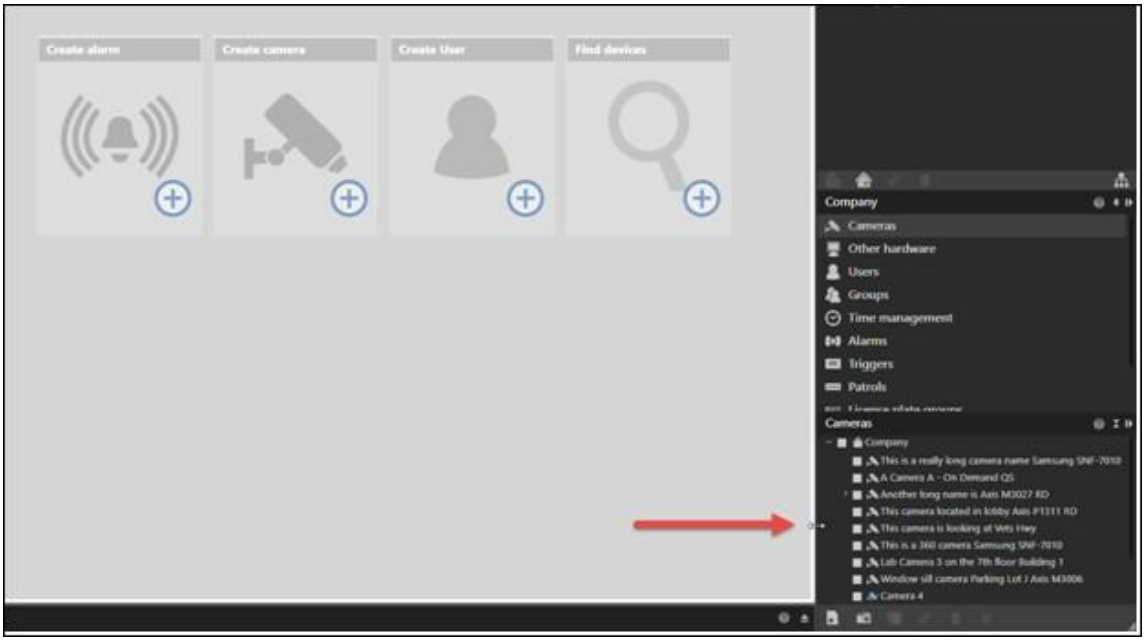
- The **mode bar** (1), which allows you to select the modes (see **The mode bar**)
- The **function bar** (2), provides basic operating functions that can very slightly depending on the mode used (see **The menus**)
- The **Work area** (3), is the main window for displaying the selected mode functions. Similar to a browser window, the work area can be displayed on multiple tabs.
- The **Information** control (4), is displayed in the lower part of the work area. The information control is used for displaying search results in configuration mode (see Work area)
- **Login information** (5), displays which user is logged in and providing user switching and easy logout (see **Easy logout**).
- The **control bar** (6), which contains the tabs for controlling the contents of the work area (see **The control bar**)

5.1 Adjustable Column Width

If a camera name or label of any entity in the Ocularis Recorder Manager is longer than twenty-one characters, the item is truncated. You can manually adjust the width of the control bar to accommodate lengthy labels.

Position the mouse cursor on the edge between the main screen and the control bar until you see a double- arrow cursor. 

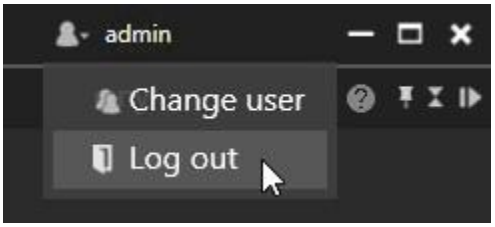
Click and drag left or right to adjust the width of the panels.



The width of the panes will remain in place for all users on the local PC until manually changed again.

5.2 Easy logout

When logged in, the user interface displays the current user in the menu bar.



1. Click on the icon in the menu bar.
2. Click **Change user** to log out the current user from the server. The user can only log in at the same server.
3. Click **Log out** to log out the current user from the server. After logging out, the user can log in to any server.

5.3 The function bar

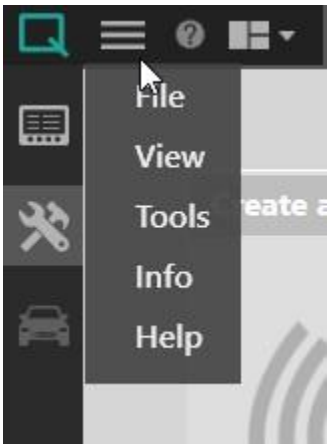
The menu bar contains the menus you can use regardless of the mode you have selected:

- **Menu** icon (1). Click to open the menus: File, View, Tools, Info, Help
- **Help** (2). Launches the browser-based Help system (see **Help**).
- **Layer** menu (3). This function allows the user to close layers (tabs) or open in a separate window.
- **Tabs** (4). Open configuration screens are displayed as tabs on the function bar.
- **Current Date & Time** (5). Displays the current system date and time.
- **User information**(6). Displays the current user and provides functions to quickly log off or change the user
- **Windows controls** (7). Icons to quickly minimize, maximize or close the software window.

5.4 The menus

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

- **File**. Changes the settings of the software, the language, password, profile, installation, installation manager, and switches the user.
- **View**. This menu has no purpose in this version.
- **Tools**. Provides the ability to manually set reference image comparison.
- **Info**. Displays information on the system and license (see **Info**).
- **Help**. Calls the Help system and provides options for solving problems (see **Help**).



5.4.1 File

The menu "File" displays the following options:

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

5.4.1.1 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:

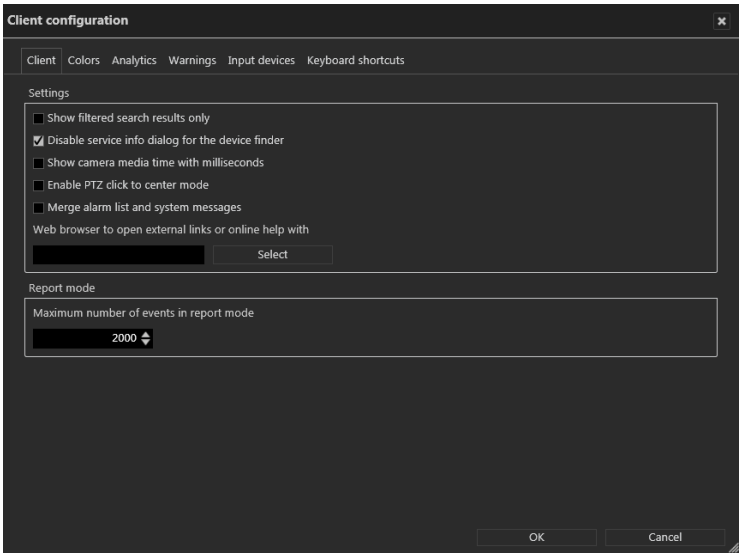
- Client
- Colors
- Analytics
- Warnings
- Input devices
- Keyboard shortcuts

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

Client

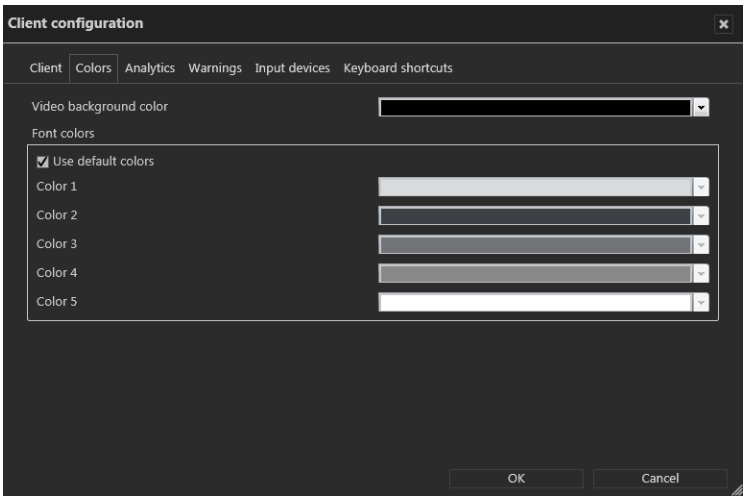
- **Show filtered search results only** to display only the relevant search results in the search results list. If not checked, the search results will be highlighted in the control bar but all items are displayed.

- **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 Device Finder. If the checkbox is checked, the user will be asked to install the service if it is not available.
- Show camera media time with milliseconds - this feature is not used in Ocularis.
- **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
- Merge alarm list and system message
- **Web browser** to open external links or online help with - you can specify which web browser is to be used. If this is left blank, the default web browser will be used for external links or online help.
- **Maximum number of events in report mode** limits the amount of events in report mode.



Changing the font color

The font colors for the user interface can be configured.

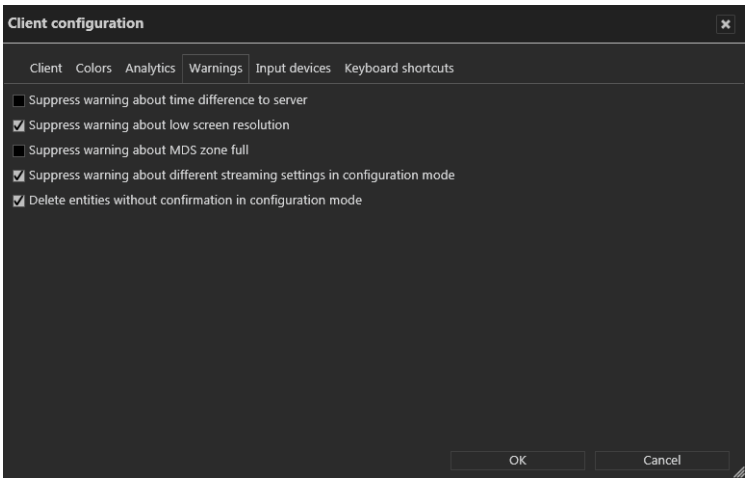


1. Select File...Client Configuration and then the Colors tab. .
2. Set the color for the font
   - **Color 1** on a darkbackground,
   - **Color 2** on a lightbackground,
   - **Color 3** on a mixed background like the main menu,
   - **Color 4** on a mixed background like table headings,
   - **Color 5**.on a video player border (black background).
3. To revert to the default settings, activate **Use default colors**.
4. Restart the Ocularis Recorder Manager for the changes to take effect.

Analytics

This screen is not applicable to this version of Ocularis.

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.
- **Suppress warning about MDS zone full** to prevent a warning when the storage depth limit of the multimedia database is reached.
- **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 in MPEG-4/H.264 recording.
- **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 click the Delete button in configuration mode.

Input devices

(The screen will be blank if there are no connected input devices).

1. Select the **Input devices** tab. All input devices, such as joysticks, that are connected to the system and available before startup of the software are displayed. Any combination of devices is supported. Every device can be configured independently of the others.
2. Select from the list the device you want to configure. The device's functions are listed on the right-hand side of the dialog box.
3. Activate the device.
4. If necessary, activate the z-axis (depending on the hardware).
5. Press the joystick button to which you want to assign an action, and then select the desired action.
6. To use the Axis T8312 keyboard for selecting and displaying cameras, activate **Enable virtual sequence**.

Select and display cameras with the keyboard

Using the Axis T8312 keyboard, a camera can be displayed on a local screen or on a DisplayAgent. To reduce the number of buttons that must be configured, each camera is numbered. Refer to the man- ufacturer's documentation of the keyboard.

1. To display a camera with the keyboard, start by entering a special key combination.
2. Enter a multi-digit number on the number keys of the keypad.
3. Press another special key, then enter the number of the monitor or display agent.
4. Start by pressing the tab bar. It is also possible to show a temporary layer with a joystick button and to show a camera in a tile in such a temporary layer. The keys are assigned as follows:
   - First row:
     - F1: Monitor
     - F2: Display Agent
     - F5: Webpage entity
   - Second row:
     - B1: predefined layer
     - B2: camera

  - B3: Tile
  - B4: temporary layer
  - B5: map
- Last row:
  - Tab: enter

Pattern:

[B1, B2, B3, B4, B5, F5] (number of entity or temporary layer) --> [F1, F2] (number of monitor or display agent) --> [optional: 3] (number of tile of temporary layer that has focus) Tab

Examples:

Opening of cam 444 on monitor 3 in tile 12: B2 F1 3 B3 4 Tab

Opening of cam 444 on monitor 3 in full screen: B2 444 F1 3 Tab

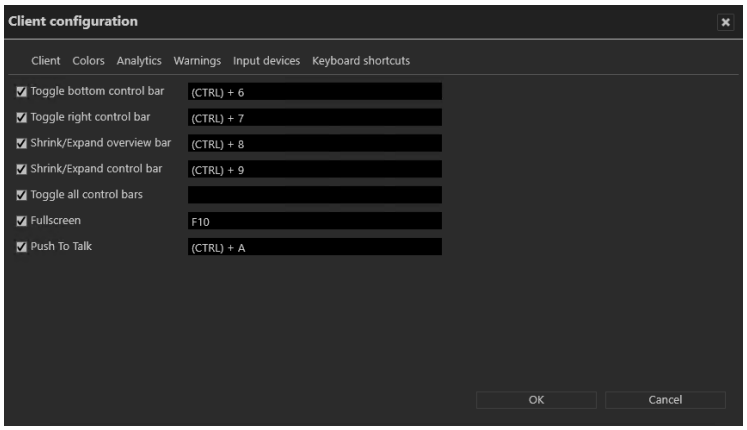
Opening of predefined layer 555 on display agent 2: B1 555 F2 2 Tab

Restrictions and special cases

- The jog dial and shuttle wheel are supported in archive mode for the Axis T8312 keyboard.
- Up to 112 virtual buttons can be configured for the Axis T8312 control unit by selecting the **Enable virtual buttons** option.
- The Axis T8312 keyboard has 9 buttons.
- If you want to assign an action to button 56, press button 5 and 6 in rapid succession, and then select the desired action.
- Specify for **Timeout (ms)** the time period within which the two buttons must be pressed.
- 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

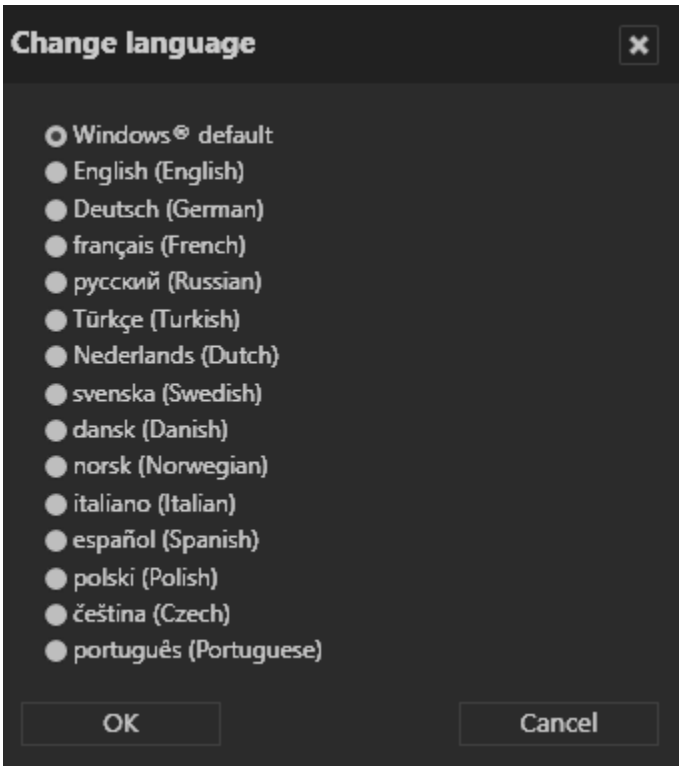
You can define your own keyboard shortcuts for rearranging the client surface.



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: empty)
- Full screen: (default: F10)
- Push to Talk: does not apply to this version of Ocularis

5.4.1.2 Changing the language



The following languages are available for the user interface:

- English
- German
- French
- Russian
- Turkish
- Dutch
- Spanish
- Swedish
- Danish (o
- Norwegian

- Italian
- Polish
- Portuguese

Additionally, you can define the user interface with a user defined language (see "Technical Guide").

1. Choose **Change language** from the **File** menu, and then select the desired language. If you select the **Windows default**, the operating system's language environment is used.
2. Click **OK** to apply your selection, and then restart the client.

5.4.1.3 Changing the password

You can change the user's password at any time.

To allow the user to change the password, the respective setting has to be activated in the configuration menu in the File menu (see **File**).

1. Choose **Change password** from the **File** menu, and then enter the new password for the current user.
2. Enter the newpassword.
3. Click **OK** to apply thepassword.

5.4.1.4 Changing the user

If multiple users are created, you can change to a different user.

1. Choose **Change user** from the **File** menu, and then 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**).

5.4.1.5 Switching installation

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

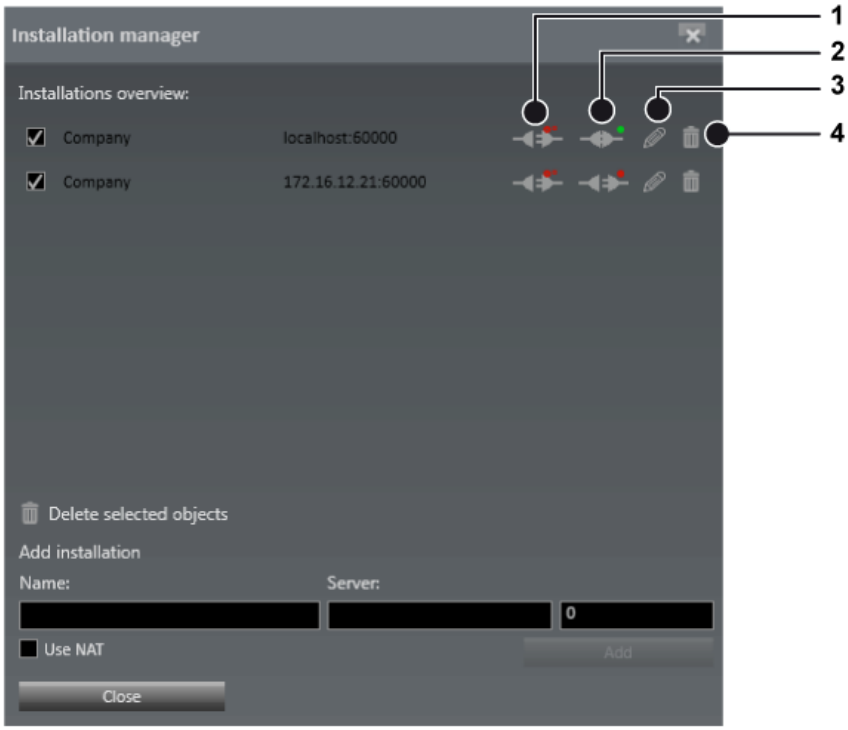
1. Choose Switch installation from the File menu.
2. Enter the server name or IP address and the user name and password.

The current installation is terminated, and the selected installation is started.

5.4.1.6 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.



- **Autoconnect** (1): Activates or deactivates the client to connect to the selected installation automatically.
- **Connect** (2): Connects the client to the selected installation
- **Edit** (3): Allows editing the installation's connection settings
- **Delete** (4): Removes the installation from the list

Requirements

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

Select and add an installation

1. Choose **Installation-Manager** from the **File** menu, and then 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** to confirm your selection.

Reorder installations

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

Disconnect and reconnect an installation

Disconnects connected installations from the current system. The color marker in the symbol indicates the connection state.

1. Click the **Autoconnect** icon (1) of the installation that you want to disconnect.
2. For automatic connecting and disconnecting, click the **Enable auto-connect** icon or **Disable auto-connect** icon (4) of the installation.

Edit installations

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

Delete saved installations

Tidies up the list of installations most recently called by the client (see **Login**).

1. Click the Delete icon (2) of the installation that you no longer want to be available for selection the next time you log in on the client.
2. To delete multiple installations at once, select the installations you want to delete and click **Delete selected objects**.

5.4.1.7 View

The View menu has no function in this version of the software.

5.4.1.8 Tools

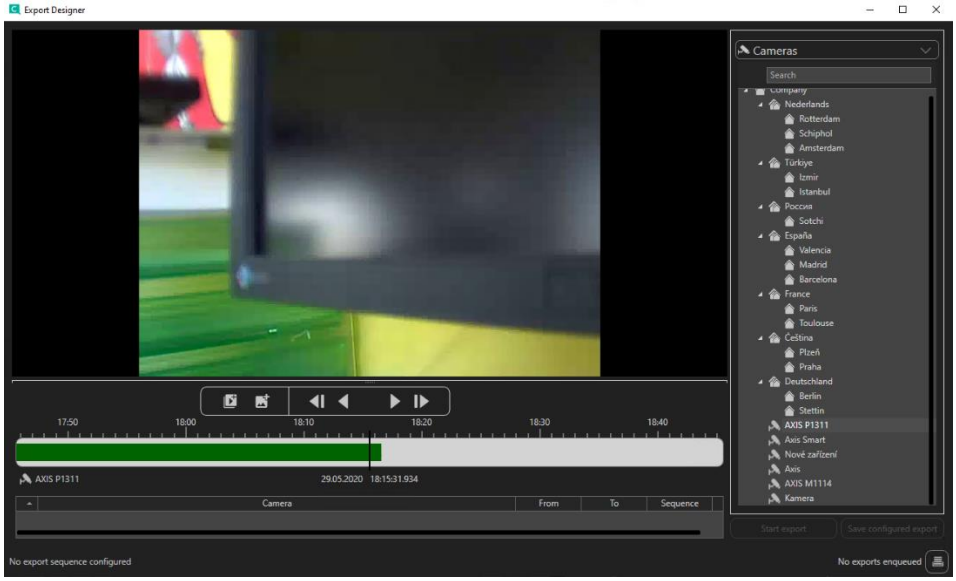
This menu displays the following options:

- The Export Designer
- Manual reference image comparison

The Export Designer

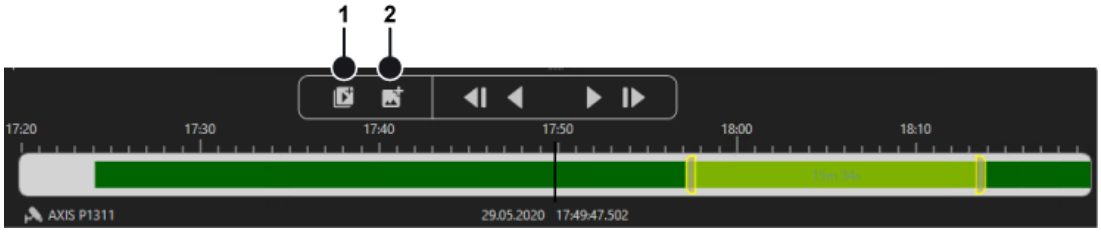
Using the Export Designer, you configure the image export by adding shapes to mask specific areas of the exported images to increase privacy or defining a time range.

Creating a new export



Defining the image or image sequence:

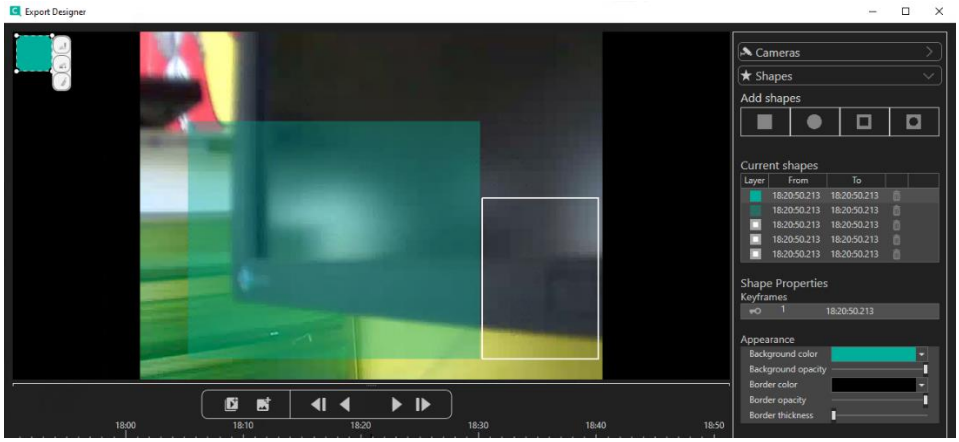
1. In the Export Designer, select **Create New** from the **Tools** menu.
2. Select a camera from the list or search for a camera in the search box above the list.
3. Move the timeline to the desired position. The corresponding frame is displayed. Zoom in or out of the timeline using the scroll wheel of the mouse for more detail.



4. Click **Add sequence** (1) to set the starting point of an image sequence.
5. Drag the handle of the sequence delimiter to the right. This defines the time frame for the export.
6. To mark only a single image for the export, click **Add single image** (2) and drag the marker to the position on the timeline.

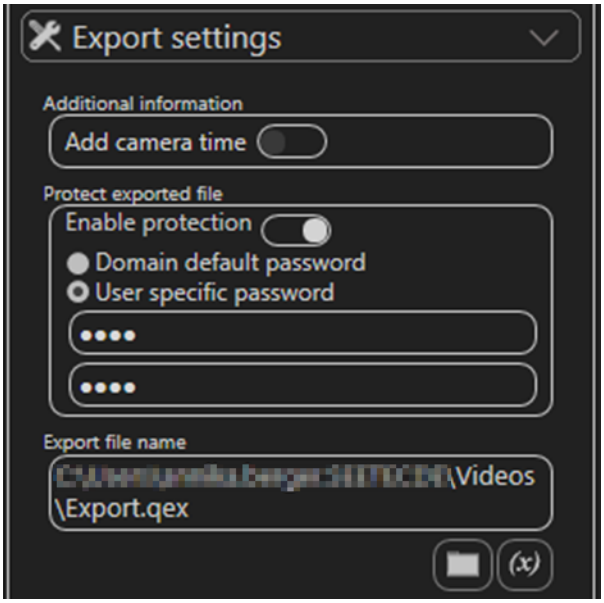
Adding shapes

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.



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 the **Delete** icon next to the shape in the toolbar.

Defining the export settings



1. To define the export settings such as a password protection, open **Export settings** in the toolbar on the right.
2. Enable the display of the camera time as additional information in the image.
3. Enable the password protection if required, and set either a domain default password or a user specific password.
4. Click the folder icon and select the export location of the file.

5. 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.
6. Save the export settings.
7. Select Start export.

Resuming the image export

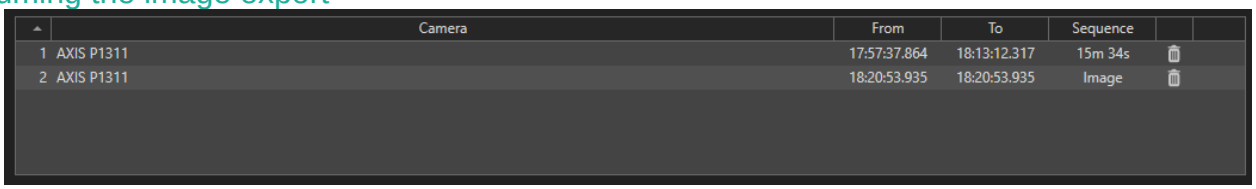


Image exports are queued in the export designer. The export settings can be restored in case of failure. The settings file that has previously been configured in the export designer is reloaded into the export queue.

1. In the Export Designer, select **Resume** from the **Tools** menu.
2. Optionally, reconfigure the export settings.
3. Start the export.

Loading any file for export

Any setting that has 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.

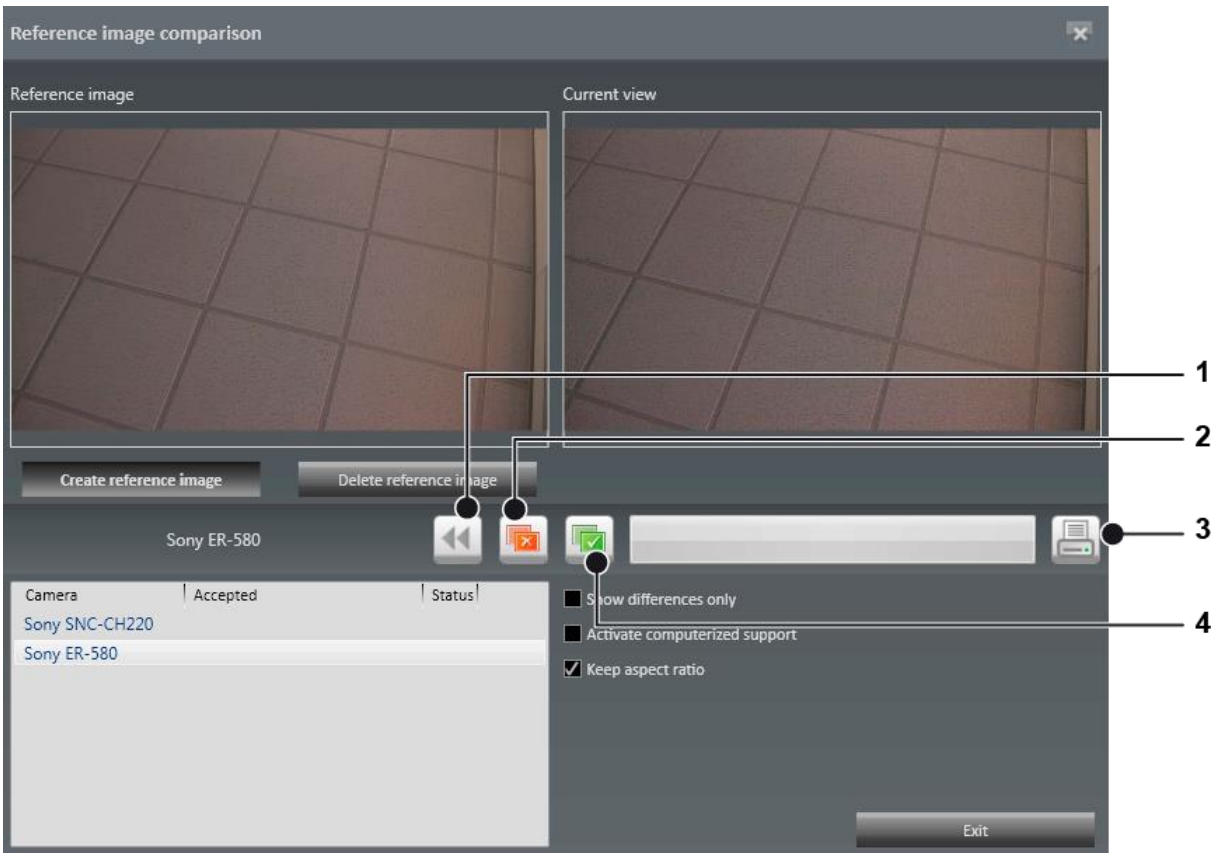
1. In the Export Designer, select **Load** from the **Tools** menu.
2. Optionally, reconfigure the export settings.
3. Start the export.

Deleting a marker

1. To delete a marker from the file, select the **Delete** icon in the item's row.

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.



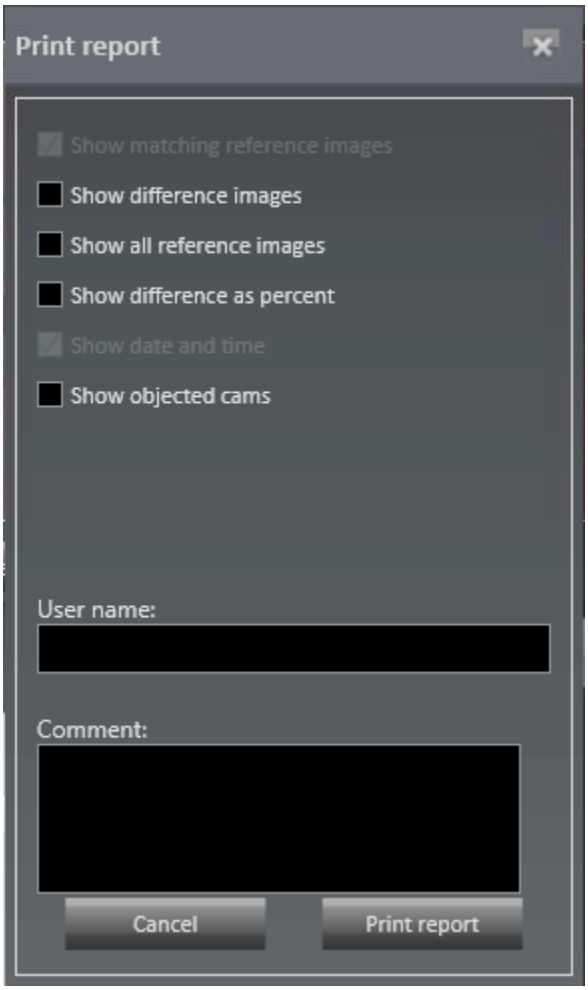
The manual reference image comparison helps detect changes in the camera orientation.

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.
2. To delete a reference image, select the camera from the list and click **Delete reference image**.
3. Select the cameras and check both images for changes.
4. If changes are detected, click the red con (2) to mark the change as not identical.
5. If the images are identical, click the green icon (4) to mark the image as identical.
6. If the changes are difficult to see, select **Show differences only**. The changes detected by the image processing software will be displayed as red 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. Deselect **Keep aspect ratio** to display both images filling the frame. Depending on the camera image, this setting may distort the image's aspect ratio.

10. To print the images, click the printer icon (3).

Printing the reference image comparison



1. In the print report dialog, select **Show difference images** to print the current views with the differences highlighted.
2. Select **Show all reference images** to print the reference images alongside the current views.
3. Select **Show difference as percent** to print the percentage of the detected differences.
4. Select **Show objected cams** to display only those cameras with images differing from the reference image.
5. Enter the **user name** and add **comments**, if necessary.
6. Click Print report.

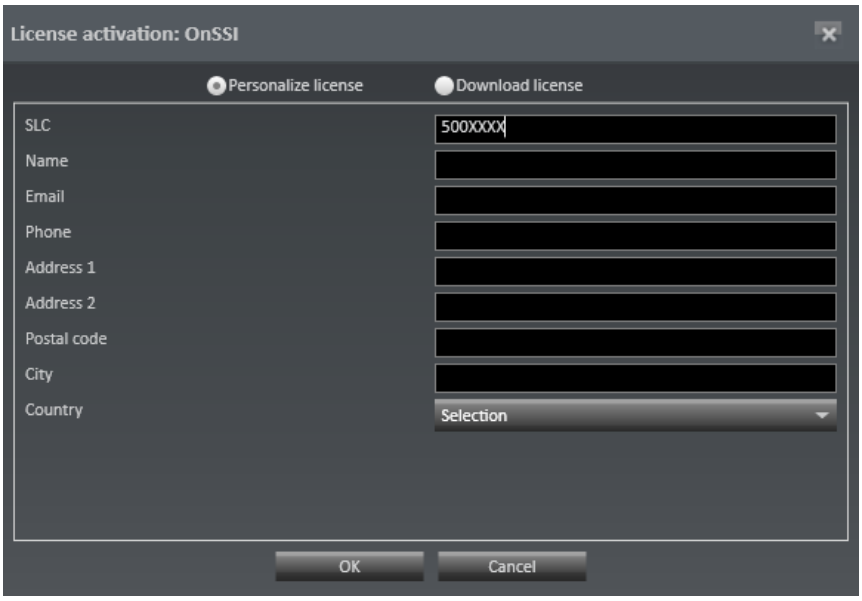
5.4.1.9 Info

The menu **Info** displays information about the system and both procedures to obtain a license for the Ocularis 5 Recorder . The installation must be activated within 30 days to purchase a new license. This requires sending an automatically generated activation key, the product ID, to Qognify.

Activate the product online

Using this method, you cannot activate or download the licenses unless the client is connected to the Inter- net.

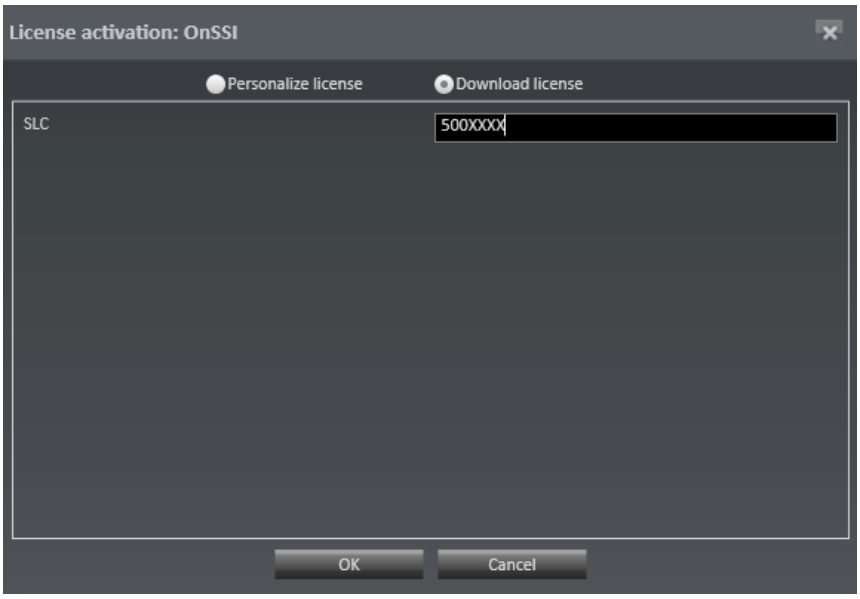
Personalize a license



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 (**SLC**) and user details.
5. Click **OK** to confirm your entries. software connects to the Qognify license registration server and transfers the license key to the computer.

Download a license

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



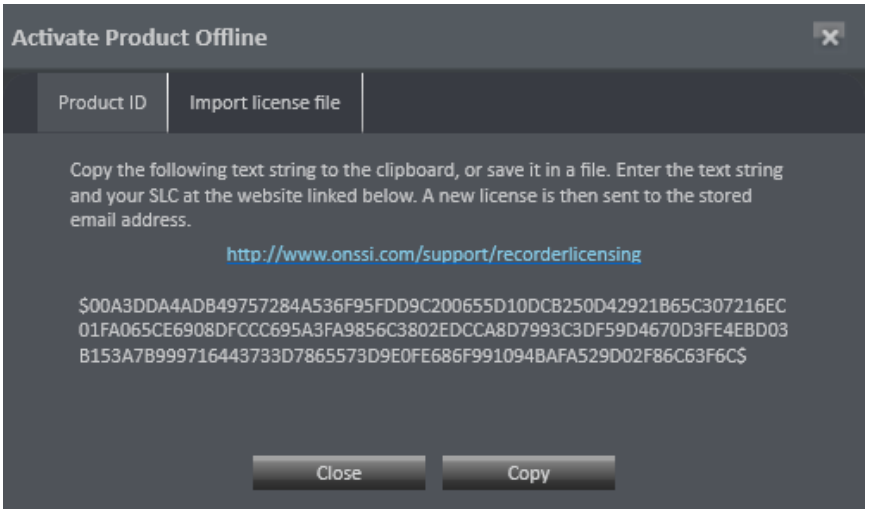
1. Select Download license.
2. Enter your installation number (SLC).
3. Click OK to confirm your entries. The software connects to the Qognify license registration server and transfers the license key to the computer.

If the product ID has changed (e.g. due to changes to the server hardware), contact the Qognify support.

Activate the product offline

If the Ocularis Recorder Manager has no internet access, the license can be activated on the Qognify web- site.

Applying for a license

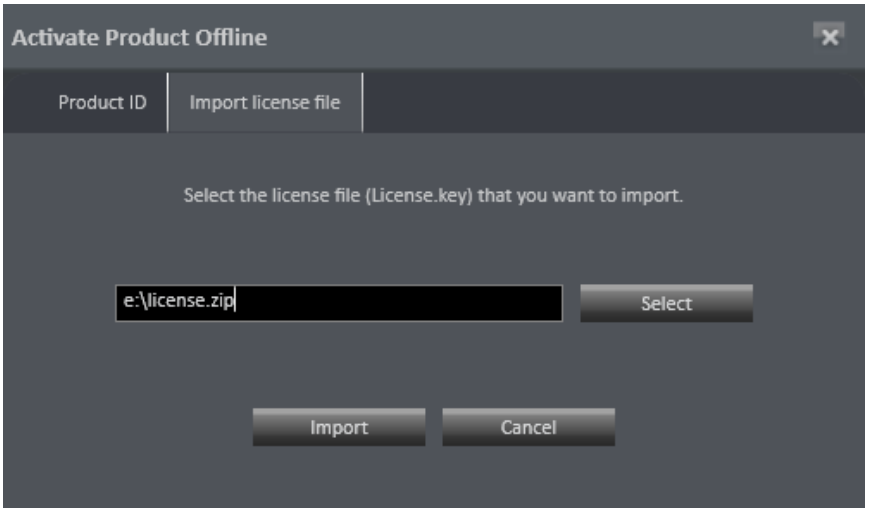


1. In the Info menu, select Activate Product.
2. Select Offline.

3. The tab Product ID should already be selected. The software creates a unique product ID.
4. Click Copy to copy the displayed product ID to the clipboard.
5. Paste the product ID to a text file, such as Notepad, and transfer the file to portable media.
6. Bring the portable media to any PC the does have internet connectivity.
7. Open and browser and go to the Qognify website. Navigate to 'Support' and then 'Ocularis Recorder Licensing'.
8. Enter your SLC, product ID and the other information requested. The Installer Email Address will receive a license file as an attachment by email.
9. Detach the license file (license.zip) and transfer to portable media back to the original PC. It is not necessary to unzip the file.

Importing a license file

After obtaining the license file per email, it must be imported.



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

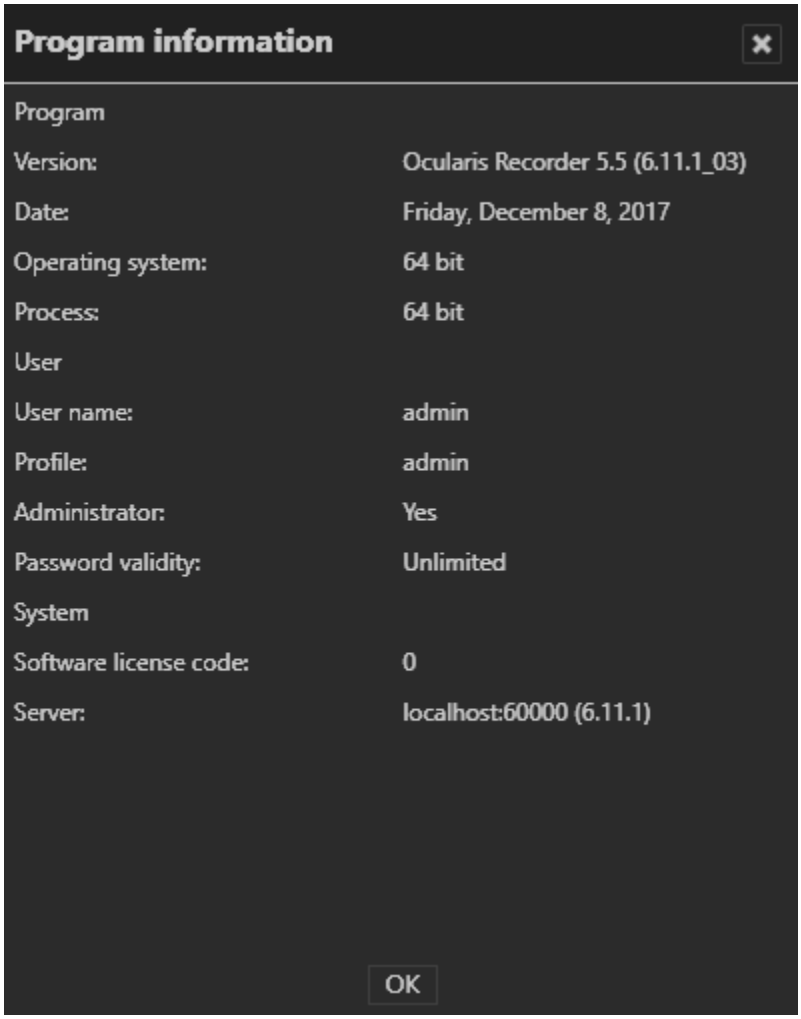
Show license

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.

1. In the **Info** menu, select **Show information**.
2. Select **Show license**. Information on the license is displayed in three tabs.

3. Select the tab **Overview** to see general information of the product, e.g. the SLC.
4. Select the **Features** tab to see the features activated by the installed license file.
5. Select the **Modules** tab to see how many modules like cameras (devices), servers, etc. are activated by the installed license file.

Show program information



1. Choose **Show program information** from the **Info > Show information** menu. The information on items such as the program version, current user and profile and also validity of password is displayed.
2. Click **OK** to close the window.

Display system information

1. Choose **Show system information** from the **Info > Show information** menu. The information on items such as the CoreServiceMain, the numbers of activated DeviceManagers, videosources (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 Tech Support.

3. Click **Cancel** to close the window.

5.4.1.10 Help

This menu displays the following options:

- Online help
- Start problem recording
- Display help icons

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. For newer editions of the help system and the manual, visit the Qognify website.

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 File 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. Choose **Display Help icons** from the **Help** menu. The function is activated (check mark) or disabled (no check mark).

5.4.2 The mode bar

The mode bar allows you to switch between display modes.

- **Report mode** (1). The report mode facility gives you a list of the events that have occurred (see **Report mode**).
- **Configuration mode** (2). Configuration mode is for managing and configuring the video sources, users and locations.

5.4.3 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.

▶ To Show/hide a tab:

1. Click the gray triangle in the upper-right corner of a tab to hide the tab on the right-hand edge of the screen.

   Once the last control on the control bar has been minimized, the available size of the main window increases.

2. Click the gray triangle on the tab on the right-hand side of the screen to show the control.

   The control bar then also appears again.

5.4.4 Search

The **Search** control at the bottom of the user interface helps you find the contents of the server database more quickly.

▶ To search in configuration mode:

1. Enter the search term. 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. Click the term found. The right column shows context belonging to the found term.
3. If it is a setting, click **Open setting**. The menu belonging to the hit is opened.
4. Click the magnifying glass icon. The next term found is highlighted.
5. Double-click the item found to open the corresponding settings window in the configuration mode. To edit items in the configuration mode, administration rights may be required.

6 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 a specific camera)
- system messages (display of events that concern specific services)

In addition, the camera usage of users can be tracked.

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

1. To switch to report mode, click the **Report mode** icon on the mode bar.
2. Click a column header in the main window to sort the events in ascending or ascending order based on the column's category (data/time, alarm, description).

6.1 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:
  - Camera configuration
  - Archive
  - Export
  - Patrols
  - Actions
  - Log on or log off
  - Change mode
- 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, click **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.

6.2 Exporting the analysis

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

6.3 Saving a query as report template

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

1. Click **Save**.
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. Click **OK** to save the query.
5. To use a previously saved query, select the name of the query in the drop-down menu and click **Start query**.
6. To delete the saved query, select the query from the drop-down menu and click **Delete**.

7 Configuration mode

You must have administrator rights to enter configuration mode.

Configuration mode is where all of the settings for the hardware, network, company, alarms and users is made.

To change to configuration mode, click the **Configuration mode** tab.

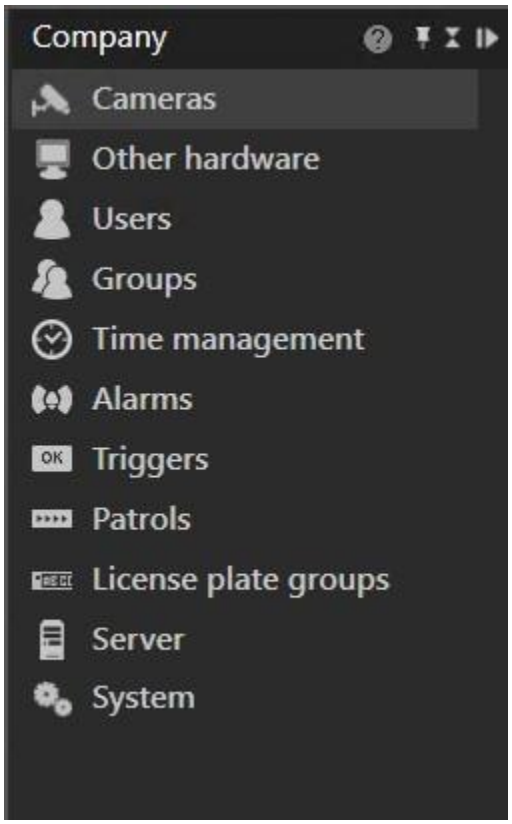
Searching for objects

You can search for all objects in configuration mode with the **Search** control below the work area. The search starts as soon as the second character is entered and shows a list of all the results (see **Searching in configuration mode**).

Additional settings

- See **Company** for further settings for the company.
- See **Administration** for further settings for cameras, triggers, other hardware, user management, etc.

7.1 Functions



The following function categories are available:

- **Cameras**: This function allows you to configure and manage the camera hardware.
- **Other hardware**: This function allows you to configure and manage additional devices.
- **Users**: This function allows you to configure and manage users of Ocularis Recorder Manager.
- **Groups**: This function allows you to configure and manage user groups of Ocularis Recorder Manager.
- **Time management**: This function allows you to configure and manage time profiles or templates which can be applied to standard recordings as well as in alarm scenarios.
- **Alarms**: This function allows you to manage and configure alarm scenarios.
- **Triggers**: This function allows you to configure and manage user defined events (manual or automatic).
- **Patrols**: This function allows you configure and manage the sequence and timing of moving a PTZ camera to its pre-configured preset positions.
- **License plate groups**: This function is not applicable to this version of the software.
- **Server**: This function allows you to configure services (e.g. core, DM, motion detection, etc.)
- **System**: This function allows you to configure system-wise settings for the network, automatic backups, communication settings and event management settings.

