Recording Component (RC-P)

User Manual

On-Net Surveillance Systems, Inc.
One Blue Hill Plaza, 7th Floor, PO Box 1555
Pearl River, NY 10965
Phone: (845) 732-7900 | Fax: (845) 732-7999
Web: www.onssi.com

Legal Notice

This product manual is intended for general information purposes only, and due care has been taken in its preparation.

Any risk arising from the use of this information rests with the recipient, and nothing herein should be construed as constituting any kind of warranty.

On-Net Surveillance Systems, Inc. reserves the right to change product specifications without prior notice.

Table Of Contents

System & Requirements

SYSTEM OVERVIEW

RC-P provides a state-of-the-art IP video surveillance system, supporting the widest choice of network cameras and video encoders, with the equipment connected to an office LAN or other TCP/IP network, such as the internet.

RC-P is the right product for small to mid-sized installations that need robust single-server surveillance software with the full functionality of advanced management, flexible scheduling, fast searching and analysis. RC-P supports up to 64 cameras simultaneously with the widest choice of network video and computer hardware equipment.

Several Targeted Components in One

RC-P consists of a number of components, each targeted at specific tasks and user types:

- The Management Application: The main application used by surveillance system administrators for configuring the RC-P surveillance system server, upon installation or whenever configuration adjustments are required, for example when adding new cameras or users to the system.

- The Recording Server service: A vital part of the surveillance system; video streams are only transferred to RC-P while the Recording Server service is running. The Recording Server service is automatically installed and runs in the background on the RC-P surveillance system server. You can manage the service through the Management Application.

- The Ocularis Client (unlicensed and free): The award winning Ocularis Client lets users view live video, play back recorded video, activate output, print and export evidence, etc.

Updates

On-Net Surveillance Systems, Inc. regularly releases service updates for our products, offering improved functionality and support for new devices. If you are a surveillance system administrator, it is recommended that you check www.onssi.com

MINIMUM SYSTEM REQUIREMENTS

For the most up-to-date *minimum* system requirements on the recording component or on any Ocularis component, see the OnSSI website: www.onssi.com.

OVERVIEW OF LICENSES

When you purchase RC-P, you also purchase a certain number of licenses for device channels. Device channels are typically cameras but could also be dedicated input/output boxes.

When you have installed the various RC-P components, configured the system, and added recording servers and cameras through the Management Application, the surveillance system initially runs on temporary licenses that need to be activated before a certain period ends. This is called the grace period.

If grace periods have expired on one or more of your devices **and** no licenses have been activated, recording servers and cameras will not send data to the surveillance system. We therefore recommend that you activate your licenses before you make final adjustments to your system and its devices.

Tip: When short of licenses—until you get additional ones—you can disable some less important cameras to allow some of the new cameras to run instead. To disable or enable a camera, expand Hardware Devices in the Management Application's navigation pane. Select the required hardware device, right-click the relevant camera, and then select Enable or Disable.

- **Which Devices Require a License?**

  You need licenses for the number of device channels—typically cameras or dedicated input/out boxes—you want to run on your RC-P system. One device channel license enables you to run one camera or one dedicated input/output box. You can use and define an unlimited number of microphones, inputs, and outputs.

  Depending on your current number of licenses you might be able to get more licenses as your surveillance system grows. See *Getting Additional Licenses* in the following.

- **Replacing Cameras**

  You can replace a camera licensed in the RC-P system with a new camera and have the new camera activated and licensed instead.

  The total number of purchased device channels corresponds to the total number of cameras able to run on the surveillance system simultaneously. If you remove a camera from a recording server, you also free a license.

  When replacing a camera, you must use the Management Application's *Replace Hardware Device wizard* to map all relevant databases of cameras, microphones, inputs, outputs, etc. When done, remember to activate the license.

- **Viewing Your License Information**

  You get an excellent overview of your RC-P licenses from the Management Application's navigation pane. Expand *Advanced Configuration* and select *Hardware Devices.* This presents you with the *Hardware Device Summary* table:

  - **Hardware Device Name:** Hardware devices (typically cameras but could also be dedicated input/output boxes).
  - **License:** Licensing status of your hardware devices. Can be either *Licensed*, *[number of] day(s) grace, Trial,* or *Expired*.
  - **Video Channels:** Number of available video channels on your hardware devices.
  - **Licensed Channels:** Number of video channels—on each of your hardware devices—for which you have a license.
  - **Microphone Channels:** Number of available microphone channels on your hardware devices.
  - **Address:** http addresses of your hardware devices.
  - **WWW:** Links to http addresses of your hardware devices.
  - **Port:** Port used by your hardware devices.
  - **Device Driver:** Names of device drivers associated with your hardware devices.