7.2 Configuration Wizard

You will find the configuration wizard on the starting page of configuration mode. This helps you quickly make settings for new cameras and alarms. You can use it to make basic settings for:

- Creating Alarms
- Creating Cameras
- Creating Users
- Finding available devices using the Device Finder

7.2.1 Creating a camera

The wizard helps you to easily create a new camera. The settings correspond to the steps you have to take in the **Cameras** control (see **Creating a camera**).

7.2.2 Creating an alarm scenario

1. Specify the **name** of the alarm scenario, and then click **Wizard** to start installation.
2. Select the events that are result in the alarm, and then click **Next**.
3. Select the camera to be used as the alarm camera.
4. Specify the recording time of the alarm camera (in seconds).
5. Indicate whether you want a pre-alarm duration to be activated, and then set the duration (in seconds), if applicable.
6. Click **Next**.
7. Specify which users are to be notified in the event of an alarm and whether the selected users are to be notified by means of a message window.
8. Click **Next**.
9. Check the settings you have made, and then click **Finish**. The alarm configuration is displayed. You can make further settings here.

7.2.3 Find cameras

By using the IP address assigned uniquely to a camera (device), the software is able to generate an over- view of all devices currently present in the network.

7.2.3.1 Searching for devices

1. Select **Find devices** in the Configuration mode view. The Device Finder window is displayed. All network devices (cameras) are displayed. Unknown net- work devices (i.e. not yet configured cameras or routers) are displayed as gray text.
2. Click the arrow triangle (**1**) to start a new scan through the network.
3. To display additional network options, click on the circle icon (**2**). The IP Finder currently supports Onvif (**4**), UPnP (**3**), and Bonjour (available if installed on the system) protocols .
4. Specify the timeout (in Seconds) (**5**) for the protocols. This defines the time each protocol "listens" fornew devices. After the timeout, the search has to be triggered manually.
5. Click the search filter icon (**6**) to toggle the display between all or only unknown devices. Installed devices are hidden or shown.
6. The Import tool (**7**) is used to bring in camera data from .csv or .xml files. See **How To Import Data**_bookmark130.
7. Enter one of the following search items in the search field (**8**):
   - IP address or
   - manufacturer or
   - device type or
   - name
8. Click the IP address of a camera to open the configuration page supplied by the camera software in a browser.
9. Click on a column heading to sort the list by that column.

NOTE: Do not use special character in camera names. This will cause erratic behavior with Ocularis. Rule of thumb: use the same characters supported by Microsoft Windows file names.

7.2.3.2 Adding Individual Devices

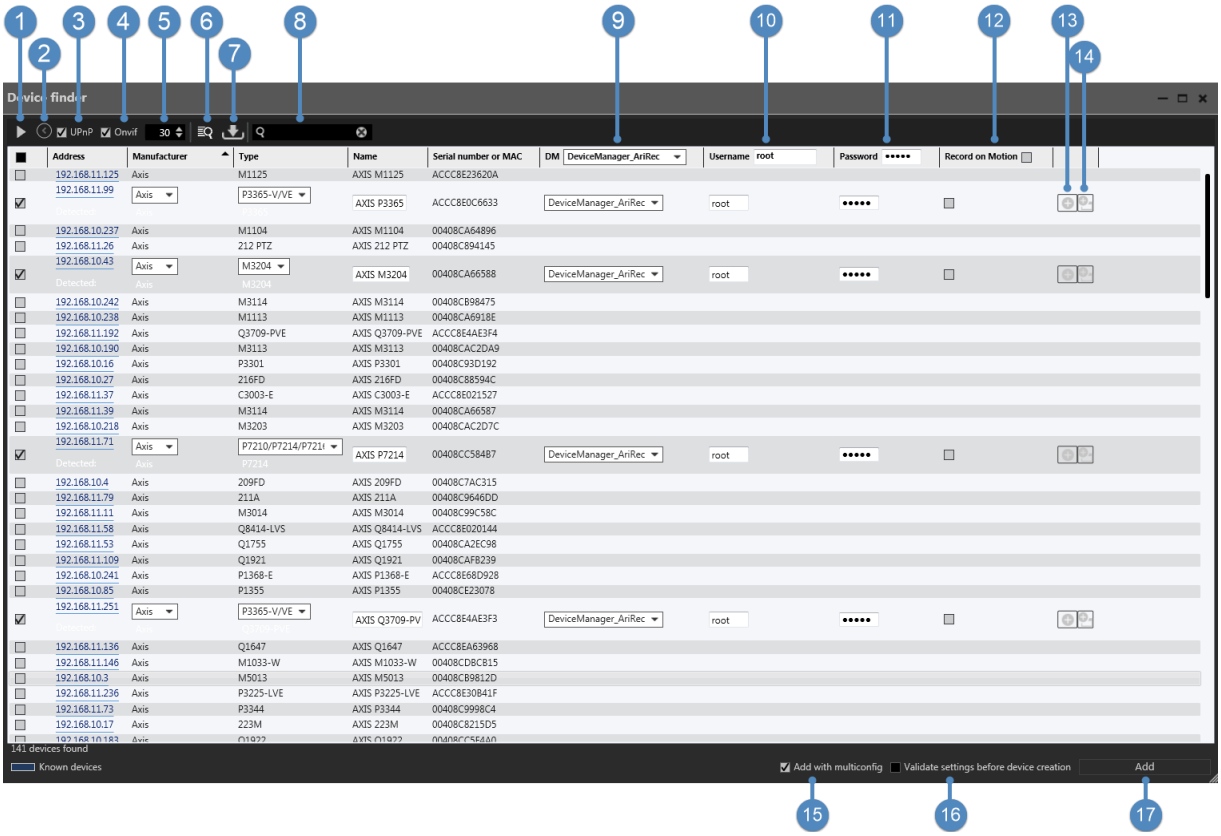
1. Select the camera to be added by clicking the checkbox in the first column.
2. If required, modify the settings for Manufacturer, Type and Device Manager (DM).
3. Optionally, rename the camera or change the username or password.
4. Click **Add** (**13**) in the camera row or click **Add and Configure** (**14**). After clicking **Add and Configure**, the configuration settings window for this device is displayed.
5. Configure the camera.

7.2.3.3 Adding Multiple Devices

For all selected devices, the following settings may be made in the column header:

- Device Manager (**9**)
- Username (**10**)
- Password (**11**)
- Record on Motion (**12**)

1. Select the cameras to be added by selecting the checkboxes in the first column.
2. If required, change the settings for **Manufacturer**, **Type** and camera **Name**.
3. To apply common settings across all selected cameras, select a **Device Manager** (DM) (**9**), **Username** (**10**), **Password** (**11**), and/or **Record on Motion** checkbox (**12**) from the column heading section. Once modified, all selected cameras should update to reflect the item shown in the column heading.
4. To configure all devices at once, be sure that the **Add with multiconfig** (**15**) checkbox is selected.
5. Optionally, select the **Validate settings before device creation** (**16**) checkbox to validate the settings for these cameras.
6. Click **Add** (**17**).



7.2.3.4 Importing devices

Ocularis includes migration tools to aid in the transition of moving to Ocularis. The **Recorder Migration Tool** imports data from a legacy recorder to include: camera name, IP address, username and password. The remaining configuration of the device, such as framerate, resolution, etc. are not imported.

To assist in configuration of views and maps on Ocularis Base, a **Camera Migration Tool** has been developed to assign one camera to replace another in all instances where the camera appears in views and maps. You can find more information on the Camera Migration Tool in the document *Ocularis Administrator User Manual*.

Recorder Migration Tool

The Recorder Migration Tool is used to import cameras in bulk into an Ocularis recorder (recorder version R8 or later). Supported by all models of Ocularis this feature quickly adds cameras into the recorder. Once imported, however, additional configuration is still required such as choosing the compression, resolution, framerate and other configuration parameters.

Supported Configuration Files

The following files are supported for import:

1. Legacy Ocularis PS, IS or CS Configuration File
   - Filename: 'configuration.xml'
   - Supported with v8.0 and later recorders

By default, the configuration.xml file is located in the folder:

c:\Program Data\OnSSI\RC-X

where 'X' represents the model (e.g. RC-C, RC-I, RC-P)

Reminder: Program Data is a hidden folder by default so you may need to change your Windows view set- tings in order to locate this folder.

NOTE: The camera authorization credentials are not imported when using configuration.xml file

2. CSV file with the following structure:
   - Columns: DisplayName, IPAddress, UserName, Password

NOTE: Do not use spaces in the header labels. The labels are case-sensitive and must appear EXACTLY as shown above.

The order of the columns is irrelevant.

   - Separator: a comma (,)

Example:

DisplayName,IPAddress,UserName,Password Camera A,172.16.101.153,root,pass

Camera B,172.16.117.70,admin,admin

   - A Microsoft Excel spreadsheet may be used provided it is saved as a .csv file

NOTE: The camera authorization credentials are imported when using a .csv file import.

Ocularis LS and ES: If you require a direct import from an RC-L or RC-E recorder and you do not have a .csv formatted file, con- tact Professional Services for assistance with this type of import.

7.2.3.5 How Import Works

The Ocularis Device Finder works with UPnP and ONVIF by using multicast via UDP. If there are Layer 3 switches on the network, multicast packages may be blocked by default. In this case, the Device Finder will not be able to find devices in other subnets. After the initial broadcast scan, the Device Finder sends a uni- cast message to the devices in the import file provided.

For the configuration.xml import to work properly, devices must have UPnP or ONVIF enabled. Otherwise, the device will not be recognized by the scan.

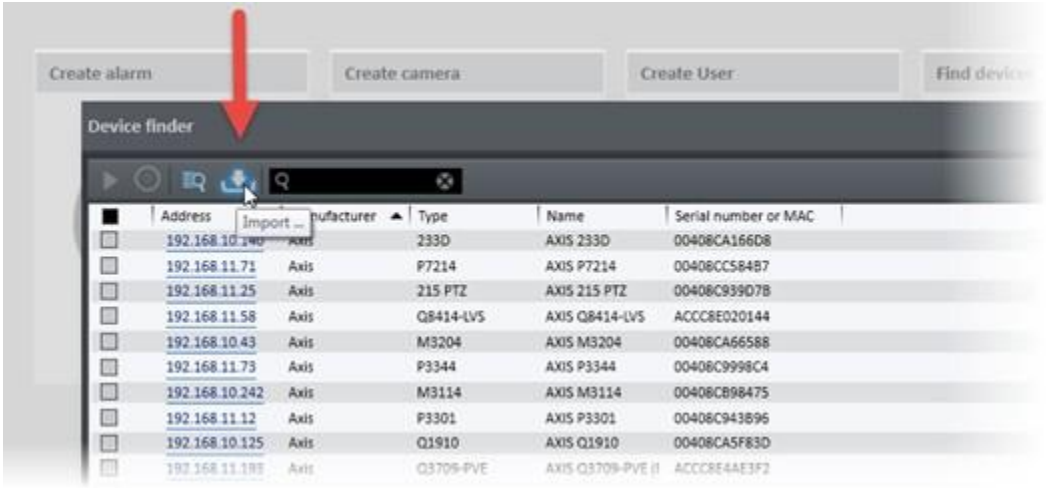
▶ To Import Data

1. Obtain the configuration.xml or .csv file

By default, the configuration.xml file is located in the folder: c:\Program Data\OnSSI\RC-X where 'X' rep- resents the model (e.g. RC-C, RC-I, RC-P)

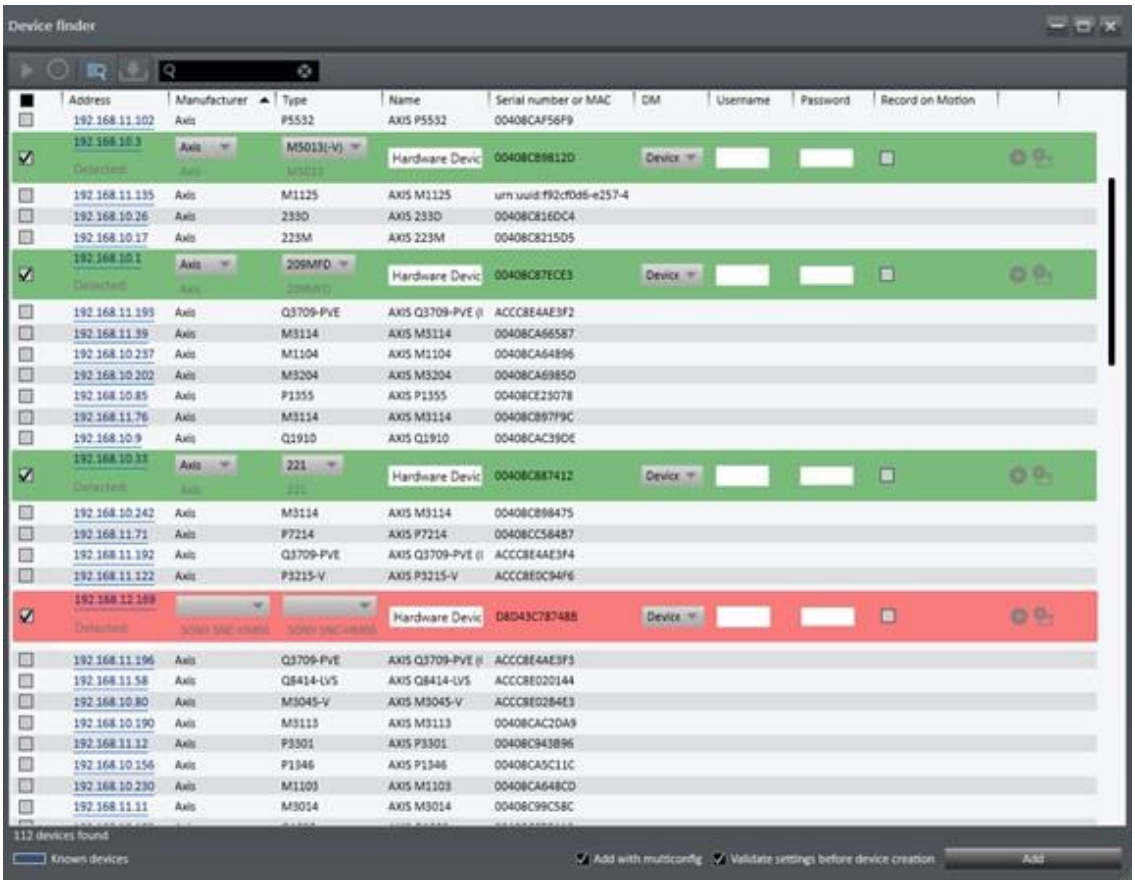
NOTE: Reminder: Program Data is a hidden folder by default so you may need to change your Windows view set- tings in order to locate this folder.

2. Bring the configuration.xml or .csv file to the PC with Ocularis Recorder Manager (if not already there).
3. Launch Ocularis Recorder Manager.
4. Click 'Find Device' to start the Device Finder. Allow it to complete its search process.
5. Click the 'Import' icon.

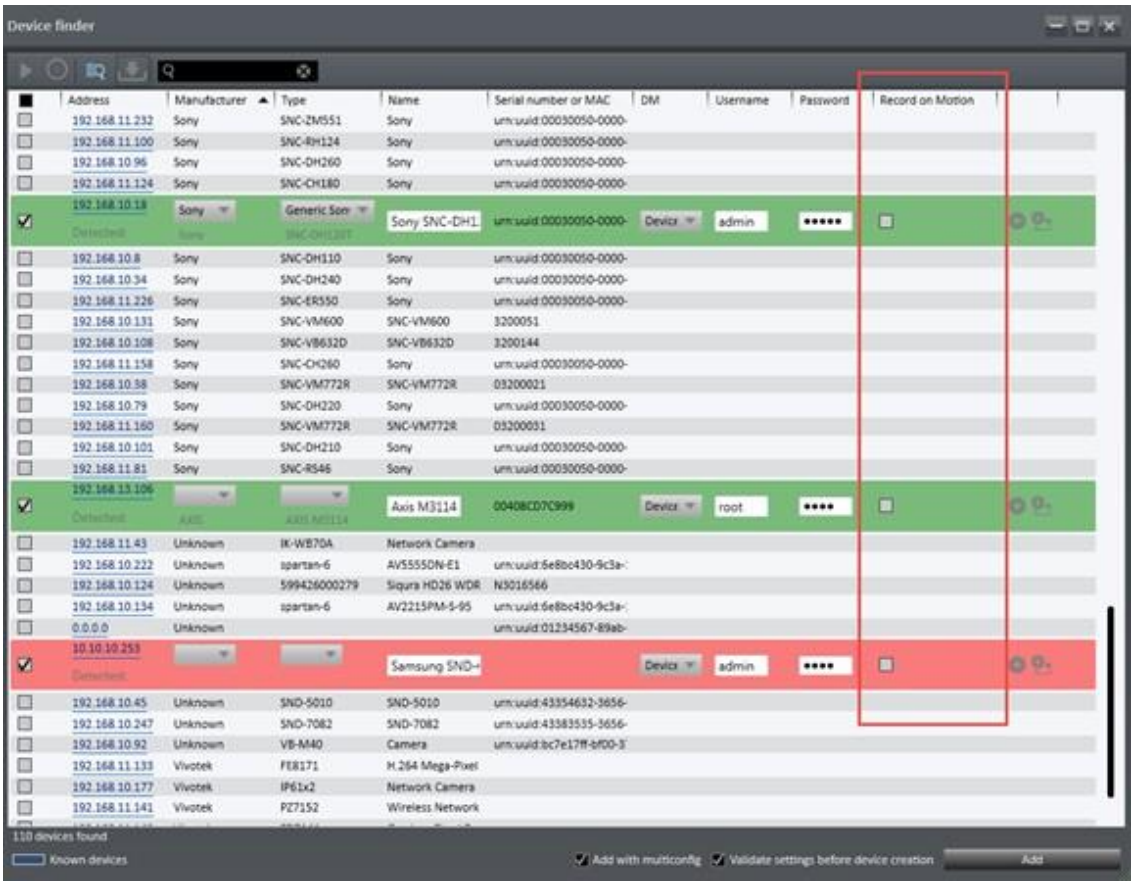


6. A Windows Open dialog appears. Select the file you wish to import (configuration.xml or the .csv file) and then click 'Open'.
7. A message appears notifying that there was an error or that the configuration was successfully loaded. Then, the devices are imported.
   - If the device is already in the Device Finder list, the information will be updated (i.e. the name of the device used in the legacy recorder). In most cases, the 'Name' field in the Device Finder is set to the name of the model so it is the same as the 'Type' field before the import.
   - If the device was not in the Device Finder list, a unicast message will be sent via UPnP and ONVIF to the device, requesting its information (i.e. manufacturer, model).
   - If the unicast message fails, the device will be added to the found devices list with a red background. In this case, the name of the formerly used driver in the legacy system, the name of the camera, and the IP addresses are listed in or below the corresponding fields.
   - If the unicast message succeeds, the device will be added to the devices found list and highlighted with a green background. Information, such as the name of the device, is used from the configuration. Manufacturer and type come from the device directly and are used for the regular matching process to preselect the correct driver (if possible).

In the example shown below, the three devices shown in green were successfully contacted via UPnP. For the device highlighted in red, there was an issue with the communication. Notice though that the Manufacturer and driver name are shown in the area below the drop-down menus. You can select the corresponding fields from the drop-downs to manually set this data. Also, in all cases using a configuration.xml import, you must manually enter the device's username and password.



The next example shows an import using a .CSV file. Notice that it too can be unsuccessful if the devices are not configured with the UPnP protocol. You can select the Manufacturer and Type for these manually.



Notice that you can set Record on Motion as you add cameras with the Device Finder. You can also set Record on Motion using the multi-configuration feature.

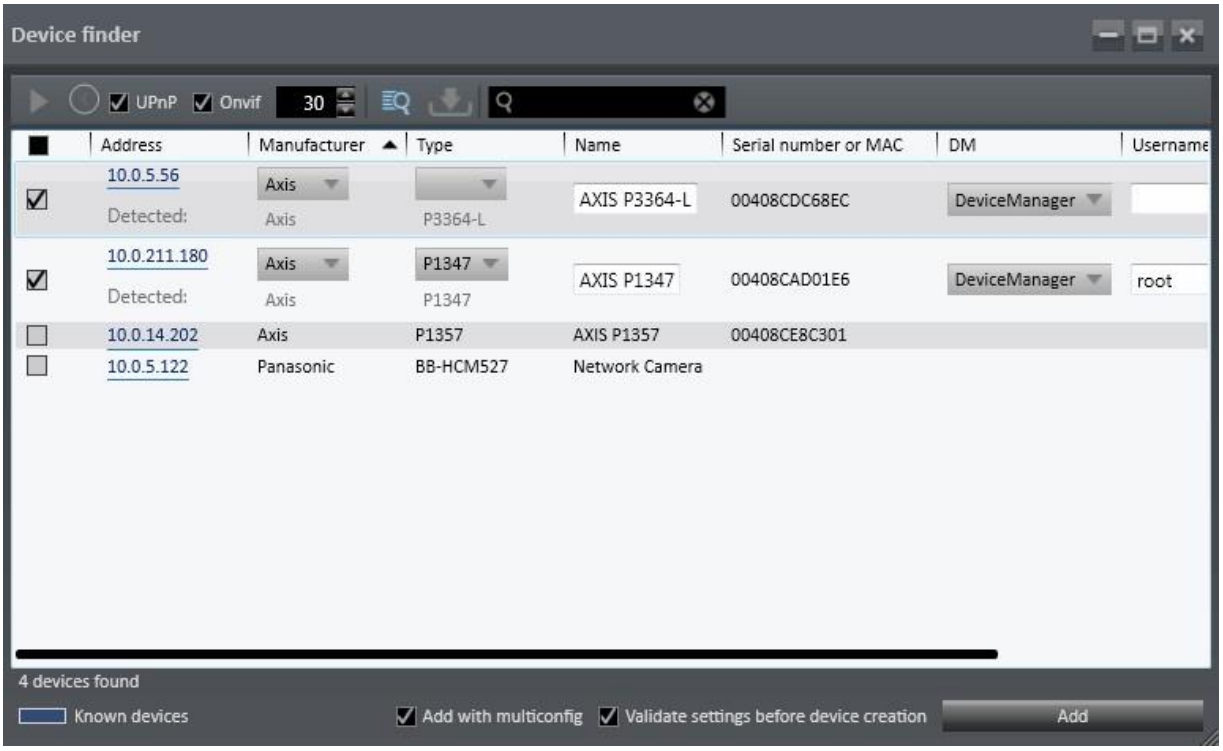
7.2.3.6 ONVIF

The ONVIF standard states that when requesting device information, authentication is required. Therefore, there could be some devices that do not respond properly. The example below using the manufacturer Axis, shows where the authentication is necessary before getting the details from the camera. In order to request ONVIF information from Axis, an ONVIF user (administrator profile preferred) must be added via the camera's web-configuration page.

7.2.3.7 UPNP

The import tool also uses UPnP. This protocol must be enabled on the camera in order for the search to work during a configuration.xml import. Here's an example of another Axis camera's configuration webpage showing that UPnP is enabled.

7.2.3.8 Adding individual devices



1. Select a camera.
2. If required, modify the settings for Manufacturer, Type, and DeviceManager. Rename the camera or change user name and password. (Do not use commas or special characters in camera names).
3. Click the **Add** icon in the camera row or click the **Add and Configure** icon. After clicking on the **Add and configure** icon, the configuration settings for this device are displayed.
4. Configure the camera (see **Cameras**).

If **Validate settings before device creation** is checked, the Username, Password, Manufacturer and driver class will be validated for accuracy. Uncheck this box to add the camera without this validation text. This is useful when remotely setting up a system prior to being physically located at the system.

NOTE: Note: do not use special characters in camera names. This will cause erratic behavior with Ocularis. Rule of thumb: use the same characters supported by Microsoft Windows file names.

7.2.3.9 Adding Multiple Devices

1. Select multiple cameras to be added by selecting the checkboxes in the first column.
2. If required, change the settings for **Manufacturer**, **Type**, and Camera **Name**.
3. To apply common settings across all selected cameras, select a **DeviceManager**, **Username**, **Password** and/or **Record on Motion** checkbox from the column heading section. Once modified in the column heading, all selected cameras should update to reflect the item shown in the header. Or you can modify individually per row.
4. To configure the cameras with the multi-configurations option, select **Add with multi-config**.

5. Optionally, select the **Validate settings before device** creation checkbox to validate the settings for these cameras.
6. Click **Add**.

If **Validate settings before device creation** is checked, the Username, Password, Manufacturer and driver class will be validated for accuracy for all devices being added. Uncheck this box to add the camera without this validation text. This is useful when remotely setting up a system prior to being physically loc- ated at the system.

7.2.4 Creating a user

The wizard helps you to easily create a new user. The settings correspond to the steps you have to take in the **Users** control (see **Creating a user**).

7.3 Company

This control allows you to configure your company's branches and the hardware used at each location. 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 branches to it. The main branch can have sub-branches, but branches cannot have sub-branches (for the relationship between the "company" and the branches, see **About the relationship between the "company" and its branches**).

7.3.1 Editing the company name

For changing the name of the company, see **Editing the name of the "company"** .

7.3.2 About the relationship between the "company" and its branches

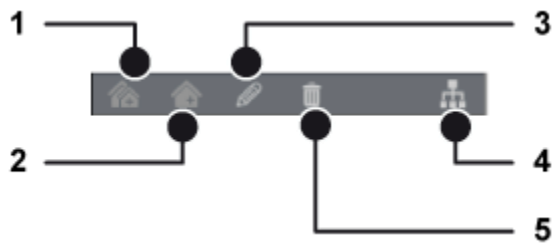
Branches are dependent subgroups of a "company". Hence the administration of the main branch can extend into the administration of a sub-branch, but not vice versa. Equally, one sub-branch cannot manage another sub-branch or the main branch itself. With the exception of cameras and DeviceManagement servers, 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).

For a detailed description of the relationship between the main branch and its sub-branches, see **Relationship between the main branch and its sub-branches**.

Administrative rights from the company are not inherited by the branch.

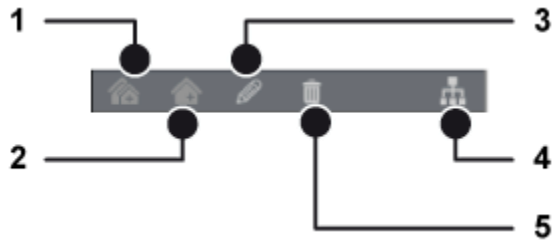
7.3.3 Editing the name of the "company"

By default, the headquarter or main branch of the company is named "company". The name can be adapted to the specificneeds.



1. To edit the name of the company, select the company in the window of the control.
2. Click the **Edit** icon (3).
3. Enter a new name for the company, and then click **OK**.

7.3.4 Working with branches



7.3.4.1 Creating a branch or branch group

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

7.3.4.2 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 the **Edit** icon (3).
3. Enter a new name for the branch or group, and then click **OK**.

7.3.4.3 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 into a branch group, select a branch and drag the branch on the branch group.
2. To remove a branch from a branch group, select the branch and drag it on the company name.

7.3.4.4 Deleting a branch or branch group

Branches may be deleted whether they are empty or include other entities.

3. To delete a branch or group, select the branch or group and click the **Delete** icon (5).

NOTE:	When deleting a branch that contains at least one entity (e.g. a camera), a warning pop-up displays that the branch is not empty. Also, a statistic about the content of the branch is displayed

4. Click **Yes** to delete. The branch or group is deleted.

The top-level branch (company) cannot be deleted.

7.3.4.5 Moving objects between branches

Moving objects between branches requires administrator rights for the main branch. Administrators of branches do not have access to the main branch ("company").

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. Moving objects between branches may cause inconsistent references.
4. To display all the objects and branches, click the **Site map** icon (4).
5. Select **Consistency check** to display any inconsistencies. For "legal" and "illegal" references, see **Relationship between the main branch and its sub-branches**.

7.4 Administration

The Administration control contains all configuration settings. 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, for example.

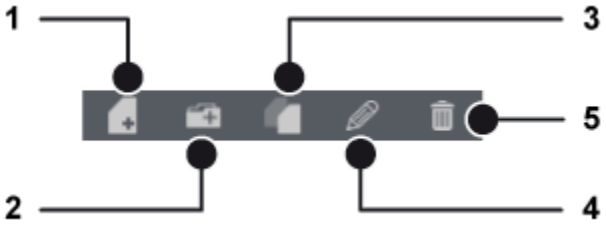
It is recommended to obtain a basic understanding of the concept of the underlying rights management before configuring the system.

Functions

Depending on the hardware and network architecture, you can configure the following functions:

- **Cameras**: This function allows you to configure and manage the camera hardware and the associated video server.
- **Other hardware**: This function allows you to configure and manage additional devices.
- **Users**: This function allows you to configure and manage users.
- **Groups**: This function allows you to configure and manage user groups.
- **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.
- **Alarms**: This function allows you to configure and manage alarm scenarios.
- **Triggers**: This function allows you to configure and manage the sequences of actions that can be manually executed in Ocularis Client, Ocularis Web or Ocularis Mobile.
- **Patrols**: This function allows you to configure and manage the sequences of actions in which multiple set PTZ presets are approached one after the other and/or actions are triggered.
- **License plate groups**: This function is not supported in this version.
- **Server**: This function allows you to configure the device services.
- **System**: This function allows you to configure and manage system-wide settings for the network, automatic backups, communication settings and event management settings.

Editing menu



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

- Create new object (1).
- Create new folder (2).
- Duplicate object (3). Only one object can be selected.
- Edit object (4). Depending on the context, many different configuration pages or a multiple configuration can be open.
- Delete object (5).

7.4.1 Cameras

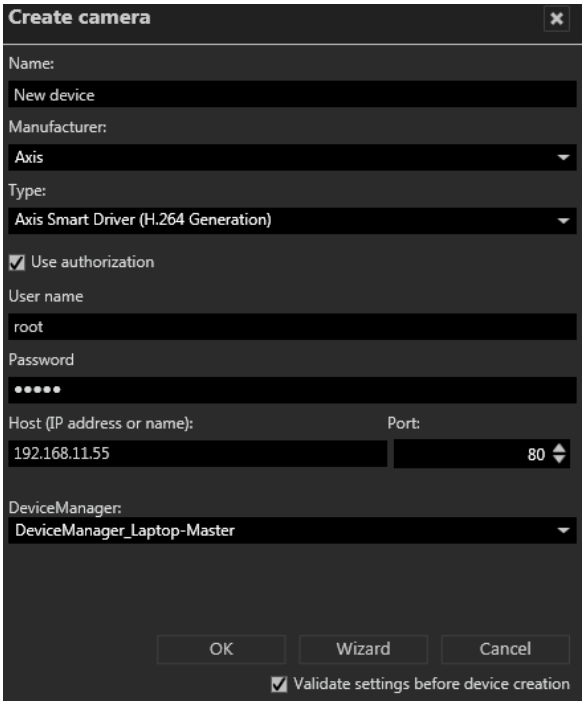
The **Camera** function on the control bar allows you to configure and manage the video hardware, e.g. cam- eras and video encoder.

1. Select the location in the Company control. The selected location is displayed in the title bar of the control bar.
2. Select **Cameras** in the control bar.

7.4.1.1 Creating a camera

NOTE: For creating multiple cameras quickly, see Find cameras.

1. Click **Create new object** in the camera control bar.



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, select **Wizard**. The wizard cannot be used for creating a camera using Smart Drivers. The Smart Driver only receives the standard image stream from the camera.
3. Select the **manufacturer** and **type** of the camera.
   - **Generic Video driver**: The Generic Video driver can be used to add cameras that are not integrated into the software. The functions are restricted to displaying and recording the camera image. The video para- meters, 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 Driver** (vendor specific): The Smart camera Driver obtains the supported features directly from the camera. Qognify provides Smart Camera drivers for Axis, Hikvision, Samsung, Canon, Arecont, Inter- logix, ALLNET (ALL-CAM23xx Series), W Box, Northern, Sony, Bosch, Vivotek and more! Always check the Qognify website for the most up-to-date list of supported Smart Drivers. All models available at the time of the current release are supported.

NOTE: Some models that are different from the manufacturers' standard can cause different behavior of the Smart Driver. Any camera planned to be used with a Smart Driver should be tested before making any binding agreements

NOTE: Smart 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 / ONVIF Profile S**: The ONVIF video driver can be used to add 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 depend- ing on the ONVIF version. Qognify does not accept liability for correct operation of cameras that are integ- rated by the ONVIF video driver.

- **SeeTec Archive**: Choose **SeeTec** and then **Archive** to create a camera that is able to view video from a Video Backup. A SeeTec Archive camera allows the import of recordings that appear as a regular camera. For configuration of the camera archive see **Configuring an Archive Camera**.

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 Device Manager**), the available servers are displayed.
7. Click **OK** to confirm the entries.

The new camera is displayed in the camera control bar.

If **Validate settings before device creation** is checked, the Username, Password, Manufacturer and driver class will be validated for accuracy. Uncheck this box to add the camera without this validation text. This is useful when remotely setting up a system prior to being physically located at the system.

NOTE: Do not use special characters in camera names. This will cause erratic behavior with Ocularis. Rule of thumb: use the same characters supported by Microsoft Windows file names

7.4.1.2 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.

7.4.1.3 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**.

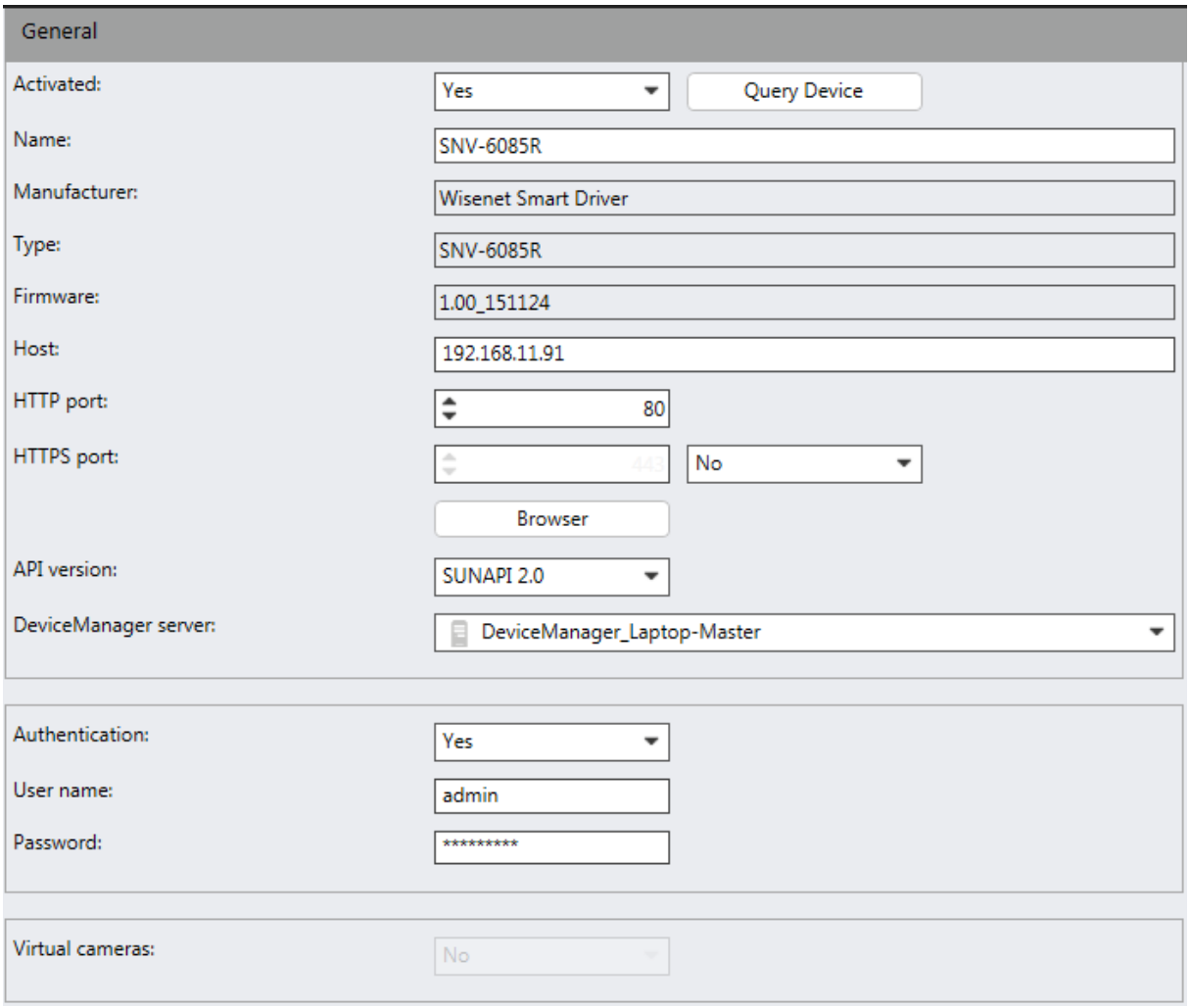
1. Close all camera configuration tabs.
2. Click **Cameras** in the company control.
3. Select the cameras you want to configure.
4. To configure multiple cameras at once, close all camera tabs in the work area.
5. Click **Edit**. The camera configuration view is displayed. Options that are not available 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**.

7.4.1.4 Configuring a camera

Select the camera in the overview. The settings of the camera are displayed in the main window.

Network cameras consist of at least one camera unit and a video server unit (Encoder). That is why the video server and one or more cameras are displayed under **Hardware**. Accordingly, the settings of a net- work camera are always subdivided into video server settings and camera settings. The video server set- tings include all of the connection-specific parameters, while the camera settings include all of the image quality and image storage settings.

Encoder – general



1. Activate or deactivate the camera or encoder. Choosing 'No' will release a license and deactivate the camera without deleting its settings. You can reactivate the camera at a later time without losing set- tings.
2. The **Query Device** button appears when a Smart Driver is used. If you want to re-query the device after settings have changed or just to refresh, click this button and the system will check the camera for its functions and features. This button will not be visible if using a static driver.
3. Enter the **Name** of the network camera. This is how the camera will appear in Ocularis.
4. Select the protocol type (http or https), and then change the **port** number, if necessary.
5. To test the incoming camera signal, click the **Browser** button. The browser defined in the system set- tings ("standard browser") starts up, and the camera image is displayed in the browser window.

6. The application programming interface (API) is identified automatically. If the API version cannot be retained, ask Support for the correct assignment of the API version to the camera firmware.
7. If necessary, change the **DeviceManager Server**.

NOTE: If you change device managers after recordings have been made to the first device manager, those recordings will be orphaned and inaccessible. The regular aging process will not eliminate the data. Contact Tech Support for instructions on manually purging this orphaned data

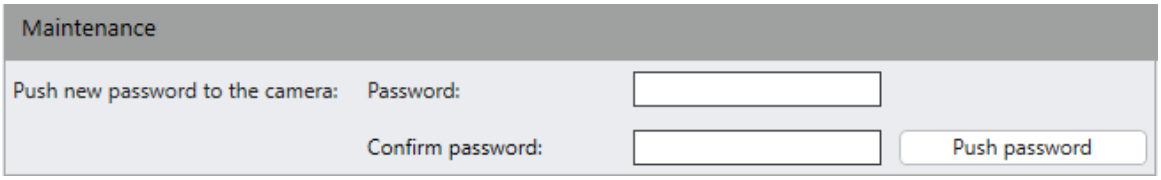
8. Specify whether separate **authentication** is to be required for the camera and, if necessary, enter a **user name** and **password**.
9. Select **Virtual cameras** to display and save multiple image details from a camera as a separate camera. The image details can then be specified in the virtual camera configuration.
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.

Maintenance

This management only applies to cameras using the Axis or Bosch Smart Drivers.

The maintenance feature supports modifying the camera password in a bulk operation instead of setting the password for each camera individually.

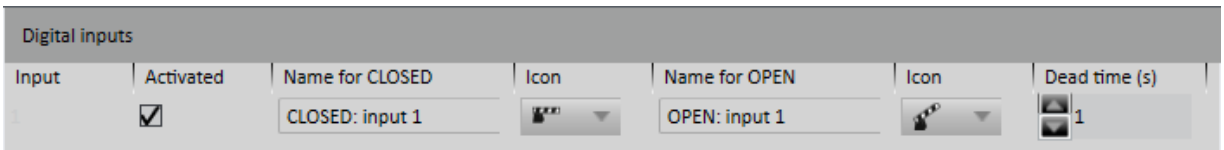


▸ To push camera password:

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 cam- era or switching on the camera light.

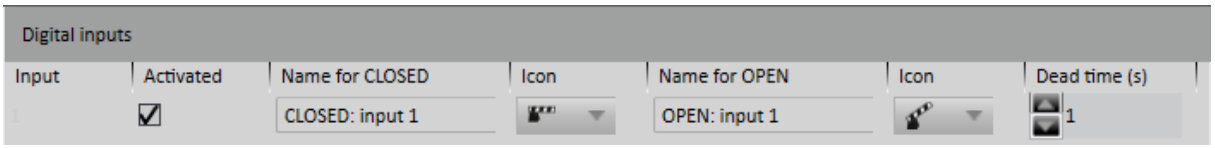


1. Select the digital inputs and specify unique names for **Name for CLOSED** and **Name for OPEN**.
2. Specify the interval for the **dead time** (in seconds) after which a signal is analyzed again. That prevents the event database from becoming unnecessarily large when events in rapid succession occur. This setting may also be used to trigger an alarm (see **Alarms**).
3. **Apply** the set values if you want to make further settings.

4. **Save** the set values to apply the values and conclude input.

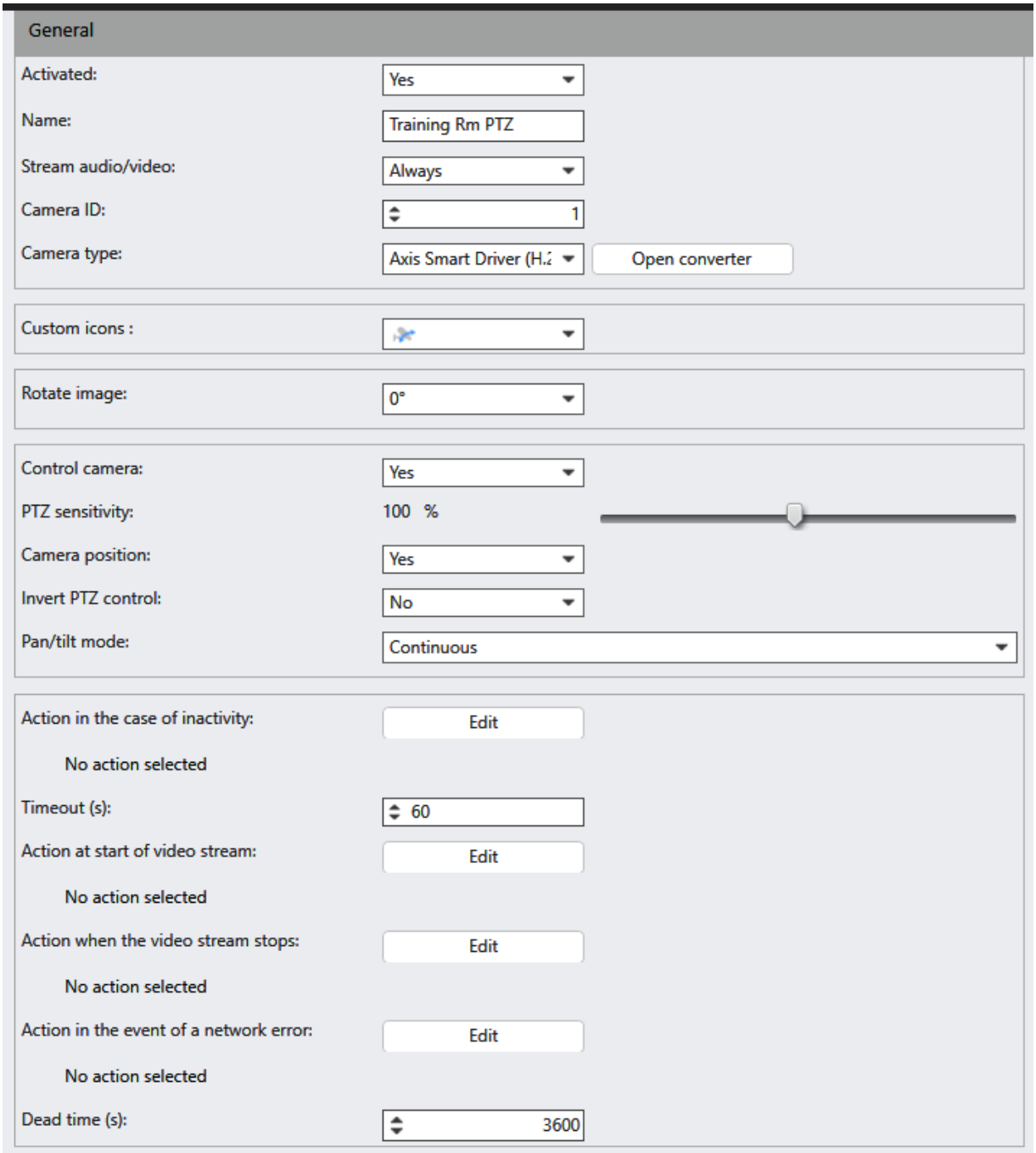
Digital outputs

Some cameras provide digital outputs. A state change can be used e. g. as a start event in a alarm scenario.



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

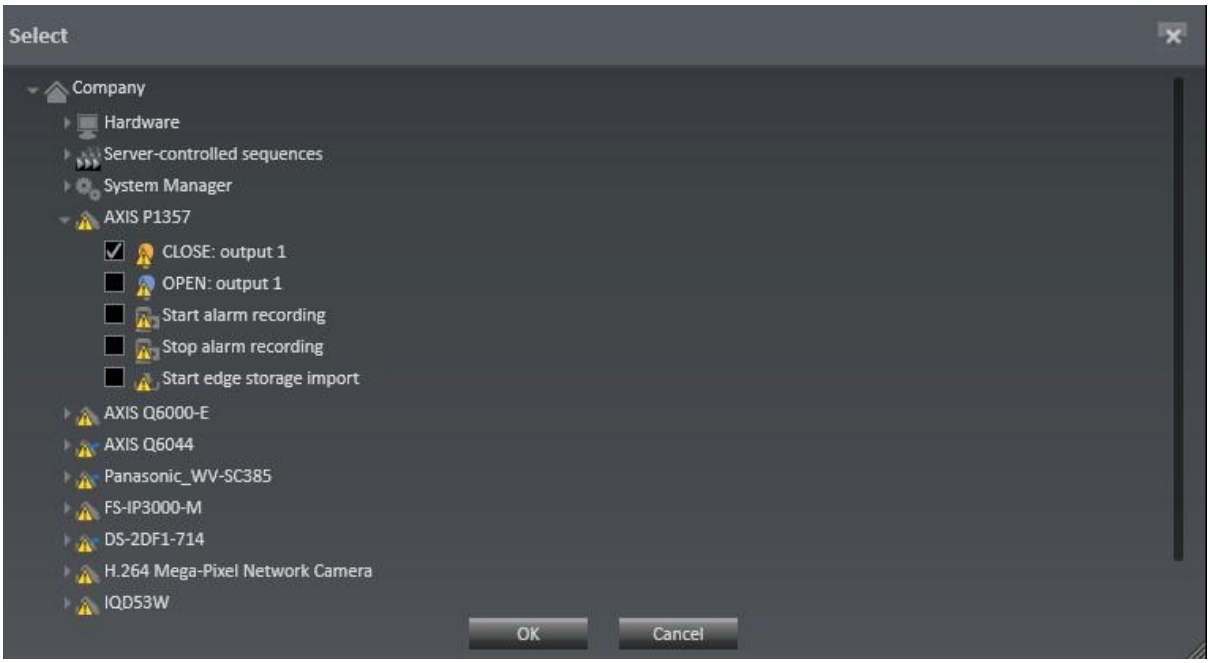


1. Activate or deactivate the camera. You can deactivate the camera without deleting it. This frees up one camera license and allows you to reactivate the camera at a later time without losing configuration settings.
2. If desired, modify the **Name** of the camera. This is how it will appear in Ocularis Administrator.
3. **Stream audio/video** is set to Always by default. This means that the camera will always stream live video (and audio) to the device manager whether anyone is viewing the stream or not. You can change this to 'On Demand' or 'On Demand - Quick Stream Start' if you want to be able to enable or disable a

stream whenever you want via Trigger or Alarm Scenario. See **Stream On Demand** for more information.

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. The Camera type:
   - **Camera**: The camera is used with or without the PTZ control functions, depending on the camera type.

   This field displays the camera driver currently used.
   - **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 driver to a different model or manufacturer, click **Open converter** (see **Converting a camera**). If you are replacing one camera with the exact same make and model, you do not need to run the converter. Simply assign the new camera with the same IP address and user account credentials and replace the hardware. The system will recognize this new device and start recording immediately. The video from the replaced camera (whether it is the same model or not) will be retained for the duration of its retention period.
7. Select a **Custom icon** for the camera (see Managing sound and icon files) to change how it appears in the Cameras list.
8. If the camera was not mounted upright, you can use the **Rotate image** function. You can rotate the image in 90° steps (90°, 180°, 270°). Some rotation angles are only available for specific camera models.
9. Select **Control camera** if you are configuring a PTZ camera or a control unit in order to give the user the option of controlling the camera. This field may be active for non-PTZ cameras. In this case, it is non-functional.
10. Specify the **PTZ sensitivity** (available for PTZ cameras only) of the camera control.
11. Select the **camera position** (available for PTZ cameras only) to give the user the option of defining and using the preset camera positions.
12. Select **Invert PTZ control** (available for PTZ cameras only) to correctly control cameras that are mounted upside down.
13. 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.
14. Specify for **Timeout (s)** in seconds the time after which the action is to be performed if the PTZ-camera is inactive.
15. 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 not used in this version.
- The **Action when the video stream** is not used in this version.

16. 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.
17. Define a **Dead time (s)** in seconds for the selected action in which a network error will not trigger the action again.

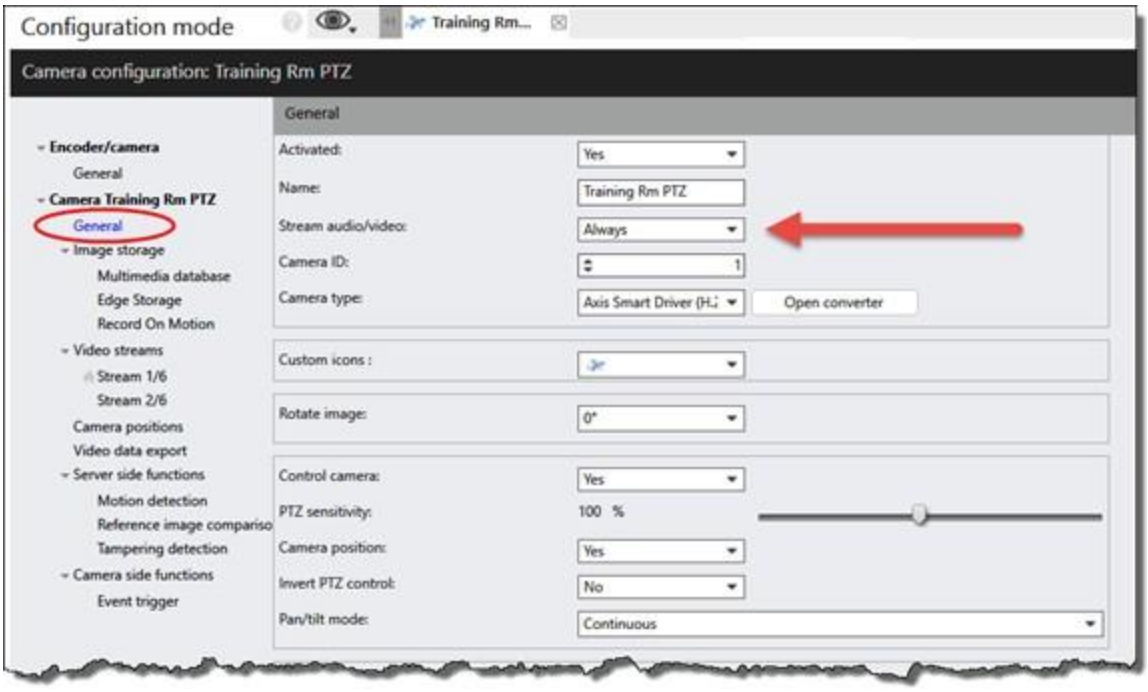
Stream On Demand

Some settings have been introduced on the recorder related to a camera's stream. Through the **Stream audio/video** option on the camera configuration screen you can determine whether a camera's stream is always streaming to the device manager or whether you want to reduce network traffic and only stream video when you need it. Similarly, you have the option to stop the stream as well.

This feature is commonly used in interview or interrogation rooms or anytime a meeting needs to be completely private. Not streaming video from a camera can also reduce network traffic and is especially useful in LTE environments. This feature applies to all streams from the camera. When a stream is stopped, video is not recorded nor available live to any client user. Audio is also not recorded or transmitted.

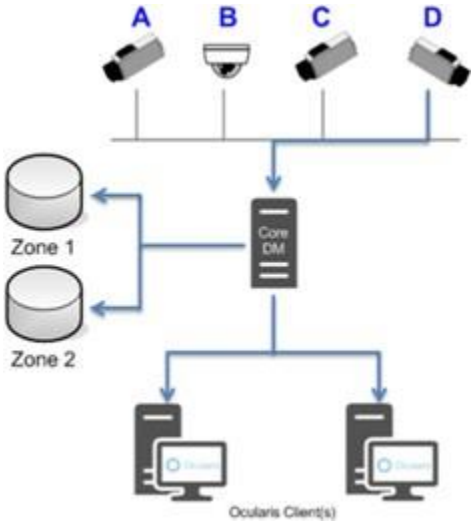
There are three options for the **Stream audio/video** field:

- Always
- On Demand - Quick Start
- On Demand



Streaming - Always

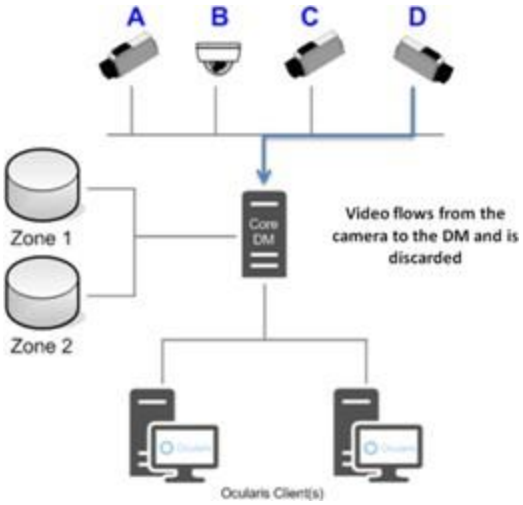
When the **Stream audio/video** drop-down is set to 'Always', the default value, live video streams from the camera to its assigned device manager. If Standard Recording is set to 'Yes' and the recording period is set to 'Always', the camera streams 24/7/365 and cannot be turned off manually. If configured, video is recorded to its corresponding zone(s) and sent to any authorized client (Ocularis Client, Ocularis Web or Ocularis 5 Mobile) seeking to view it.



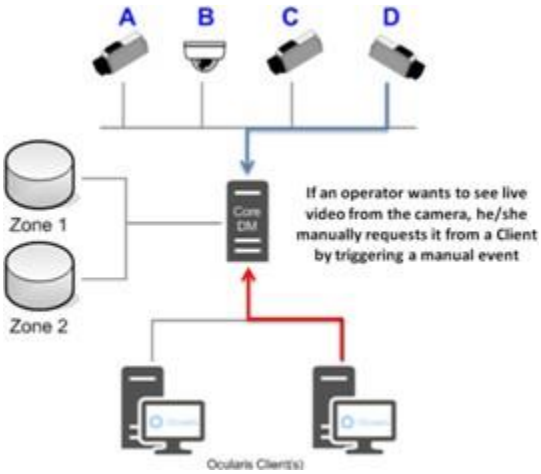
Streaming - On Demand - Quick Stream Start

When the option **On Demand - Quick Stream Start** is selected, video streams from the camera to its device manager but is then discarded. In *Ocularis Client*, a view pane with this camera appears empty with the message 'Camera connection lost' when a view with the camera is displayed. If an operator wants to view video from that camera, he/she must manually request it from a client by alarm scenario or executing a manual

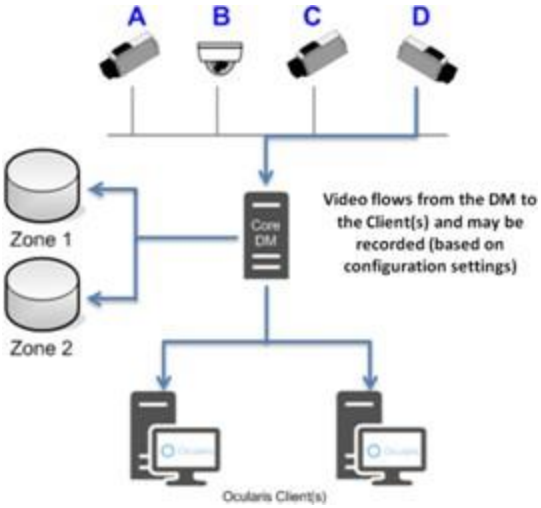
event (such as a trigger). Once the stream is enabled, it can be recorded (if configured to do so) or displayed to any client requesting it. The stream remains active until disabled via another event (either manual or automated).



Video flows from the camera to the DM and is discarded.



If an operator wants to view live video he or she can request it via manual trigger from Ocularis Client, Ocularis Web or Ocularis Mobile. (providing that a camera level trigger has been configured in advance).



Streaming - On Demand

When the option **On Demand** is selected, video does not stream from the camera to its device manager. A view pane with this camera appears empty with the message 'Camera connection lost' when a view with the camera is displayed. If an operator wants to view video from that camera, he/she must manually request it from a client by alarm scenario or executing a manual event (such as a trigger). Once the stream is enabled, it can be recorded (if configured to do so) or displayed to any client requesting it. The stream remains active until disabled via another event (either manual or automated). Since the video when using the 'On Demand' option does not stream from the camera to the device manager by default, network traffic is reduced. This feature is also useful if transmitting camera video via wireless over broadband.

Using Triggers to Control Streams

In order to take advantage of the On Demand streaming function, you need a mechanism to be able to start or stop the live stream. This is done by using a trigger or alarm scenario. Triggers may be camera specific or global.

Camera Specific Triggers

Camera specific triggers may be used to disable or enable a stream set to 'On Demand' or 'On Demand Quick Stream Start'. These triggers are available for use (given permission) with Ocularis Client, Ocularis Web and Ocularis Mobile. They are accessible via the 'aux' menu on the camera pane in Ocularis Client. For Ocularis Web, they appear when the trigger icon in the camera's pane is selected. For Ocularis Mobile, a list of camera specific triggers appears when the camera is selected (you may have to swipe left or right in portrait mode to view the list).

To Create a Camera Specific Trigger

These steps assume that the camera's stream mode is already set to 'On Demand' or 'On Demand Quick Start'.

1. Using *Ocularis Recorder Manager*, select 'Triggers' from the Control Bar and create a new trigger by clicking the 'Create new object' tool.
2. Provide a name for the trigger. Keep in mind this is the label that is visible in a client. It should be as descriptive as practical and will be listed in the order in which it is created. You will create a trigger to start or enable the stream as well as to stop or disable the stream. Click **OK**.
3. If you want to change the icon that will appear adjacent to the trigger in *Ocularis Recorder Manager*, select it from the Icon drop-down menu. This is optional.
4. Click the checkbox for 'Specific camera'.

5. Select the camera you are configuring.
6. Next, select 'Action' on the left panel.
7. Select the 'Perform action' radio button which enables a **Select** button.
8. Click the **Select** button.
9. Expand the camera you are configuring. You should see an entry to 'Disable stream' and to 'Enable stream'. Select one of these and click **OK.**
10. Click **Save** to save changes and close the tab.
11. Repeat these steps to create a second trigger to start or stop the stream.
12. Once all triggers have been created, perform a manual refresh on the recorder within *Ocularis Administrator* (right-click and select 'Refresh Server').

▸ To Use a Camera Specific Trigger

From *Ocularis Client*, select the 'aux' overlay icon in the camera's view pane to access the enable or disable stream trigger.

From *Ocularis Web*, the trigger appears when the trigger icon is clicked from within the camera pane.

From *Ocularis Mobile*, select the camera and view the camera specific triggers after selecting a camera for viewing.

NOTE: Since a camera set to 'On Demand' or 'On Demand Quick Start' will initially be disabled, the 'aux' overlay icon in Ocularis Client will not be initially visible. Therefore, it is recommended to also set a Global Trigger to enable a camera

Global Triggers

Global triggers may also be used to disable or enable a stream set to 'On Demand' or 'On Demand Quick Stream Start'. These triggers are available for use (given permission) with *Ocularis Client* and *Ocularis Web*. They are accessible via the 'Triggers' menu in *Ocularis Client*. For *Ocularis Web*, they are accessed from the Triggers icon in the Task Bar.

▸ To Create a Global Trigger:

These steps assume that the camera's stream mode is already set to 'On Demand' or 'On Demand - Quick Start'.

1. Using *Ocularis Recorder Manager*, select 'Triggers' from the Control Bar and create a new trigger by clicking the 'Create new object' tool.
2. Provide a name for the trigger. Keep in mind this is the label that is visible in a client. It should be as descriptive as practical and will be listed in alphabetical order in the menu list. Therefore, you may want to prepend the name of the trigger with the name of the camera such as:
   - Camera 1234 - Start Stream Camera 1234 - Stop Stream
   - The naming convention will group the triggers for the camera together based on alphabetical order. You can create a trigger to start or enable the stream as well as to stop or disable the stream.
3. Click **OK**.
4. If you want to change the icon that will appear adjacent to the trigger in Ocularis Recorder Manager, select it from the Icon drop-down menu. This is optional.
5. Next, select 'Action' on the left panel.
6. Select the 'Perform action' radio button which enables a **Select** button.

7. Click the **Select** button.
8. Expand the camera you are configuring. You should see an entry to 'Disable stream' and to 'Enable stream'. Select one of these and click **OK**.
9. Click **Save** to save changes and close the tab.
10. Repeat these steps if you want to create a second trigger to start or stop the stream.
11. Once all triggers have been created, perform a manual refresh on the recorder within *Ocularis Administrator* (right-click and select 'Refresh Server').

To Use a Global Trigger

- From *Ocularis Client*, select the 'Triggers' menu when in Live mode. Expand 'Global Triggers'. Select the global trigger from the displayed list .
- From *Ocularis Web*, the trigger appears when the global trigger icon is clicked from the Task Bar at the bot- tom of the screen.

Global triggers are not supported with *Ocularis Mobile* as of this writing.

Using Global Triggers to Control Multiple Cameras:

You may wish to enable or disable a group of cameras at the same time. For instance, if you have multiple cameras in a conference room and have a private meeting, there is a way to disable all cameras in one step. (Conversely, you can enable them in one step as well). In this case, you need to configure an alarm scenario to disable or enable the cameras and then create a trigger for each scenario.

1. The first step is to create the alarm scenario. From *Ocularis Recorder Manager*, select 'Alarms' from the Control Bar and create a new alarm scenario by clicking the 'Create new object' tool.
2. Provide a name for the scenario such as 'Conference Room A - Enable All Cameras' and click **OK**.
3. If you want this feature available at only designated times, change the 'Validity' period by selecting another Time profile. Otherwise, it will be available 'Always'.
4. Click 'Server' from the left panel.
5. Click the **Edit** button under 'Actions at start of alarm'.
6. For each camera you wish to configure, expand it in the pop-up and select 'Enable stream'. This assumes that you have already configured the camera's stream mode to 'On Demand' or 'On Demand Quick Start'. You may select as many cameras as necessary. When done, click **OK**.
7. Click **Save**.
8. Repeat the above steps for an alarm scenario to disable the same cameras.
9. When done, create a new Trigger for each alarm scenario. Select 'Triggers' from the Control Bar and create a new trigger by clicking the 'Create new object' tool.
10. Provide a name for the trigger. Keep in mind this is the label that is visible in a client. It should be as descriptive as practical and will be listed in alphabetical order in the menu list. Therefore, you may want to prepend the name of the trigger with the name of the camera such as:

    Conference Room A - Disable All Cameras Conference Room A - Enable All Cameras
    The naming convention will group the triggers for the camera together based on alphabetical order. Click **OK**.
11. If you want to change the icon that will appear adjacent to the trigger in *Ocularis Recorder Manager*, select it from the Icon drop-down menu. This is optional.

12. Next, select 'Action' on the left panel.
13. Select the 'Start alarm scenario' radio button which enables a drop-down menu.
14. Select the corresponding alarm scenario from the list.
15. Click **Save** to save changes and close the tab.
16. Repeat these steps if you want to create a trigger to start or stop the streams.
17. Once all triggers have been created, perform a manual refresh on the recorder within *Ocularis Administrator* (right-click and select 'Refresh Server').

Alerts From an Enabled or Disabled Stream

Alerts with Streams

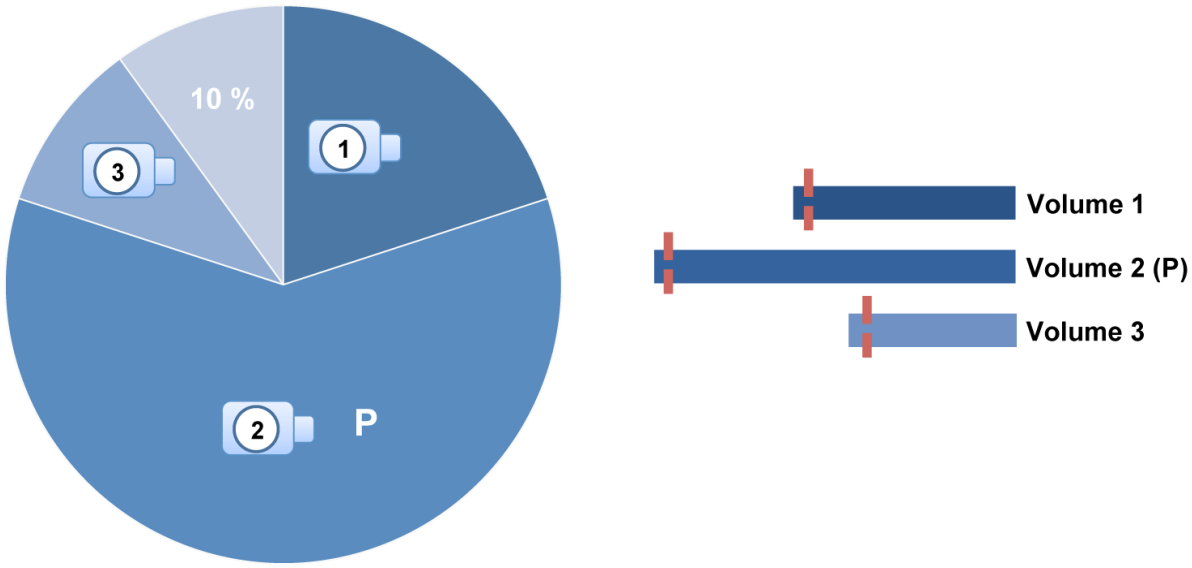
If you want to be notified when a camera stream is enabled or disabled, you may do so using a new event for this in the 'Event Filters' list of the *Ocularis Recorder Proxy*. Under 'Camera Events' you can select 'Disable Stream' and / or 'Enable Stream'. You still need to configure the event using *Ocularis Administrator* as you would any other event (i.e. map a camera to the event in the Servers / Events Tab and designate event distribution rules in the Distribution Groups Tab.)

7.4.1.5 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

Images are stored according to the so called "ring buffer" queue. For a brief overview, see the following illustration:



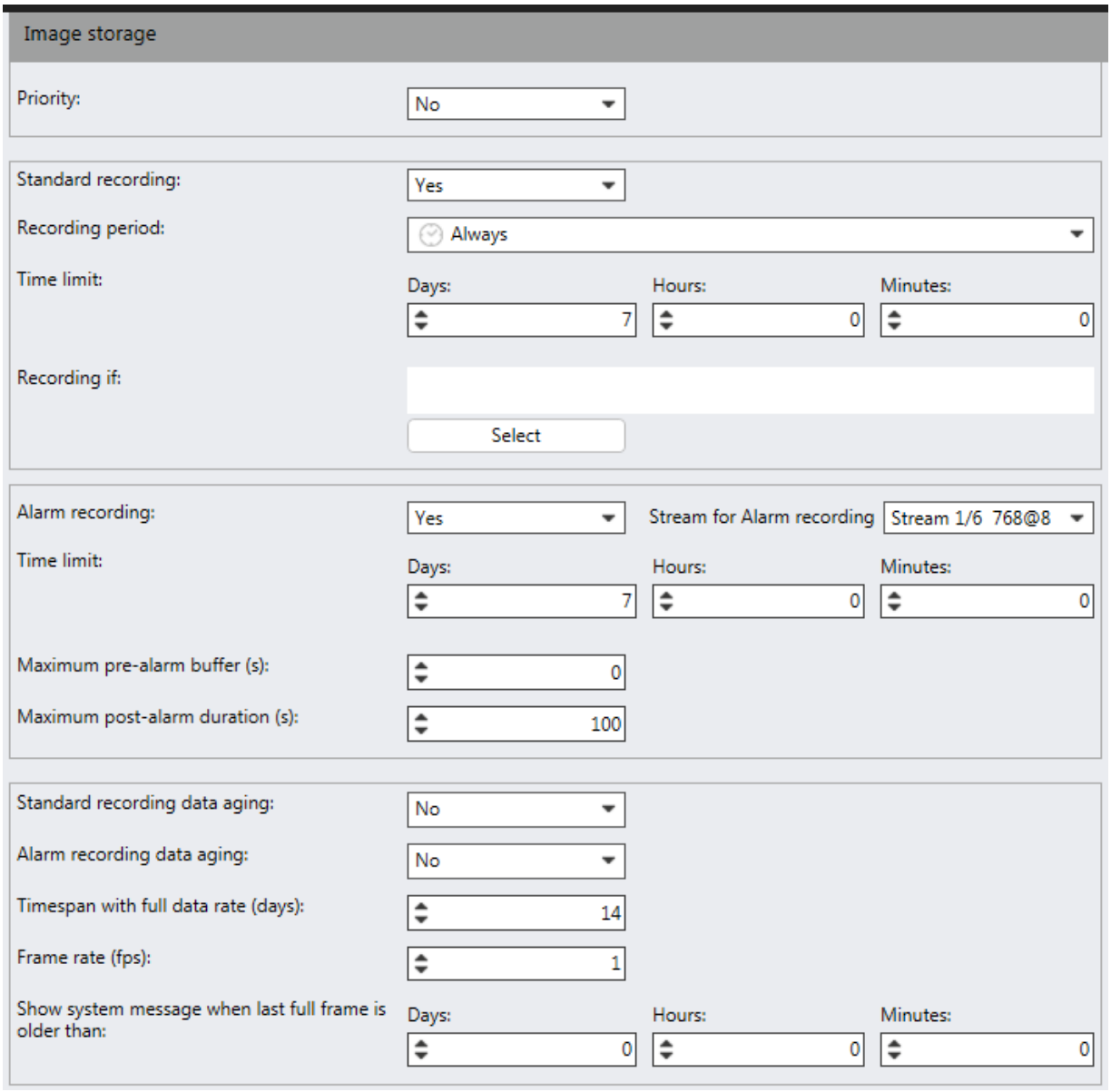
All of the image storage settings (e.g. the size of a camera's storage area on the hard disk) are configured here. To prevent sensitive image data from being overwritten, standard and alarm recordings are configured separately.

Images must be deleted in the following order:

1. Standard recordings
2. Alarm recordings
3. Prioritized standard recordings
4. Prioritized alarm recordings

When the storage capacity reaches 90%, a message is triggered via SNMP, email or as message in the client.

As soon as the storage capacity reaches 95%, the ring buffer system starts deleting the oldest image data. The image data of the prioritized cameras are the last to be deleted.



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. The default value is **Yes**.
4. Select the **Recording period**. You can specify an exact period using a time profile that you create in time management (see **Time management**). By default, continuous recording is started ("Always"). Stream 1 is always used for Standard recordings.
5. Select the **Time limit** to retain this video and enter the maximum storage duration. If the time limit is exceeded, some of the oldest recordings will be deleted to free storage.

6. You can specify a condition on available digital inputs for starting image recording.

7. Select whether **Alarm recordings** are to be carried out with this camera. The default value is **Yes**.
8. If you want a different stream to be used for alarm recording, select it from the **Stream for alarm recording** drop-down menu. The stream should be created prior to configuring in the Image storage screen. You may consider configuring a second stream at a higher resolution than stream 1 and use this stream for alarm recordings.
9. Select the **Time limit** to retain this video and enter the maximum storage duration. If the time limit is exceeded, the oldest recordings will be deleted to free memory.
10. In the **Maximum Pre-alarm buffer** (up to a maximum of 3600 seconds) field, enter a value you would like to be the maximum for any alarm scenarios that use alarm recording. This value can be changed individually on each alarm scenario. This value is only used in alarm scenarios.
11. Specify a **Maximum post-alarm duration** to be used as the highest amount of time to be used for duration when setting up alarm scenarios that use alarm recording. This can be changed individually for each alarm scenario. This value is only used in alarm scenarios.
12. In Ocularis Ultimate only: 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.

1. Specify the **Timespan** after which the recordings are to be compressed and released from the audio track. Keep in mind that this value should be less than the retention time limit for Standard or Alarm recordings.
2. 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 recordings will be reduced to i-frames (the p-frames will be deleted

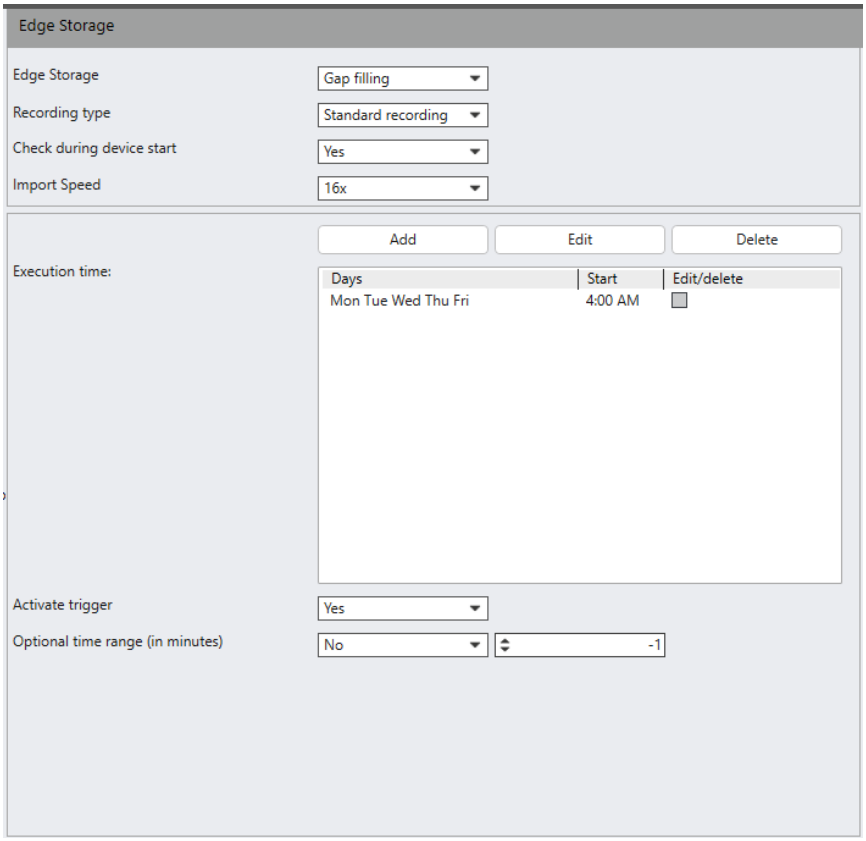
NOTE: The **Standard recording data aging** and **Alarm recording data aging** values must be less than the **Time limit** values set on the screen above. If they are greater than these values, the data aging process will not take place.

Also, any audio recorded will be removed during the aging process.

3. Set a time frame after which a system notification is triggered if the last full frame recorded is older than the specified time.

Edge storage

The menu item "Edge storage", an Ultimate only feature, is only displayed if supported by the selected camera.



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 the camera. Both use cases require a license which includes edge storage functions.

There are various options to configure edge storage in configuration mode:

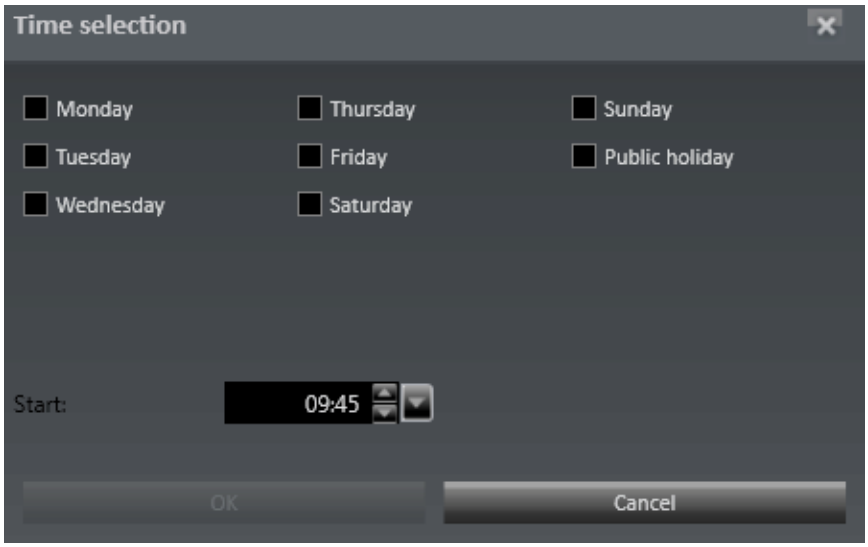
- Edge Storage: Options are: Disabled, Gap filling or Full import
- **Recording Type**: Standard recording or alarm recording

- **Check on device start**: If set to 'Yes', when a device is started or reboots after network failure, the import will be triggered
- **Import Speed**: some cameras allow for faster imports than the default 1x ratio
- Import triggered by schedule (see **Gap filling**)
  - Manual import of a time range in archive mode (this feature is not supported in this version)
  - 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

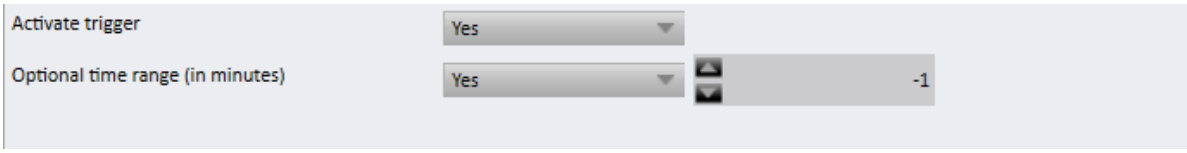
Important remarks:

- The transmission speed of the video can be set in the DM configuration file(C:/Program Files/Qognify/Ocularis Recorder/conf/dm.conf.xml).
- The Tag <EdgeStorageSpeed> holds the value for video transmission from Edge Storage to Ocularis. After changing the speed setting, restart the DM service.
- 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 dataloss.
- Make sure that the camera date / time is synchronized with the date and time on the Ocularis 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.
- 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.
- Overwrite protection of recordings will be ignored.
- 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.

Gap filling



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 Ocularis Recorder looks automatically for gaps in the recordings and fills them up. A daily system check is recommended.

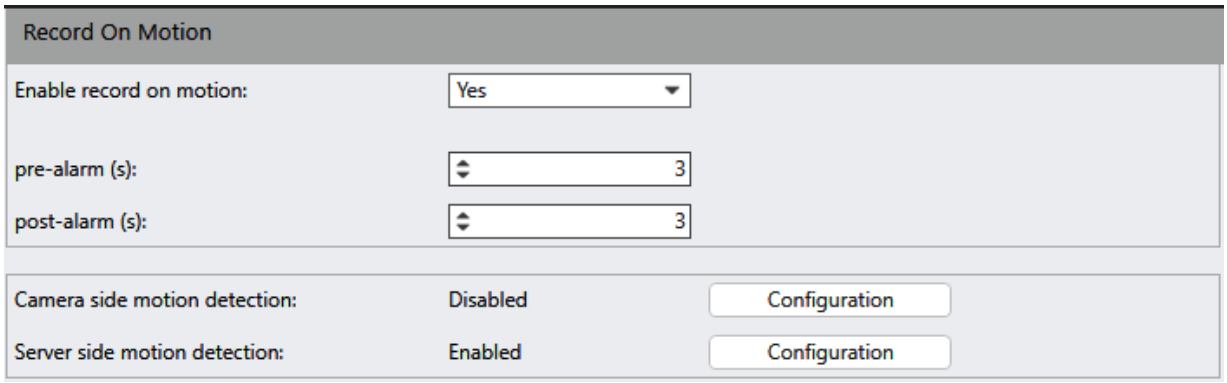


4. To trigger an alarm scenario, set **Activate trigger** to **Yes**.
5. Activate **Optional time range (in minutes)** and specify the number of minutes of excess time before and after the actual gap filling. The data from the camera will deliver not only the missing time frame, but also a surplus to prevent gaps.

Record on motion

The feature Record on motion allows a quick and simple configuration of an alarm recording due to motion. When motion is detected, video is recorded. When motion stops, video recording stops. (this is unlike an alarm scenario where video is recorded for a set duration whether there is motion or not.)

Record on motion does not replace a complete alarm scenario (see **Alarms**). Qognify recommends converting your motion alarms to Record on Motion.



1. Activate **Enable record on motion** if there should be an alarm recording as the result of an enabled server-based or camera-based motion detection.
2. Deactivate **Enable record on motion**. You will be asked if server-based motion detection should be deactivated.
3. Specify a pre-alarm duration or "pre-buffer" (optional).
4. Specify a post alarm duration or "post-buffer" (optional).
5. The **Configuration** buttons adjacent to Camera side or Server side motion detection will switch to the corresponding configuration screen.

You must have either server-side or camera-side motion detection enabled first prior to enabling record on motion in this screen.

Also, the Idle timer or Dead time value in the server-side/camera-side motion detection screens is ignored with Record on Motion.

More Information on Record on Motion

Record on Motion differs from the early versions of Ocularis in that if enabled, video will be recorded when there is motion only. When motion stops, recording stops. In Ocularis.1, the only option for motion recording was where video was recorded for a set duration whether motion continued or not. While this form of motion detection recording is still available in v5.2 and later, **Record on Motion** is much more efficient and makes better use of storage space. It also eliminates the need for alarm scenarios which frees up resources on the core. Video recorded using Record on Motion will be categorized as alarm recording. With **Record on Motion**, you can set pre and post buffers on a camera-by-camera basis. Multi-camera configuration is also supported and you can enable **Record on Motion** when adding cameras using the Device Finder.

Record on Motion may be used with either camera side or server side motion detection. It also supports the use of motion detection regions inside an image.

Configuring Record on Motion

In order to enable **Record on Motion**, either camera side or server side motion detection must be enabled first. The following examples will be discussed:

- Configuring Record on Motion on a Single Camera
- Configuring Record on Motion on a Group of Cameras
- Configuring Record On Motion When Adding Cameras

To Configure Record On Motion on a Single Camera

1. In Ocularis Recorder Manager, open the configuration screen for the camera you wish to configure.
2. Choose Motion Detection under either 'Server side functions' or 'Camera side functions'.
   - Camera side:
     a. Activate one or more preconfigured windows to be used for motion detection analysis.
     b. The Dead time setting will be ignored by **Record on Motion**.
     c. Click **Apply**.
   - Server side:
     d. Set Activate motion detection to Yes using the drop-down.
     e. Set the desired **Sensitivity** and **Threshold**.
     f. The Idle timer will be ignored by Record on Motion.
     g. If you want to apply **Activate Filter**, set this field to **Yes**. (for more information see **Motion detection**)
     h. If you wish to set one or more regions in the image, use the plus and polygon tools
     i. Adjust **Sensitivity** and **Threshold** for each region separately.
     j. Click **Apply**.
3. Choose **Record On Motion** under 'Image Storage'.
4. Enable **Record on Motion** by selecting **Yes** from the drop-down list.
5. Pre and post buffer is defaulted to 3 seconds for each. Modify these values if desired.

NOTE: The system recognizes that Camera side or Server side motion detection is enabled. You must first enable it prior to saving this screen.

6. Click **Save** to save these settings.

That's it! You are done!. Alarm scenarios need not be configured. The video that is recorded due to motion will be coded in red on the Kinetic Timeline in Ocularis Client.

To Configure Record On Motion on a Group of Cameras:

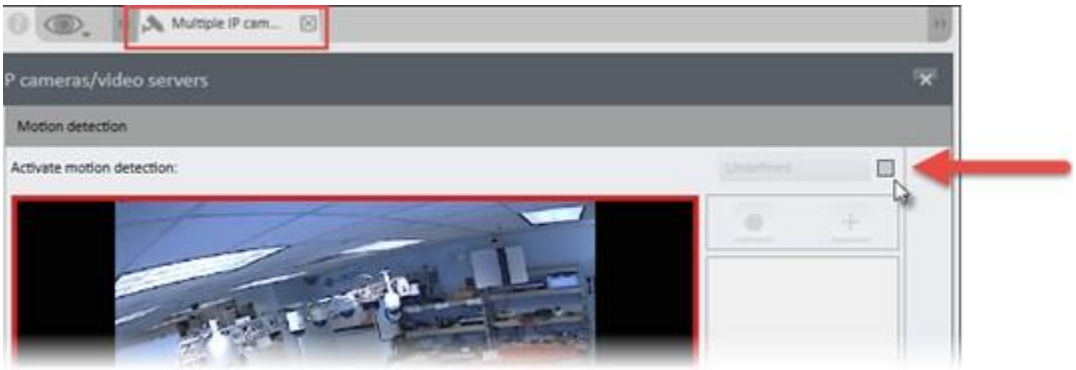
Multi-camera configuration is supported with **Record on Motion**. Remember that either camera side or server side motion detection must be enabled first. This example is going to use server side motion detection.

1. In Ocularis Recorder Manager, select the checkbox next to each you wish to configure.

2. Click the **Edit** tool.

NOTE: The configuration tab is labeled 'Multiple IP cam...' to indicate that multiple cameras will be configured.

3. Choose **Motion Detection** under 'Server side functions'.



4. Check the checkbox next to the drop-down for **Activation Motion detection**.
5. Once checked, the drop-down is enabled. Set this to **Yes**.
6. Click **Apply**.
   Sensitivity and **Threshold** will need to be adjusted later for each camera individually.
7. Choose **Record On Motion** under 'Image Storage'.
8. Click the checkbox next to **Enable Record on Motion**.
9. Select **Yes** from the drop-down list.
10. If you want to apply the same Pre and post buffer settings to the cameras, click the corresponding checkboxes to enable the field entry and set the desired change. Otherwise, the defaults of 3 seconds each will be applied.
11. Click **Save** to save these settings on all cameras.

To Configure Record On Motion During Camera Installation

When using the Device Finder Tool to add cameras, you may also enable server side motion detection and Record on Motion.recording.

1. In Ocularis Recorder Manager, launch the Device Finder.
2. Locate and select the cameras you wish to add. You may also use the Recorder Migration Tool to add cameras.
3. For each camera that you wish to enable Record on Motion, click the checkbox under Record on Motion.

4. When done, click Add. You can add with mult-config if you want.

Now these cameras will have server side motion detection activated and Record on Motion enabled. You should still review and if necessary modify the **Sensitivity** and **Threshold** settings for each camera in the Server Side Motion Detection screen.

Motion Detection Recording and Upgrades From V5.1

If you have what was considered 'Basic' motion detection recording configured on your v5.1 system (i.e. where the Record on Motion drop-down was set to 'Yes' but no alarm scenarios were created. Video was recorded for 30 seconds regardless of whether there was continued motion and with no pre or post buffer) and you upgrade to v5.2 or later (including upgrading the recorder), the system will convert these camera con- figurations and enable Record on Motion. No further action is required. Keep in mind that the default values for pre- and post- buffers of 3 seconds will be used. If you want, you may modify these settings. The set- tings in the server side or camera side motion detection screens remain unchanged.

If you have motion detection already configured in v5.1 using alarm scenarios and you upgrade to v5.2 or later (including upgrading the recorder), your alarm scenarios and motion detection recording will still con- tinue to work as before. No action is required.

However, we recommend that you enable some or all of your cameras for Record on Motion to take advant- age of its efficiencies. Remember that you can enable Record on Motion with multi-config for a group of cam- eras to make it easier. Also, if you do decide to enable Record on Motion, you will need to delete or deactivate the corresponding alarm scenarios. If you do not deactivate alarm scenarios that do motion detec- tion recording, they will continue to function as before and will result in excess video. Deactivating alarm scenarios is

supported with group edit to modify multiple scenarios in bulk. Reducing the number of alarm scenarios will also free up resources on the core.

7.4.1.6 Video streams

Under 'Video streams' you can specify and configure different profiles for the transmission of image data from the camera. Ocularis Recorder creates a base stream during installation of the camera. The base or Home stream, also known as Stream 1, cannot be deleted.

Two Camera Streams Created by Default

With the introduction of Ocularis 5.6 (R12), the default is to create two streams per camera when a new camera is added.

When a new camera is added to an Ocularis recorder, two streams will be created by default. This can save a huge amount of configuration time for the administrator. Having multiple streams is essential in Ocu- laris 5 since:

- Clients can automatically select the best stream for the display, improving performance and saving network bandwidth
- Operators can manually switch between streams, depending on the situation, saving CPU and RAM utilization
- Server-side motion detection can be configured to use an optimal stream
- Ocularis Web users will save time by having a second lower resolution H.264 stream created automatically

This functionality is enabled by default. Administrators have the option to disable it.

Creating a new video stream

Click **New** to create a new video stream. The maximum number of streams depends on the camera type.

Creation of Two Video Streams

Two camera streams will be created automatically when a camera is added.

- Applies to new cameras using a Smart Driver
- Cameras on upgraded systems will not be affected. However, the new feature will be enabled by default so any new cameras will be created with two streams
- This feature applies to cameras created manually, using the Device Finder or via .csv import

Automatic Stream Creation

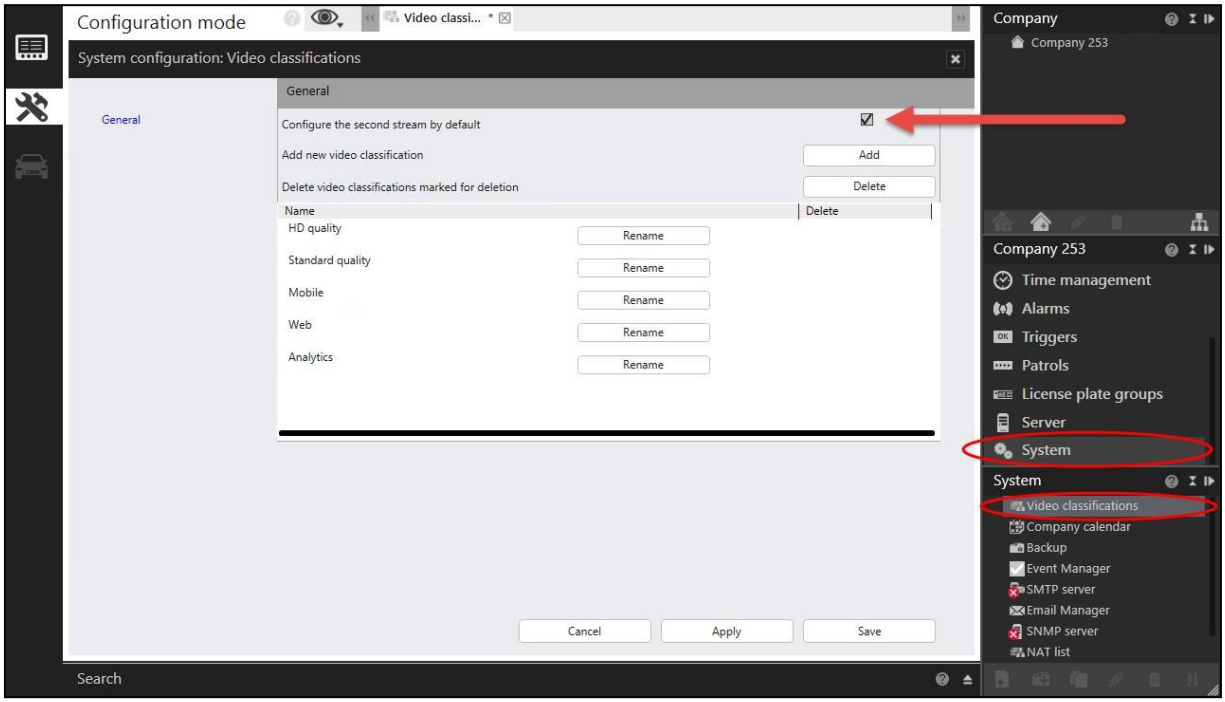
The first stream created is set to H.264 using the device's maximum resolution. The stream is automatically assigned the Video Classification of **HD quality** or whatever label that classification was renamed to. All other default values remain the same as before and may be edited manually.

The second stream is set to H.264 with a resolution as close to (but not exceeding) 800 x 600. It will be assigned the Video Classification **Standard quality** (or whatever label it was replaced with). Modify other fields manually.

If using Onvif check to see that the correct streams are chosen and if not, configure them as desired.

▸ To Enable / Disable Creation of Two Streams

1. In Ocularis Recorder Manager, select **System**.
2. Select Video Classification.
3. The checkbox **Configure the second stream by default** is checked. Uncheck to disable the feature.
4. Click **Apply** or **Save**.



Deleting a video stream

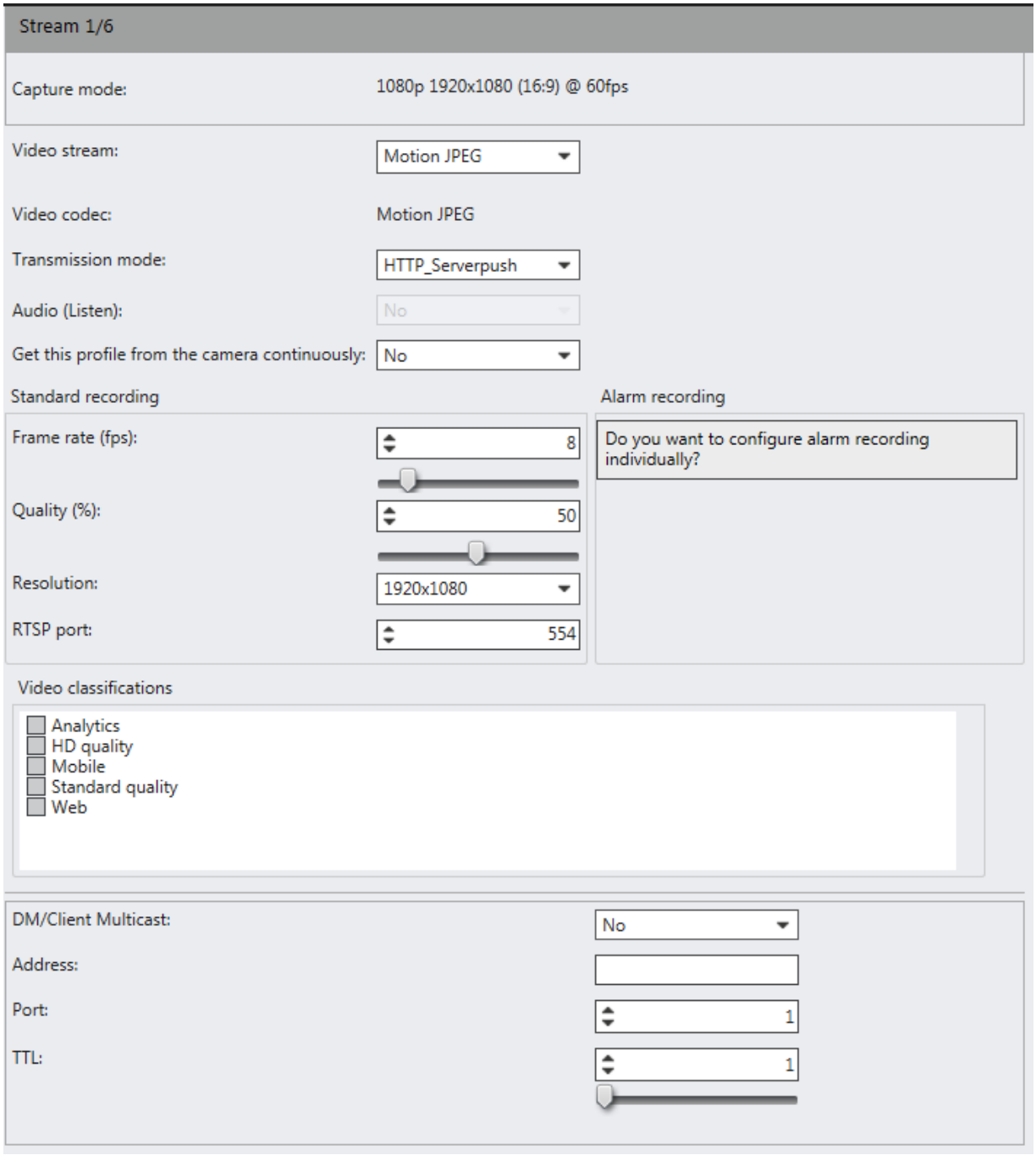
1. Select the video stream and click **Delete**.