  You can activate licenses online or offline. On the Management Application's toolbar*,* click *File* and either *Activate License Online* or *Manage License Offline.*

- **Getting Additional Licenses**
  Want to add—or have already added—more device channels than you currently have licenses for? In that case, you must buy additional licenses before the cameras will be able to send data to your RC-P system.

  To get additional licenses for your RC-P system, contact your integrator or dealer.

When your license file (.lic) is updated, you can activate your licenses. See Activate Licenses for more information on activating.

ADMINISTRATOR RIGHTS

When you install RC-P, it is important that you have administrator rights on the computer that should run RC-P. If you only have standard user rights, you will not be able to configure the surveillance system.

PRIVACY OPTION SETTINGS

To help OnSSI improve the usability and customer experience of using recording components, you were presented with the option to *Sign me up for the Customer Experience Improvement Program* during the installation of the recording component.

- If you **declined**, **no software** contributing statistical information is included in your software installation.
- If you **accepted**, a cookie issuing a Global Unique IDentifier (GUID) is included as part of the software installation. As a result, the recording component anonymously collects relevant information about your installation and operation of the recording component at regular intervals. See the following for a detailed list of what data is being collected.

Furthermore, if you accepted, a setting makes it possible to turn the collection of information off or on as needed (see the following for details).

How Do I Disable Information Collection?

1. In the Management Application's toolbar, click *Help*, *Privacy Options*.
2. On the *Privacy options* tab, clear the *Yes, I would like to improve RC-X information collection* check box.
3. Click *OK.*

- **What Information Is Collected from RC-P?**
    - No personal information about the equipment (PC) RC-P is installed on, or about any of the recordings you make.
    - The country where the software is installed
    - Hardware platform information such as Operating System version, Microsoft .NET framework version, CPU type, and memory size
    - RC-P version information
    - Information about the number, and type of hardware devices (cameras) used with RC-P
    - Information on which RC-P features are used, and how often they are used
    - Information about which RC-P menus and buttons are activated, and how often they are used
    - Execution time for specific operations in your RC-P installation
    - Error reports and exceptions generated by your RC-P installation.
- **When Is Information Collected from RC-P?**

  Information is only collected when the Management Application is active.

The automatic collection of information can be disabled by either removing RC-P or by disabling it using the Management Application (see earlier for details on how).

- **How Does OnSSI Protect Collected Information?**

OnSSI is committed to protecting the security of the information collected from RC-P installations. OnSSI has implemented security measures to help protect against the loss and misuse of data being collected.

The information is stored in a secure server environment that uses firewall and other advanced technologies to prevent interference or unauthorized access from outside intruders.

IMPORTANT PORT NUMBERS

RC-P uses particular ports when communicating with other computers, cameras, etc.

What is a port? *A port is a logical endpoint for data traffic. Networks use different ports for different types of data traffic. Therefore it is sometimes, but not always, necessary to specify which port to use for particular data communication. Most ports are used automatically based on the types of data included in the communication. On TCP/IP networks, port numbers range from 0 to 65536, but only ports 0 to 1024 are reserved for particular purposes. For example, port 80 is used for HTTP traffic when viewing web pages.*

When using RC-P, make sure that the following ports are open for data traffic on your network:

- **Port 20 and 21 (inbound and outbound):** Used for FTP traffic. FTP (File Transfer Protocol) is a standard for exchanging files across networks. FTP uses the TCP/IP standards for data transfer, and is often used for uploading or downloading files to and from servers.

- **Port 25 (inbound and outbound):** Used for SMTP traffic. SMTP (Simple Mail Transfer Protocol) is a standard for sending e-mail messages between servers. This port should be open since, depending on configuration, some cameras may send images to the surveillance system server via e-mail.

- **Port 80 (inbound and outbound):** Used for HTTP traffic between the surveillance server and cameras, Ocularis Client, and the default communication port for the surveillance system's Image Server service. HTTP (HyperText Transfer Protocol) is a standard for exchanging files across networks; widely used for formatting and transmission of data on the world wide web.