Editing a video stream

1. Select the video stream, and then 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 with 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 then 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), see **Motion JPEG (M-JPEG)**
   - MPEG-4 / H.264 (required for audio), see **H.264 (MPEG-4)**

- H.265
- MxPEG
- RTSP

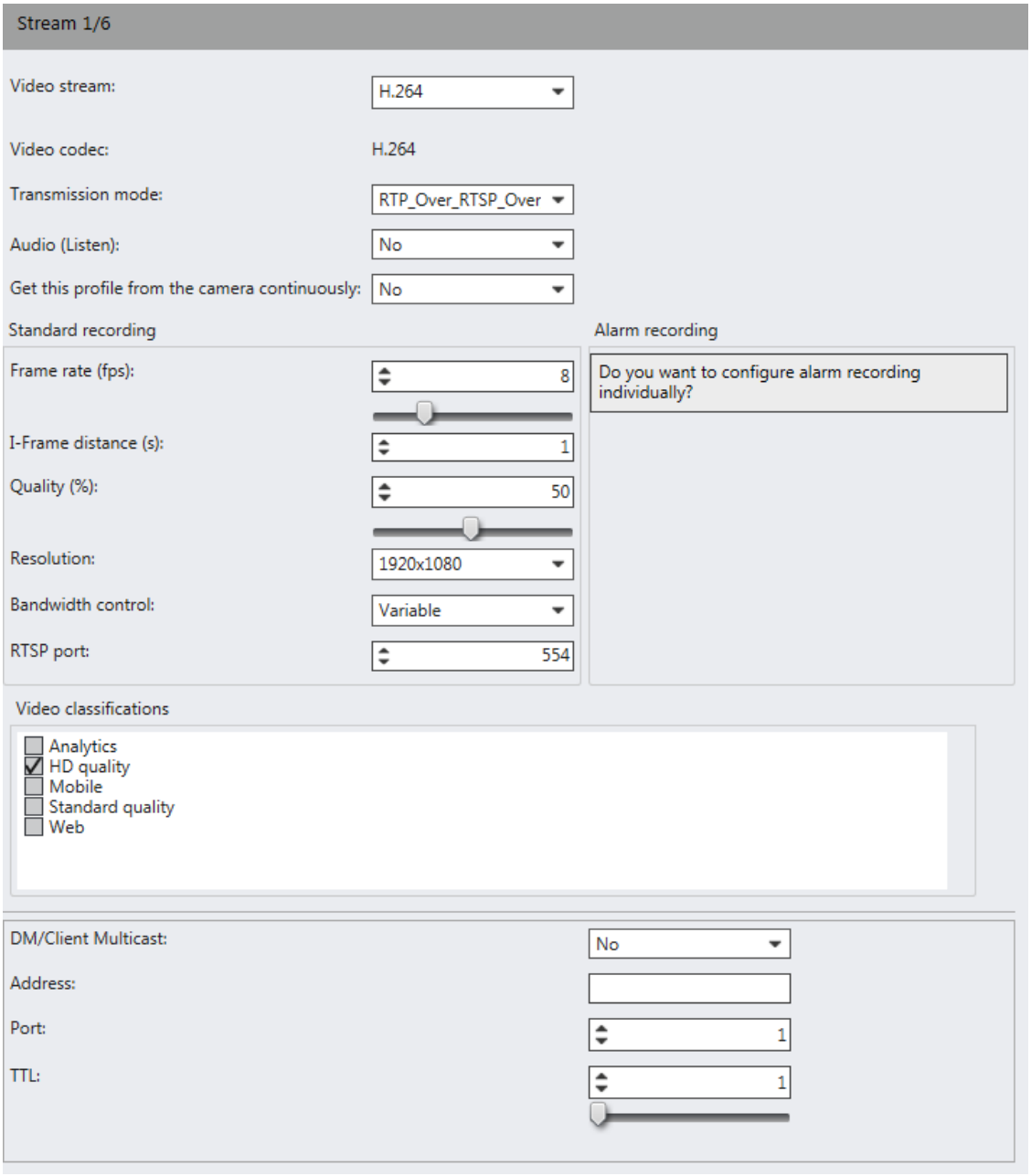
Motion JPEG (M-JPEG)



1. Select the **transmission mode** (only available mode for Motion JPEG): HTTP server push (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.
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.

NOTE: If you want the ability to set a default live stream, other than Stream 1 in Ocularis Client, you must assign a video classification to all streams. You cannot assign a video classification to Stream 1 until at least one other stream is created. Also, if using Ocularis Media Server for Ocularis Web and Mobile, and you have two or more streams, all streams must be assigned a video classification

H.264 (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 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 recorder and camera is via TCP port 554 (RTSP port). Image transmission is via a multicast address provided by the camera. RTP over UDP

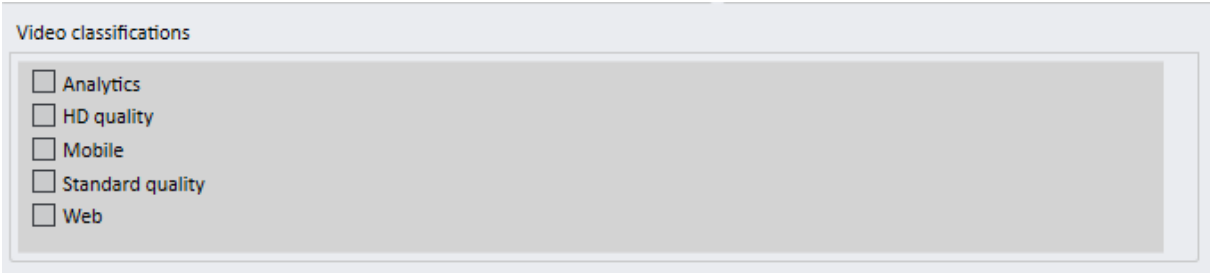
Multicast should only be used if third-party systems (e.g. Barco or eyevis) and the recorder access the camera simultaneously.

- **RTP over RTSP over TCP**: Communication between the recorder and camera and image trans- mission is via TCP port 554 (RTSP port). This setting is recommended for poor network connection between recorders 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 recorders and cam- era. Latency times may occur due to repeated transmission of corrupt data.

2. Select the transmission of audio signals. This function is available only if the camera can process audio signals in MPEG-4-based video streams.
3. Specify the **Frame rate (fps)** for standard recording
4. Define the I-frame distance for MPEG-4/H.264
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 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.
9. Optionally configure 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.

NOTE: If you want the ability to set a default live stream, other than Stream 1 in Ocularis Client, you must assign a video classification to all streams. You cannot assign a video classification to Stream 1 until at least one other stream is created. Also, if using Ocularis Media Server for Ocularis Web and Mobile, and you have two or more streams, all streams must be assigned a video classification.

Video classifications



This option is only available when multiple video-streams are specified for a camera. In this case, each stream must be classified. Classified streams can be used for multiple purposes. For example, the classification

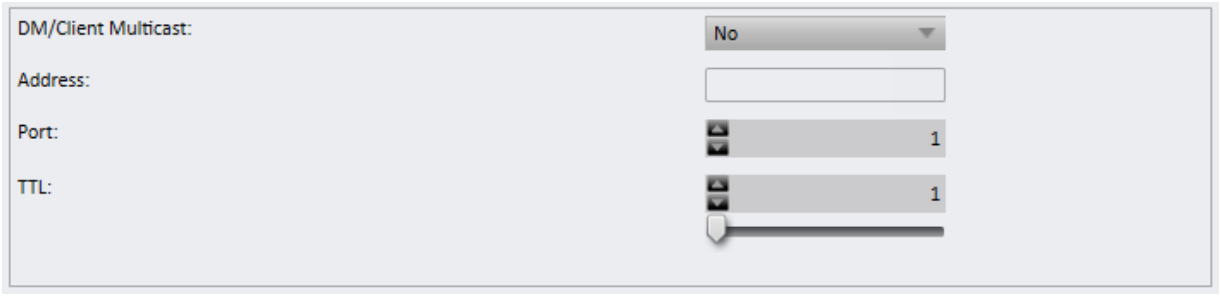
“Standard quality” can be used for standard recording and alarm recording may have the classification “HD quality”. You are able to select different viewing streams in Ocularis Client based on the Video Classification. These classifications are simply labels. You can modify the text of the existing classifications, delete or add your own.

NOTE: If you want the ability to set a default live stream, other than Stream 1 in Ocularis Client, you must assign a video classification to all streams. You cannot assign a video classification to Stream 1 until at least one other stream is created. Also, if using Ocularis Media Server for Ocularis Web and Mobile, and you have two or more streams, all streams must be assigned a video classification

1. Select the appropriate video classification (see **Configuring the video classification**).

DM / Client Multicast

This feature is only available in Ocularis Ultimate.



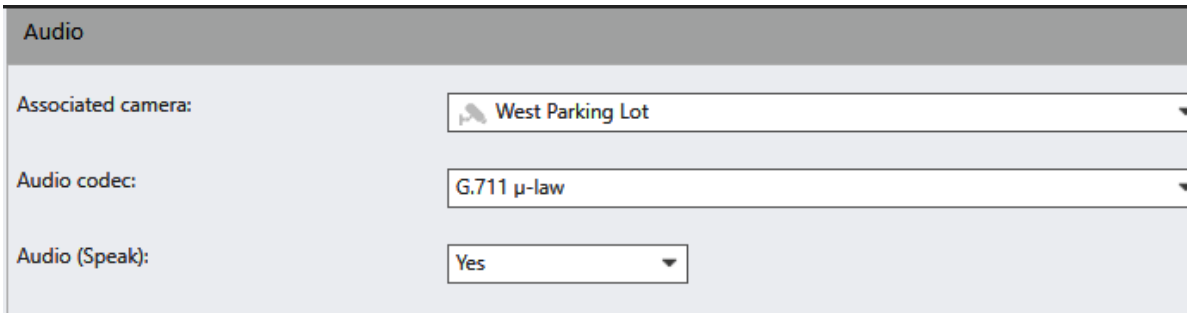
1. Select **DM / Client Multicast** streaming to display a single video stream simultaneously on multiple clients. Multicast should only be used if there is low bandwidth between the DeviceManager and clients. Multicast-capable network hardware is required for multicast streaming.
2. Enter the network address and port number of the multicast server.
3. Specify the validity period **TTL** after which the client has to log in to the multicast server again. A short TTL results in a higher network load.

7.4.1.7 Audio

If the camera supports transmission of audio signals, the audio codec can be configured. To listen to audio signals, the transmission has to be activated in the video stream settings (see **Video streams**).

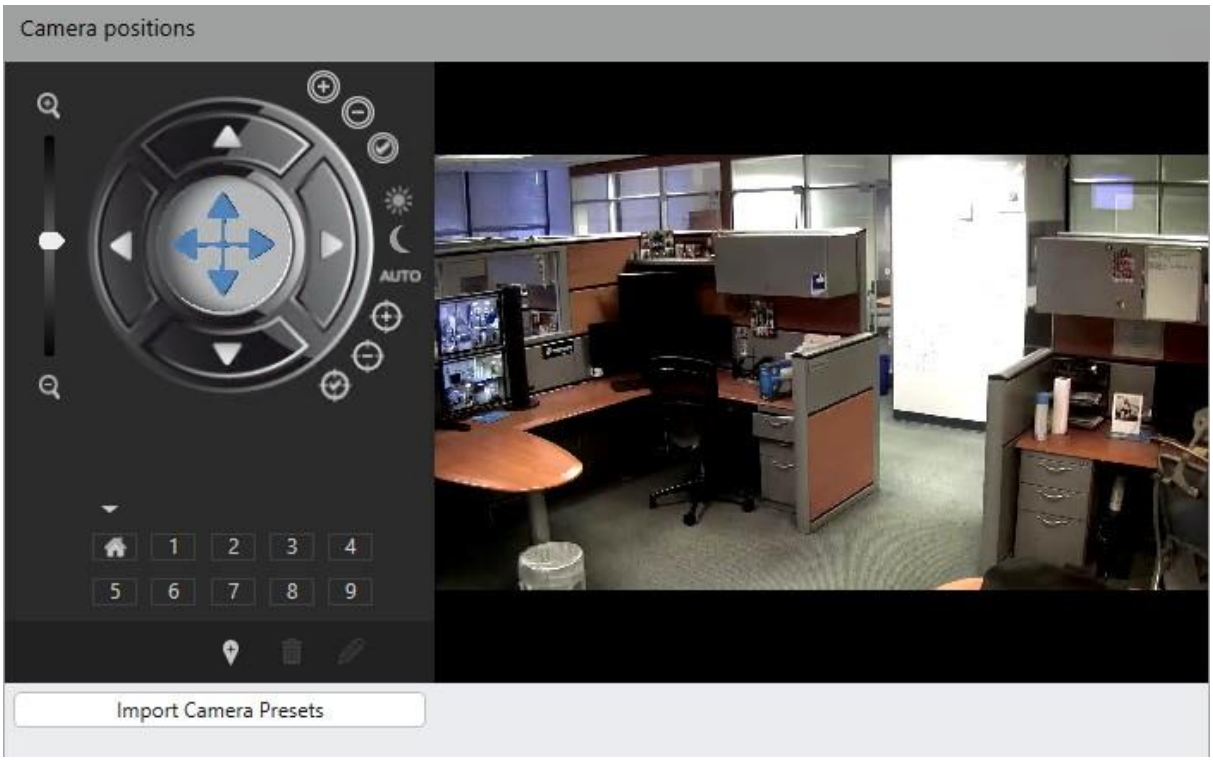
Camera selection is only necessary for multi-channel devices.

1. Select the MPEG-4/H.264 mode for video streams in the video stream settings
2. Select the associated camera.
3. Select the corresponding **audio codec**.
4. If the camera supports two-way audio, select **Yes** adjacent to 'Audio (Speak)'. When set to **Yes**, operators may communicate to the camera via connected microphone via *Ocularis Client*.



7.4.1.8 Camera positions / digital presets

If the selected camera is a PTZ camera, select 'Camera positions' to manage its presets. Camera positions can be created, deleted and modified.

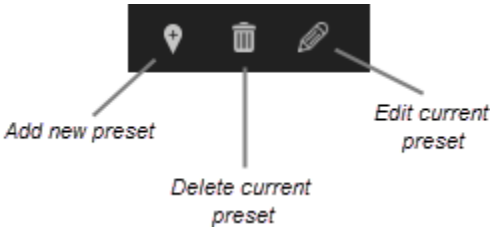


Depending on the camera the following features are available:

- Iris +
- Iris -
- Auto iris
- Day mode
- Night mode
- Auto day/night
- Close-up focus
- Long-range focus

- Auto focus

Presets are created and managed by the administrator. Use the preset toolbar to manage presets.



1. Use the PTZ controller or an external controller device to move the camera to the required position.
2. Click the **Add new preset** icon.
3. Enter the **name** of the new preset position, and then 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.

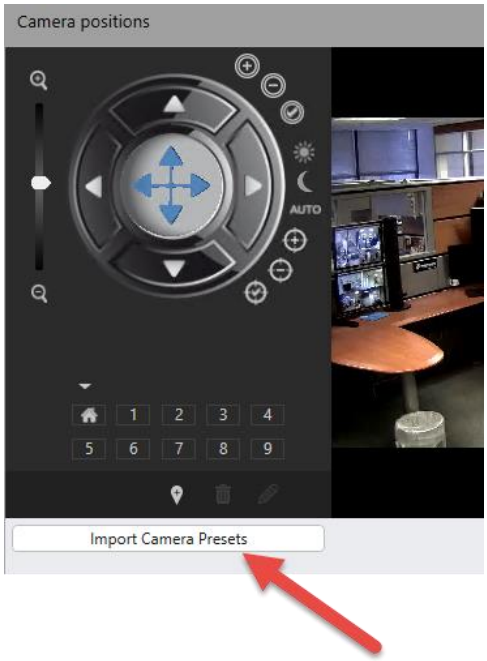
4. To remove a preset position, select the name from the list and click the **Delete current preset** icon.

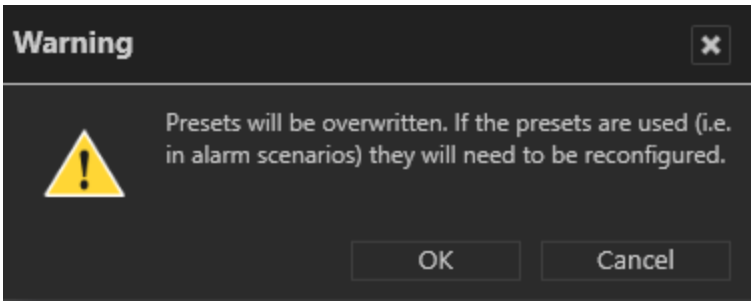
Importing Camera Presets

Preset positions that are already configured on the camera can be imported into the recorder configuration.

NOTE: This option is only available when the user has rights to create presets and camera position must be enabled in the General Camera Configuration screen.

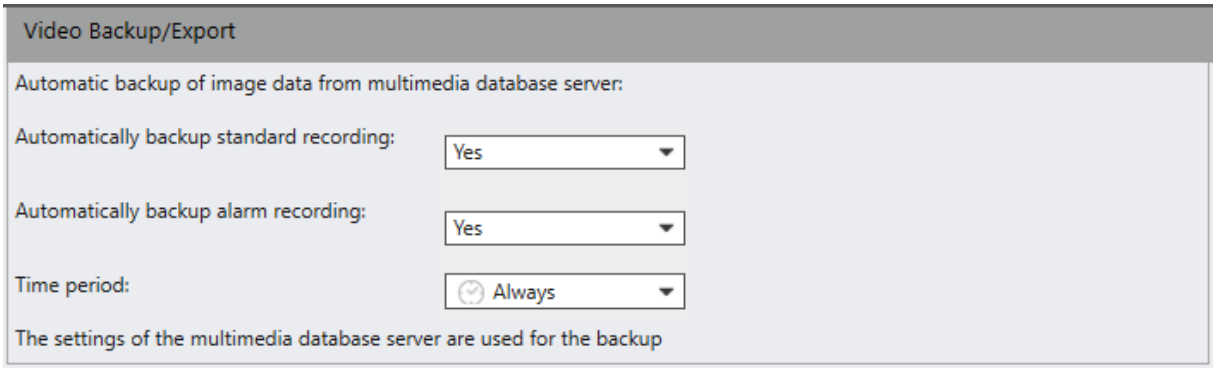
1. Click the **Import Camera Positions** button under the PTZ controls. A pop-up warning appears.





2. When importing preset positions from a camera, all presets already configured in Ocularis Recorder Manager will be overwritten!
3. Click **OK** to import the presets.

7.4.1.9 Video Backup/Export



Automatic export of image data from the database server

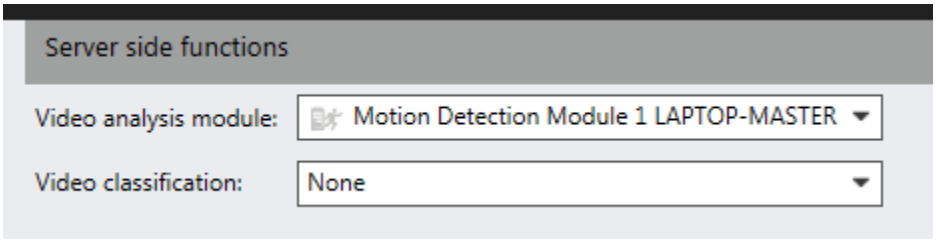
Recordings can automatically be exported to a path on the DeviceManager e.g. for long-time archiving of recordings.

1. Specify whether standard recordings and alarm recordings are to be exported automatically. The time and path for the automated export must be configured in the DeviceManager configuration (see **Configuring the Device Manager (DM)**). 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**).

NOTE: If the export process is interrupted (e.g. due to a network error), it will be automatically resumed as soon as possible.

The remaining portion of this screen is not used in this version.

7.4.1.10 Server side functions

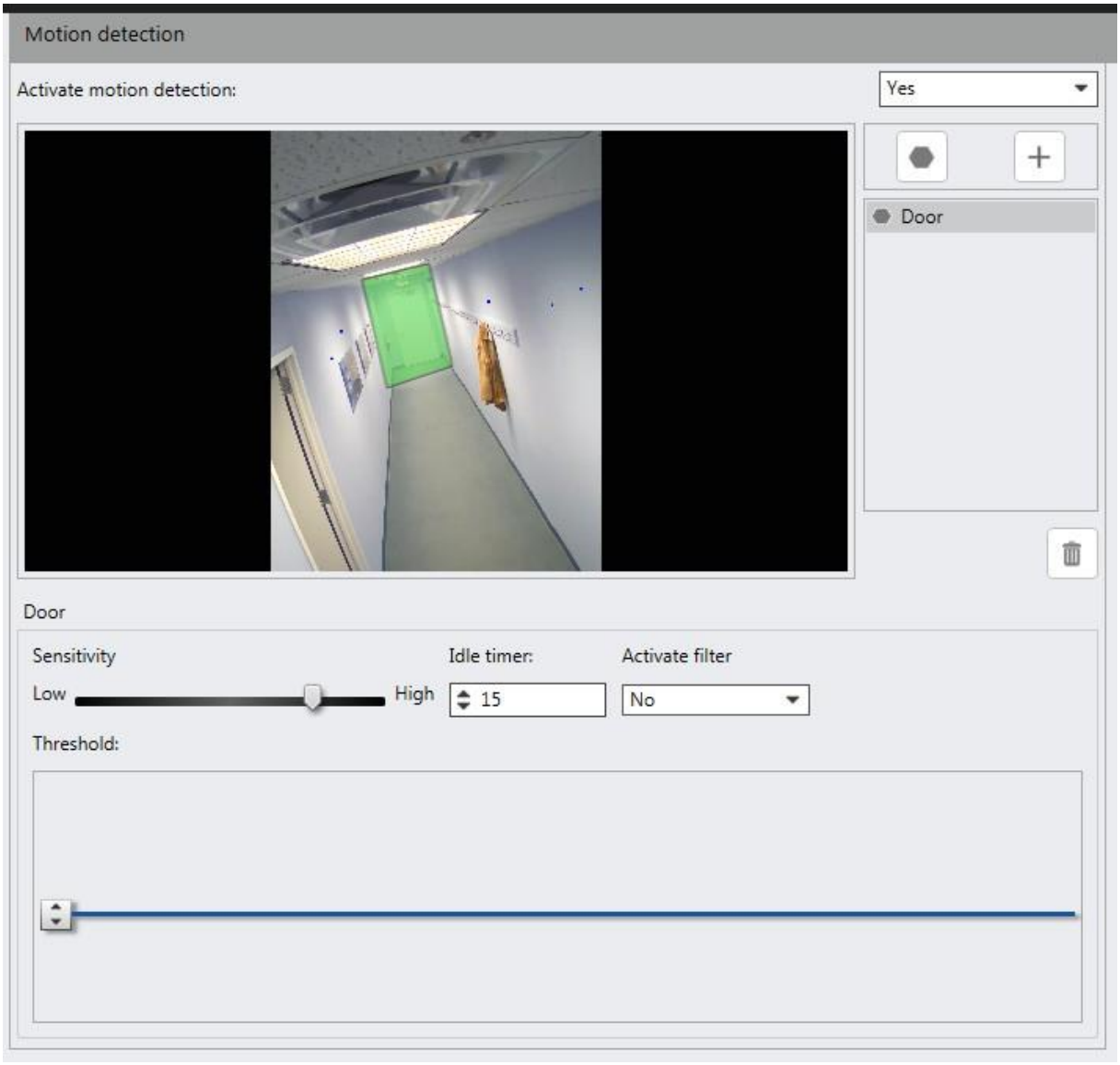


Server side functions detect motion within an image, tampering attempts on the camera, and differences to a reference image. For server side functions, images are analyzed by motion detection modules on the server (see **Adding server-based motion detection module**). For example, a server side motion detection event can be used to trigger an alarm scenario.

Server side image analysis by the motion detection module can result in high resource load. Therefore it is recommended to use the camera side motion detection (see **Camera side functions**).

1. Select the 'Server side functions' menu item.
2. Select a video classification (see **Video streams**). The video classification determines which video stream is used for motion detection analysis. The default video classifications are ordered according to their use of network bandwidth ("HD quality" requires a broadband connection, whereas "Mobile" decreases the image quality for slow networks. But remember that you can modify these labels). For image comparison, select a video stream for low bandwidths. Motion detection, reference image comparison and tampering resize the images to 320x240 pixels internally if they are larger.

Motion detection



The motion detection feature delivers the best results with indoor use. You can use the entire image for motion detection analysis or create up to 10 regions for each camera with individually configured sensitivity, Idle timer, and threshold values

1. Select **Motion detection** from the Server side functions menu (you may have to click on the triangle in front of the menu to expand it).
2. To activate the motion detection, select **Yes** from the drop-down menu.
3. If you want to configure a specific region within the image to be used for motion detection analysis, click the plus sign to the right of the camera image. You may change the name of the region.
4. Use the polygon tool to draw the region on the camera image. Different sections are only required if you want to monitor each specific section. Use the left mouse button to draw the polygon. Double-click when you return back to the starting point. You can provide unique Sensitivity and Threshold settings to each region.

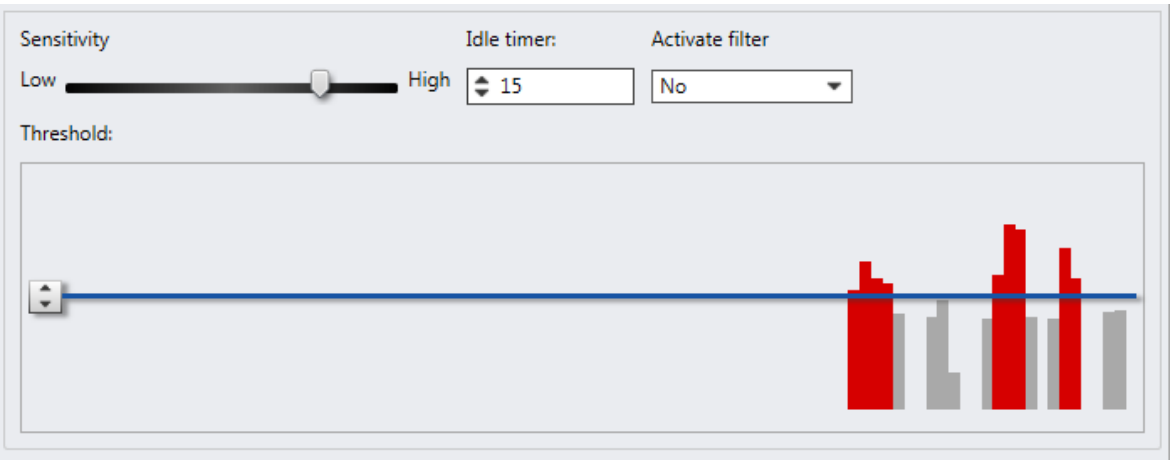
5. Adjust the motion **sensitivity** as appropriate. The sensitivity value determines how big or small a difference in the image has to be in order to count as motion.
   - With a high value, even small changes in the image will be treated as motion.
   - With a low value, only big changes in the Image will be treated as motion.
6. Increase the value, if you get too many false negative results and decrease it if you get too many false positive results. watch the threshold area. Grey bars will not be recognized as motion. Red bars will. Adjust the **Threshold** until you achieve the desired results.
7. If you use an alarm scenario for motion detection, specify the interval for the **Idle timer** (in seconds) after which a signal is analyzed again. This field is ignored by **Record on Motion**.
8. The **Activate Filter** feature can reduce excess false positives due to environmentally induced motion when using server side motion detection. Examples include: low light scenarios that emit excess noise, places where the light reflection causes noise, etc.

Be aware that this feature is not intended for use on cameras at long distances.

To activate the filter, in the Server side functions > Motion detection screen, set the drop-down under 'Activate Filter' to Yes. Then, we recommend setting the Sensitivity to close to High and Threshold close to Low. As always, we recommend that you review the motion detection settings in different lighting scenarios such as during daylight and night time hours. We also recommend reviewing the recorded video to ensure that only actual motion is being detected and recorded.

9. Adjust the **Threshold**. The threshold determines how big the motion in the images needs to be in order to trigger an alarm.
   - Set the threshold to a high value if only big motions are supposed to trigger a alarm.
   - Set the threshold to a low value if small motions are supposed to trigger a 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 an alarm was triggered

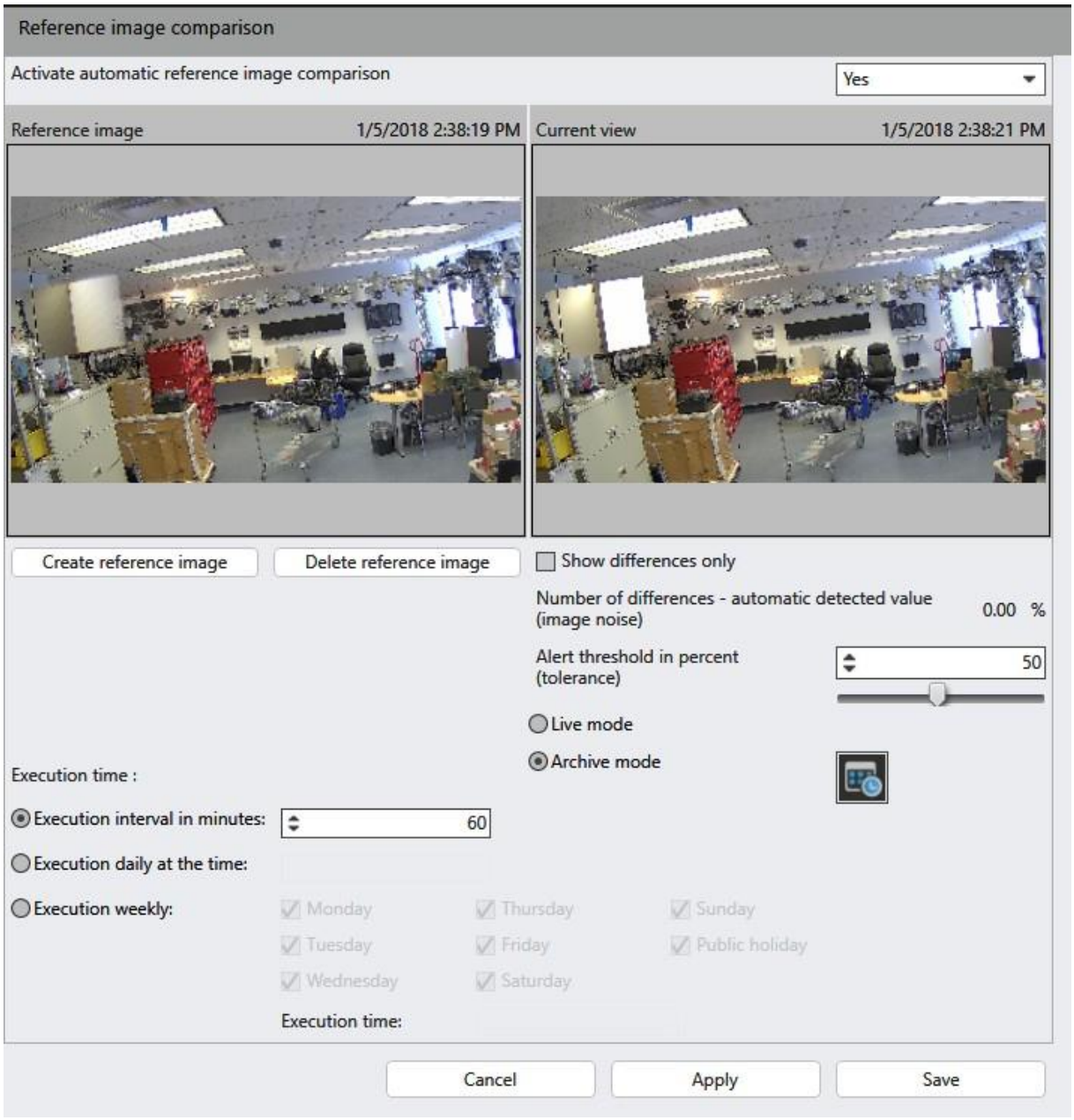
As you adjust the sensitivity and threshold settings, and there is motion in the image or selected region, you'll see vertical bars appear in the Threshold section of the screen. When a bar is red, it indicates that motion has beentriggered.



10. **Save** the settings.

If you want to record video upon motion, see **Record on motion**.

Reference image comparison



The live camera image is compared to a defined reference image of the same camera view (see **Manual reference image comparison**). An alarm will be triggered if the images do not match and triggers a second alarm when the original camera view is restored. This feature is used to monitor gradual changes within a camera image.

1. Select **Reference image comparison** in the 'Server side functions' menu.
2. To activate the automatic image reference comparison, select **Yes** from the drop-down-menu.

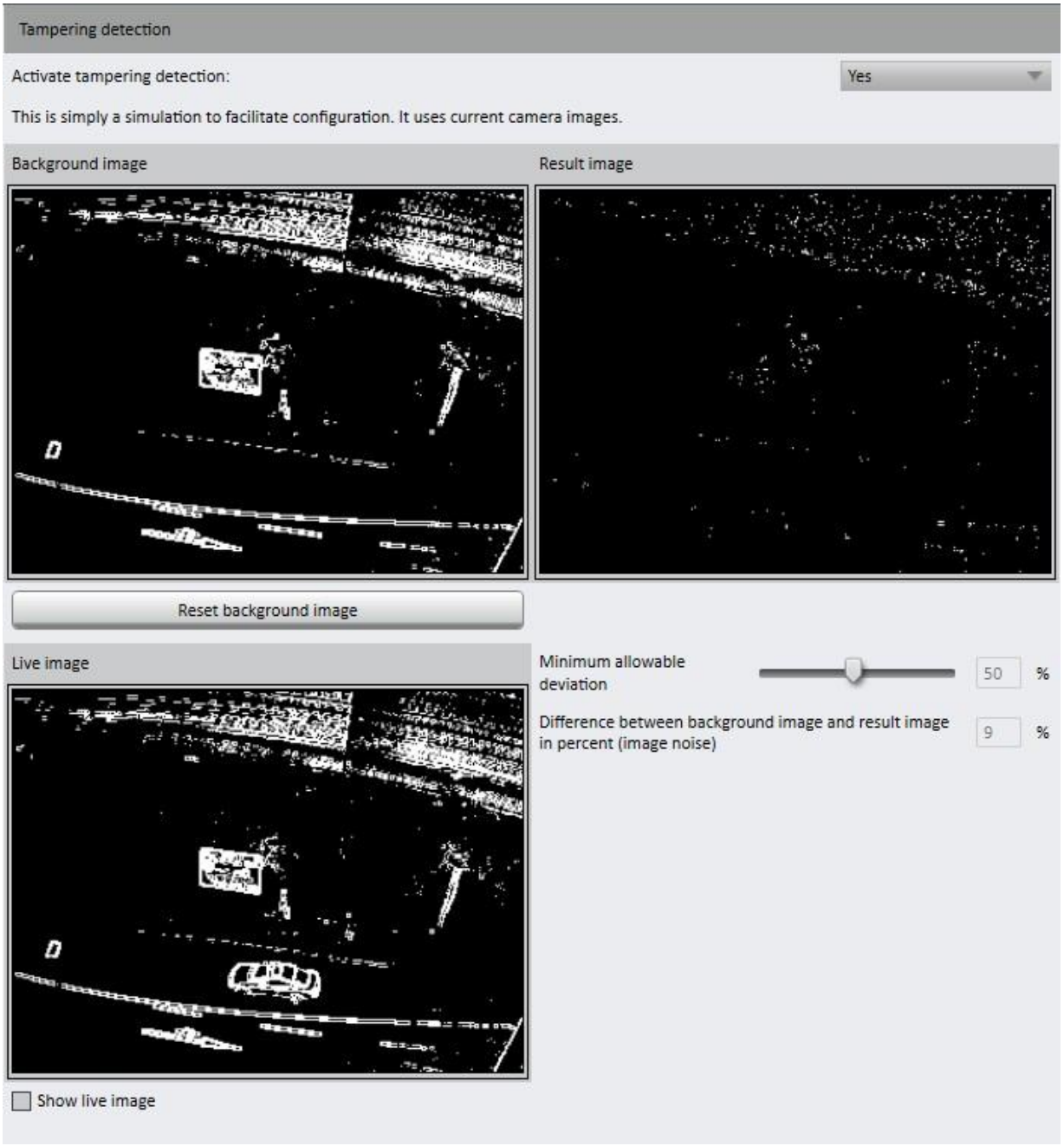
3. Click **Create reference image** to select an image from the camera that serves as a backdrop for the motion detection.
4. Select **Show differences only** to show only the differences between the live-image and the reference image.
5. Adjust the **Alert threshold (tolerance)** in percent. An alarm will b e triggered only if the differences between the live image and reference image are above the threshold.
6. If you prefer, select 'Archive mode' to select a pre-recorded frame as the baseline. Click the calendar

icon to specify date and time for the frame.

7. Specify the values for the **Execution time** 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.
8. Click **Save** when done.

If you want to be alerted when these conditions are met, be sure that the event 'Reference Image Events' is selected in the Ocularis Recorder Proxy. Then, in Ocularis Administrator, set an alert for this event on the camera as you would any other event.

Tampering detection



The Server side 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. Click **Reset background image** to define a new reference image.
3. To display the actual live image, activate **Show live image**.

4. 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 can be configured for the camera. Or, to configure the event via Ocularis, be sure that the event 'Camera Tampering - Server Based' is selected in the Ocularis Recorder Proxy. Then, in Ocularis Administrator, set an alert for this event on the camera as you would any other event.

5. **Apply** the set values if you want to make further settings.
6. **Save** the set values to apply the values and conclude input.

7.4.1.11 Camera side functions

If supported by the camera, camera side functions include motion detection within the image and tampering attempts on the camera. If using a Smart Driver, additional camera side events may be available.

For example, a motion detection event can be used to send an alert.

Motion detection - Static Drivers

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. You should have already configured one or more motion windows on the camera using the manufacturer's configuration tool.
3. Click **Save** or **Apply** when done. If you want to also record video when there is motion, select 'Record On Motion' and enable the function there.

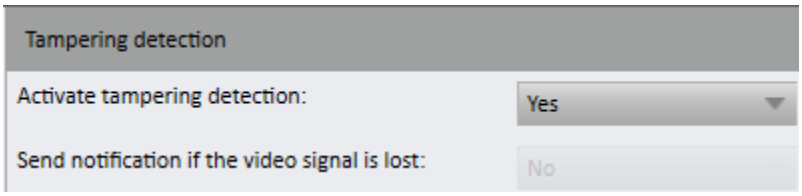
Qognify recommends using camera side motion detection whenever possible.

Motion detection - Smart Drivers

When using a Smart Driver, the software can access motion detection as well as other camera side events specific to that camera model. Under Camera side functions, you'll see Event trigger.

1. Click **Event trigger**.
2. The camera's events should be listed. Click **Update generic event trigger** to refresh the list.
3. You can activate one or more camera side events as set on the camera. Remember that each camera will have adifferent list.
4. Click the **Record On Motion** checkbox if you want to record video upon the event triggering.
5. Click **Save** or **Apply** when done.

Tampering detection - Static Drivers



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).

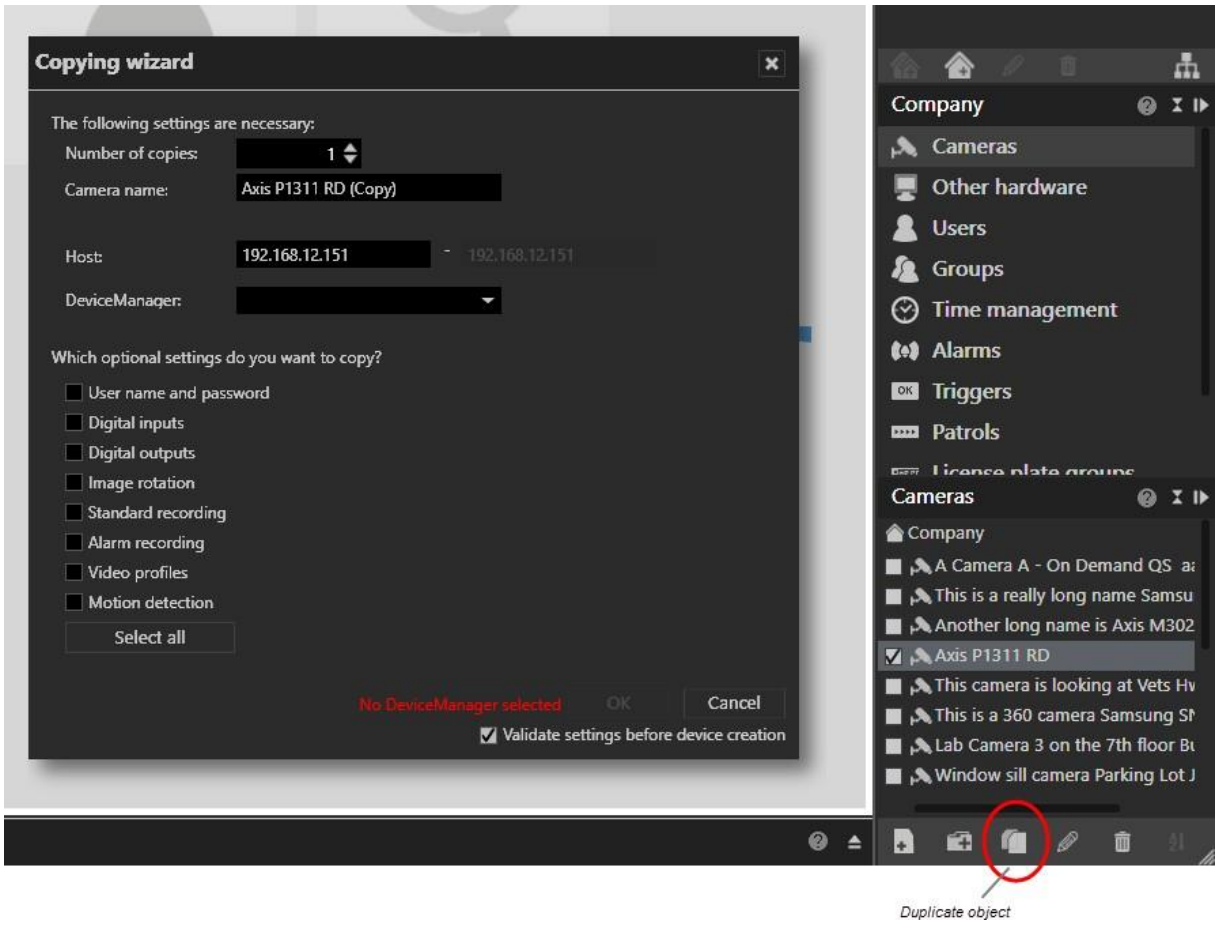
An action can be started once notification is received. This setting may also be used to trigger an alert.

1. Select **Yes** to activate camera side tampering detection.
2. If supported by the camera, select **Yes** for sending notifications if the video signal is lost. This will trig- ger a notification in the alarm list if the video signal drops out. This setting may also be used to trigger an alert.

7.4.1.12 Duplicating a camera

Duplicating a camera enables camera settings to be applied to a large number of identical cameras. This can be a huge time saver when configuring similar cameras.

1. Click the checkbox adjacent to the camera in the control bar camera list.
2. Click the **Duplicate object** icon. This launches the **Copying wizard**.



3. Specify the numberof copies.
4. 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**)
5. 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. This can be modified after the camera has been created.

6. Select the **DeviceManager**. This will be the Device Manager for all camera copies.
7. Activate the properties that are to be transferred to the copied cameras.
8. If you want to validate settings (username, password, IP address, etc.) Leave the 'Validate settings before device creation' checkbox checked. Otherwise, uncheck this box. If you are setting up cameras offline, uncheck this box.
9. Click **OK** to accept.

The new cameras are displayed in the camera list. You can now modify one or all if desired.

7.4.1.13 Deleting a camera

1. Select the camera in the overview camera list by clicking the checkbox adjacent to its name.
2. Click the **Delete object**icon.
3. Click **Yes** at the "Are you sure you want to delete" pop-up.

All saved recordings of the camera are deleted.

If you think you might want to return to this camera at a later time, you might want to deactivate the camera, rather than delete it. See **Encoder - general** for more details on camera deactivation.

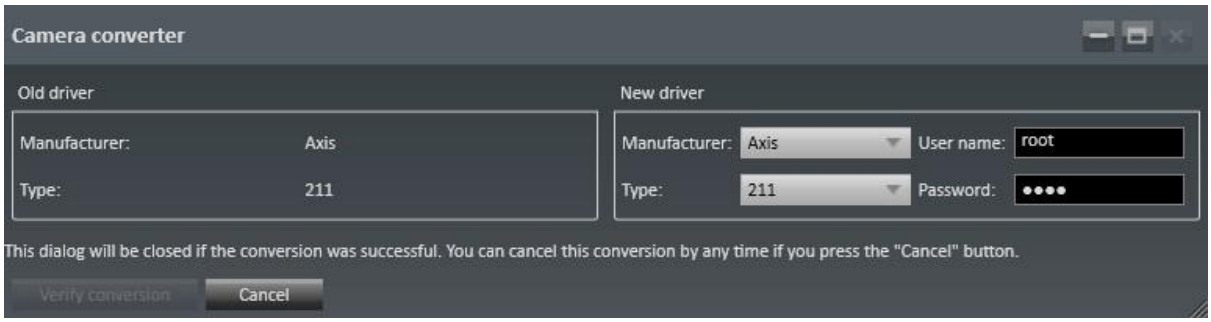
7.4.1.14 Converting a camera

An installed camera can be converted into a new camera by transferring the camera configuration and recordings. This can be a 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.

NOTE: If you are replacing a camera with the exact make and model, you do not have to use this tool. Simply give the new camera the same IP address, username and password as the old camera and plug in the hardware. The camera will come online and should work immediately. The recordings from the old camera will be retained with those from the new camera for the retention period duration.

1. Select the camera archive in the overview camera list. The settings of the camera are displayed in the main window.
2. Click **Open converter** in the general settings of the selected camera.



3. Select the **Manufacturer** and the camera **Type** of the new camera.
4. Enter **User name** and **Password**, if required.

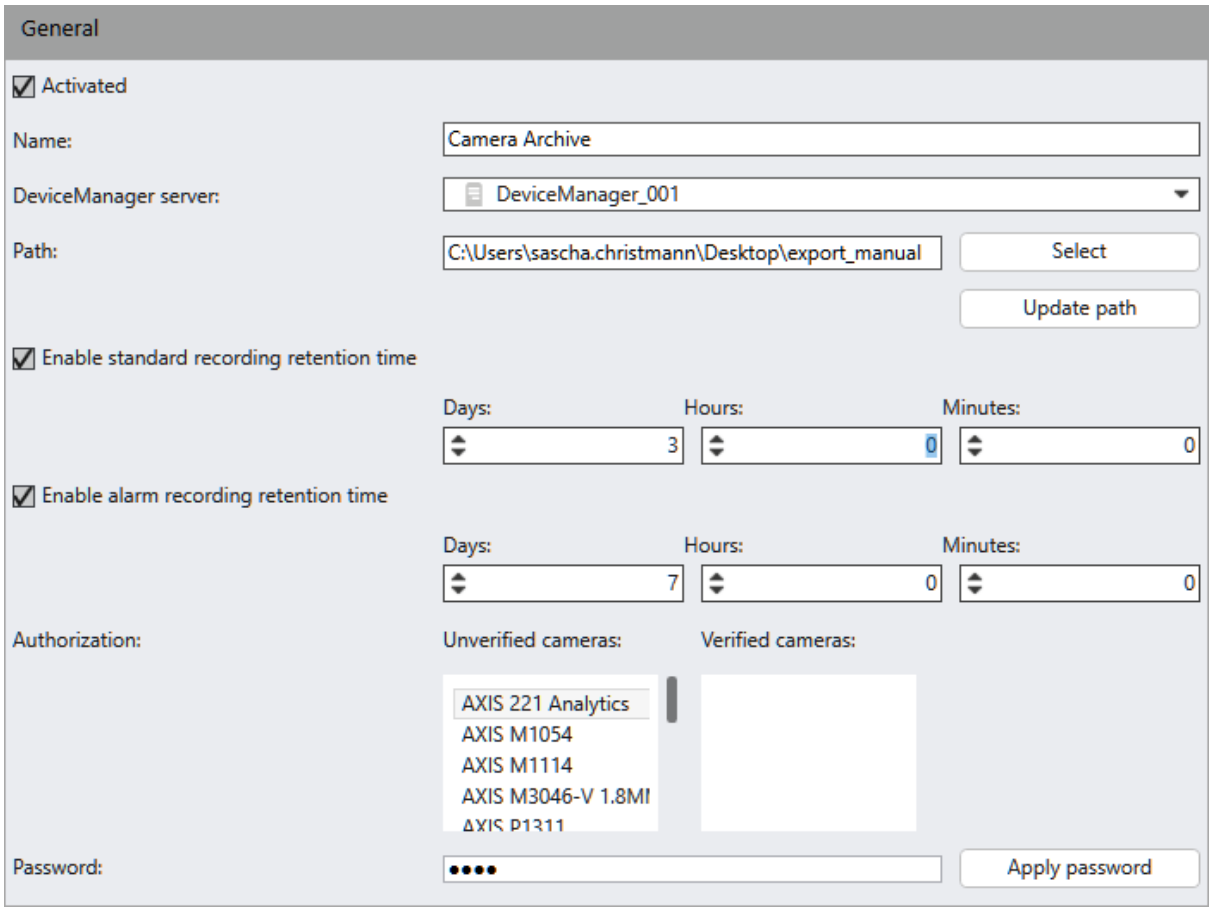
5. Click **Verify conversion**. A list of possible conversion issues is displayed. You can click on each item to switch to that section and modify settings.
6. After resolving any issues, click **Apply** to start the conversion process.

7.4.1.15 Configuring an Archive Camera

An archive camera is used to view recorded video that may have been copied during a Video Backup/Export.

NOTE: For this feature to work you need to enable Video Backup/Export on a per camera basis (for those cameras you want backed up) as well as to enable the 'Activate automated backup' check- box and configure setting in the Device Manager Video backup screen.

7. Select the camera archive in the overview camera list. The settings of the camera are displayed in the main window.
8. Click **Activated** to activate or deactivate the camera archive.
9. If necessary, change the **Device Manager server** for the camera archive.
10. Select the **Path** to the exported recording.
11. Click **Update Path**. All exported cameras are loaded from the path and displayed as unverified cameras.
12. Optionally, define the retention time for standard and alarm recordings. Recordings int he camera archive which are older than the retention time will be deleted automatically.
13. Enter the **Password** which was provided when exporting the recordings.
14. Click **Apply Password**. Recordings for which the password is correct get verified and will be accessible in *Browse* mode.



7.4.2 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, alarm systems and I/O modules. The devices can be partly administered and actuated with the software 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.

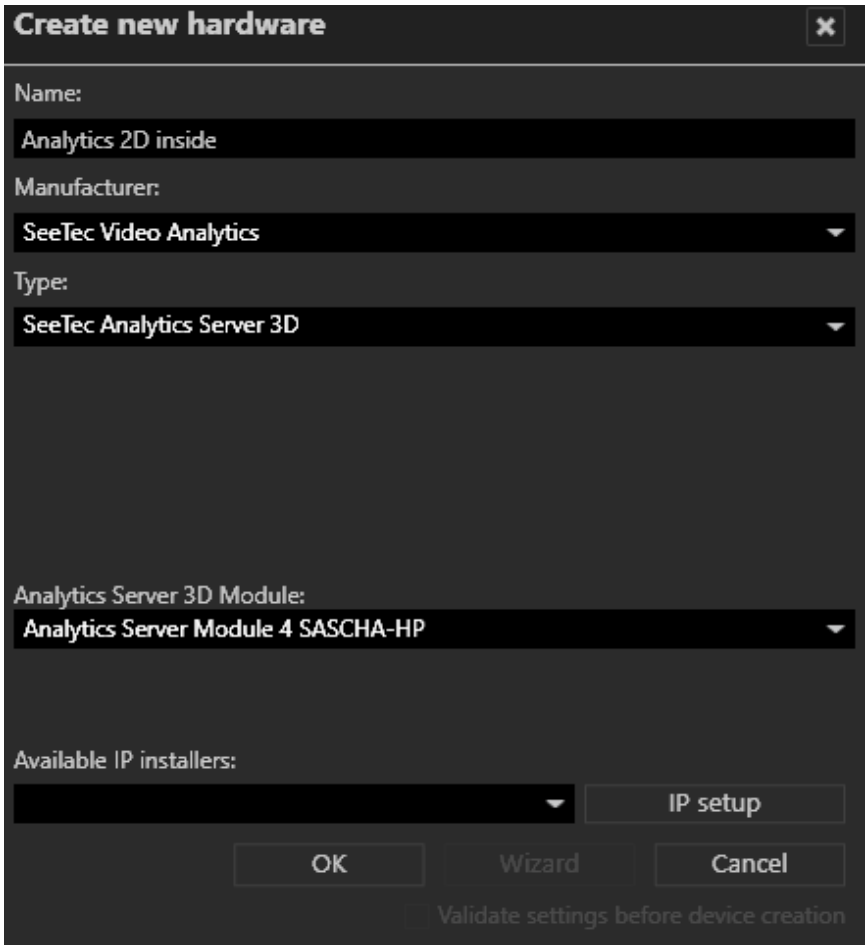
2. Select **Other hardware** in the control bar.

7.4.2.1 Working with other hardware

Working with other hardware follows the same basic procedures.

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:
   - SeeTec: network I/O, display agent and VoIP
   - **SeeTec Video Analytics**: Generic VCA Channel, license plate recognition, Qognify Analytics Basic / Enterprise / Premium, Qognify Counting Suite
   - **Advantech**: ADAM 6050/6050W, ADAM 6052, ADAM 6060/6060W/6066
   - **Axis**: P8221, A9161, A9188
   - **Wago**: Wago System 750 I/O module
   - **Third-party interface**: eyevis wall, SPC alarm system, Aritech Alarm Center, Schneider Intercom ICX Connection, Siemens SPC 4000/5000/6000, SiPass Access Control Software, TDSi access control.

   See Integrating other hardware or ask Qognify support about the use of third party interfaces.
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.

Integrating other hardware

For the integration and configuration of other hardware, consult the following technical guides:

- Bettini DVRs "Integration Bettini DVR"
- Samsung DVRs: "Integration Samsung DVR"
- Aritech Alarm Center: "aritech_alarm_center_(ATS)"
- TDSI Access Control Software: "tdsi-connection"
- Schneider Intercom Software: "schneider_intercom_icx"
- Siemens SPC Alarmsystem Software: "siemens_spc_alarmsystem_(EDP_protocol)"
- SiPass access control software: "Siemens SiPass Integrated"

Configuring hardware

1. Select the hardware in the **Other hardware** overview.
2. Edit the settings for the hardware.
   - **Third-party interface**
   - **SeeTec**
   - **Advantech**
   - **Wago**

Deleting hardware

1. Select the hardware in the **Other hardware** overview.
2. Click the **Delete object** icon.

7.4.2.2 Third-party interface

This section includes the configuration of

- Aritech Alarm Center
- Schneider Intercom ICX Connection
- Siemens SPC 4000/5000/6000
- SiPass Access Control Software
- TDSi access control

Generally, third-party interfaces have to be pre-configured on the side of the third-party component. This section describes only the configuration in the Ocularis Recorder.

All analytics products or software mentioned in this guide are third party products.

SeeTec

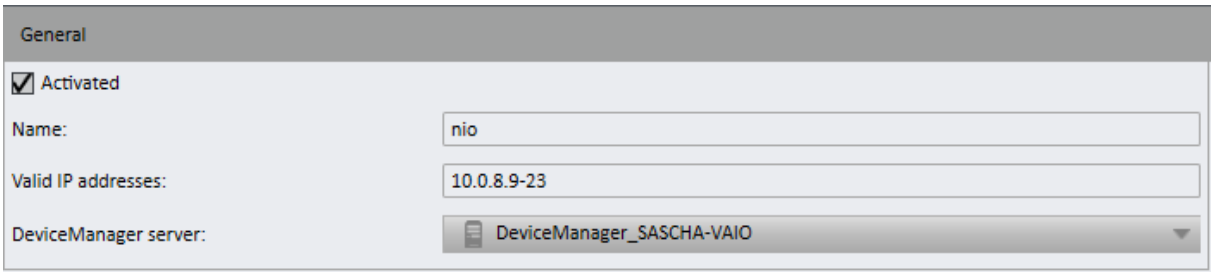
Other hardware from SeeTec includes the configuration of

- Network input and output
- VoIP

SeeTec network I/O

SeeTec can provide network I/O, e.g. to trigger a hardware function over the network.

▶ 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.*.*.*

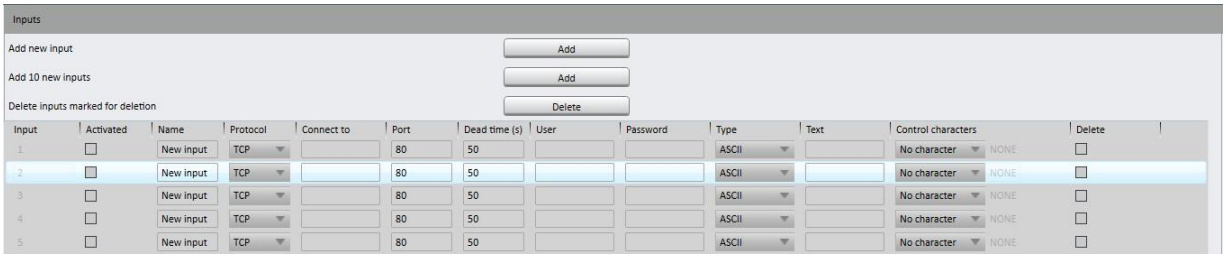
   Three restrictive masks have been defined:

   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 subnet 192.

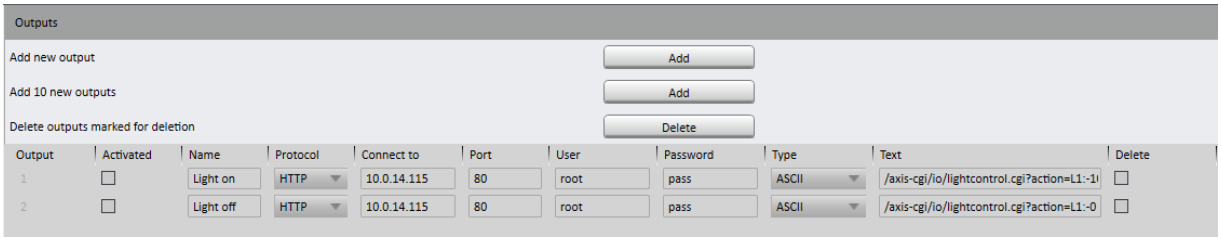
4. If necessary, change DeviceManager server (see **Installation of a Device Manager**).

▶ Inputs



1. Click the **Add new input** or **Add 10 new inputs** button to create one or ten new inputs.
2. Click the **Activated** checkbox to activate or deactivate an input. To set the activation state for multiple inputs, hold down the [SHIFT] or [CTRL] 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
   - HTTP for connections over the Internet.
5. In the 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, and (optionally) specify the control character encoding for the correct display of paragraph changes, for example.
10. To delete inputs, select the inputs you want to delete, and then click **Delete** next to **Delete inputs marked for deletion**. Use [SHIFT] or [CTRL] for multiple selections.

▸ Outputs



1. Click the **Add new output** or **Add 10 new outputs** button 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 [CTRL] key on the keyboard while selecting other 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.
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 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 then click **Delete** next to **Delete outputs marked for deletion**. Use [SHIFT] or [CTRL] for multiple selections.

SeeTec Video Analytics

Because the attention of the observers falls as the number of monitors that are observed increases, the Qognify 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
- SeeTec Analytics

For performance reasons, the video analysis module should be installed on a dedicated server (see **Custom installation**).

Analytics Server

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.:

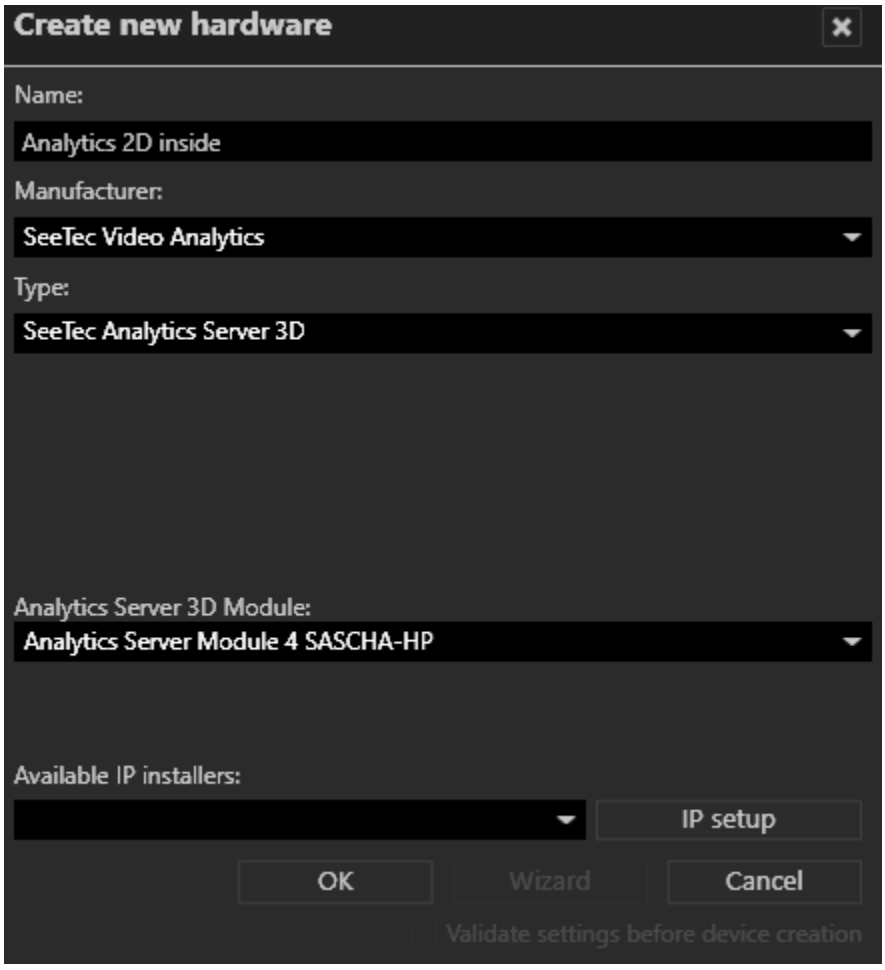
- The calibration is not possible (e. g. test person is not allowed to walk in front of the camera)
- The camera position is too low or rolled
- The camera is inside – 3D Analytics does not work well inside because in most situations there are too many obstructing objects (person cannot be seen from 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)

Notes

- To add and configure a Qognify Analytics Server functionality, the required module must first be created with the VA administration tool. Alternatively, it must be installed during a user-defined installation (see Custom installation).
- The Qognify Analytics hardware has to be added.
- 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



Adding Analytics Server module

1. Select **Other hardware** and create a new object.
2. Enter a **Name** for the object.

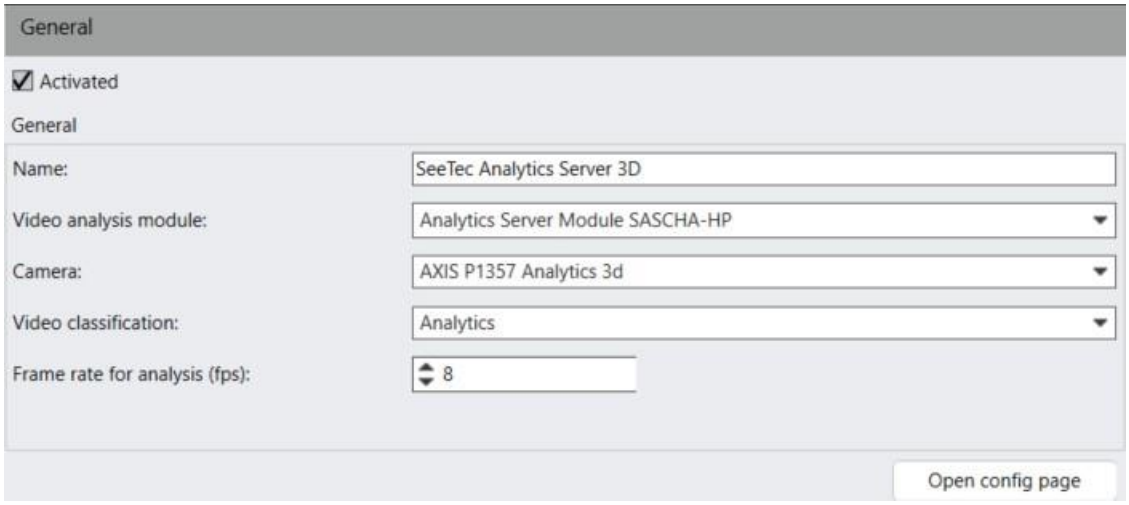
3. For **Manufacturer** select "SeeTec Video Analytics".
4. For **Type** select "SeeTec Video Analytics Server 3D".
5. For **Analytics Server 3D Module** select the required "Analytics Server module" (see Adding an Analytics Server module).
6. Click **OK**.

For module configuration see Configuring a SeeTec Analytics Server module, below.

Configuring a SeeTec Analytics Server module

General

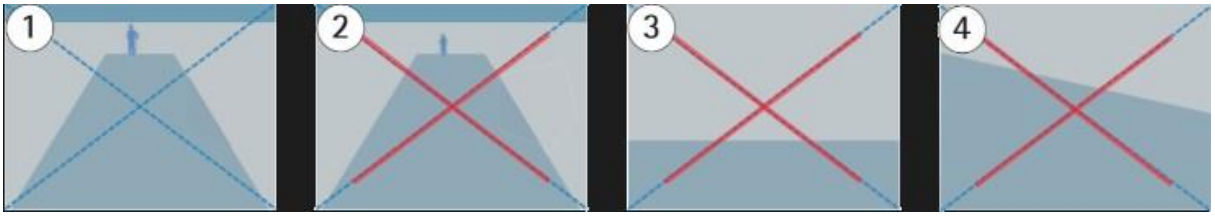
1. Select the SeeTec Analytics Server module in the overview.



▸ To configure an Analytics Server module:

1. Activate the module and, if necessary, change the **Name**.
2. Select the **Video analysis module** to specify which video analysis channel is used to analyze the video data.
3. Select the **Camera** for delivering the video stream.

NOTE: 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 Qognify Support.



4. 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).

Analytics scene setting

For the analytics to work properly, make sure you meet the following requirements. The scene in general should look like item 1 in the figure above:

- 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 item 2 in the figure above).
- The center of the image is below the horizon line (negative example with horizon line above the center of the image see item 3 in the figure above).
- There is almost no camera roll (negative example with too significant camera roll angle see item 4 in the figure above).

5. Specify the **Frame rate for analysis (fps)** to set the number of images per second to be sent to the video analysis channel.

NOTE: A frame rate of 8 frames per second (fps) is recommended.

6. Click **Open config page** for configuring the 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 SeeTec Analytics Server):
   - 2D intelligent Motion Detection
   - 3D Analytics

NOTE: Make sure the Analytics setup tool is installed.

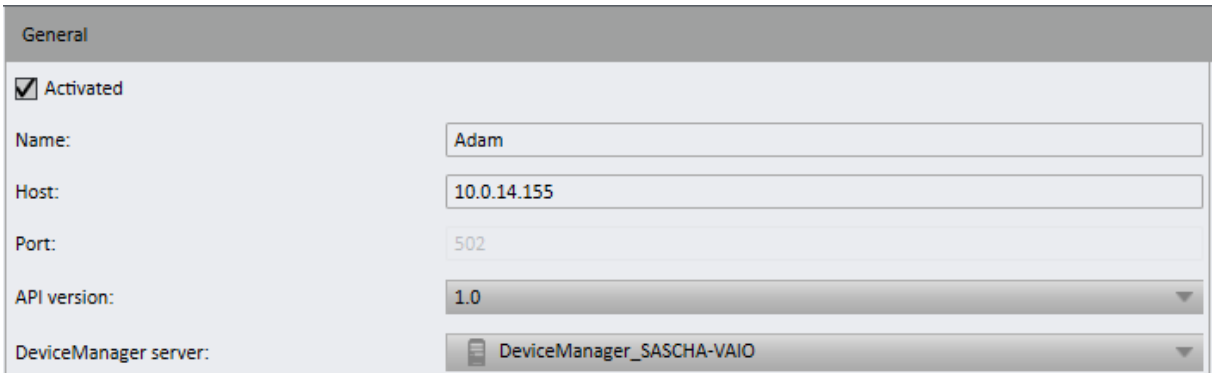
Advantech

This section includes the configuration of

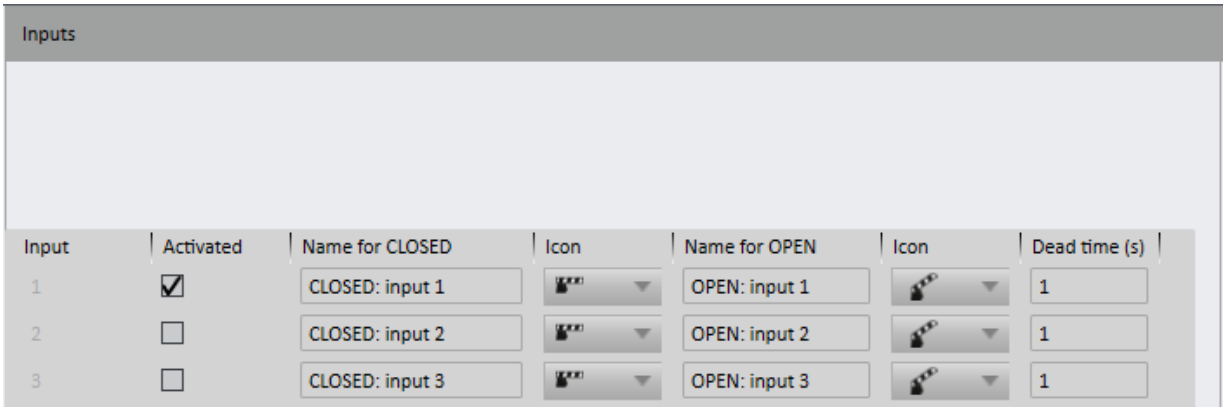
- ADAM 6050 / 6050W
- ADAM 6052
- ADAM 6060 / 6060W / 6066

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



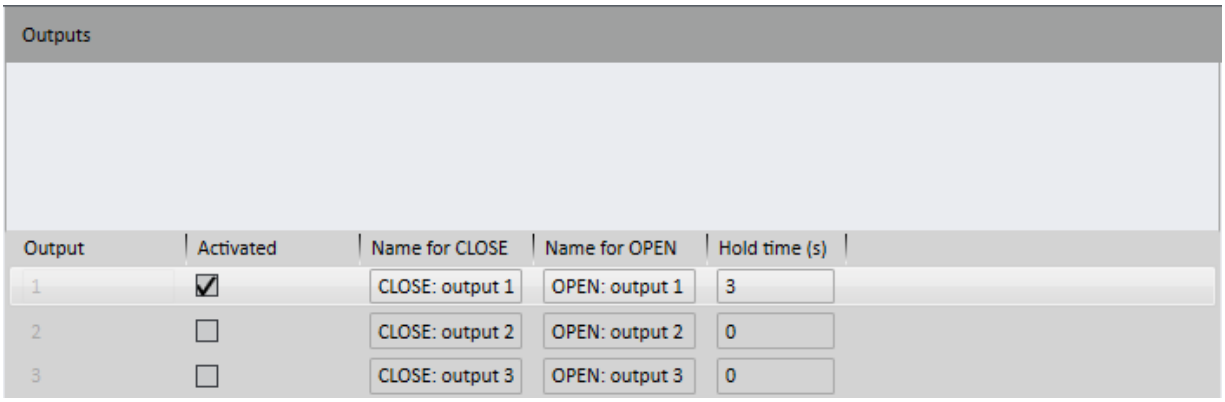
1. Activate or disable the module.
2. If necessary, alter the name.
3. If necessary, change the IP address or the name of the **host**.
4. If necessary, select the appropriate **API version**.
5. Change the server for managing the **DeviceManager server**. **Inputs**



The number of inputs depends on the device type.

6. Activate the desired input and change the **name for CLOSED**.
7. 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.
8. Change the name for OPEN.
9. 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.
10. Specify the interval for the **dead time** (in seconds) after which a signal is analyzed again.

▸ 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.

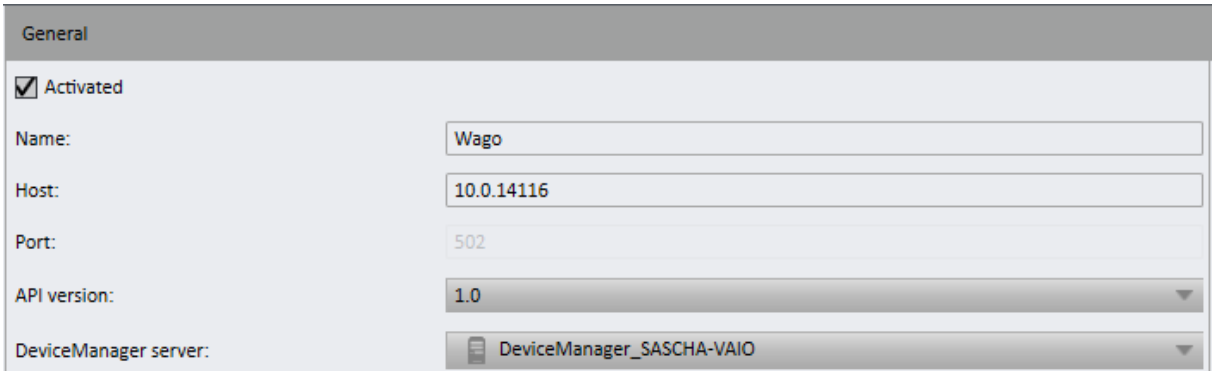
Wago

This section includes the configuration of:

- 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.

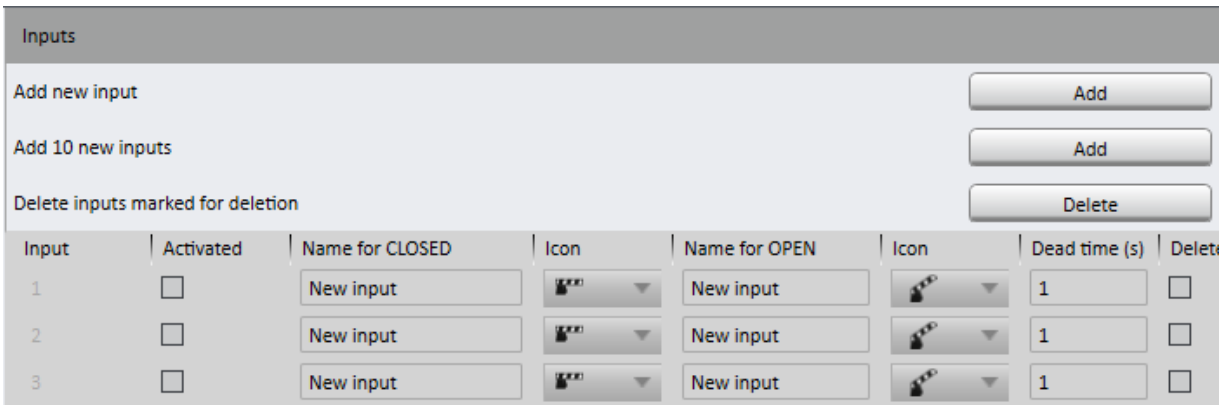
▸ General



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**.

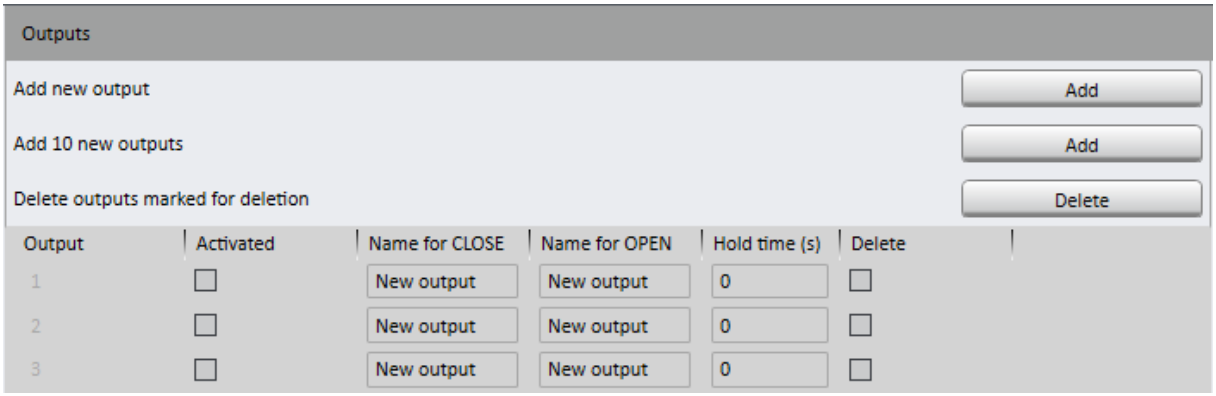
5. Change the DeviceManager server.

▸ Inputs



1. Click the **Add new input** or **Add 10 new inputs** button to create one or ten new inputs.
2. Activate 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 the **Delete inputs marked for deletion** button.

▸ Outputs



1. Click the **Add new output** or **Add 10 new outputs** button 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 the **Delete outputs marked for deletion** button.
6. **Apply** the set values if you want to make further settings.
7. **Save** the set values to apply the values and conclude input.

7.4.2.3 Event Interfaces (SEI)

The Event Interface (SEI) function in the Administration control allows you to configure and manage third party safety systems that can be integrated into the Ocularis Recorder on a generic basis, such as burglar alarm, fire panel, access control etc. These devices can be partly administered and actuated with the recorder 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.

The Event Interfaces require some specific plug-in files which need to be copied into the VA-Plugin directories ("C:\Program Files\Qognify\Ocularis Recorder\VersatileApplications64\AccessControlPlugins" or "C:\ProgramFiles\Qognify\OcularisRecorder\VersatileApplications64\EventPlugins"). For further information contact Tech Support about the use of third party event based plugins.

To configure an event interface or a generic access control module, it must be created in the Ocularis Recorder VA administration tool.

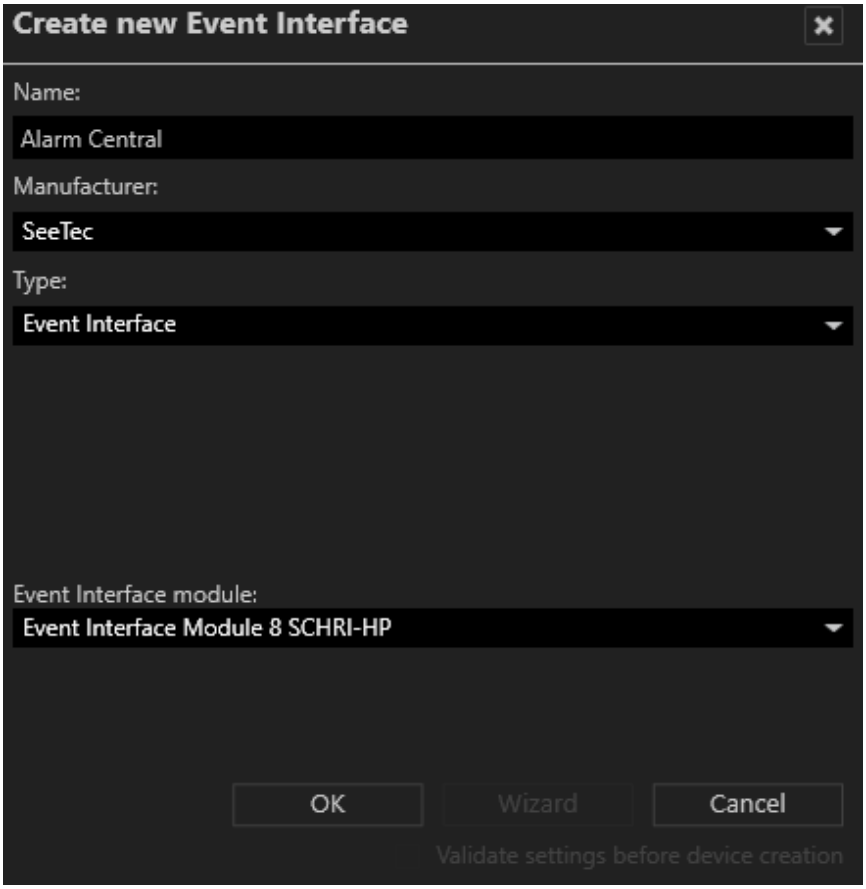
For the generic access control at least one of the following access control modules has to be installed:

- 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, so they can be accessed at any time without reconfiguration.

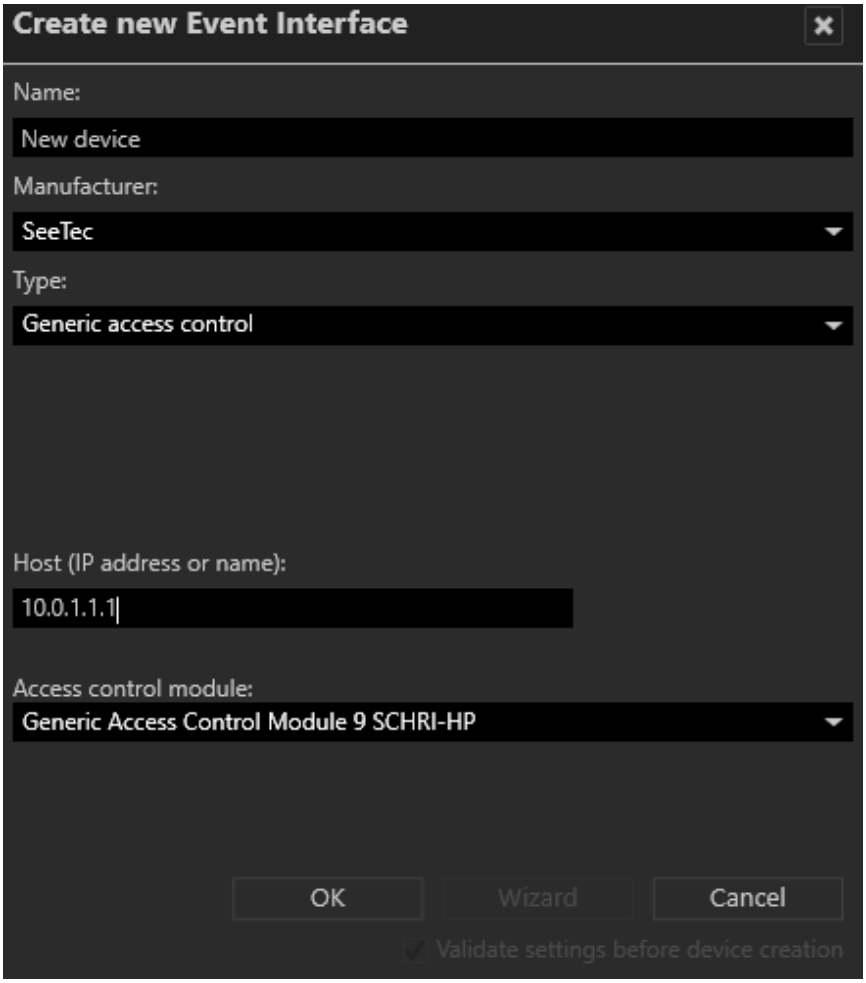
Creating an event interface



Creating new event interface

1. Create a new Eventinterface.
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

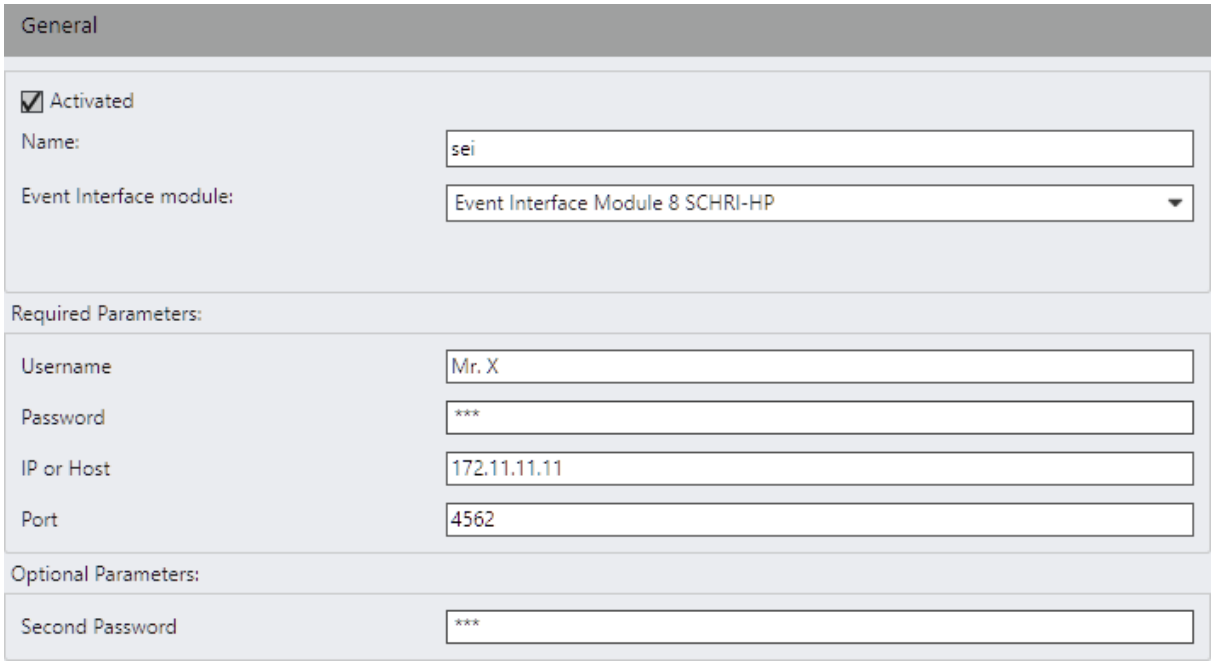


Creating new access control module

1. Create a new **Event interface** item.
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**.
7. Click **OK**. The new access control is available within the selected company item.

Configuring event interfaces

- General

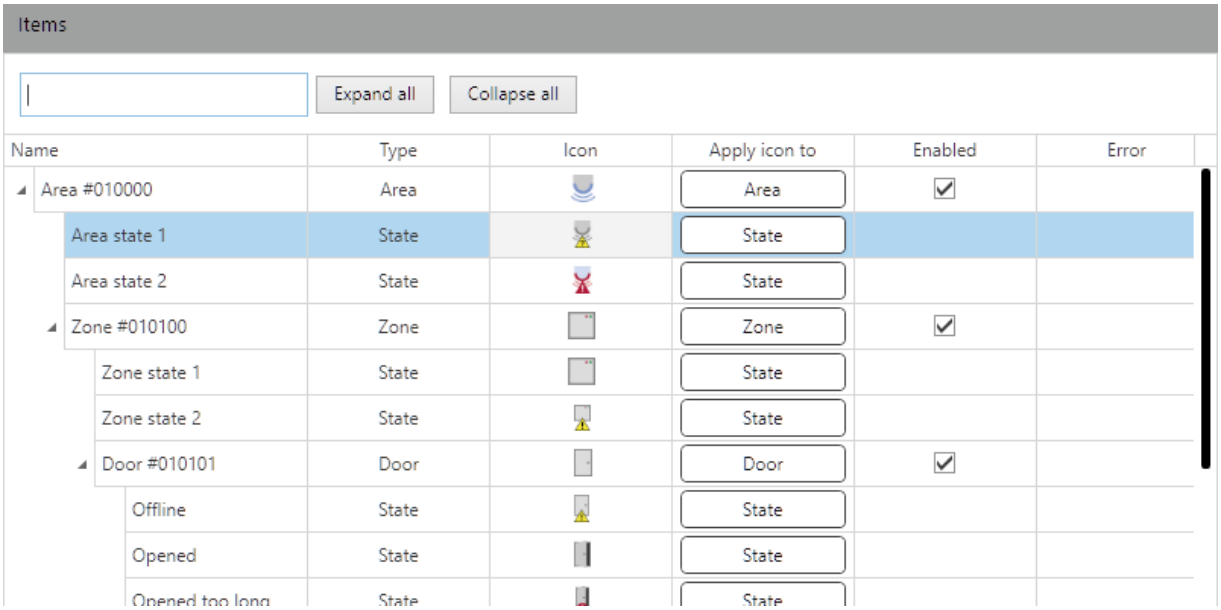


Event interface settings - General

1. Select the event interface in the **Event interface** overview.
2. **Activate** the eventinterface
3. Edit the **Name**.
4. Select the Event Interface module.
5. Configure the required and optional parameters which are requested by the plug-in. Those parameters could be e.g.:
   - **User name** and **Password** for the access control module.
   - **Port** number and **IP** address of the module
   - **Second password** to access the module.
6. Click **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.



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

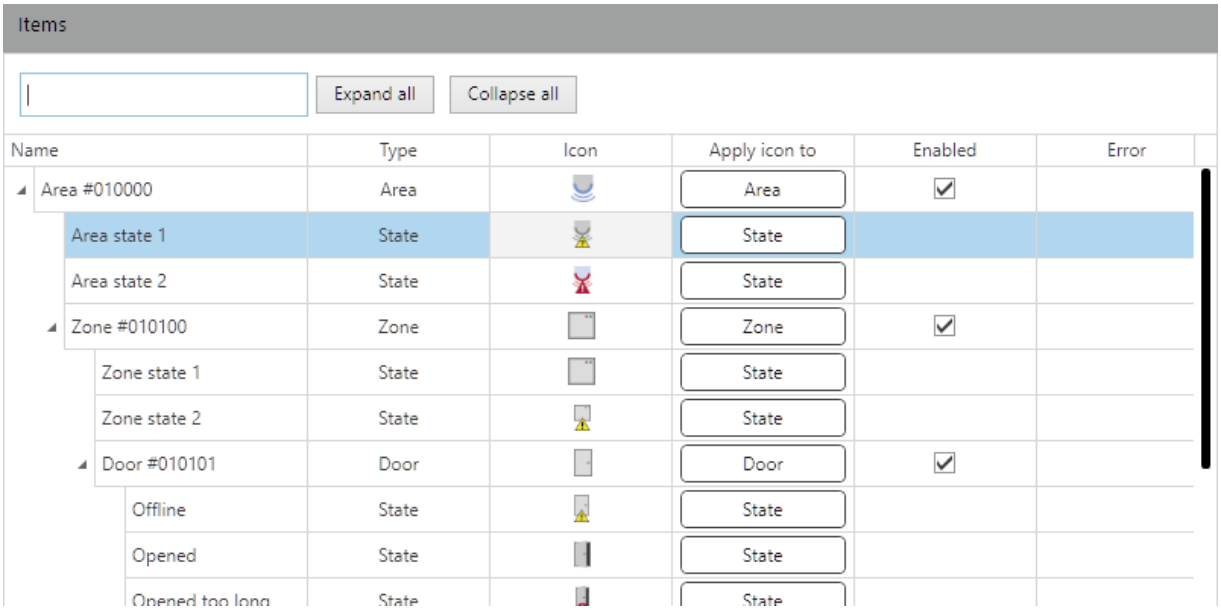
1. Click on the displayed icon.
2. Select another on.
3. Click on the apply to item button.

- Enabling or disabling an item

1. Click the **Enabled** check box. The state changes accordingly.

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.



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 theitem by double-clicking.
3. Select Active (see General).

- Deleting an item

1. Select the item and click **Delete**.
2. Click **Yes** to confirm deletion. The item is permanently deleted.

- Deleting event interfaces

1. Select event interface (or generic access control) in the **event interface** overview.
2. Click the **Delete object** icon.

7.4.2.4 Users

The **User** function in the **Administration** control allows you to create and delete user accounts. 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**.

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

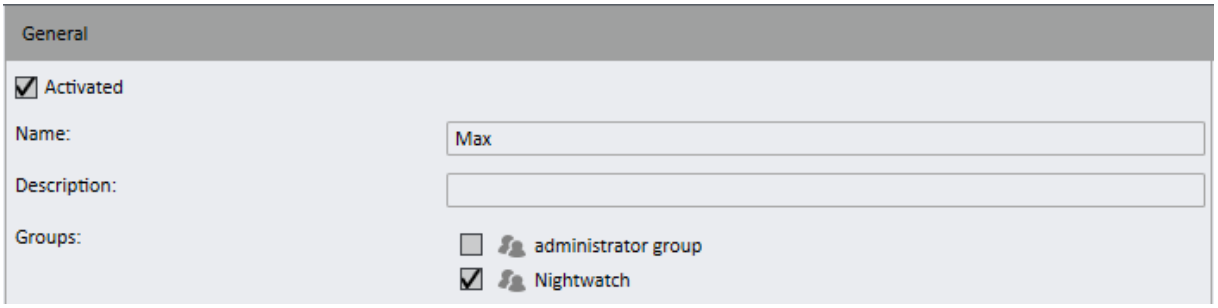
1. Select Create new object in the Users control.
2. Create a newuser.
3. Enter the name and password of the new user.
4. Click **OK** to accept the name.

The new user is displayed in the control.

Configuring a user

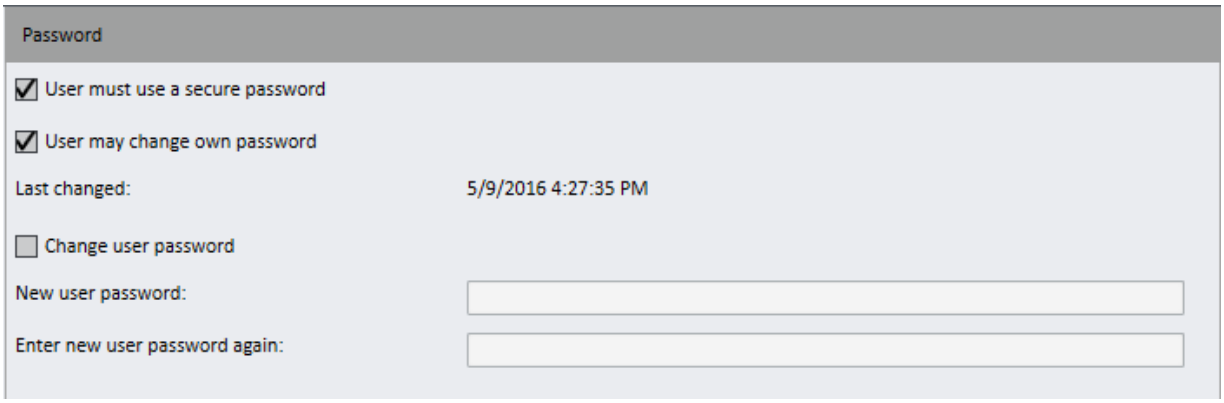
1. Select the user in the **Users** control.

General



1. Activate or deactivate the user. The administrator cannot be deactivated.
2. If necessary, alter the **Name** of the user.
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**). The association with a group is optional.

Password



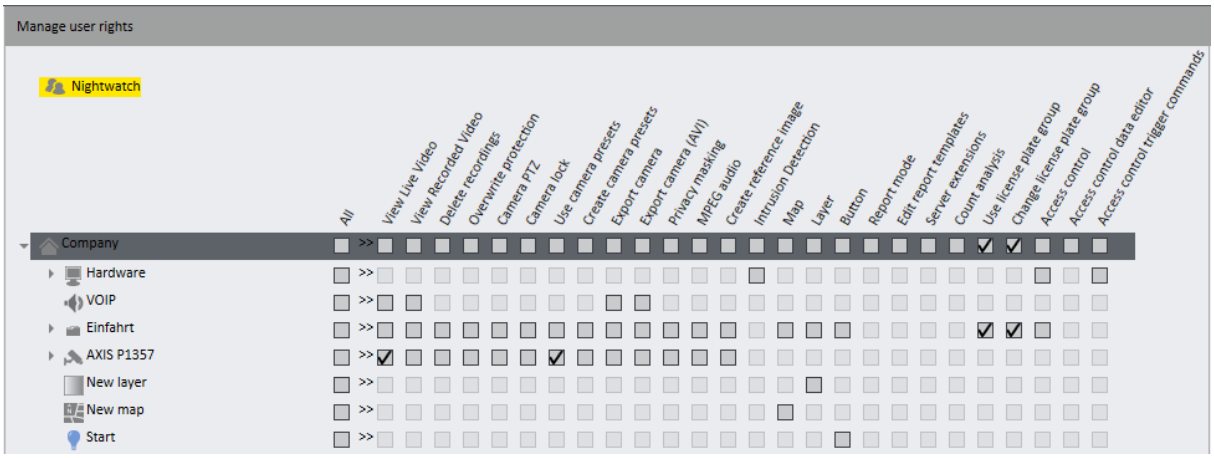
1. Select User must use a secure password.

   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 **Change user password**, and enter a new user password.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.
4. Enter the user password again.

Managing 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. This feature is typically used only by an OpenSight user or when someone has been given rights to manage their own branch.



1. Select or deselect the rights for the selected user to perform specific actions on the installed devices and objects. 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.
   - **View Recorded Video**: The user can use cameras in browse mode.
   - **Delete recordings**: This feature is not supported in this version.
   - **Overwrite protection**: This feature is not supported in this version.
   - **Camera PTZ**: The user can use the PTZ camera except for preset camera positions.
   - **Camera lock**: This feature is not supported in this version.
   - **Use camera position**: The user can use the set camera preset positions.
   - **Create camera position**s: The user can create camera presets or delete presets that have been defined.
   - **Export camera**: This feature is not supported in this version.
   - **Export camera (AVI)**: This feature is not supported in this version.
   - **Privacy masking**: This feature is not supported in this version.
   - **MPEG audio**: The user can use audio transmission.
   - **Map**: This feature is not supported in this version.
   - **Layer**: This feature is not supported in this version.
   - **Button**: The user can use buttons.

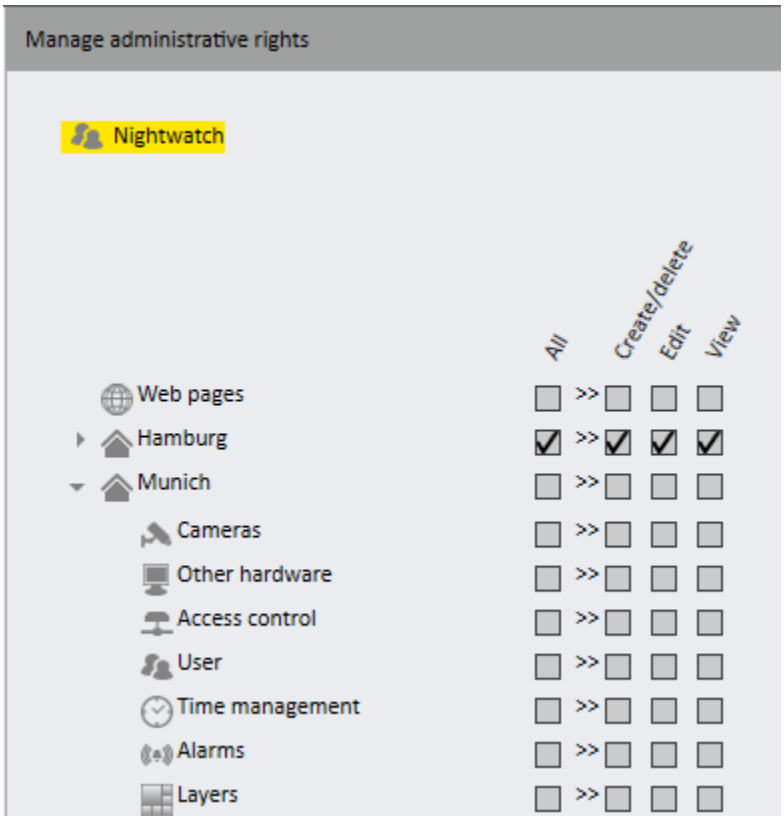
- **Report mode**: The user can view report mode.
- **Edit report templates**: The user can create and edit report queries in report mode and save them as templates.
- **Server extensions**: This feature is not supported in this version.
- **Count analysis**: This feature is not supported in this version.
- **Use license plate group**: This feature is not supported in this version.
- **Change license plate group**: This feature is not supported in this version.
- **Access Control**: This feature is not supported in this version.
- **Access Control Data Editor**: This feature is not supported in this version.

Managing 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**).



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.

Deleting a user

1. Select the user in the overview list by click the checkbox adjacent to the user name.
2. Click the **Delete object**icon.
3. At the "Are you sure you want to delete [user]?" pop-up, click **Yes**.

Duplicating a user

1. Select the user in the overview user list by checking the checkbox adjacent to the user name.
2. Click the **Duplicate object** icon, and enter a name for the duplicated user.
3. Click **OK** to accept the name.

   The new user is displayed in the overview. It inherits the settings from the original user. You may modify the settings further.
4. Click **Apply** or **Save** when done.