- **Port 554 (inbound and outbound):** Used for RSTP traffic in connection with H.264 video streaming.

- **Port 1024 and above (outbound only):** Used for HTTP traffic between cameras and the surveillance server.

- **Port 1234 (inbound and outbound):** Used for event handling.

- Any other port numbers you may have selected to use, for example if you have changed the server access

VIRUS SCANNING INFORMATION

Virus scanning on the RC-P server, and computers to which data is archived, should if possible be avoided:

- If you are using virus scanning software on the RC-P server, or on a computer to which data is archived, it is likely that the virus scanning will use a considerable amount of system resources on scanning all the data which is being archived. This may affect system performance negatively. Also, virus scanning software may temporarily lock each file it scans, which may further impact system performance negatively.

- Similarly, virus scanning software on the RC-P server is likely to use a considerable amount of system resources on scanning data used by the Download Manager.

If allowed in your organization, you should therefore disable any virus scanning of affected areas (such as camera databases, etc.) on the RC-P server as well as on any archiving destinations.

TIME SERVER RECOMMENDED

All images are time-stamped by RC-P upon reception, but since cameras are separate units which may have separate timing devices, power supplies, etc., camera time and RC-P system time may not correspond fully, and this may occasionally lead to confusion.

If supported by your cameras, we thus recommend you auto-synchronize camera and system time through a time server for consistent synchronization.

For information about configuring a time server searching www.microsoft.com for *time server*, *time service*, or similar.

Installation

Install Recording Component Software

Do not install RC-P on a mounted drive (that is a drive attached to an empty folder on an NTFS (NT File System) volume, with a label or name instead of a drive letter). If using mounted drives, critical system features may not work as intended; you will, for example, not receive any warnings if the system runs out of disk space.

Prerequisites: Shut down any existing surveillance software. If upgrading, read Upgrade from a Previous Version first.

1. Follow the installation prompts from the Ocularis installation page. Click the Recording Component and select *New* or *Upgrade*.

   Alternatively, you may run the .exe installation file from the location you have saved it to.

   Depending on your security settings, you may receive one or more security warnings (such as *Do you want to run or save this file?*, *Do you want to run this software?* or similar). When this is the case, click the *Run* button.

2. When the installation wizard starts, select the language for the installer and click *Continue*.

3. When asked, it is important that you:

   - Select installation language.
   - Specify the location of your license file.
   - Read and accept the license agreement.
   - Indicate if you wish to participate in the OnSSI data collection program.
   - Select *Typical* installation (advanced users may select *Custom* installation, and choose application language, which features to install and where to install them).

4. Let the installation wizard complete.

IMPORTANT: If you are installing on a Windows Server 2003 and installation fails, installing a Microsoft hotfix might solve the issue and allow you to complete your RC-P installation.

The Microsoft hotfix is downloadable here:
http://www.microsoft.com/downloads/en/details.aspx?FamilyId=8EFFE1D9-7224-4586-BE2B-42C9AE5B9071&displaylang=en

When you have installed the hotfix, restart the RC-P installation.
If the problem continues, please contact your system provider for help.

You can now begin configuring your RC-P through its Management Application: Double-click the Management Application desktop shortcut or select *Start* > *All Programs* >OnSSI > *Management Application*. See more under Get Your System Up & Running.

Upgrade from a Previous Version

Upgrading your entire RC-P system configuration is a fairly easy task.

- **Back Up Your Current Configuration**

  When you install the new version of RC-P , it will inherit the configuration from your old version.

  However, we recommend that you make regular backups of your server configuration as a disaster recovery measure. Upgrading your server is no exception. While it is rare to lose your configuration (cameras, schedules, views, etc), it *can* happen under unfortunate circumstances. Luckily, it takes only a minute to back up your existing configuration:

  1. Create a folder called *Backup* on a network drive, or on removable media.

  2. On the recorder machine, navigate to the recorder installation folder.

  3. Copy the following files and folders into your *Backup* folder:

     - All configuration (.ini) files
     - All scheduling (.sch) files
     - The file *users.txt* (only present in a few installations)
     - Folders with a name ending in *...ViewGroups*

  Note that some of the files/folders may not exist if upgrading from old software versions.