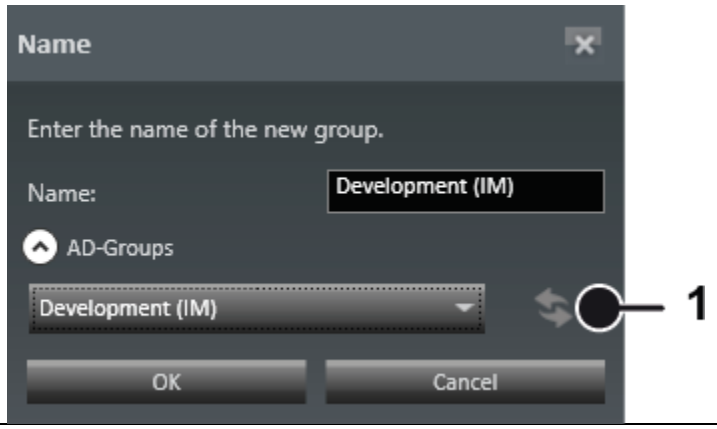
7.4.2.5 Groups

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 he or she is logged in under a user name or as a group.

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

3. Click **New** to create a new group.



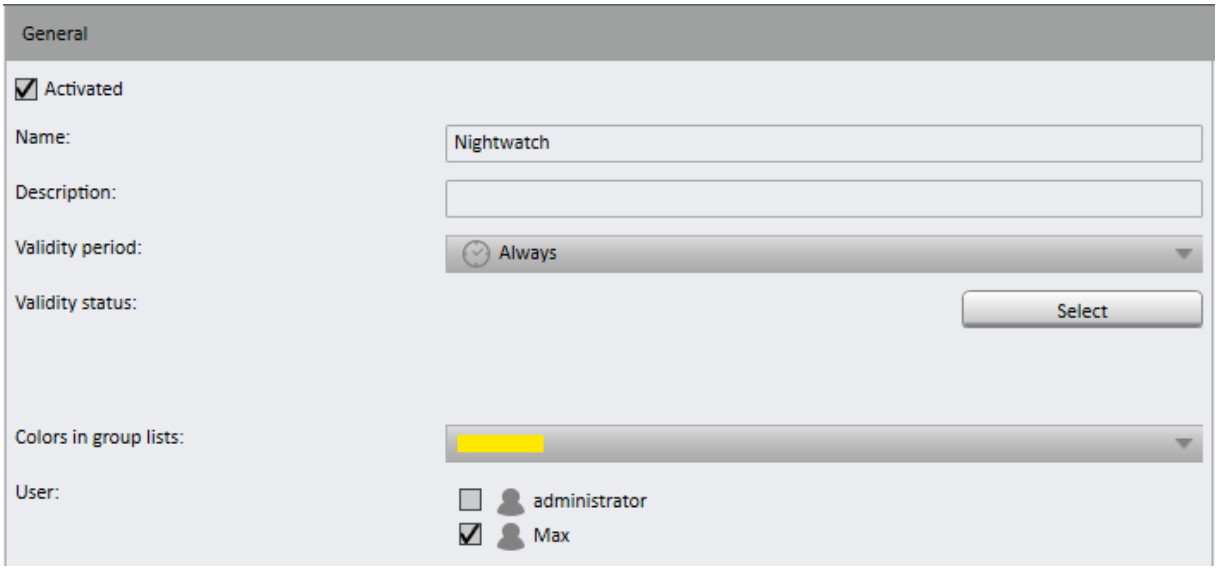
4. Enter the **name** for the new group.
5. If Active Directory groups are available (the client must be connected to an Active Directory network), select the appropriate AD-group. Click the Refresh button (1) to fetch the current group settings from the Active Directory server.
6. Click **OK** to accept the name.

The new group is displayed in the overview.

Configuring a group

1. Select the group in the overview.

General



2. Select or deselect the group.
3. If necessary, alter the **name** of the group.
4. Enter an optional **description** of the group.
5. Select a **validity period** for the group, within which a user belonging to the group can log in to the system.

   The possible periods are specified in the **Time management**.
6. Specify the **validity status** to activate or deactivate the group.

   All users belonging to this group can thus be prevented from accessing certain cameras.
7. **Colors in group lists**: This feature is not supported in this version.
8. Select the **users** to be assigned to the group.

Rights options

Limit archive access is not supported in this version.

Select **Activate Active Directory support** to apply the authorization settings of a connected Active Directory server. This is the only option used on this screen.

Use secure password for exports is not supported in this version.

Comment necessary for changing to archive mode is not supported in this version.

Using Windows® Active Directory®

1. Create a new group in Active Directory®.
2. In Active Directory®, add the domain users of the group who are to log in using the Active Directory® login.
3. In the software, create a group that is analogous to the one in Active Directory®.

   Be sure to use upper and lower case in exactly the same way.
4. Assign the group in the software the required authorizations, and select **Activate Active Directory support**.

   When the software starts up, the users can use the Active Directory® login button to log in to the system with their Active Directory® user name and password.
5. To automate Active Directory® login, enter the AutoADLogin command line parameter in the link for the

   surveillance software (see **Command line parameters**).You don't have to create any users in the software in order to log in using Active Directory®. Rights are assigned by means of the data stored in the group.

Managing user rights

1. Select or deselect the rights to perform specific actions on the installed devices and objects for the selected group (see **Managing user rights**)

Managing administrative rights

1. Select or deselect the rights to make changes or settings in the administration settings for the selected group (see **Managing administrative rights**).
   - **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 group list by checking the checkbox adjacent to the group name.
2. Click the **Delete object**icon.
3. At the "Are you sure you want to delete [group name]?" pop-up, select **Yes** to delete.

Duplicating a group

1. Select the group in the overview group list by checking the checkbox adjacent to the group name.
2. Click the **Duplicate object** icon, and enter the name for the duplicated group.
3. Click **OK** to accept the name.

   The new group is displayed in the overview.
4. Settings for the new group are inherited from the original group. You may modify settings as needed.
5. Click **Apply** or **Save** when done.

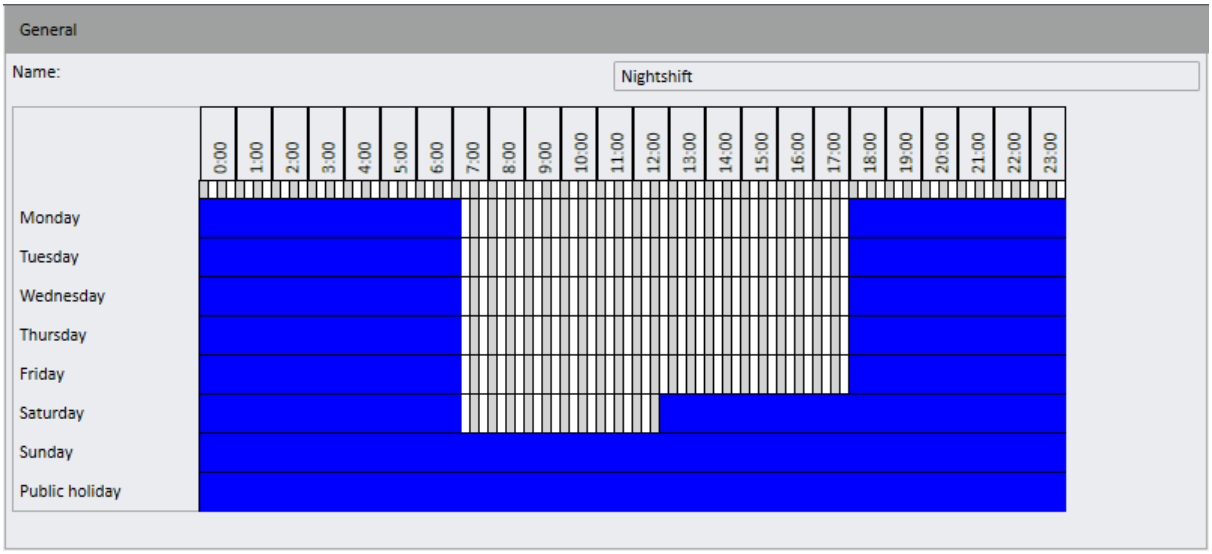
7.4.2.6 Time management

Time management in the Administration control allows you to create time templates or profiles 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.

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.



Creating a new time management template

Create a new time management template.

1. Select Time management.
2. Click the Create new objecticon.
3. Enter the name for the new time management template.
4. Click **OK** to accept the name. A calendar for defining the time template is displayed.
5. 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. Click the day of the week to select the entire 24 hour period for that day. Click the box under the time to select that time period for all days of the week.

6. To remove parts of the selected time sections, hold down the mouse button and drag again over the period.
7. Click **Apply** or **Save** when done.

Configuring a time management template

1. Select the time management template in the overview.
2. 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.
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 time management template

1. Select the time management template in the overview Time management list by clicking the checkbox adjacent to its name.
2. Click the **Delete object**icon.
3. At the "Are you sure you want to delete [time template]?" pop-up, click **Yes**.

Duplicating a time management template

1. Select the time management template in the overview by checking the checkbox adjacent to its name.
2. Click the **Duplicate object** icon, and then enter the name for the duplicated time management template.
3. Click **OK** to accept the name. A calendar for defining the time management template is displayed in the overview.
4. Edit the calendar as needed (see **Creating a new time management template**).
5. Click **Apply** or **Save** when done.

7.4.2.7 Alarms

Ocularis Recorder allows you to define complex alarm routines individually. In a sort of matrix, any start events (e.g. motion detection, 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 workflow can be set up for each alarm situation.

The **Alarms** function on the Administration control allows you to configure and manage alarm scenarios. You may also configure alarms/alerts within Ocularis Administrator.

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 a new alarm scenario

1. Create a new alarm scenario.
2. Enter the name for the new alarm scenario.

3. If you want to configure the new alarm scenario using the configuration wizard, select Wizard in the dialog box (see **Creating an alarm scenario**) or confirm the name with **OK**. The new alarm scenario is displayed in the overview.

Configuring an alarm

1. Select the alarm in the alarm overview.
2. For further settings, see **Creating a new alarm scenario**.

Deleting an alarm

1. Select the alarm in the overview.
2. Click the **Delete object**icon.

Duplicating an alarm

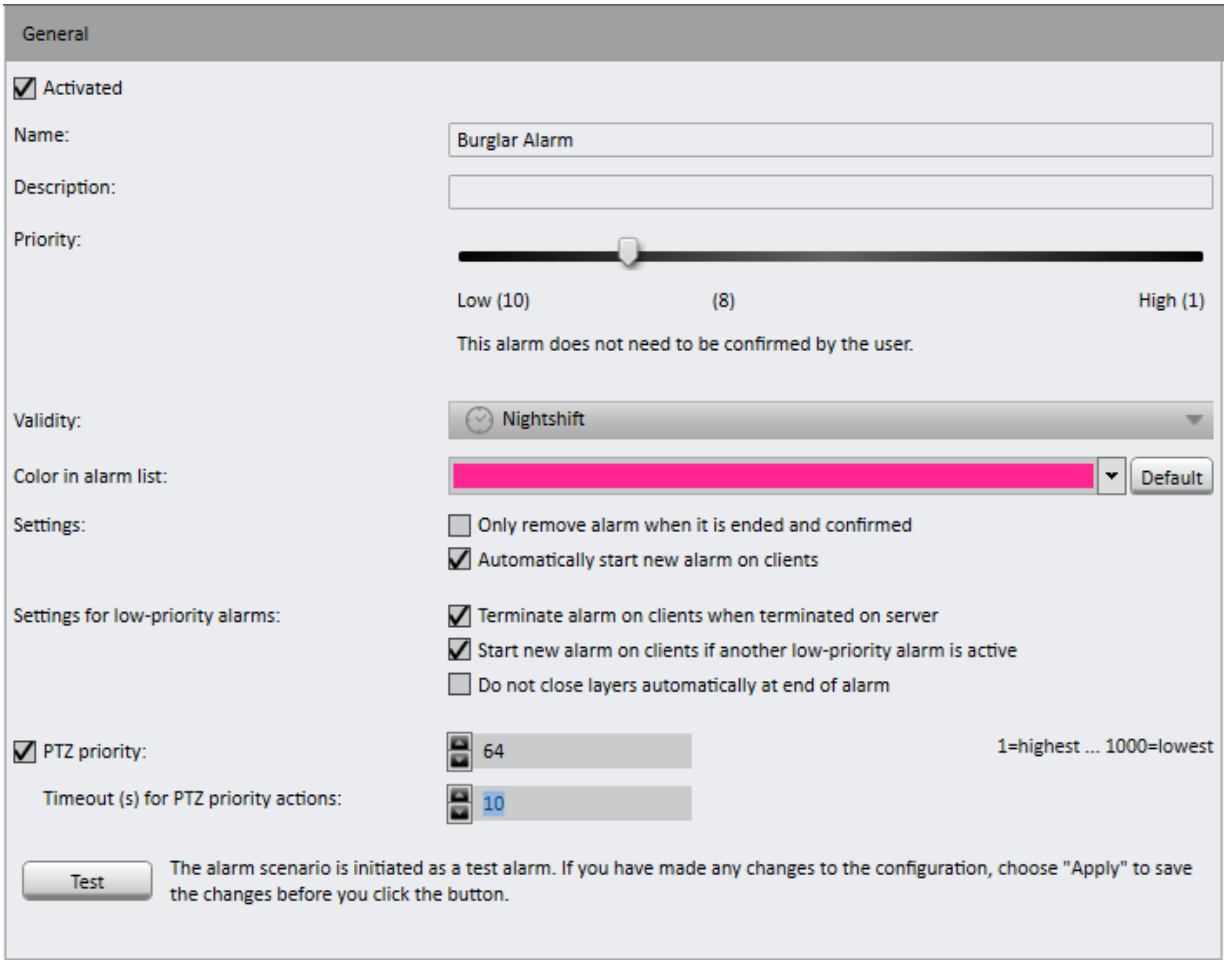
1. Select the alarm in the overview.
2. Click the **Duplicate object** icon, and enter a name for the duplicated alarm.
3. If you want to configure the new alarm using the configuration wizard, select **Wizard** in the dialog box (see **Creating an alarm scenario**)
4. Click **OK** to accept the name. The new alarm is displayed in the overview.

Creating an alarm with the wizard

Ocularis Recorder provides an alarm wizard that guides the user step by step to the goal. The alarms are based on the detailed rights concept and can be assigned to individual users or user groups.

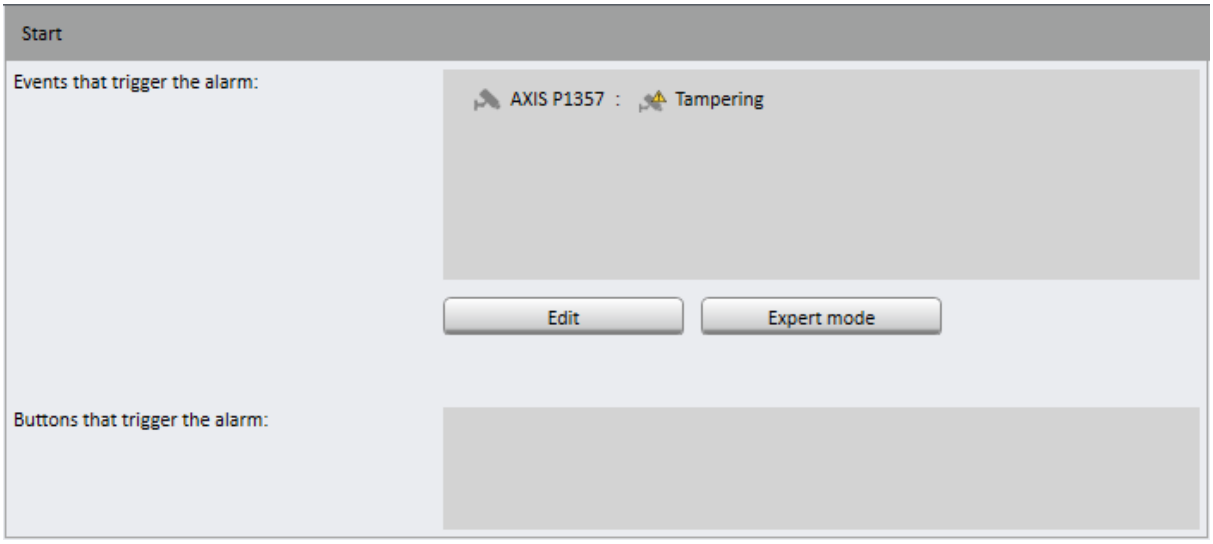
1. Click Configuration menu and select Createalarm.
2. Enter the **name** of the new alarm scenario and select **Wizard**.
3. Open the list of available objects for the location.
4. Activate the objects that are to trigger an alarm event, and then click **Next**.
5. Select the camera that is to be displayed as the alarm camera, and set the duration for alarm recording (in seconds).
6. Specify whether you want to add a pre-alarm duration, and set the duration in seconds.
7. Click **Next**.
8. Skip the section on notifying users as this feature is not supported in this version.
9. Skip the section on notifying users by means of a message window as this feature is not supported in this version.
10. Click **Next**, and then check the settings. If you wish to make changes, click **Back** and change the settings.
11. To apply the settings, click **Finish**.

General



1. Select or deselect the alarm scenario.
2. If necessary, alter the **name** of the alarm.
3. Enter an optional **description**.
4. The **Priority** slider is not supported in this version.
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**).
6. The remaining fields on this page may be ignored as they are not supported in this version.

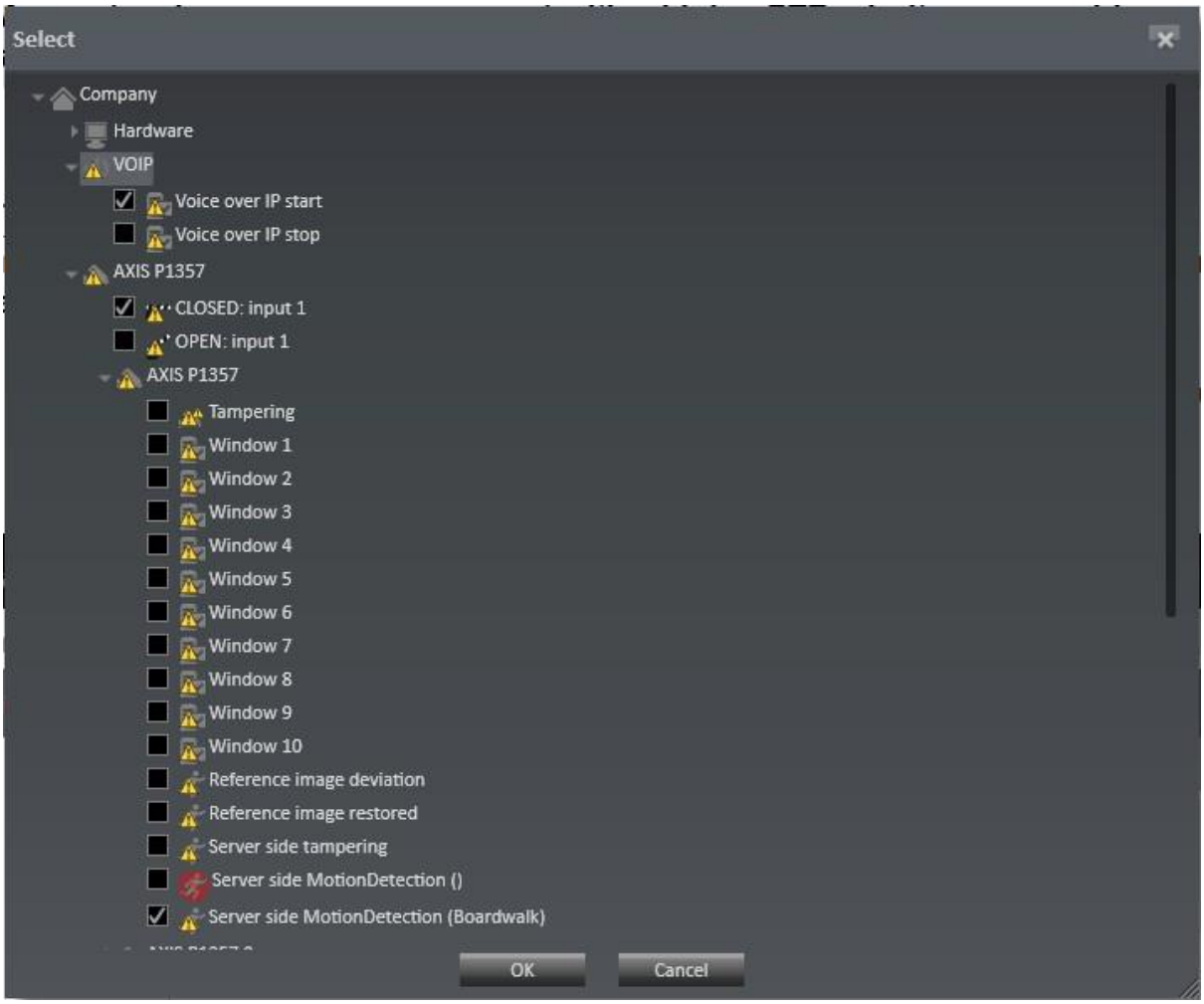
Start



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.

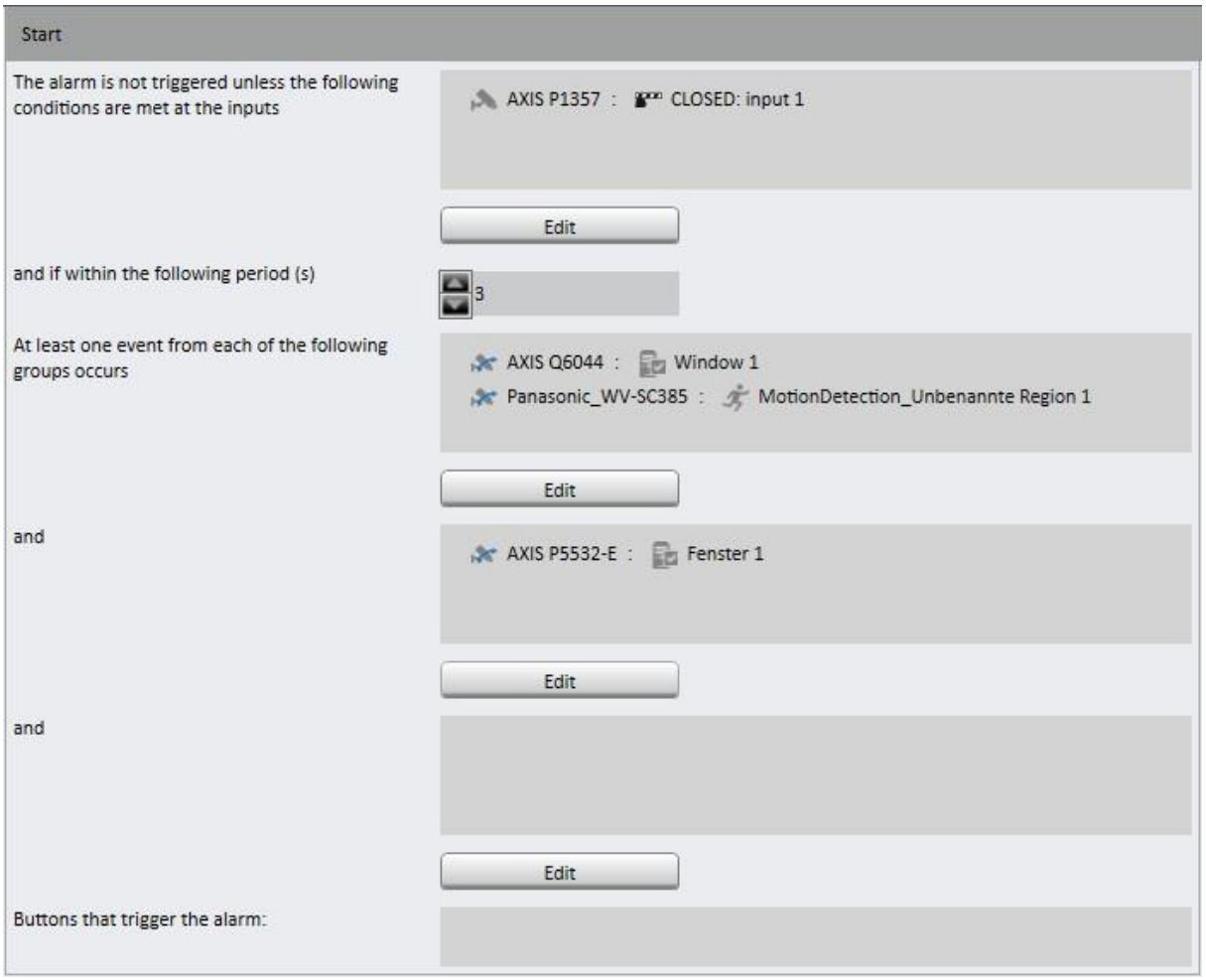


NOTE: The trigger must be created or activated before configuring the alarm scenario. One excep- tion to this are buttons, which can be defined later in the buttons control (see Buttons). A starting event can be, for example, the receipt of a TCP signal from a camera when it detects motion. This is implemented via the network I/O.

2. Click **Expert mode** to specify the settings.

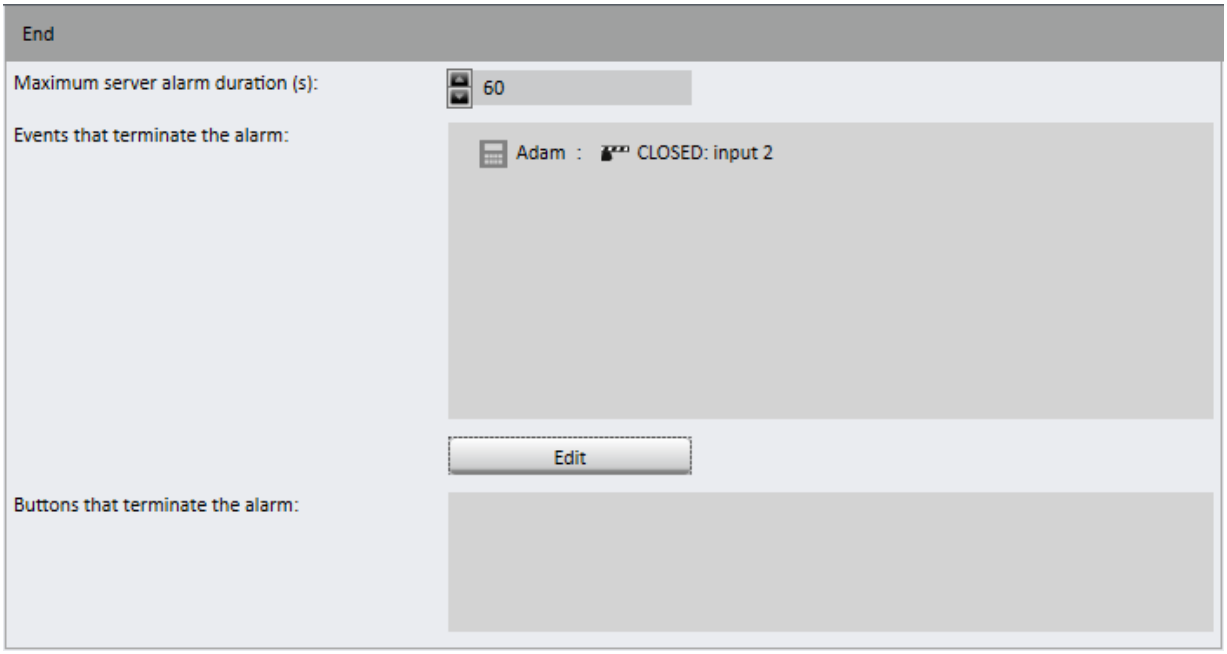
Expert mode

Expert mode can be used to create complex alarm scenarios. The alarm is triggered by different conditions that are logically linked (AND / OR conditions).



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

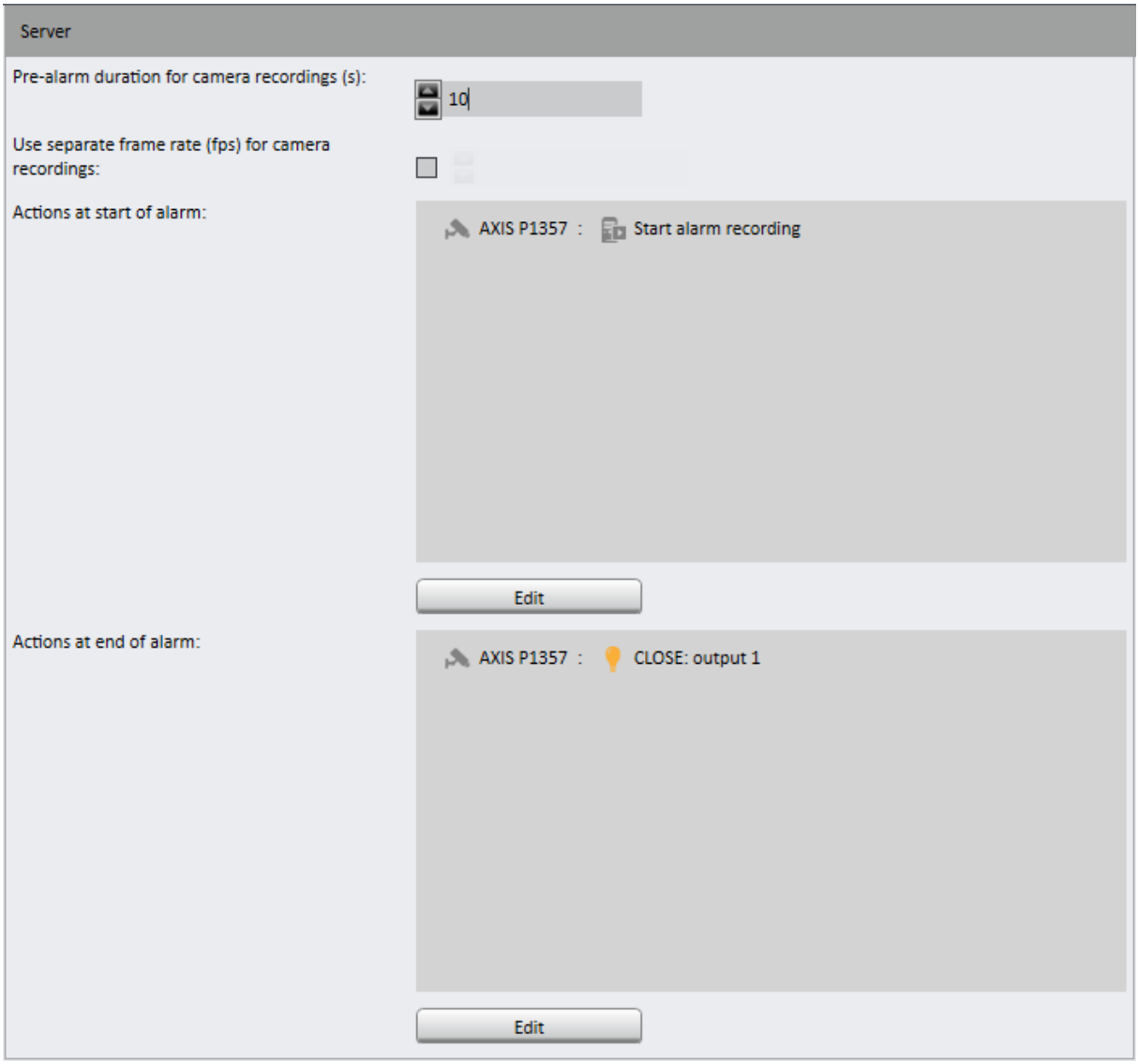


1. Specify the **maximum server alarm duration** (in seconds) to specify how long the alarm is to be recorded for.
2. Optional: click **Edit** to select the **events that terminate the alarm earlier**. The hardware and events are displayed.

Persons involved

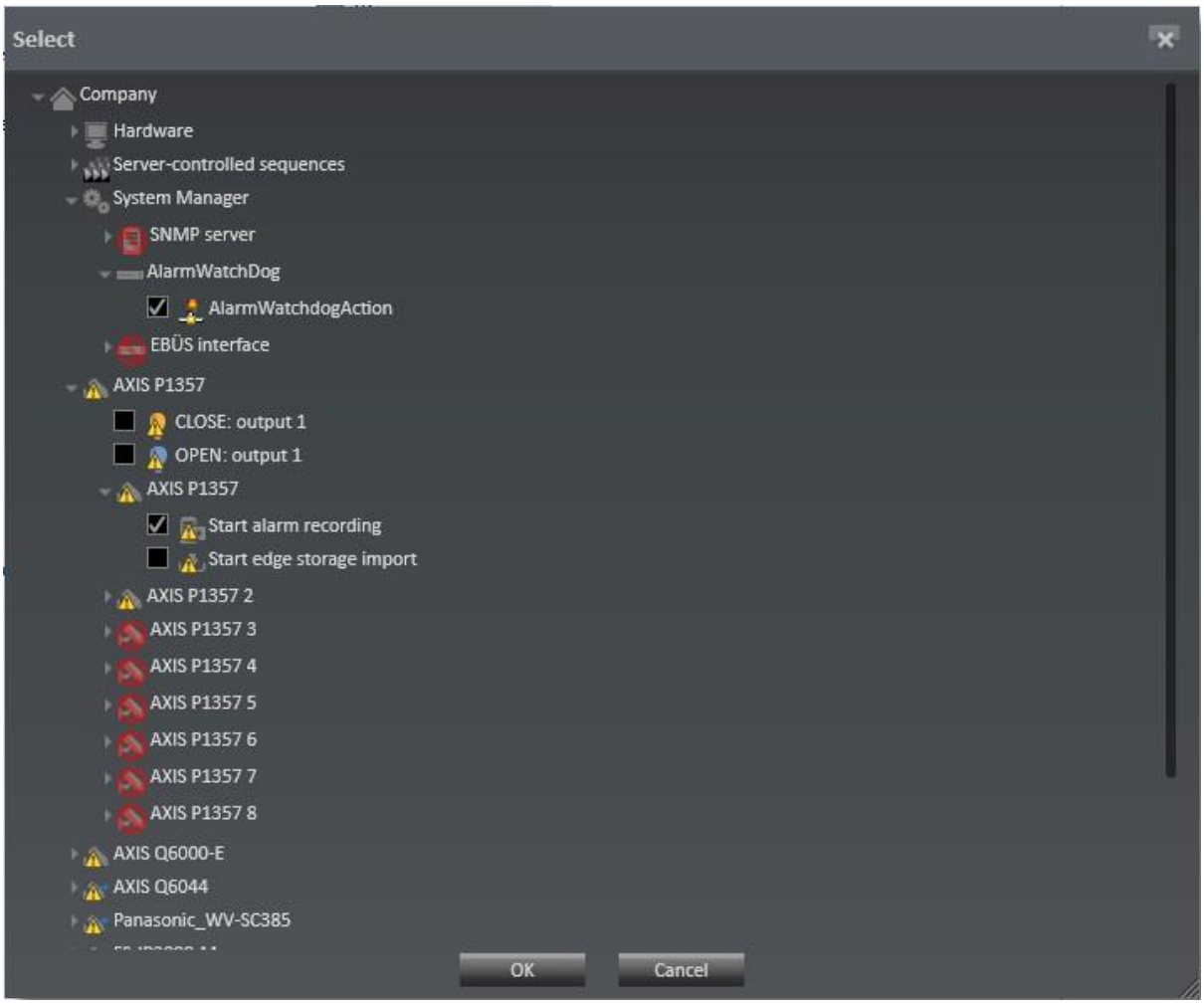
This screen is not supported in this version.

Server



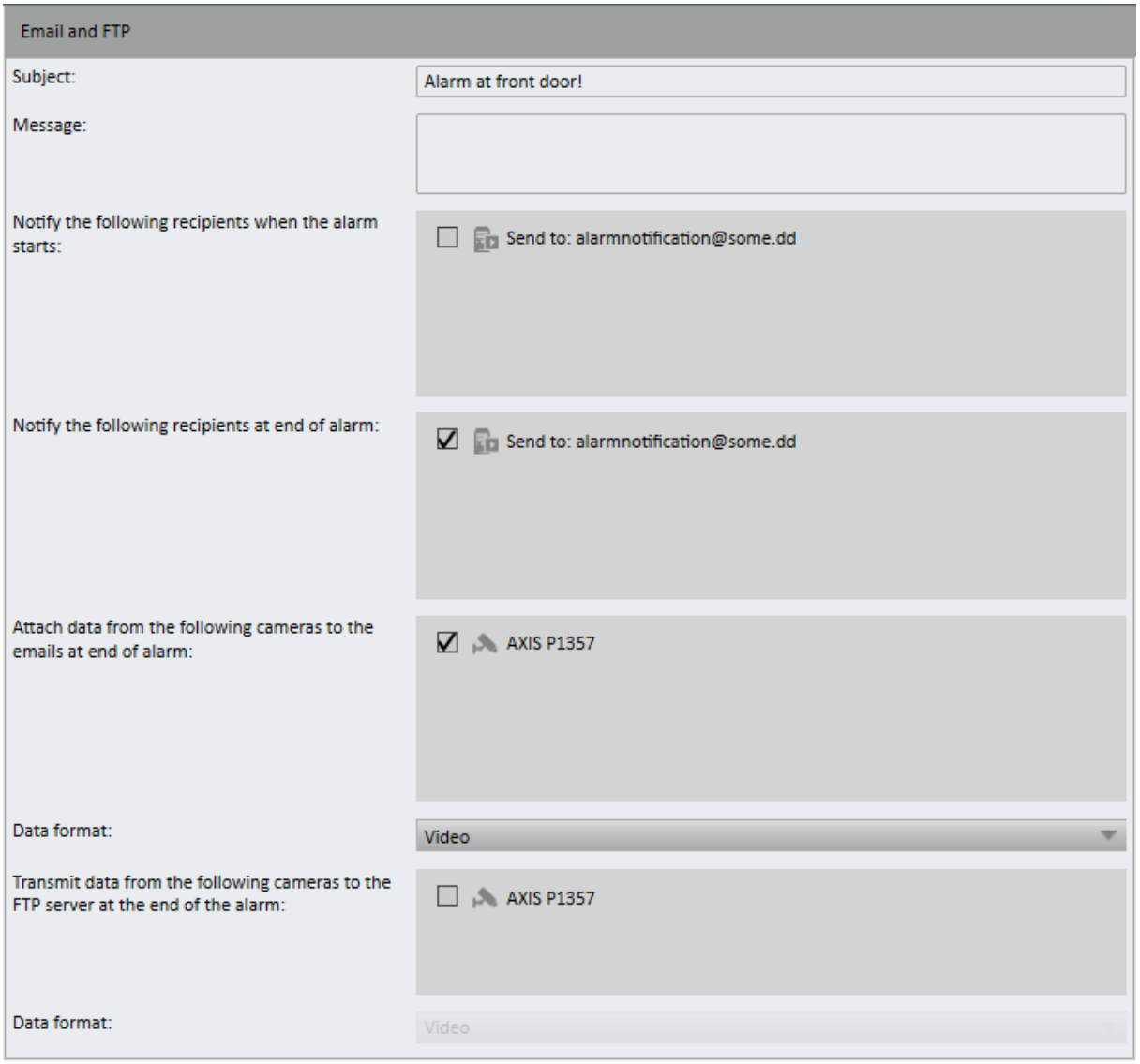
1. Specify the **pre-alarm duration for camera recordings** (up to a maximum of 3600 seconds) to record a period before the alarm is triggered in alarm recording.
2. Select Use separate frame rate (fps) for camera recordings, and enter the required frame rate. The frame rate can only be changed with M-JPEG.

3. Choose **Edit**, and then activate the **actions at the start of an alarm**. The selected actions are displayed. Typically, you want to select **Start alarm recording**.



4. Choose **Edit**, and then activate the **actions at the end of an alarm**. The selected actions are displayed.

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**).

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**).
3. Select the cameras whose **data at the end of the alarm** is to be attached to the email and specify the **data format**. Two types of file format are possible:
   - Video: the files are sent unencrypted as *.avi.

- 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 Ocularis Recorder VA Administration Tool (see **Ocularis Recorder VA Administration Tool**).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.

7.4.2.8 Triggers

The **Triggers** function (formerly called 'Buttons') in the Administration control allows you to start specified processes (actions) such as camera recordings, alarm scenarios or to manually start or stop a live stream. To invoke configured triggers in Ocularis Client, click on either Trigger in the aux menu of a camera pane (for camera specific triggers) or from the Triggers menu.

1. Select the location in the **Company** control. The selected location is displayed in the title bar of the Administration control.
2. Select **Triggers** in the Administration control.

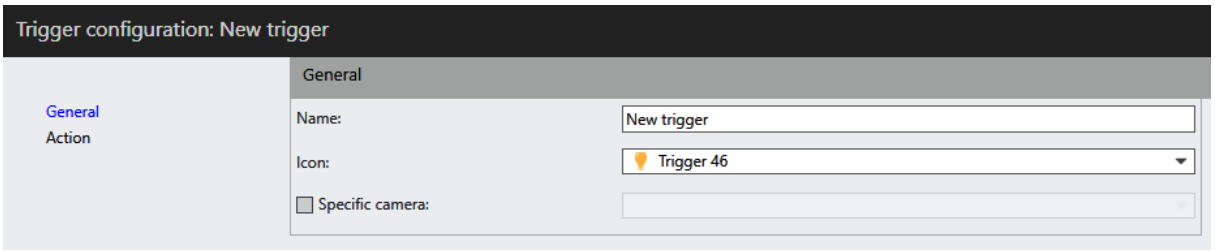
Creating a new trigger

1. Create a new trigger by clicking the **Create new object** icon.
2. Enter the name for the new trigger.
3. Click **OK** to accept the name. The new trigger is displayed in the overview.

Configuring a trigger

1. Select the trigger in the overview triggers list.

General



1. You can modify the trigger name if desired. This is the label it will display in all Ocularis clients.
2. Select an **icon** to make it easier to recognize in Ocularis Recorder Manager (optional).
3. Optional: To create a camera specific trigger, check to box **Specific camera**, and select the camera. In this case the trigger will be available in the aux menu on the camera's pane in Ocularis Client or Ocularis Web. It will also be available in Ocularis Mobile.

Action

1. To perform and action, select the **Perform action** option. Then click **Select** and then select the action. (For example, 'Enable stream')
2. To invoke an alarm scenario, select the **Start alarm scenario** option and then the alarm scenario. The alarm scenario must already have been created.
3. To stop an alarm scenario, select the **Terminate alarm scenario** option and then the alarm scenario. The alarm scenario must already have been created.
4. If you want the trigger to run an application, select the **Run program** option, and then click **Select** to select a program that is to be started. The selected program must be installed on the client computer. This works in Ocularis Client only.
5. Enter any **parameters** required by the program you will run. A document can be opened using the selected program, for example.
6. **Apply** the set values if you want to make further settings.
7. **Save** the set values to apply the values and conclude input.

Creating a Trigger to Disable a Camera Stream for a Single Camera using the 'aux' overlay

Be sure that the camera has 'Stream audio/video' set to either 'On Demand' or 'On Demand - Quick Stream Start'.

1. From *Ocularis Recorder Manager*, select Triggers and then 'Create new object'.
2. Enter a name for the Trigger. For example: 'Disable Stream for Camera A'
3. Click **OK**.
4. Check the 'Specific camera' checkbox.
5. In the adjacent drop-down, select the camera that you want to assign to the Trigger.
6. Click Action.
7. Select 'Perform Action'.
8. Click **Select** adjacent to 'Perform Action'.
9. Expand the camera identified in step 5 and select 'Disable stream'.
10. Click **OK**.
11. Click **Save**.
12. Refresh the server in *Ocularis Administrator*.

The trigger will be available to the operators in the Ocularis Client 'aux' overlay in the pane of the camera. It will also appear in the camera's pane for Ocularis Web users and in the triggers menu for Ocularis Mobile users.

NOTE: Triggers is a privileged function. If you do not see a trigger that you believe you should have, ask your system administrator to verify your privileges to triggers.

Creating a Trigger to Enable a Camera Stream for a Single Camera using the 'aux' overlay

Follow the same instructions as above except create a different trigger name (e.g. 'Enable Stream for Camera A') and choose 'Enable stream' in step 9.

Creating a Global Trigger to Disable a Camera Stream for a Single Camera

These steps will create a trigger that is executed from the Triggers menu in Ocularis Client. The camera need not be displayed in order to disable or enable its stream.

1. From *Ocularis Recorder Manager*, select Triggers and then 'Create new object'.
2. Enter a name for the Trigger. For example: 'Camera A - Disable Stream'

NOTE: Tip: if you include the camera label at the beginning of the name, the trigger to enable and dis- able will be grouped together in the menu list.

3. Click **OK**.
4. Click Action.
5. Select 'Perform Action'.
6. Click **Select** adjacent to 'Perform Action'.
7. Expand the camera whose stream you want to disable and select 'Disable stream'.
8. Click **OK**.
9. Click **Save**.
10. Refresh the server in *Ocularis Administrator*.

The trigger will be available to the operators in the *Ocularis Client* Triggers menu and to Ocularis Web users in the trigger icon on the main control bar. Global triggers are not available in Ocularis Mobile.

Creating a Global Trigger to Enable a Camera Stream for a Single Camera

Follow the instructions above except create a different trigger name (e.g. 'Camera A - Enable Stream) and choose 'Enable Stream' in step 7.

Using a Global Trigger to Enable or Disable a Camera Stream for a Single Camera

From *Ocularis Client*, select the Triggers menu and expand Global Triggers. Find the desired trigger in the list and select it.

Creating a Global Trigger to Disable a Camera Streams for a Multiple Cameras

Global Triggers may also be used to disable or enable multiple cameras. For instance, if you have four cam- eras displayed in a view, you can use a global trigger to disable the streams for all four cameras at once.

This is done using an alarm scenario. Enabling all four cameras is also supported by global triggers. There is no limit to the number of cameras that may be enabled or disabled using this method.

1. From *Ocularis Recorder Manager*, select Alarms and then 'Create new object'.
2. Enter a name for the alarm scenario. (e.g. 'View A - Disable All Cameras')
3. Click **OK**.
4. If desired, modify the 'Validity' period by selecting another time profile. The default is that the scenario will be available always.
5. Click 'Start'. If you want to trigger the cessation of camera streams by an event, click the Edit button and select the event that will trigger the stopping of camera streams. Click OK.
6. Click 'Server'.

7. Click **Edit** under 'Actions at start of alarm'.
8. Expand each camera of the view and select 'Disable stream'. When done, click **OK**.
9. Click **Apply** to save changes.
10. If you want to create a scenario to enable the streams, repeat steps 1 - 9 but change the name of the alarm scenario (e.g. 'View A - Enable All Cameras') and choose 'Enable stream' in step 8.
11. To use a manual global trigger to enable or disable the streams, create another trigger. Select Triggers and then 'Create new object'.
12. Assign the Trigger a logical name (e.g. 'View A - Disable Cameras').
13. Select 'Action'.
14. Click 'Start alarm scenario'. In the adjacent drop-down list, select the alarm scenario to disable the cameras from View A.
15. Click **Apply** to save changes.
16. Create another Trigger to enable the streams from View A.
17. Check: if you go back and review the alarm scenario, the trigger now appears under 'Triggers that start the alarm'.
18. Refresh the server in *Ocularis Administrator*.

The trigger will be available to the operators in the *Ocularis Client* Triggers menu.

Deleting a Trigger

1. Select the trigger in the overview Triggers list by selecting the checkbox adjacent to its name.
2. Click the **Delete object**icon.
3. At the "Are you sure you want to delete [trigger name]?" pop-up, click **Yes**.

Duplicating a Trigger

1. Select the trigger in the overview Triggers list by selecting the checkbox adjacent to its name.
2. Click the **Duplicate object** icon, and enter a name for the duplicated trigger.
3. Click **OK** to accept the name. The new trigger is displayed in the overview.
4. Modify settings as needed.
5. Click **Save** or **Apply** when done.

7.4.2.9 Patrols

The **Patrols** function on the **Administration** control allows you to create patrols in which multiple preset positions are approached one after the other and/or actions are triggered with a PTZ camera.

General information on patrols

- Multiple times and/or time periods can be added to a patrol.
- A time input is not required if the patrol is to be started by an alarm scenario.
- If a patrol is started by an alarm scenario, the patrol in progress is stopped. The patrol in progress is run once and then restarted at the previously stopped time.

- If a patrol is started by an alarm scenario, the patrol is processed in full. The patrol is also processed in full if the alarm scenario is stopped earlier.
- If a patrol in progress is stopped by an alarm scenario, the patrol is only interrupted for a defined time period.
- A recording can only be started in connection with an alarm scenario.
- Patrols do not have exclusive access to the camera positions. If a PTZ camera is controlled during an ongoing patrol, the preset positions are approached with a dead time of one minute not included in the patrol.
- A preset position can also be approached by an alarm scenario, even if the patrol approached a different preset position of the same camera shortly before. The same applies to an additional patrol.