- **Remove the Current Version**

  In most cases, you do not need to manually remove the old version of old recorder before you install the new version. The old version is removed when you install the new version. In fact, manual removal of some versions may cause problems. Please refer to the *Upgrading to Ocularis Guide* for more specific information.

- **Install the New Version**

  Run the installation file for the new software version. Select the installation options that best fit your needs.

- **Restore a Configuration Backup (if Required)**

  If for some reason, after installing the new software version, you have lost your configuration, you can restore your configuration, provided you have followed the previous instructions.

  If for some reason after installing the new software version you have lost your configuration, you can easily restore your configuration, provided you have followed the previous instructions in this chapter.

  1. Close the *Management Application* if it is open.

  2. Stop the Recording Server Service.

  3. Make a copy of the contents of the following directory (RC-P is used in this example):

  C:\ProgramData\OnSSI\RC-P

  Note: on Windows 2003 Server, the location is: C:\Documents and Settings\All Users\Application Data\OnSSI.

  These directories may be hidden from view. If you cannot see the folder, be sure to modify folder options to display hidden files and folders.

4. Delete the contents of the folder:

   C:\ProgramData\OnSSI\RC-P

   Do not delete the folder.

5. Make sure the RC-P installation folder contains a folder named ConfigurationBackup, and that the folder contains the .ini and .sch files from your old configuration. If not, create the folder, and copy your backed-up configuration files into the folder.

6. In Windows' *Start* menu, select *Run…*

7. Type *cmd* and click *OK*.

8. Change directories to: C:\Program Files\Onssi\ProSight

9. In the command line window, type the following TWICE:

10. `Configurationupgrader.exe C:\ProgramData\OnSSI\RC-P`   Press [ENTER]
11. `Configurationupgrader.exe C:\ProgramData\OnSSI\RC-P`   Press [ENTER]

    This should copy the necessary older configuration files as well as create a configuration.xml to the C:\ProgramData\OnSSI\RC-P directory. It may take a few moments for the configuration.xml file to appear.

10. Close the command line window.

11. Open the Management Application again.

Tip: Once the configuration has been converted, your entire configuration will be contained in a single file. When you later want to back up your configuration, you can simply make a copy of the file configuration.xml.

Upgrade Video Device Drivers

Video device drivers are used for controlling/communicating with the hardware devices connected to an RC-P system.

Video device drivers are installed automatically during the installation of your RC-P system. However, new versions of the video device drivers—called Device Packs—are released and made available for free on the OnSSI website from time to time.

We therefore recommend that you visit the OnSSI website and download the latest Device Pack.

When updating video device drivers, there is no need to remove the old video device drivers first; simply install the latest version on top of any old version you may have. For detailed information, see Update Video Device Drivers.

Getting Started

GET YOUR SYSTEM UP & RUNNING

The following outlines the tasks typically involved in setting up a working RC-P system. Note that although information is presented as a checklist, a completed list does not in itself guarantee that the system will match the exact needs of your organization. To make the system match the needs of your organization, it is highly recommended that you monitor and adjust the system once it is running.

For example, it is often a very good idea to spend time on testing and adjusting the motion detection sensitivity settings for individual cameras under different physical conditions (day/night, windy/calm, etc.) once the system is running. The setup of events and associated actions typically also depends entirely on your organization's needs.

Install Ocularis Base

The first step for installation, is to install Ocularis Base. See the *Ocularis Installation and Licensing Guide* available in the installation package/DVD or from www.onssi.com.

License Ocularis

Use the *Ocularis Licensing Activation* application to license Ocularis. See the *Ocularis Installation and Licensing Guide* available in the installation package/DVD or from www.onssi.com.

Verify Initial Configuration of Cameras and other Hardware Devices

Before doing anything on RC-P, make sure the hardware devices (cameras, video encoders, etc.) you are going to use are correctly installed and configured with IP addresses, passwords, etc. as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the network and RC-P.

Register Your RC-P Software

You must first register your software and next activate your licenses. See Manage Licenses.

Install RC-P

See Install Surveillance Server Software. If upgrading an existing version of RC-P, see Upgrade from a Previous Version.

Open the Management Application

See Access the Management Application.

Add Hardware Devices in RC-P

RC-P can quickly scan your network for relevant hardware devices (cameras, video encoders, etc.), and add them to your system. See Add Hardware Devices.