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

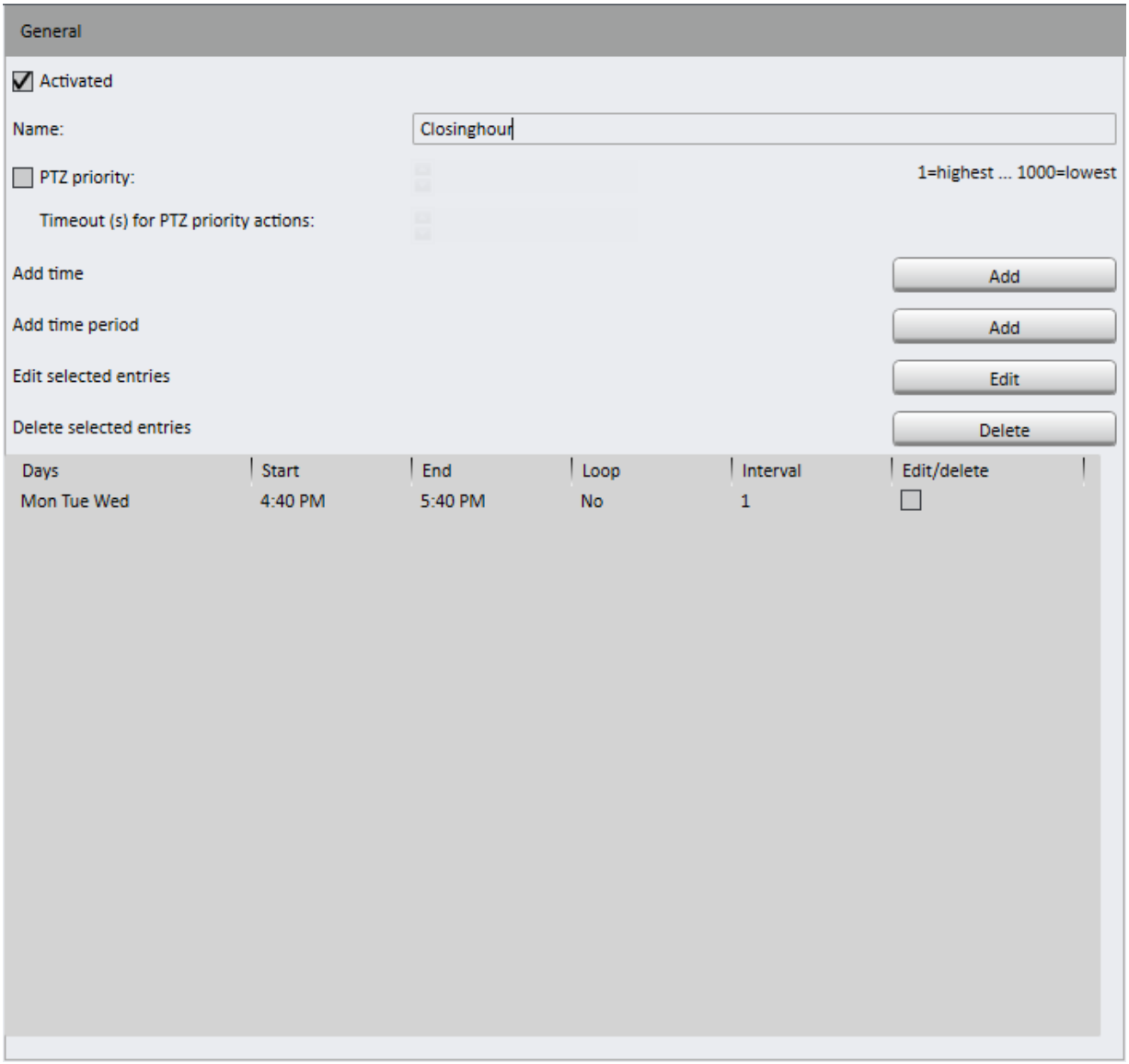
1. Create a new patrol by clicking **Create New Object** icon.
2. Enter the name for the new patrol.
3. Click **OK** to accept the name.

The new patrol is displayed in the overview.

Configuring a patrol

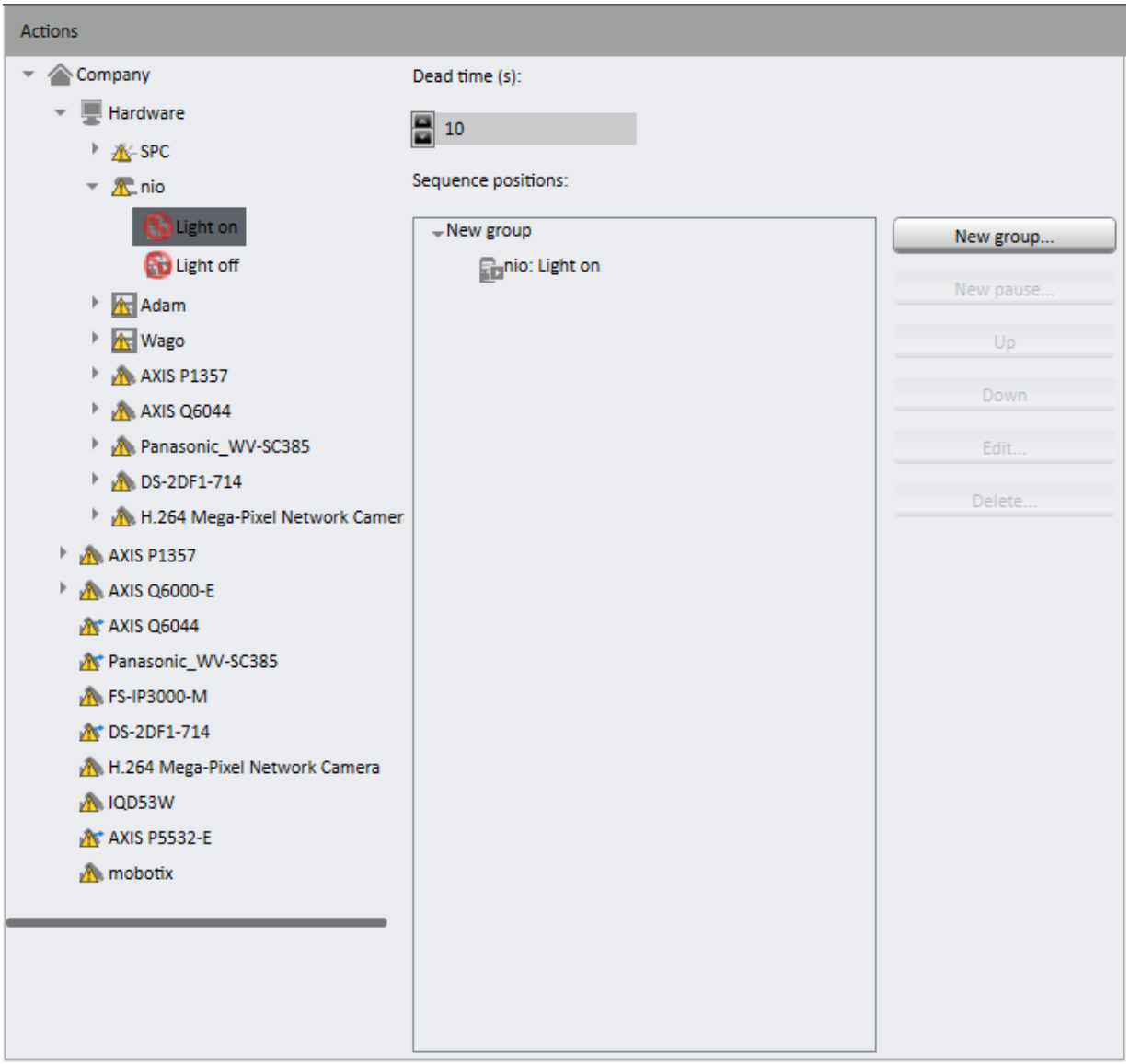
1. Select the patrol in the overview.

General



2. Select the patrol and, if necessary, alter the **name**.
3. The **PTZ priority** counter is not supported in this version.
4. Use the **Times** and **Time periods** buttons to make additions for when the patrol should be run.
5. **Time**: The patrol is started once at the selected time on every selected day.
6. **Time period**: The patrol is started multiple times depending on the duration of the patrol on every selected day within the time period.
7. Select one or more entries, and then click the **Edit selected entries** button to edit the entries one after the other.
8. Select one or more entries, and then click the **Delete selected entries** button to delete the entries.

Actions



1. Create a **new group** and give it a name.
2. Specify the **dead time** (in seconds) to identify the interval in which no new signal is displayed.
3. Drag one or more camera positions or actions to the group.
4. Select a group, and then use the **New pause** button to adjust the pause (in seconds) to specify how long the camera preset is displayed.
5. Select a group or an entry, and use the **Up** or **Down** button to move it up or down in the list.
6. Select a group or pause, and then click the **Edit** button to edit the name of the group or the duration of the pause.
7. Select a group or an entry, and then click the **Delete** button 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 patrol

1. Select the patrol in the overview by clicking the checkbox adjacent to its name.
2. Click the **Delete object**icon.
3. At the "Are you sure you want to delete [patrol name]?" pop-up, click **Yes**.

Duplicating a patrol

1. Select the patrol in the overview Patrols list by selecting the checkbox adjacent to its name.
2. Click the **Duplicate object** icon, and then enter the name for the duplicated patrol.
3. Click **OK** to accept the name.

   The new patrol is displayed in the overview. Modify settings as needed.
4. Click **Save** or **Apply** when done.

7.4.2.10 Server

The **Server** function on the Administration control allows you to configure the server services. The following services are available after a standard installation:

- CoreService main
- DeviceManager
- 2 MotionDetection modules

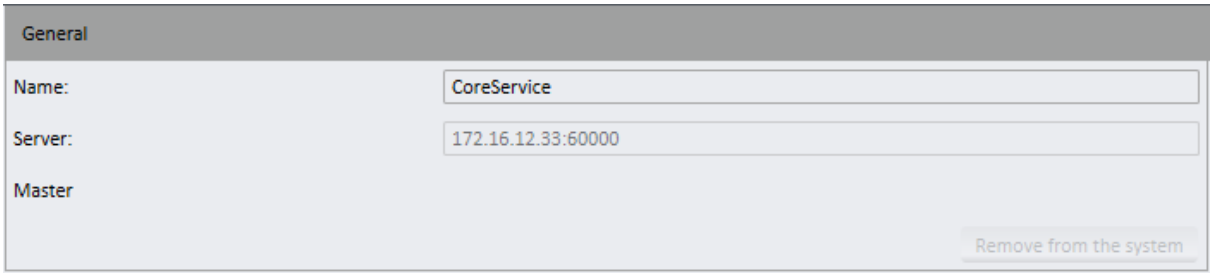
The following modules can be created by a user defined installation (see **Custom installation**) or with the VA-Administration tool (see **Ocularis Recorder VA Administration Tool**):

- Server based Motion Detection

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 CoreService

- The main tasks of the CoreService 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



General

1. If desired, change the **name** of the **server**. The network address and port number of the core server can be changed with the Ocularis Recorder Administration tool.
2. Click the **Remove from the system** button to remove the core server from the system configuration.

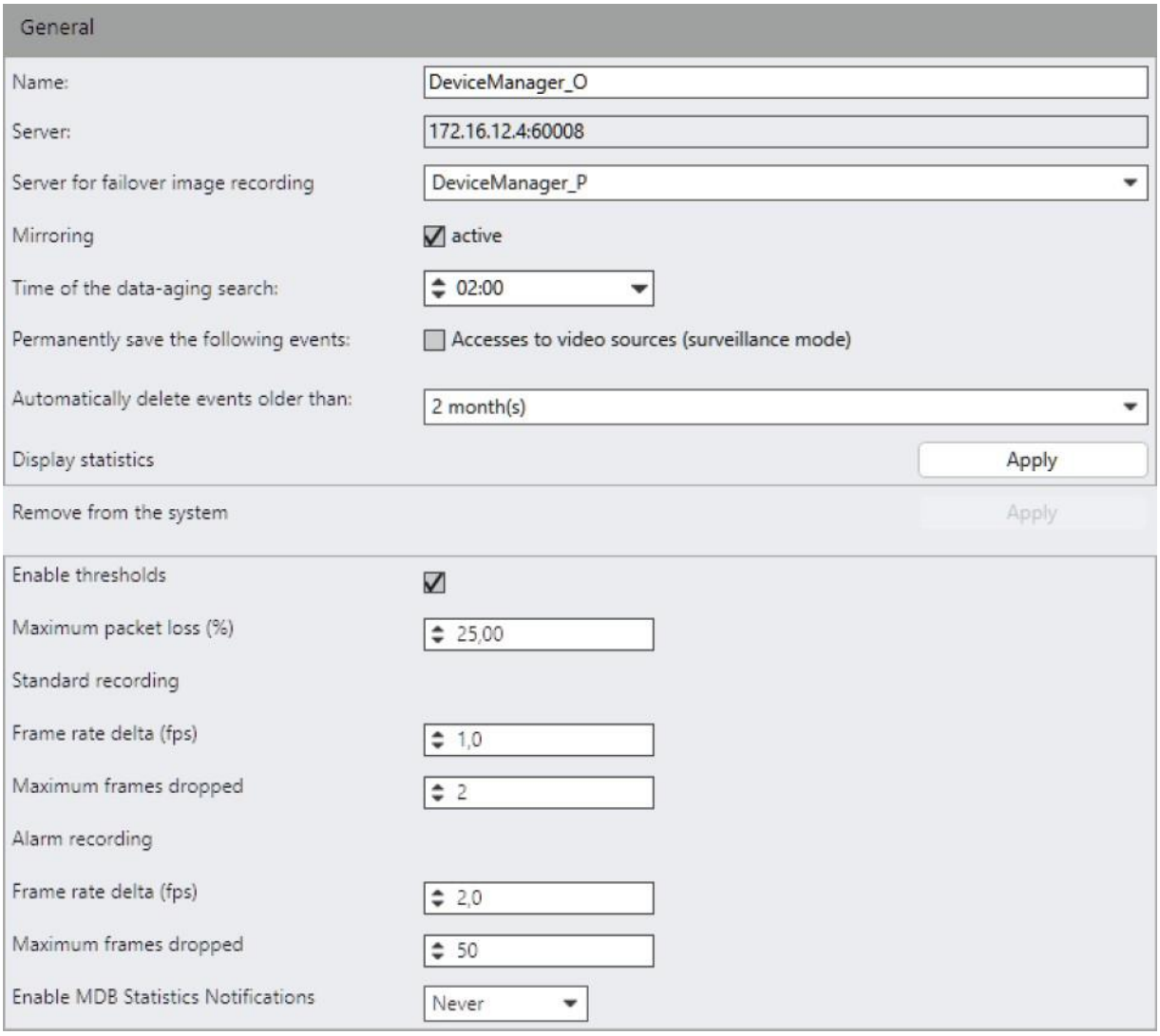
   Removing from the system is only available for a CoreService Secondary (CSS) if the server is not connected to the CoreService Main (CSM).Always contact Qognify support before deletion.
3. **Apply** the set values if you want to make further settings.
4. **Save** the set values to apply the values and conclude input.

Configuring the Device Manager (DM)

The main tasks of the Device Manager are:

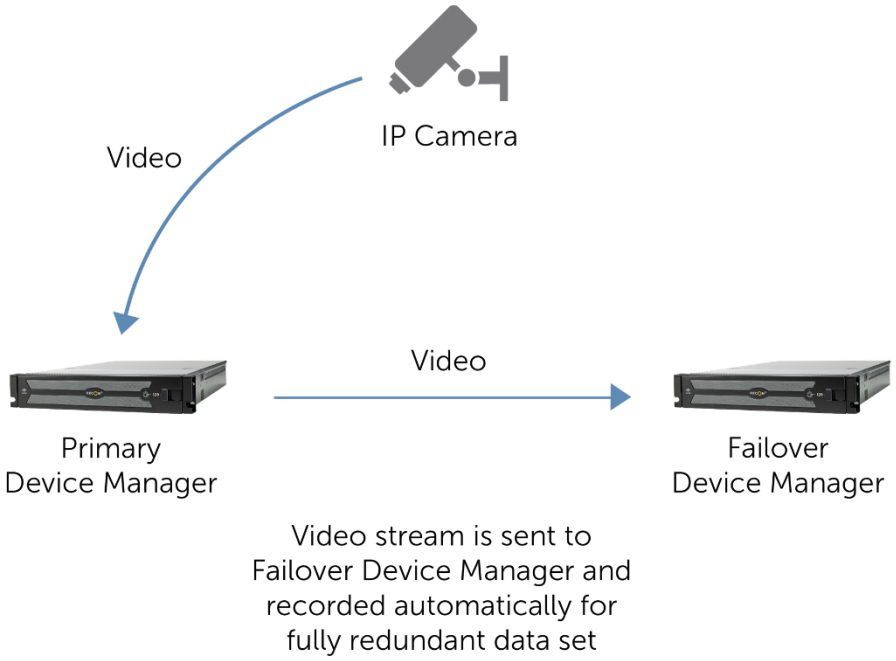
- Management of all connected hardware like cameras, video servers, Adam-modules
- Distribution of image data e. g. to the clients, multimedia database
- Communication with other services
- Event handling

General



1. If desired, modify the **Name** of the device manager. When there are multiple DMs in an environment, the naming convention used is important to be able to distinguish one from another.
2. Ocularis Ultimate or Enterprise: Select the failover **Server for failover image recording**. In the event of the failure of the device manager, all connected devices are transferred to the failover server. A distributed DeviceManager installation is required (see **Installation of a Device Manager**), since the failover server must have sufficient capacity to take over the devices (see **System requirements**).
3. **Mirroring**: This option activates the redundant recordings of all connected cameras. If activated:
   - To be able to be activated, a second DM must be configured as a failover DM.
   - The productive (R16) DM has the lead and multiplexes the data to both MDSs 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, redundant recording resumes.



– 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.

Mirroring is available in Ocularis ULT only and requires additional licensing. Contact Technical Support for more information.

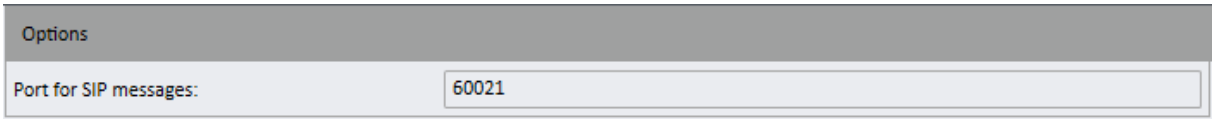
1. Specify the time of the data aging search.
2. Activate **Accesses to video sources** to save these events.
3. Select the period after which the events are automatically deleted. Note: due to legal regulations, some events may not be deleted for installations in France.
4. Click the **Apply** button adjacent to **Display statistics** to display the available recordings of the individual cameras. For more detailed statistics, thresholds may be set for better visualization of critical streaming behaviors. See the section on **Device Manager Thresholds**
5. Click the **Apply** button adjacent to **Remove from the system** button to remove the DeviceManager from the system configuration. Always contact Qognify Support before deletion

For more information see **Device Manager Statistics** and **Device Manager Thresholds** .

Core Extensions Provide Performance Improvements By Default

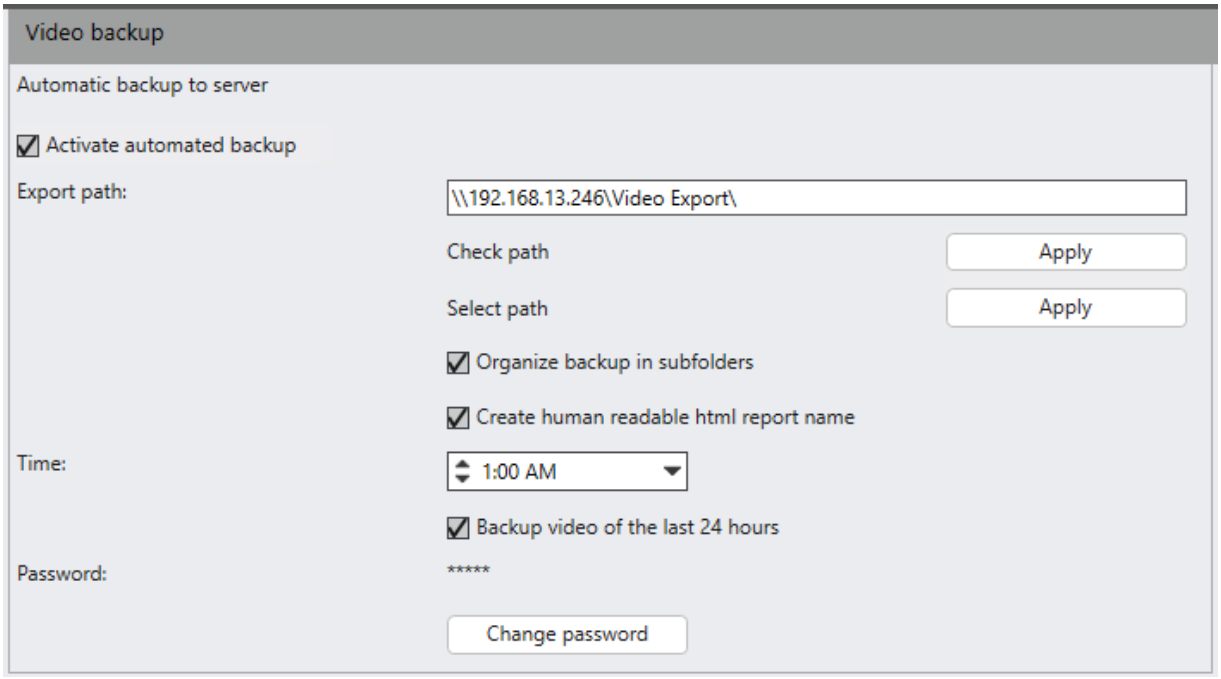
Changes have been made to improve the failover time between Device Managers in Ocularis v5.6 (R12). Previously, this enhanced mode could be configured manually in the Core configuration file. This manual step is no longer necessary.

Options



1. If necessary, alter the **port for SIP messages** (see VoIP and SIP).

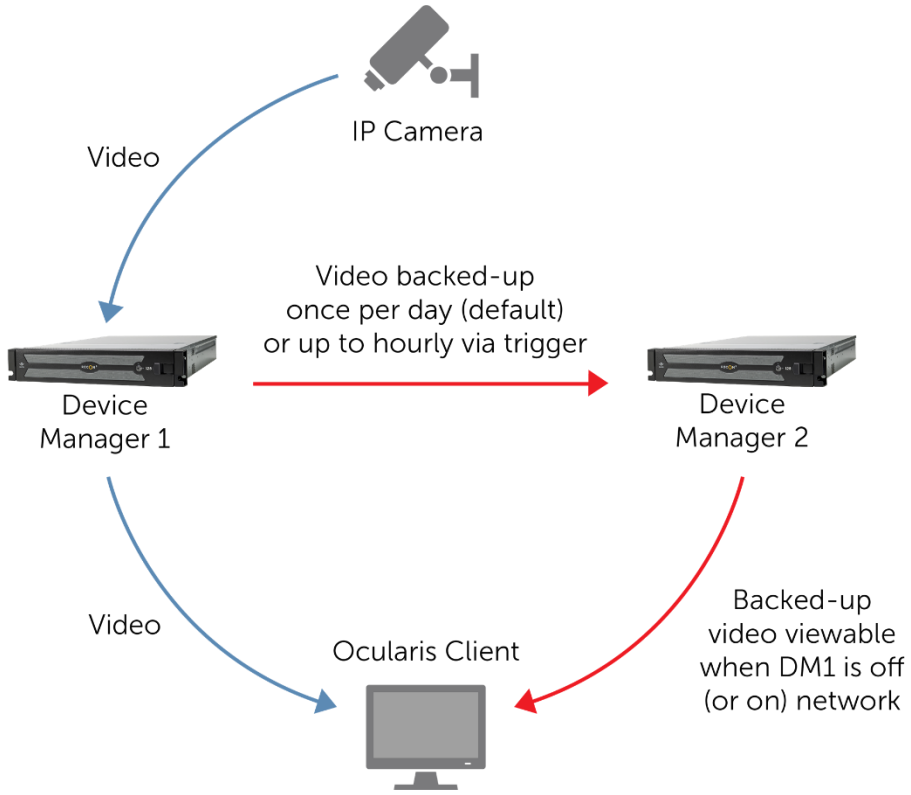
Video backup



Automatic video export to server

1. Check the box Activate automatic export.
2. Create the **export path** for the automatic storage of the image data, or click **Apply** adjacent to **Select path** to select the folder directly in Windows Explorer.Client and server must be installed on the computer for the export folder to be specified. The export path must be accessible by the DeviceManager server.
3. Click the **Apply** button next to **Check path** to check the availability of the specified folder.
4. Check the box **Organize backup in subfolders** if you want the exported recordings to be stored in folders named after camera names. Otherwise, the computer timestamp is used as the filename of the report.
5. Check the box **Create human readable html report name**. Otherwise, the computer timestamp is used as the filename of the report.
6. Specify the **time** that the export will 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 (mid-night to midnight) are exported.

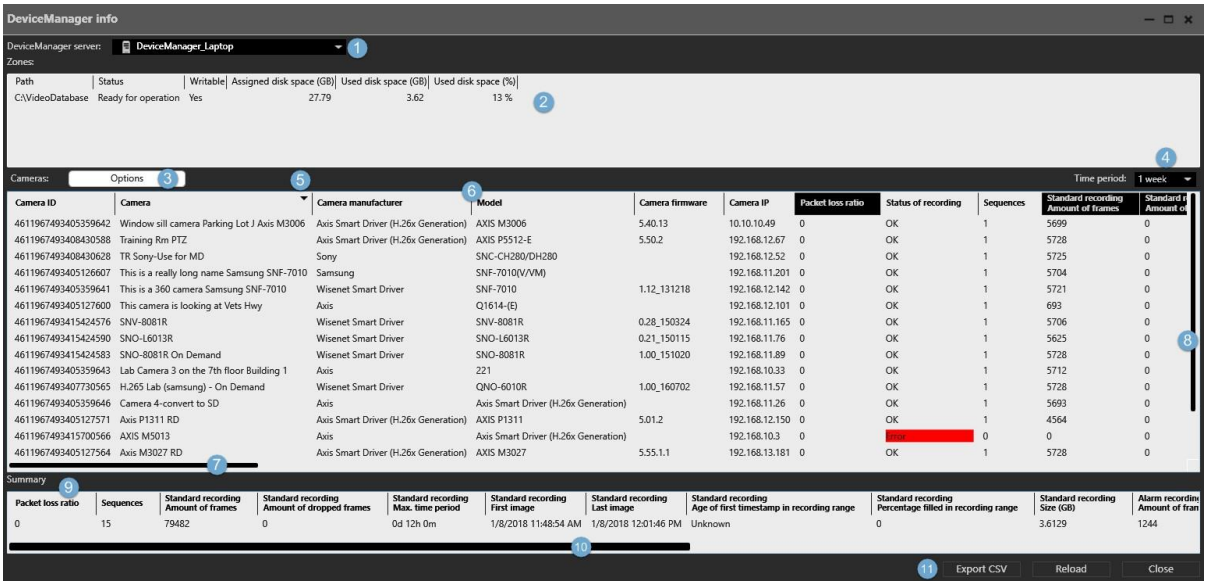
8. Specify a **password**, with which the image data is encrypted.



Generating a Report

Generate a Device Manager Statistics report from the Server control. Choose a Device Manager. Then, click the **Apply** button adjacent to 'Display Statistics'.

Refer to the graphic below for additional functionality indicated by number.



1. You can switch to a different device manager by using this drop-down menu.
2. The top section provides at-a-glance information about the Device Manager's zone(s). You can easily see if one it running out of disk space.
3. Use the **Options** button to control which columns appear in the report. The report will update as you add or remove columns.
4. Select a **Time period** of 1 hour, 1 day or 1 week
5. Click on the name of a column heading to sort the report by that column. Click it again to reverse the sort order. A triangle appears to indicate the sort column and its order.
6. Position the mouse between two column headings if you want to resize the columns. Click and drag the mouse left or right to lengthen or shorten the column.
7. Use the horizontal scroll bar to move the report data left or right.
8. Use the vertical scroll bar to move the report data up or down.
9. The Summary area provides an overview of the report content.
10. Use the horizontal scroll bar to move the summary data left or right.
11. You can click **Reload** to refresh the data displayed. Click **Export CSV** to export the visible data to a CSV file for use in Microsoft Excel or a text editor. Click **Close** when done with the report.

Device Manager Statistics

Device Manager display statistics is a valuable report providing statistical information about each Device Manager. It can help you troubleshoot the system and identify cameras that may be recording more data then they should. It can help you determine the free and used disk space on your zones.

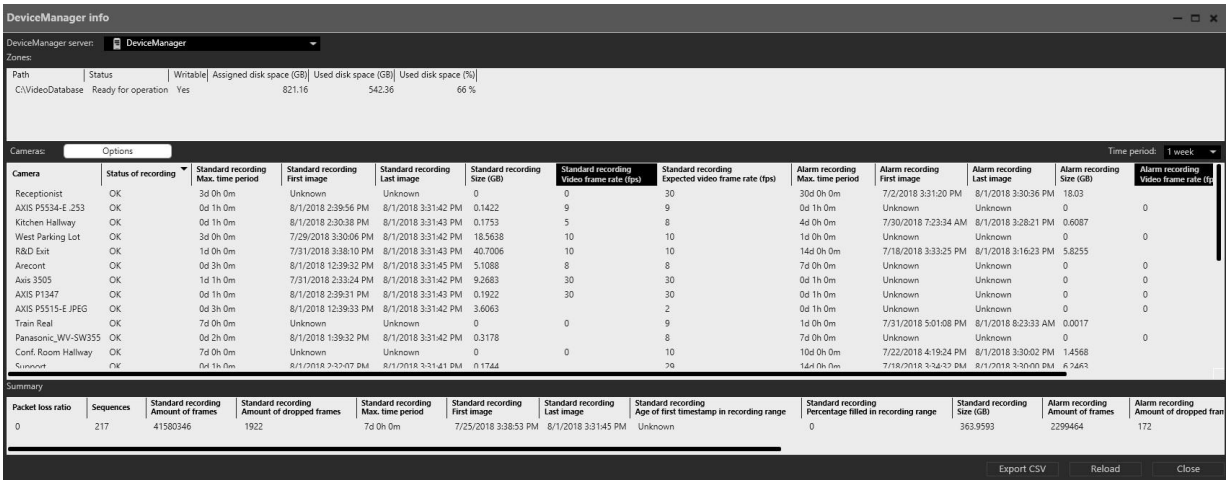
Access the Device Manager Statistics report by clicking the **Apply** button adjacent to 'Display statistics' under Server > Device Manager.

Available Columns

The statistic report can display the following values as of this writing:

- Camera ID
- Camera
- Camera manufacturer
- Model
- Camera firmware
- Camera IP
- Packet Loss ratio
- Status of recording
- Sequences
- Standard recording Amount of frames
- Standard recording Amount of dropped frames
- Standard recording Max. time period
- Standard recording Actual time period
- Standard recording First image
- Standard recording Last image
- Standard recording Age of first timestamp in recording range
- Standard recording percentage filled in recording range
- Standard recording Size (GB)
- Standard recording Width
- Standard recording Height
- Standard recording Expected width
- Standard recording Expected height
- Standard recording codec
- Standard recording Expected codec
- Standard recording Video frame rate (fps)
- Standard recording Expected video frame rate (fps)
- Standard recording Video bit rate (kbps)
- Standard recording Expected video bit rate (kbps)
- Alarm recording Amount of frames
- Alarm recording Amount of dropped frames
- Alarm recording Max. time period
- Alarm recording Actual time period
- Alarm recording First image
- Alarm recording Last image
- Alarm recording Age of first timestamp in recording range
- Alarm recording Percentage filled in recording range

- Alarm recording Size (GB)
- Alarm recording Width
- Alarm recording Height
- Alarm recording Expected width
- Alarm recording Expected height
- Alarm recording Codec
- Alarm recording Expected codec
- Alarm recording Video frame rate (fps)
- Alarm recording Expected video frame rate (fps)
- Alarm recording Video bit rate (kbps)
- Alarm recording Expected video bit rate (kbps)
- Pre-alarm recording Video frame rate (fps)
- Pre-alarm recording Amount of dropped frames
- Pre-alarm recording Amount of frames



The following options are available:

- **Device Manager Server** - This is the Device Manager (DM) for which the report applies. You can switch to another Device Manager using this drop-down list.
- **Zones** - All zones for the selected DM are shown with an overview of resources
- **Cameras** - Displays detailed information about the connected cameras
- **Options** - Use this button to select which columns to display
- **Columns:**
  - The columns of the statistics report may be sorted manually by clicking on the column header
  - The order of the columns may be changed by dragging the column header left or right to the desired location
  - The width of the column may be modified by clicking on the vertical column border and dragging left or right

- **Time period** - The report will reflect data for the selected time period. Available options include: 1 hour, 1 day or 1 week
- **Summary** - This area displays the summary values of all cameras connected to the selected Device Manager
- **Export CSV** - The report can be exported as a .CSV file
- **Reload** - Reloads the statistics to display the most up-to-date values
- **Close** - Closes the report window

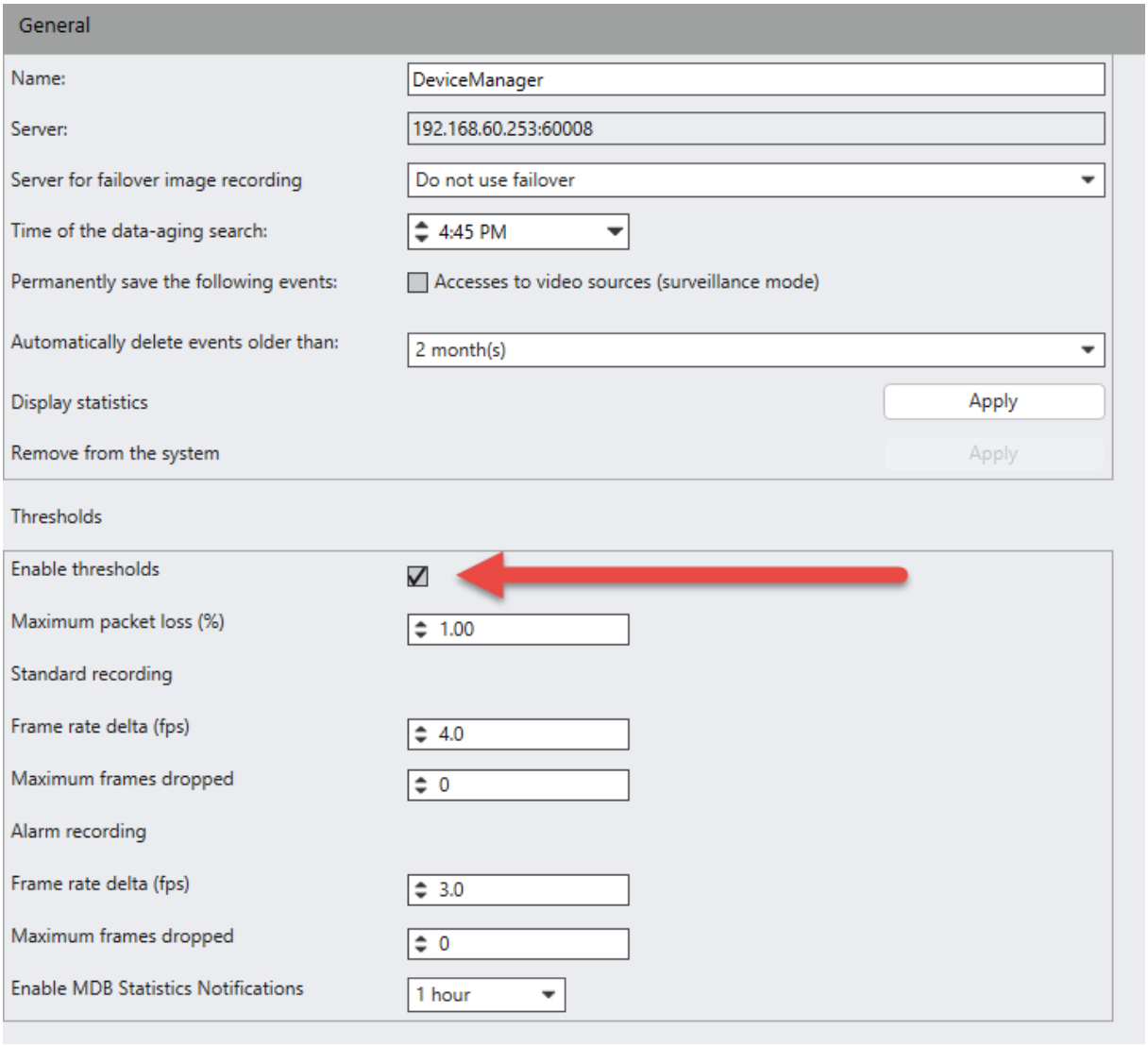
Device Manager Thresholds

To see if the device manager works according to specification, thresholds for certain parameters can be specified. If one of the values is outside the specification, the camera is marked "Limited" in the Device Manager's statistic report and the appropriate values are marked with a colored background.

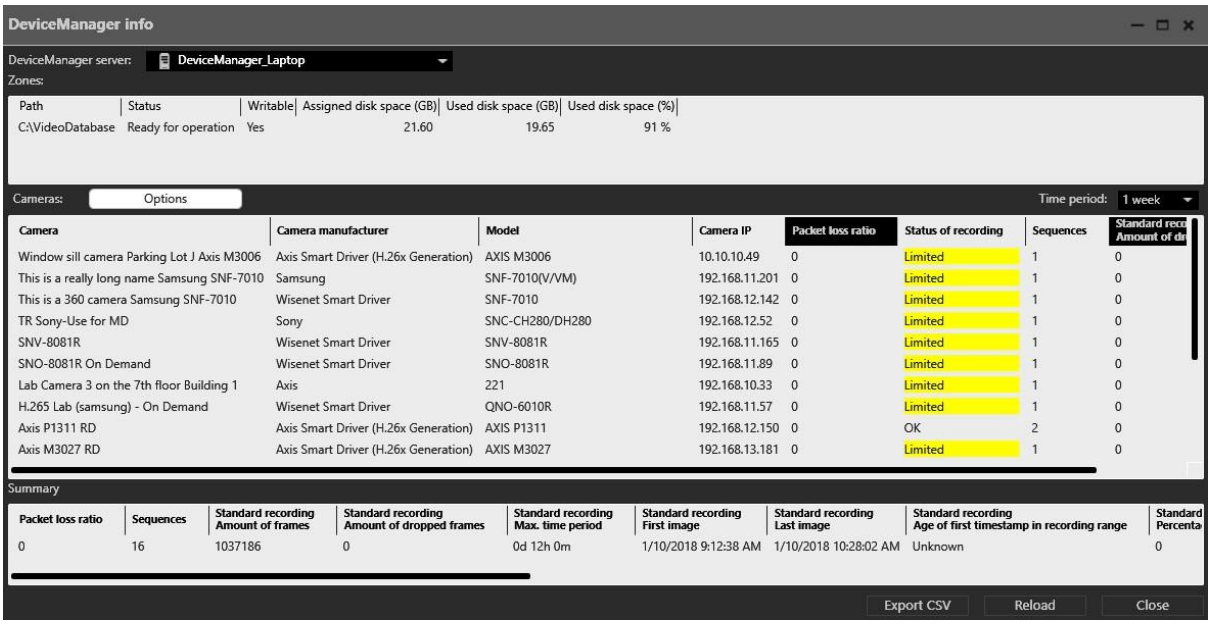
To Set Device Manager Thresholds

1. Under Server -> Device Manager, click the checkbox for **Enable thresholds**.
2. You can set the following thresholds:
   - Maximum packet loss (%)
   - Standard recording - Frame rate delta (fps)
   - Standard recording - Maximum frames dropped
   - Alarm recording - Frame rate delta (fps)
   - Alarm recording - Maximum frames dropped
3. If you want to be notified if certain threshold values are exceeded, select a time adjacent to **Enable MDB Statistics Notifications**. Available options include: **Never**, **1 hour**, **1 day** or **1 week**. Then, during this timeframe, the DM will be evaluated against the threshold parameter settings and if any exceed the threshold, a notification can be sent.

NOTE: The option Threshold values of DM have been exceeded must be activated in the Event Man- ager for this notification to function.



4. You must click **Apply** or **Save** before you can run the report. The settings will remain until changed again.
5. Click the **Apply** button adjacent to 'Display statistics' to run the report.



7.4.2.11 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.

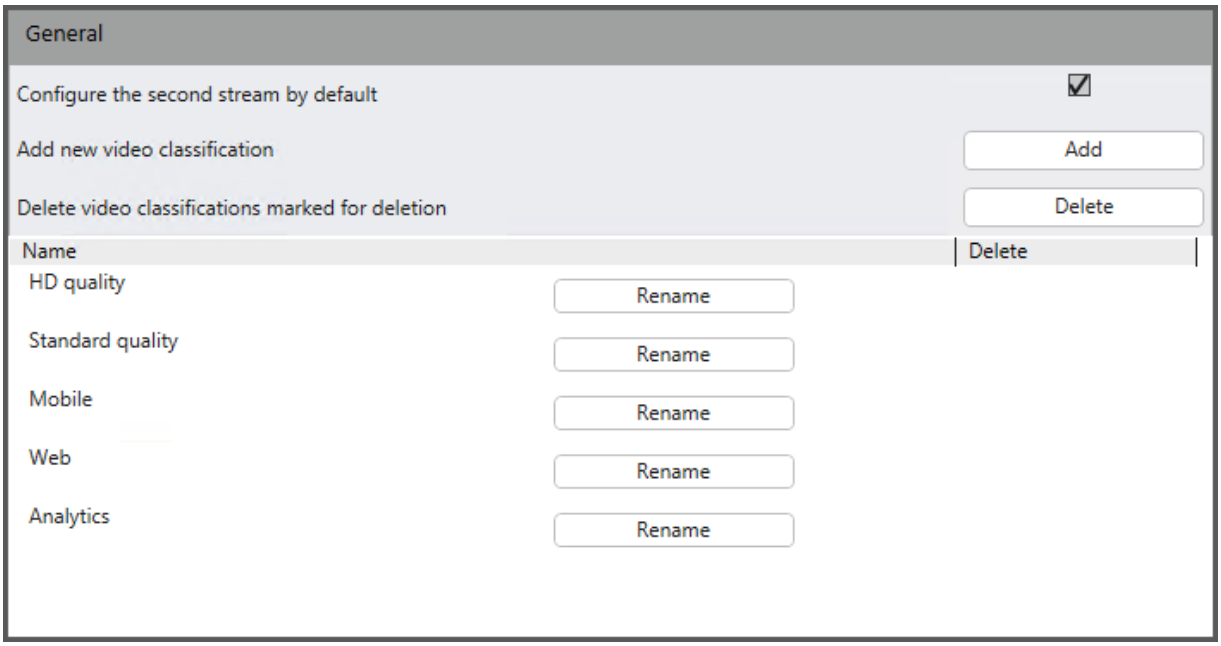
1. Select the main location in the **Company** control.

   The selected location is displayed in the title bar of the Administration control.

2. Select **System** in the Administration control.

Configuring the video classification

Video classifications are labels assigned to a camera's stream. For Ocularis, each stream must be assigned only one video classification. The labels may be modified to suit your installation and additional clas- sifications may be created here. An operator using Ocularis Client or Ocularis Mobile will (given privileges) be able to select a stream by using the video classification label.



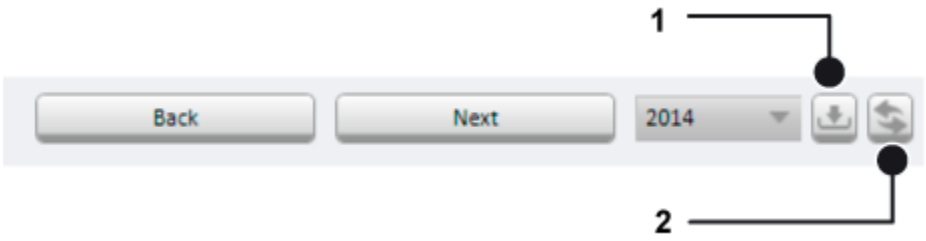
To add or modify Video Classifications

1. By default, every time a new camera is added, two video streams are created. Uncheck the box Configure the second stream by default to disable this feature. For more details, refer to **Creation of Two Video Streams** .
2. Click **Add** adjacent to 'Add new video classification', and then specify the **name** of the video classification.
3. Click **OK** to confirm.

   The new video classification is displayed in the list.
4. Select the video classifications you want to delete, and then click **Delete** adjacent to 'Delete video classifications marked for deletion'. The default video classifications ("HD quality", "Standard quality", "Mobile", "Web", "Analytics") cannot be deleted but they can 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.

Configuring the company calendar

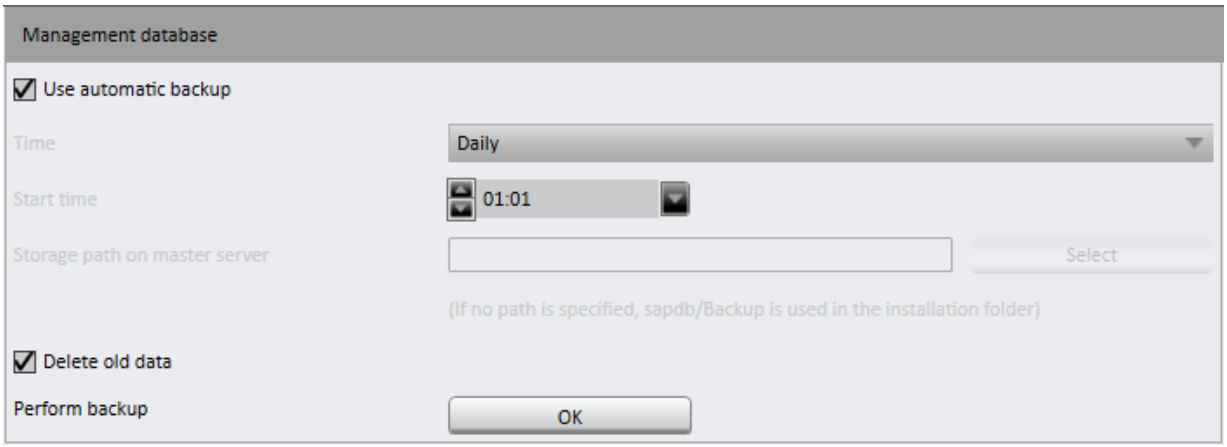
In the company calendar, you specify the days to be handled in time templates separately from normal weekdays (e.g. public holidays or non-working days). Time templates are created in the time management (see **Time management**). They allow the precise specification of recording periods or times in which alarm scenarios are started.



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 the **Jump to the current date** icon (2).
4. Click **Import** to enter the public holidays in the company calendar. The templates for public holiday import are in the Ocularis Recorder installation folder in the "\Client\calendar folder as text files.
5. Select the desired federal states, as appropriate.
6. Activate **Replace holidays** to replace all entered public holidays, and then click **OK**. The imported data is displayed highlighted in blue.
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 backup

The default setting of the automatic backup of the management database is 1:01 a.m. every night. To restore a backup the Ocularis Recorder Administration Tool is required.



1. The **Use automatic backup** checkbox to schedule automatic backups is checked by default. We do not recommend unchecking this box.
2. Select the time and start time of the **backup** if you want to change it from the default time.
3. If necessary, edit the **storage path** for data backup or click the **Select** button to select the folder directly in Windows Explorer. The export folder can only be selected if the client is installed on the CoreService Main server. Otherwise, the storage path to the export folder on the server has to be entered manually. We recommend storing the backup on a different computer than the CoreService Main server.
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. Click the **Perform backup** button to carry out a manual data backup immediately. The backup is started. The backup file is named as follows: **Cayuga_M_20yymmdd.hhmm.zip**, where yy is the year, mm the month, dd the day, hh the hour and mm the minute.

   Example:

   "Cayuga_M_20130725.1145.zip" for a manual backup performed on July 25, 2013, at 11:45 am.
   "Cayuga_A_20130725.1145.zip" for an automatic backup performed on July 25, 2013, at 11:45 am.

6. **Apply** the set values if you want to make further settings.
7. **Save** the set values to apply the values and conclude input.

NOTE: The default location for the backup file is on the local C: drive. (c:\Program Files\Qognify\Ocularis Recorder\sapdb\backup. We recommend changing the location to another drive in case of hard drive failure. (see step 3 above)

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 are stored in the corresponding DeviceManager (see **Configuring the Device Manager (DM)**).

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.

The following procedures are valid for all events:

1. Select the event in the list, and specify:
   - whether the event is to be displayed only in the daily report of the system events
   - whether an email is to be sent to all of the email addresses entered in the email manager as system addresses when the event occurs. The email settings have to be configured (see **Configuring the SNMP server**)
2. To edit one or more events, select it in the **Edit** column and click the **Edit selected objects** button.
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.
4. Click the **Back to overview** button 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.

General

Automatic deletion

1. Select **Use automatic deletion**, and then 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 the **Delete events** button to delete the events in the selected period from the database.

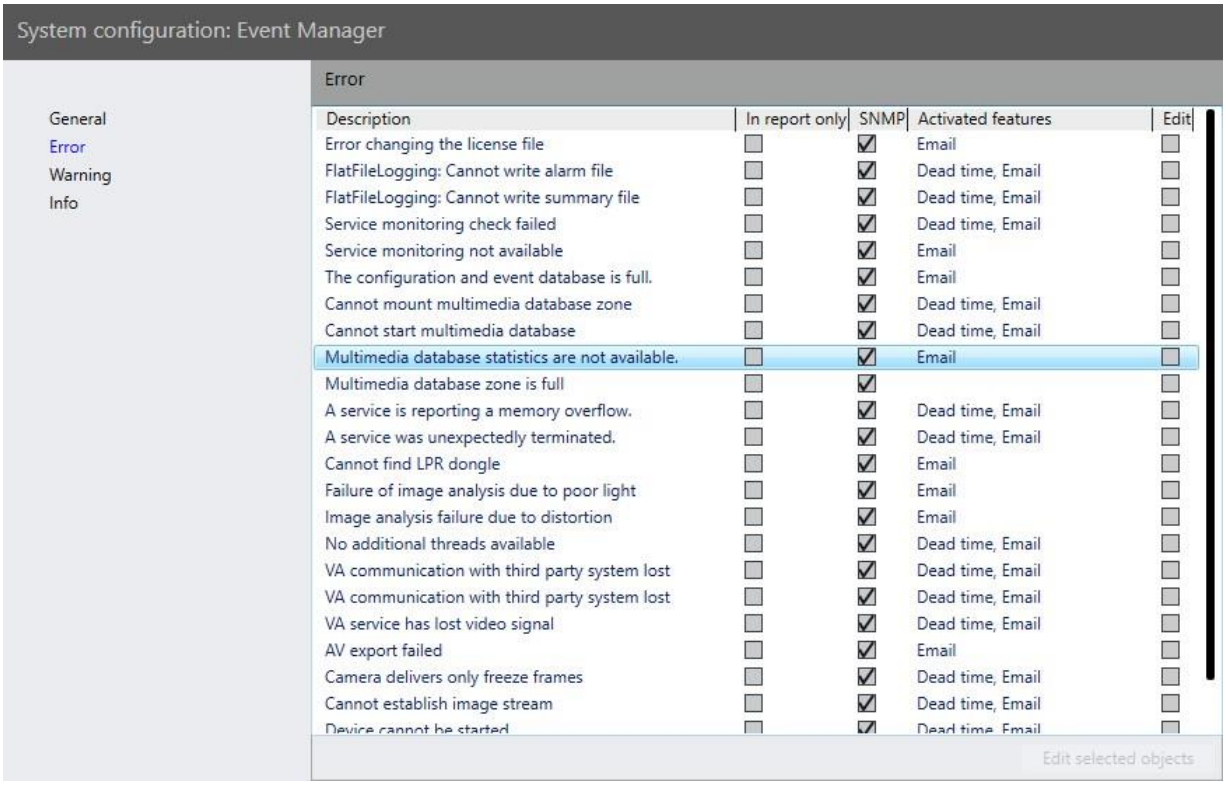
System events

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**), as well as the configuration of email addresses (see **Configuring the Email Manager**).