Configure Cameras in RC-P

You can specify a wide variety of settings for each camera connected to your RC-P system. Settings include video format, resolution, motion detection sensitivity, where to store and archive recordings, any PTZ (Pan/Tilt/Zoom) preset positions, association with microphones, etc. See Configure Video & Recording Settings.

Configure Events, Input & Output

If required, system events, for example based on input from sensors, etc., can be used for automatically triggering actions in RC-P. Examples of actions: starting or stopping recording on cameras, switching to a particular video frame rate, making PTZ cameras move to specific preset positions. Events can also be used for activating hardware output, such as lights or sirens. See Overview of Events, Input & Output.

Configure Scheduling

When do you want to archive? Do you want some cameras to transfer video to RC-P at all times, and other cameras to transfer video only within specific periods of time, or when specific events occur?

With the scheduling feature, you can specify this as well as when you want to receive notifications from the system.

Configure Users

Specify one user with full access rights who should be able to access the recording component. This is the user account which will be used to communicate with Ocularis. You may also enable password protection for the Management Application.

Configure Ocularis Base

Next, configure Ocularis Base to be able to recognize this recording component. It is in the Ocularis Base where the configuration of users, groups, views, alerts, maps and video walls takes place. . Launch the *Ocularis Administrator* application to configure Ocularis Base. See the *Ocularis Administrator's User Manual* for more details.

The above list represents the configuration steps that most administrators are likely to cover.

Note that the behavior of the Management Application can be customized. Descriptions in this help documentation are, however, always based on the Management Application's default behavior.

ACCESS THE MANAGEMENT APPLICATION

Access the Management Application by double-clicking the *Management Application* desktop shortcut.

Alternatively, use Windows' *Start* menu: *Start > All Programs > OnSSI > Management Application*.

OVERVIEW OF LICENSES

When you purchase RC-P, you also purchase a certain number of licenses for device channels. Device channels are typically cameras but could also be dedicated input/output boxes.

When you have installed the various RC-P components, configured the system, and added recording servers and cameras through the Management Application, the surveillance system initially runs on temporary licenses that need to be activated before a certain period ends. This is called the grace period.

If grace periods have expired on one or more of your devices **and** no licenses have been activated, recording servers and cameras will not send data to the surveillance system. We therefore recommend that you activate your licenses before you make final adjustments to your system and its devices.

> Tip: When short of licenses—until you get additional ones—you can disable some less important cameras to allow some of the new cameras to run instead. To disable or enable a camera, expand Hardware Devices in the Management Application's navigation pane. Select the required hardware device, right-click the relevant camera, and then select Enable or Disable.

- ### Which Devices Require a License?

  You need licenses for the number of device channels—typically cameras or dedicated input/out boxes—you want to run on your RC-P system. One device channel license enables you to run one camera or one dedicated input/output box. You can use and define an unlimited number of microphones, inputs, and outputs.

  Depending on your current number of licenses you might be able to get more licenses as your surveillance system grows. See *Getting Additional Licenses* in the following.

- ### Replacing Cameras

  You can replace a camera licensed in the RC-P system with a new camera and have the new camera activated and licensed instead.

  The total number of purchased device channels corresponds to the total number of cameras able to run on the surveillance system simultaneously. If you remove a camera from a recording server, you also free a license.

When replacing a camera, you must use the Management Application's *Replace Hardware Device wizard* to map all relevant databases of cameras, microphones, inputs, outputs, etc. When done, remember to activate the license.

- **Viewing Your License Information**

  You get an excellent overview of your RC-P licenses from the Management Application's navigation pane. Expand *Advanced Configuration* and select *Hardware Devices.* This presents you with the *Hardware Device Summary* table:

  - **Hardware Device Name:** Hardware devices (typically cameras but could also be dedicated input/output boxes).
  - **License:** Licensing status of your hardware devices. Can be either *Licensed*, *[number of] day(s) grace, Trial,* or *Expired*.
  - **Video Channels:** Number of available video channels on your hardware devices.
  - **Licensed Channels:** Number of video channels—on each of your hardware devices—for which you have a license.
  - **Microphone Channels:** Number of available microphone channels on your hardware devices.
  - **Address:** http addresses of your hardware devices.
  - **WWW:** Links to http addresses of your hardware devices.
  - **Port:** Port used by your hardware devices.
  - **Device Driver:** Names of device drivers associated with your hardware devices.