1. Specify the **time for the 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.

Error

Errors are serious events that impair the operation of the software. Administrative measures are required.



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 CoreService Main (see Flat file logging). 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 CoreService Main (see Flat file logging). 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 **Ocularis Recorder Administration Tool**).
- **Cannot mount multimedia database zone**: Without zone, video data cannot be recorded. Possible reasons can be a wrong server path or missing permissions. The zone settings have to be checked (see **Management database (MaxDB)**).
- **Cannot start multimedia database**: The MDS cannot be started. Possible reasons can be a lack of disc space(zone is full)
- **Multimedia database statistics are not available**: The statistics cannot be generated. Contact technical support.
- **Multimedia database zone is full**: The available storage space has reached 95%. The edge storage deletes the oldest recordings (see **Image storage**
- **A service is reporting a memory overflow**: This concerns the services VMS_Core, VMS_DM, or VMS_MDS.
- **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).
- **Failure of image analysis due to poor light** :This error concerns the video analysis (see Video Analytics). 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 Video Analytics). 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 **Ocularis Recorder VA Administration Tool**).
- **VA service lost video signal**: The VA service requires a reliable video stream, e.g. for motion-based detection. Possible reason 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 **Ocularis Recorder VA Administration Tool**).
- **Camera delivers only freeze frames**: This concerns only M-JPEG streams. Optionally, a H.264 stream might be established. Contact Technical Support.
- **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 logfile for-further information or contact Qognify for support (see Support).

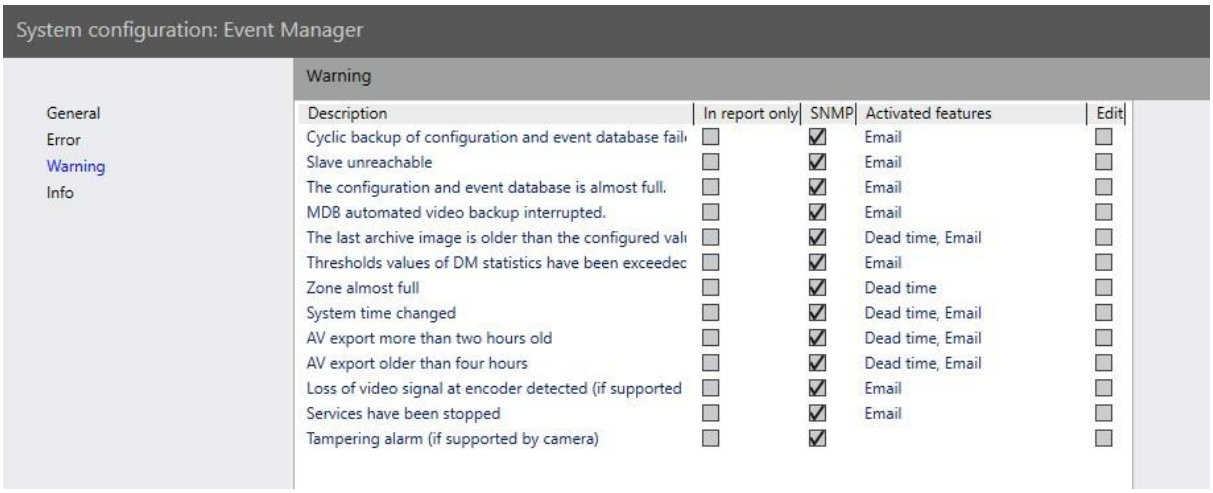
Editing Errors

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.
   - If an SNMP trap is sent to a management host when the event occurs.

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 emails is to be sent
4. Click **Back to overview** to go back to the list of events.
5. Click **Apply** to save the values and continue editing or reviewing.
6. Click **Save** to save the values and close the window.

Warning

Warning are system-relevant events that can affect the function of the whole system or parts of the system. Usually, prompt administrative actions are required.



- **Cyclic backup of configuration and event database failed**: The cyclic backup of the system databases has failed (see **Configuring the backup**).
- **Secondary Core unreachable**: When multiple CoreService servers are installed, the CoreService secondary cannot be reached (see **Relationship between the CoreServices - main and secondary**).
- **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 **Ocularis Recorder Administration Tool**).
- **MDB automated video backup interrupted:** The automatic video data backup was interrupted. (see Video Backup/Export).
- **The last archive image is older than the configured value**: A configuration error has occurred (see **Image storage**).
- **Thresholds values of DM statistics have been exceeded**: If certain thresholds of the Device Manager statistics report have been exceeded, a notification can be sent. See **Device Manager Thresholds** .
- **Zone almost full**: Only 15% of the available video storage space are remaining. The edge storage will delete the oldest recordings when 95% storage space is reached (see **Image storage**).

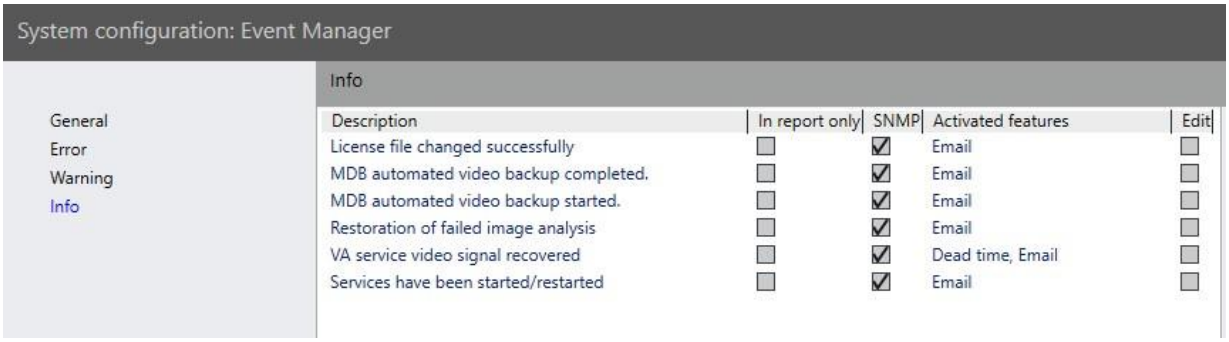
- **System time changed**: The system time change impacts the archive time stamps or the client behavior if they are not synchronous with the CoreService server.
- **AV export more than two hours old**: The configuration at the camera has to be adapted and must be activated in the alarm settings (see **Email and FTP**).
- **AV export older than four hours**: The configuration at the camera has to be adapted and must be activated in the alarm settings (see **Email and FTP**).
- **Loss of video signal at encoder detected**: This feature has to be enabled in the camera configuration (see **Tampering detection - Static Drivers**). Additionally, this event can be used as alarm trigger (see **Configuring an alarm**).
- **Tampering alarm**: This feature has to be enabled in the camera configuration (see **Tampering detection - Static Drivers**). Additionally, this event can be used as alarm trigger (see **Configuring an alarm**).

Editing Warnings

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.
   - If an SNMP trap is sent to a management host when the event occurs.
2. To edit one or more events, select it in the **Edit** column and click **Edit selected objects**.
   - Specify whether an Action is to be performed: to which recipient an email is to be sent
3. Click **Back to overview** to go back to the list of events.
4. Click **Apply** to save the values and continue editing or reviewing.
5. Click **Save** to save the values and close the window.

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.



- **License file changed successfully**: A license file has been successfully registered at the CoreService.
- **MDB automated video backup completed**: The automatic video data export is completed. (see Video Backup/Export)
- **MDB automated video backup started**: The Automatic video data export has started. (see Video Backup/Export)

- **Restoration of failed image analysis**: In some cases, an interrupted calibration of video analytics could be recovered.
- **Va service gain video**: A lost video signal could be reestablished.
- **Services have been started/restarted**: If a recorder service stops (e.g. due to an update), it automatically restarts.

Editing Infos

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.
   - If an SNMP trap is sent to a management host when the event occurs.
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 emails is to be sent
4. Click **Back to overview** to go back to the list of events.
5. Click **Apply** to save the values and continue editing or reviewing.
6. Click **Save** to save the values and close the window.

Configuring the SMTP server

To enable the recorder 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 you 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**). The email addresses are also used to the report (see **Configuring the SNMP server**).

1. Click the **Add new email list** button, and then 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 the **Delete list marked for deletion** button. 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 desiredlist.
2. Click the **Add new email address** button, and then 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 then click the **Delete email addresses marked for deletion** button. 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 > Soft- ware > 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.

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

Ports 60000-60008 are required by default for NAT.

NOTE: These ports have to be open on all distributed servers.

1. Click the Add new NAT entrybutton.
2. Enter the internal and public address.

3. To remove an entry, select list, select **Delete** at the end of each line, and then click the **Delete NAT entries marked for deletion** button.
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 more information on NAT, see the White Paper *Using NAT with Ocularis* from the Qognify website.

8 Administrative Tools

There is a suite of administration tools available to manage the servers, clients and additional modules such as the UpdateService.

- **Ocularis Recorder VA Administration Tool**: The VA Administration tool is used to configure the settings for the core server and installing the "Versatile Application" extension.
- **Ocularis Recorder Administration Tool**: The Administration Tool is used to configure the image database and the administration database of the servers.
- **Ocularis Recorder ServiceManager**: The ServiceManager is used for starting and stopping services.
- **Ocularis Recorder UpdateServer 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 **UpdateServer Configuration Tool**).

8.1 UpdateServer Configuration Tool

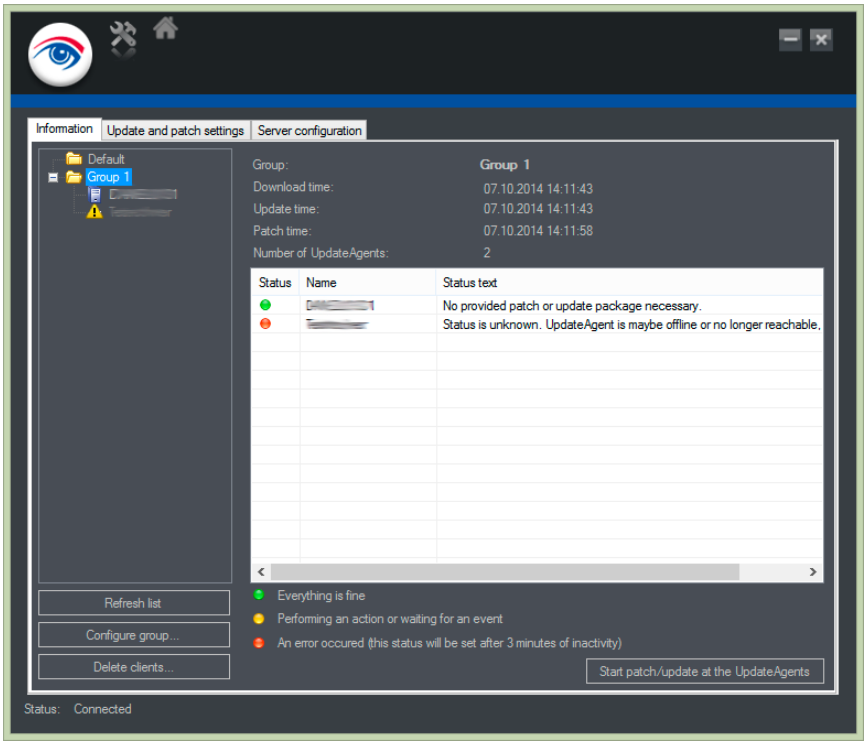
The UpdateServer Configuration Tool manages the configuration of the UpdateService and the connected UpdateAgents (i.e. device managers, cores, etc.). The configuration tool will be installed automatically with the UpdateService.

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**). The UpdateServer 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

1. Start the UpdateServer configuration tool from the Windows All Programs menu. If required, confirm the system's administration privileges. The information tab is displayed.

8.1.1 Configuring the UpdateService



The Groups column displays all groups managed by the UpdateService alphabetically. The default group contains all UpdateAgents (clients) not assigned to a group.

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**).

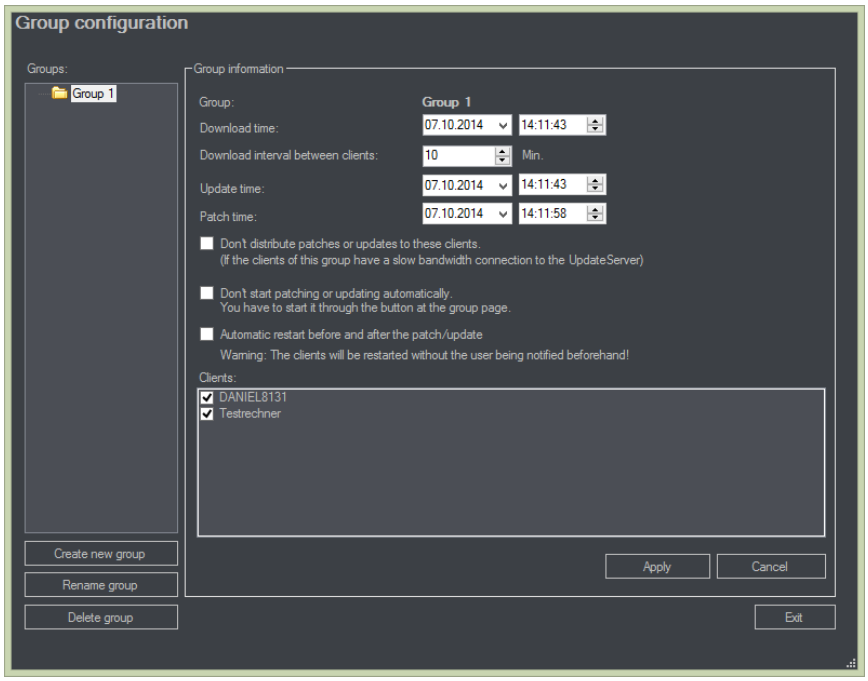
- Click on a group folder icon to display the status overview of all clients within the group. Am colored bullet point shows the current status of each client:
- **Red**: An error occurred at the client or the UpdateAgent of the client is offline for more than 3 minutes.
- **Yellow**: UpdateAgent is 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.
- Click on a client name to display the installed components (e.g. the system software, the software version, the status, and the installed patches).
- Click **Refresh list** to see a more current status.
- Click **Configure group** to create, rename or delete a group and specify the group's update and patch settings (see **Configuring a group**).
- Click **Delete clients** to remove clients that do not connect to the UpdateService anymore. The clients will not be deleted axiomatically.

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.

8.1.1.1 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 for 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

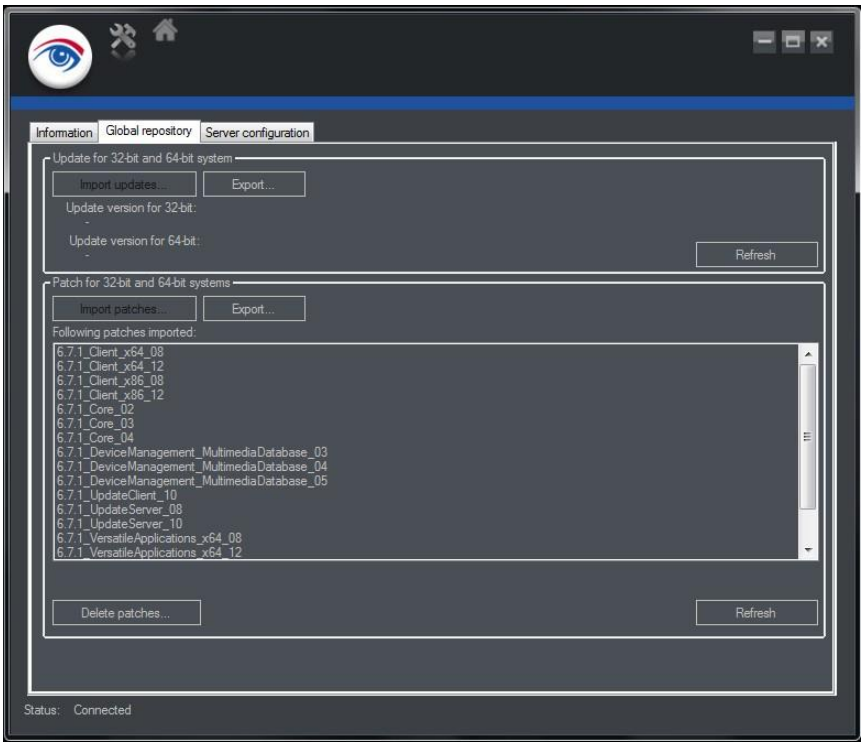
1. Click Rename group.
2. Change the name of the group and click **OK**. All assigned UpdateAgents will remain in the group and adhere to the group's settings.

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.

8.1.1.2 Global repository



The tab displays the available updates and patches. If the UpdateService has been configured for manual distribution in the Server configuration tab (see **Editing the Server configuration**), all updates and patches can be imported from the server and exported to a directory on the server or an attached media.

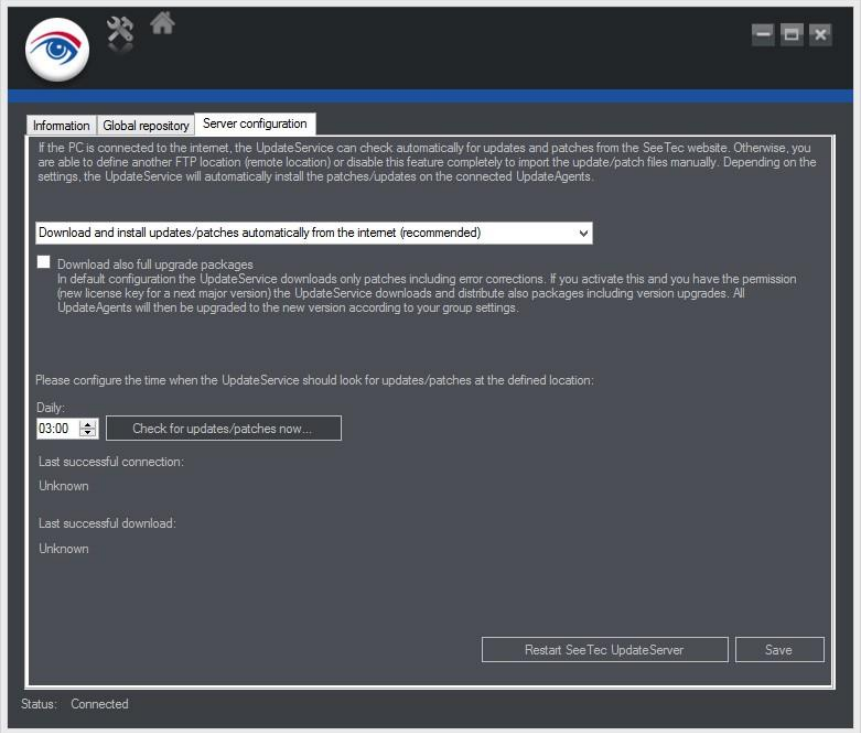
1. Click **Import updates** to download the available updates from a directory that is available in the local network.
2. Click **Refresh** to check at the server for updates not yet displayed.
3. Click **Export** to copy the updates and a " Cayuga.UpdatePatchImport.exe" to a directory that can be copied to any media such as a USB stick.

   The Cayuga.UpdatePatchImport.exe updates and patches can be installed at each client separately (see **Import of updates and patches at the UpdateAgent**).

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 " Cayuga.UpdatePatchImport.exe" to a directory that can be copied to any media such as a USB stick.

   The Cayuga.UpdatePatchImport.exe updates and patches can be installed at each client separately (see **Import of updates and patches at the UpdateAgent**).
6. If patches are not required, select the patches from the list and click **Delete patches** before exporting them. Only the patches listed will be distributed.
7. Click **Refresh** to check at the server for patches not yet displayed.

8.1.1.3 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, down- loads and distributes the updates and patches to the UpdateAgents. However, if manual distribution or a dif- ferent server for downloads is preferred, the automatic setting can be changed.

1. Select an option from the menu:
2. **Download and install updates/patches automatically from the internet**. This is the recommended setting for automatic updates and distribution of patches.
3. **Download updates/patches from the internet, but don't install them automatically**. Updates and patches will be automatically downloaded from the server, but will not be distributed to the UpdateA- gents. The updates and patches must be updated and installed manually (see **Global repository**).
4. **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 auto- matically installed at the UpdateAgents (see **Configuring the FTP server**).

5. **Download and install updates/patches from a defined remote location, but don't install them automatically**. The updates and patches will be downloaded from an FTP server that has to be configured, but will not be distributed to the UpdateAgents. The updates and patches must be updated and installed manually (see **Configuring the FTP server**).
6. **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**).
7. Select **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.)
8. Specify the daytime when updates and patches will be downloaded and installed.
9. Click **Check for updates/patches now** to manually check for available downloads. Currently active downloads are displayed.
10. Click Restart UpdateServer to restart the UpdateServer with the applied settings.
11. 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.)

8.1.1.4 Import of updates and patches at the UpdateAgent

1. After successfully exporting patches or updates (see **Global repository**) copy the directory to an USB stick, and plug it into the computer where the UpdateAgent is running.
2. Start the application "Cayuga.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.

8.2 Ocularis Recorder Administration Tool

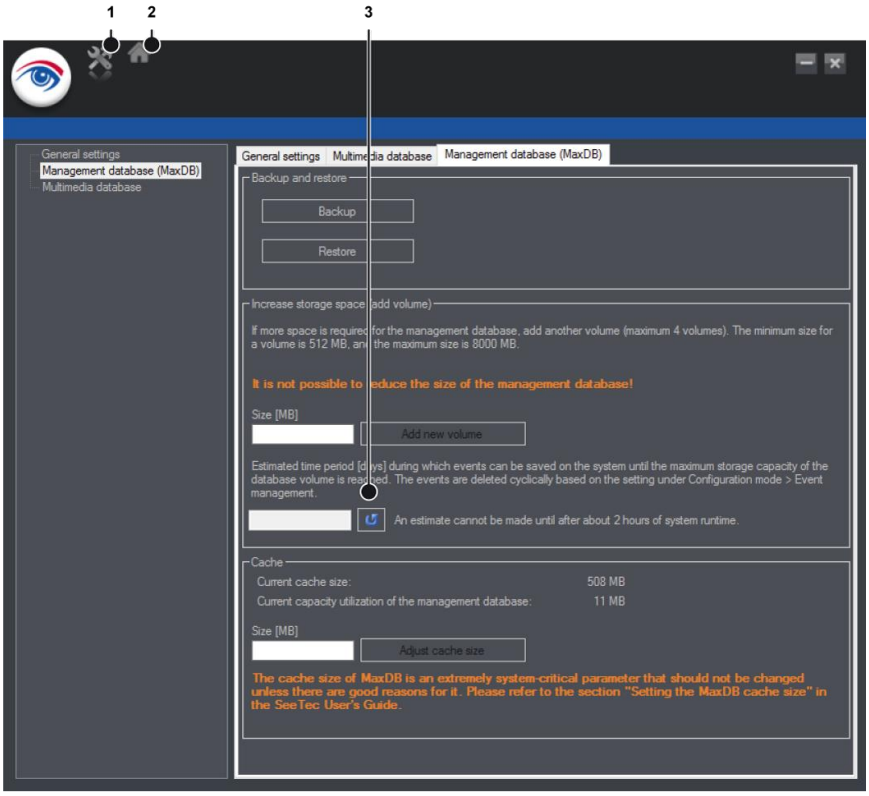
The Ocularis Recorder Administration Tool is used to configure the administration database (MaxDB) and the image database (MDB) of the servers.

Note that incorrect settings in the administration tool may result in a non-operational system.

1. Start the Ocularis Recorder Administration Tool from the Windows All Programs menu.

   All settings in the administration tool are not valid until the services or the complete computer have been restarted.

8.2.1 General settings



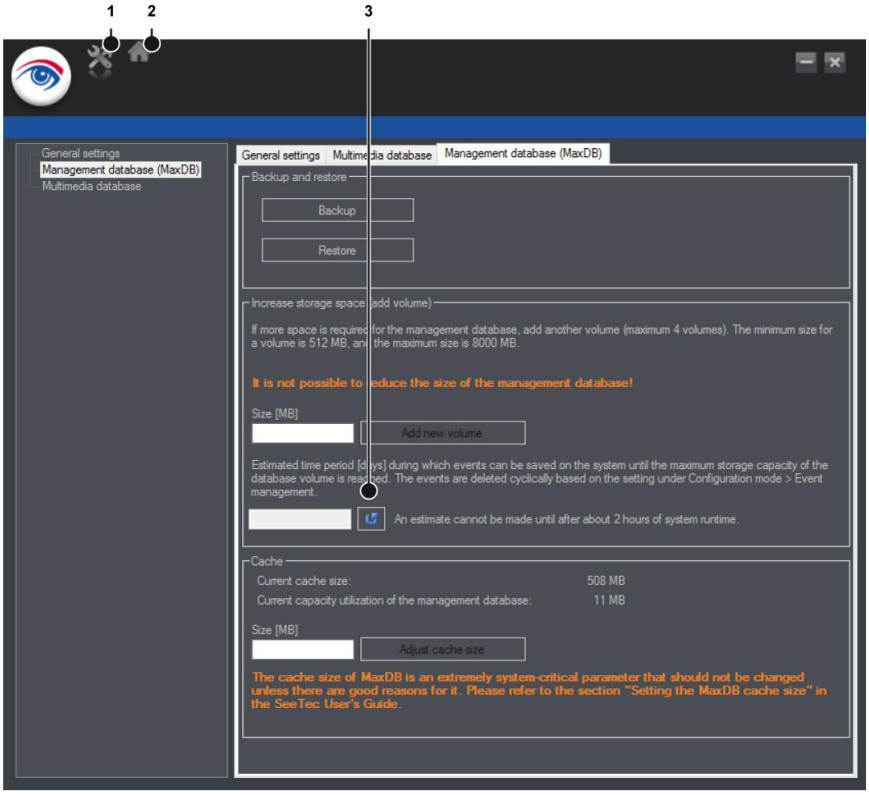
1. Configure the **server** and **port** of the CoreService server if administration was started on a distributed server. If administration was started on the main server, leave these settings unchanged (default: server: localhost, port: (60000).
2. Enter the IP address of the **server** and the **host name** for the services to connect to in the "IP address/host name for server communication" area.
3. Enter the network password.
4. Click the **Settings** (1) icon, and then choose **Save** from the **File** menu to save the changes.
5. Restart the services.

8.2.2 Management database (MaxDB)

8.2.2.1 Backup and restore

1. To create a backup of the management database, click **Backup**. The database is backed up in the "\Qognify\Ocularis Recorder\sapdb\backup" folder.
2. To restore a data backup, click **Restore** and select the required data backup.

8.2.2.2 Increase storage space (add 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 the **Refresh** (3) button 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.

8.2.2.3 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.

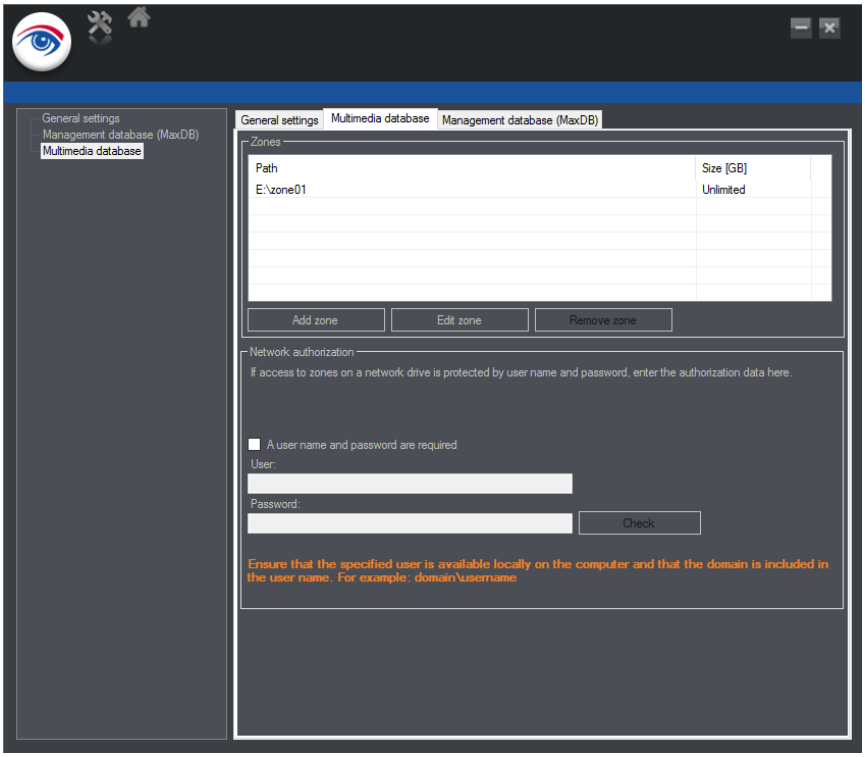
The current cache size of the RAM reserved for the MaxDB is displayed. The actual size of the MaxDB is shown under “Current capacity utilization of the management database”.

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**.

8.2.2.4 Multimedia database

The multimedia database tab is used for maintenance and editing of zones of the multimedia database on the DV. 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.



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: c:\VideoDatabase

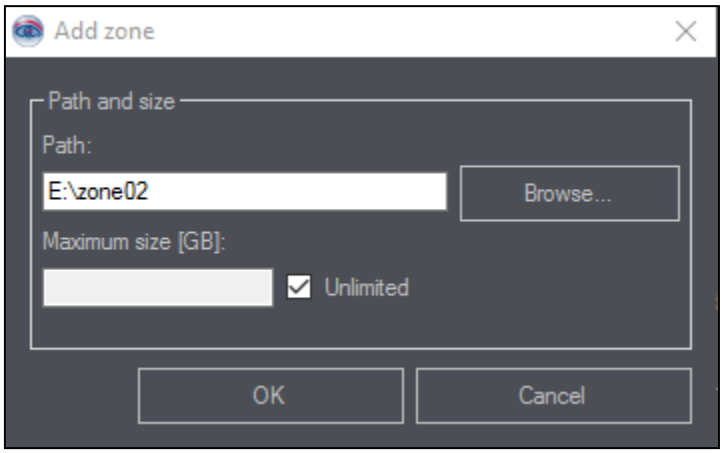
However, we recommend replacing it with a zone on a dedicated partition. Always use a sub-folder and not the root directory of the volume.

If the volume of the existing zone is not sufficient, another zone can be added at any time. A maximum of ten zones should be created. A larger number of zones 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 cam- eras, 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 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. We recommend checking the box for **Unlimited** but you may enter the maximum size for the zone (in GB).
5. Activate **Unlimited** to use all the physical space in the partition. It is recommended to use Unlimited, 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. "Unlimited" is equivalent to "Automatic".
6. Click **OK** to confirm.

Add zone in 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** (i.e. Automatic) 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.

Editing 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 zone

1. Select the desired multimedia database in the zones field.
2. Click **Remove zone**. The image data in the deleted zone is no longer available, but is not automatically deleted.

8.3 Ocularis Recorder Service Manager

The Ocularis Recorder Service Manager is used for starting and stopping services. The following functions are available in the Service Manager:

- Restart all services
- Stop all services
- Start all services

The Service Manager is automatically installed when a server service is installed.

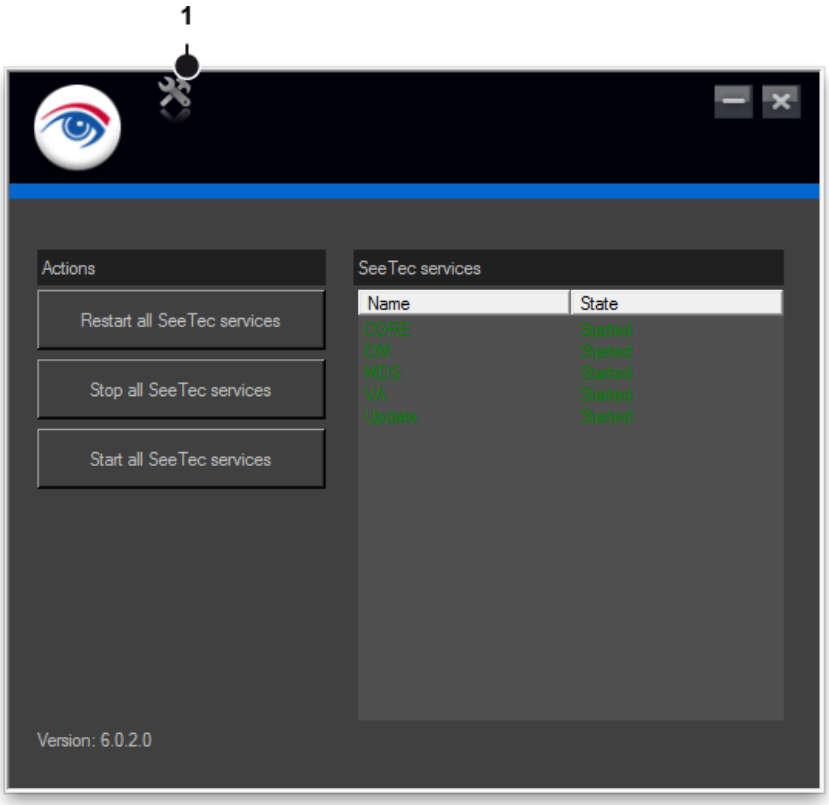
1. Start the Ocularis RecorderService Manager in the installation folder or the Windows Start menu.

8.3.1.1 Switching the display language

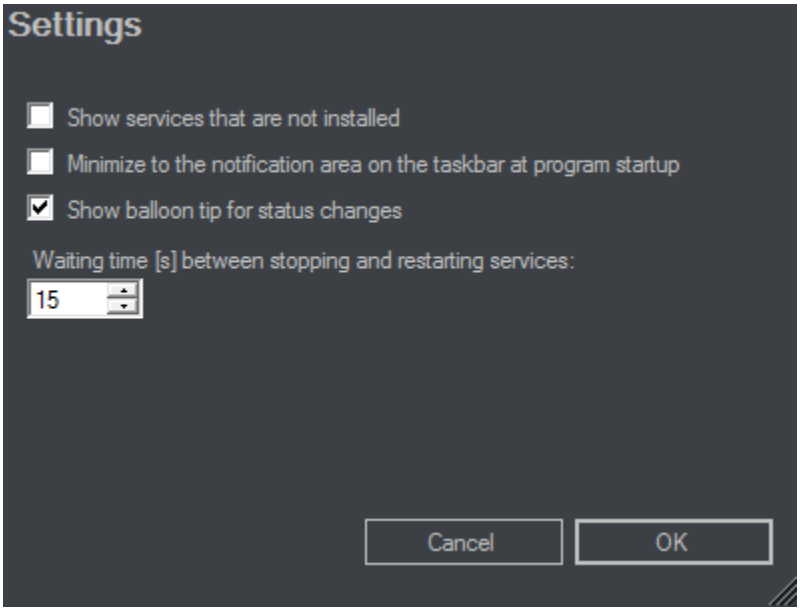
1. Exit the Service Manager.
2. Start the command prompt as the administrator and enter "VMS_ServiceManager.exe -l:<code_for_ the_display_language>".

   Example: For English: "VMS_ServiceManager.exe -l:en-us", or for French: "VMS_ServiceManager.exe -l:fr-fr"
3. Start the Service Manager.

8.3.1.2 Editing the settings



1. Click the **Settings** (1) icon to edit the Service Manager 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.

8.3.1.3 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 after the defined wait time (see Starting and stopping the services).
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.

You can also optionally start, stop or restart specific services by clicking the service with the right mouse button.

8.4 Ocularis Recorder VA Administration Tool

With the Ocularis Recorder VA Administration tool the following modules (services) can be managed:

- Server based Motion Detection

1. Start the Ocularis Recorder VA administration tool from the Windows Start menu.

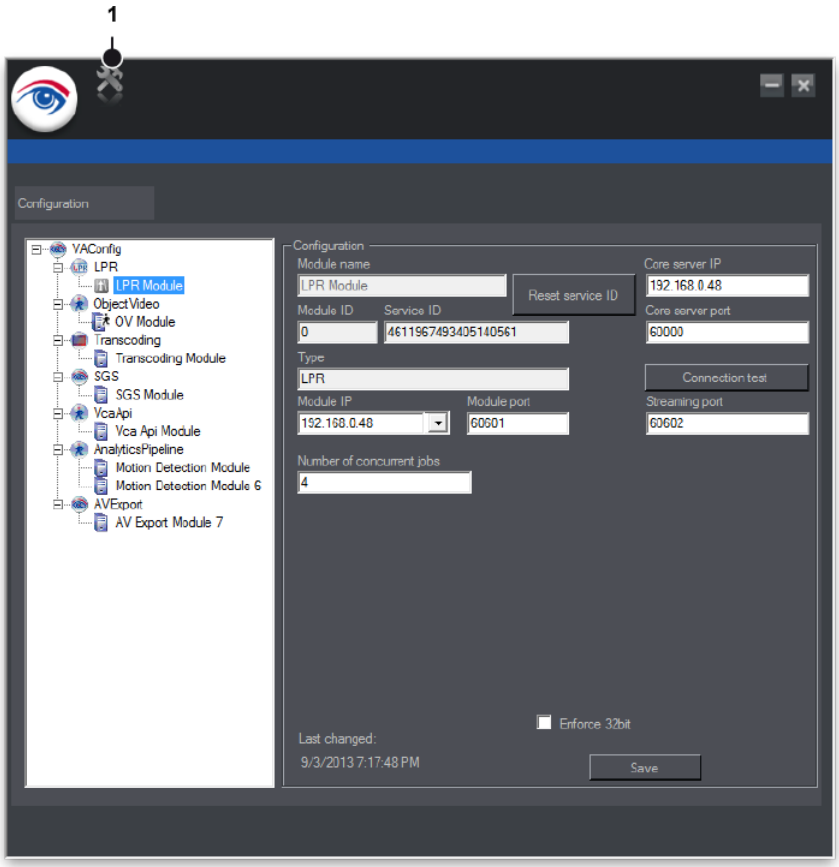
8.4.1 Switching the display language

2. Exit the Ocularis Recorder VA administration tool.
3. Start the command prompt as the administrator and enter "VMS_VA_ConfigurationTool.exe -l:<code_for_the_display_language>".

   Example:

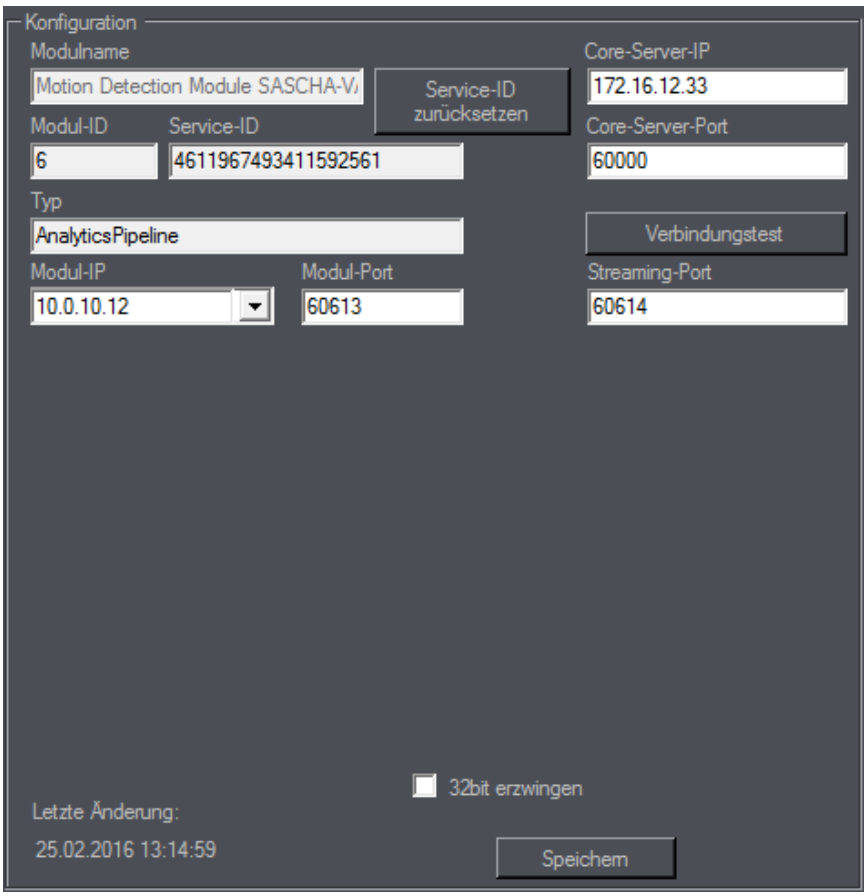
   For English: "VMS_VA_ConfigurationTool.exe" -l:en-gb or "VMS_VA_ConfigurationTool.exe" -l:en-us or for French: "VMS_VA_ConfigurationTool.exe" -l:fr-fr.
4. Start the Ocularis Recorder VA administration tool.

8.4.2 Creating a new configuration file



1. Click the **Settings** (1) icon, and then choose **Create new configuration file** from the **File** menu.

8.4.3 Adding 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**).
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.

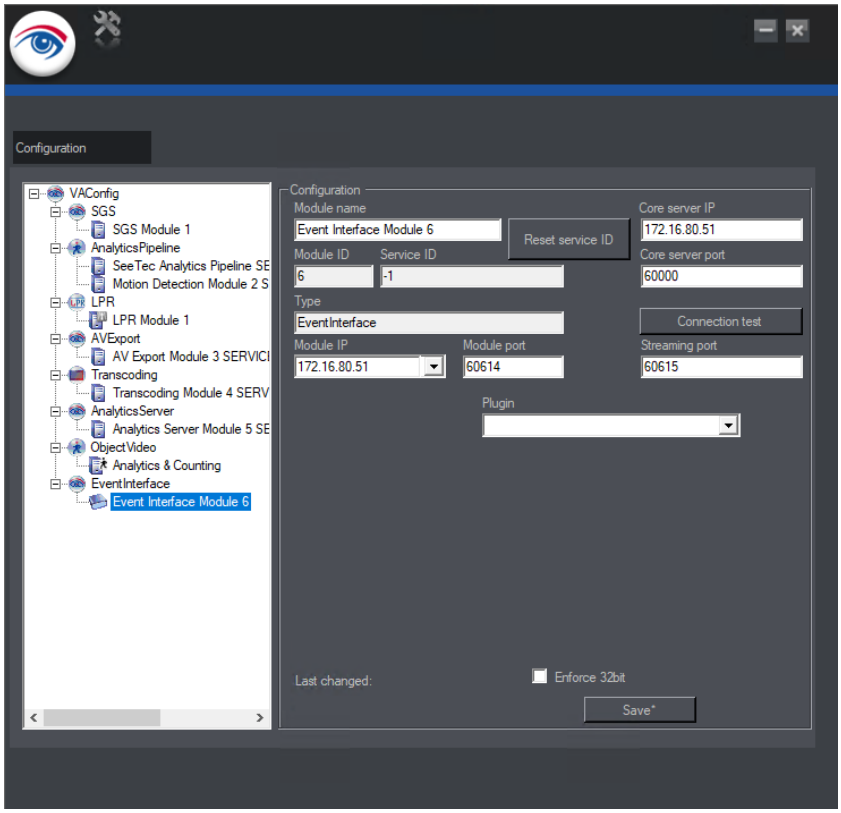
   The service ID changes on the first connection to the Core server. Do not reset the service ID without talking to Qognify Support first.
4. Click the **Connection test** button to check the connection between the module and the main server. If the module does not connect, check and configure the network 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** to save the changes.
9. Restart the services or add further modules.

8.4.4 Adding an Event Interface (SEI) module

The Qognify Event Interface (SEI) 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).



1. Copy the SEI 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,**Error! Bookmark not defined.**).
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.

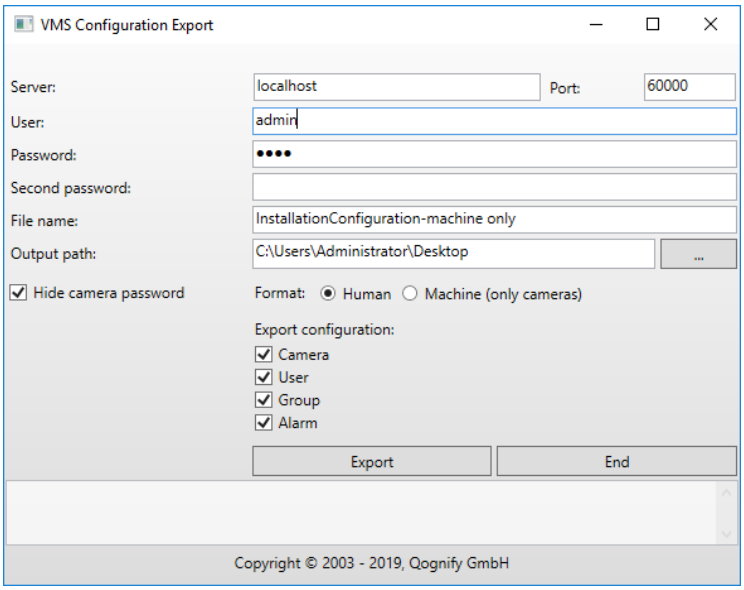
7. Click **Connection test** to check the connection between the module and the main server. If the module does not connect, check and configure the network and the firewall settings.
8. Select the **Module IP**.
9. Enter the **Module port** used by the Qognify Event Interface module.
10. Enter **Streaming port** used by the Qognify Event Interface module.
11. Select the **SEI 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) or add further modules.

8.4.5 Exporting the configuration Settings

After you have configured your system, the configured settings may be exported as an .xlsx file. This file includes camera settings and much more!

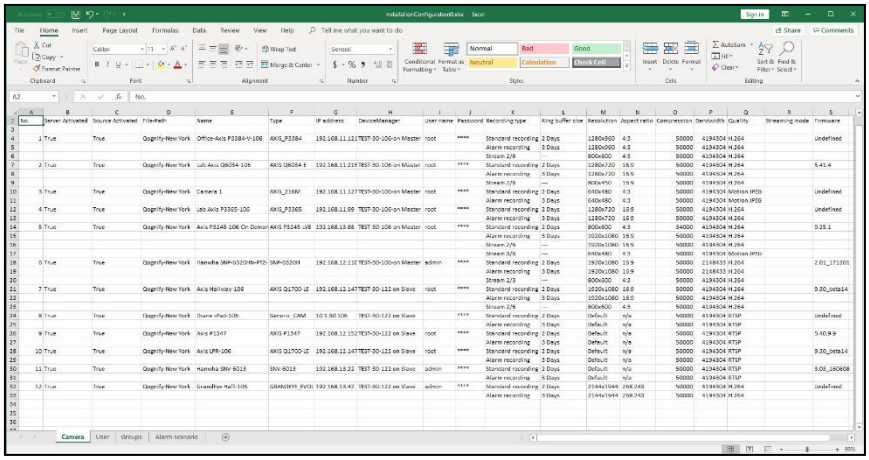
1. **Navigate to:** C:\Program Files\Qognify\Ocularis Recorder\Tools\ConfigurationExport
2. Launch the executable: VMS_ConfigurationExport.exe



3. Enter the IP address of the Main Core **Server** or use 'localhost' if the installation is on the same machine.
4. Enter the **Port** number if different from the default of 60000.
5. Enter the **User** account name for an admin user.
6. Enter the **Password** for the admin account.
7. Enter the desired **Filename** for the exported results.
8. Identify the **Output path** for the file.

9. To prevent camera passwords from being displayed in the report, check **Hide camera password**.
10. For a legible file, select the **Format** of **Human**. To export only camera data, select **Machine**.
11. Choose the items you want to include: Camera, User, Group, Alarm.
12. Click **Export**.
13. When finished, click **End**.

Sample Results



9 Command line parameters

Command line parameters	Meaning
lang:<language>	Change language: The client can be started in a different language with this command line para- meter. The following languages are available: de-de (German), en-us (English), fr-fr (French), ru-ru (Russian), tr-tr (Turkish), nl- nl (Dutch), es-es (Spanish)
pass:<password>	Password
pass2:<password>	Second password (if required)
AutoADLogin	Automatic login by means of Active Directory® login details
host:<IP/hostname>	IP address or name of the core server
port:<port>	Port for login, default: 60000
nat:<true/false>	Login by means of NAT yes (true)/no (false)
user:<user name>	User name
nolayers	Start client without layers
profile:<profile>	Profile (user or group profile)
nosip	Start client with deactivated SIP protocol
camerano:<CameraID>	Open the camera with the specified ID
alarmid:<AlarmEventID>	Open the alarm event with the specified ID
noserverip	If set, the label and the textbox of the login screen are invisible. The "Switch installation" item in the menu is not affected.
profile:<profile>	Profile (user or group profile)

The command line parameters are entered in the form <key>:<value>.

1. Add the required command line parameters to the properties of the client.
2. Right-click the program icon and select **Properties**.
3. Navigate to the **Link** tab, and add the required parameters to the text in the **Destination** text box.
4. Click **OK** to confirm and start the program.