  You can activate licenses online or offline. On the Management Application's toolbar*,* click *File* and either *Activate License Online* or *Manage License Offline.*

- **Getting Additional Licenses**

  Want to add—or have already added—more device channels than you currently have licenses for? In that case, you must buy additional licenses before the cameras will be able to send data to your RC-P system.

  To get additional licenses for your RC-P system, contact your integrator or dealer.

  When your license file (.lic) is updated, you can activate your licenses. See Activate Licenses for more information on activating.

USE THE BUILT-IN HELP SYSTEM

To use the built-in help system, simply click the *Help* button in the Management Application's toolbar. Alternatively, press the F1 key on your keyboard while using RC-P.

The help system opens in a separate window, allowing you to easily switch between help and RC-P itself. The help system in is context-sensitive. This means that when you press F1 for help while working in a particular RC-P dialog, the help system automatically displays help matching that dialog.

Printing Help Topics

To print a help topic, navigate to the required topic and click the help window's *Print* button. A dialog box may ask you whether you wish to print the selected topic only or all topics under the selected heading; when this is the case, select *Print the selected topic* and click *OK*.

OVERVIEW OF WIZARDS

Wizards guide you through common tasks in RC-P:

- The Add Hardware Devices wizard helps you add cameras and other hardware devices, such as video encoders , to your RC-P system. If microphones are attached to a hardware device, they are automatically added as well.

- The Configure Video and Recording wizard helps you quickly configure your cameras' video and recording properties.

- The Adjust Motion Detection wizard helps you quickly configure your cameras' motion detection properties.

- The Configure User Access Wizard helps you quickly configure clients' access to the RC-P server.

Configuration & Properties

Archiving

Archiving helps you store recordings, maximize storage capacity and minimize risk. You can keep recordings for as long as required, limited only by the available hardware storage capacity.

RC-P automatically archives recordings if a camera's database becomes full. You only specify **one** time limit (the retention time) as part of the general Recording & Archiving Paths properties. Note that retention time will determine when archiving takes place. Retention time is the *total* amount of time for which you want to keep recordings from a camera (that is recordings in the camera's database *as well as* any archived recordings). Scheduled archiving is possible up to 24 times per day.

- **Quick Explanation of the Archiving Feature**
  Archiving is an integrated and automated feature in RC-P with which recordings are moved after an amount time in order to free up space for new recordings. The idea is that recordings are moved from one location to another in order to continuously have space for the most recent recordings on your default recording storage. This process is handled by the software.

  You do not have to do anything yourself to enable Archiving; Archiving is a process that runs in the background, and it is enabled and carried out automatically from the moment RC-P is installed. Recorded video can take up a lot of storage space, so only your hardware will place limits on the amount of recordings you can save. Archiving will ensure that recordings are moved in order to provide space for more recent recordings. The most recent recordings are saved on a local storage in order to prevent network-related problems in the saving process.

  The Ocularis Client understands archives and can locate the moved data without any problems.

  The default settings for RC-P is to perform archiving once a day, or if your database becomes full. It is possible to change the settings for when and how often archiving is to take place, under *Advanced Configuration > Scheduling and Archiving* in the Management Application. Scheduled archiving is possible up to 24 times per day. You can also change the retention time, which is the total amount of time you want to keep recordings from a camera (that is recordings in the camera's database as well as any archived recordings) under the properties of the individual camera.

  The default archiving folder is located on the RC-P server, by default in C:\Videodata. In the archiving folder, separate subfolders for storing archives for each camera are automatically created. These subfolders are named after the MAC address of the hardware device to which the camera is connected. You can change the default archiving folder to any other location locally, or select a location on a network drive to use as the default archiving folder.

In the following section, archiving is explained in detail. If you want to configure archiving immediately, see Configure Archiving Locations and Configure Archiving Schedules.

- **Benefits of Archiving**

  With archiving, recordings are moved from their standard location to another location, the archiving location. With archiving, the amount of recordings you are able to store is thus limited only by the available hardware storage capacity:

  By default, recordings are stored in RC-P 's database for each camera. The database for each camera is capable of containing a maximum of 600000 records or 40 GB.

  However, the maximum size of a database is not in itself very important: If a database for a camera becomes full, RC-P automatically begins archiving its content, freeing up space in the database. Having sufficient archiving space is thus more important.

In addition to automatic archiving when a database becomes full, you can schedule archiving to take place at particular times up to 24 times per day. This way, you can proactively archive recordings, so databases will never become full.

By using archiving, you will also be able to back up archived records on backup media of your choice, using your preferred backup software.

- ### How Archiving Works

For each camera, the contents of the camera database will be moved to a default archiving folder, called *Archives*. This will happen automatically if a database becomes full, and one or more times every day, depending on your archiving settings.

The default archiving folder is located on the RC-P server, by default in C:\videodata.

In the archiving folder, separate subfolders for storing archives for each camera are automatically created. These subfolders are named after the MAC address of the hardware device to which the camera is connected.

Since you can keep archives spanning many days of recordings, and since archiving may take place several times per day, further subfolders, named after the archiving date and time, are also automatically created.

The subfolders will be named according to the following structure:

```
...\Archives\CameraMACAddress_VideoEncoderChannel\DateAndTime
```

Example: With the default archiving folder located under C:\videodata, video from an archiving taking place at 23.15 on 31st December 2011 for a camera attached to channel 2 on a video encoder hardware device with the MAC address 00408c51e181 would be stored at the following destination:

```
C:\videodata\Archives\00408c51e181_2\2011-12-31-23-15
```

If the hardware device to which the camera is attached is not a video encoder device with several channels, the video encoder channel indication in the sub-directory named after the hardware device's MAC address will always be *_1* (example: 00408c51e181_1).

Storing Archives at Other Locations than the Default Archiving Directory

You are also able to store archives in other directories than the default archiving directory. However, you cannot archive to external drives, only to a local drive on the computer running RC-P.

Dynamic Path Selection for Archives

With dynamic archiving paths, you specify a number of different archiving paths, usually across several drives. Using dynamic paths is recommended, and is the default setting when you configure cameras through the Configure Video & Recording Wizard

- ### Storage Capacity Required for Archiving

The storage capacity required for archiving depends entirely on the amount of recordings you plan to keep, and on how long you want to keep them (also known as retention time).

Some organizations want to keep archived recordings from a large number of cameras for several months or years. Other organizations may only want to archive recordings from one or two cameras, and they may want to keep their archives for much shorter periods of time.

You should always first consider the storage capacity of the **local** drive containing the default archiving directory to which archived recordings are always moved, even though they may immediately after be moved to an archiving location on another drive: As a rule of thumb, the capacity of the local drive should be at least twice the size required for storing the databases of all cameras.

When archiving, RC-P automatically checks that space required for the data to be archived plus 1 GB of free disk space per camera is available at the archiving location. If not, the archive location's oldest data from the camera in question will be deleted until there is sufficient free space for the new data to be archived.

In short: When estimating storage capacity required for archiving, consider your organization's needs, then plan for worst case rather than best case scenarios.

- **Automatic Response if Running Out of Disk Space**

With archiving, RC-P can automatically respond to the threat of running out of disk space. Two scenarios can occur, depending on whether the camera database drive is different from, or identical to, the archiving drive:

Different Drives: Automatic Archiving if Database Drive Runs Out of Disk Space

In case the RC-P server is running out of disk space, and

- the archiving drive is ***different from*** the camera database drive, and
- archiving has not taken place within the last hour,

archiving will automatically begin in an attempt to free up disk space. This will happen regardless of any archiving schedules.

The server is considered to be running out of disk space if:

- there is less than 10% disk space left, and the available disk space goes below 30 GB plus 1.5 GB per camera

  - or -

- the available disk space goes below 150 MB plus 20 MB per camera (example: with ten cameras, the server would be running out of disk space if the remaining available disk space went below 350 MB (150 MB plus 20 MB for each of the ten cameras))

The difference ensures that very large disks will not necessarily be considered to be running out of disk space just because they have less than 10% disk space left.

On the archiving drive, RC-P automatically checks that the space required for data from a camera to be archived plus 1 GB of free disk space per camera is available. If not, the archive drive's oldest data from the camera in question will be deleted until there is sufficient free space for the new data to be archived.

IMPORTANT: You will lose the archive data being deleted.

Same Drive: Automatic Moving or Deletion of Archives if Running Out of Disk Space

In case the RC-P server is running out of disk space, and the archiving drive is ***identical to*** the camera database drive, RC-P will automatically do the following in an attempt to free up disk space:

- **Backing Up Archives**

Many organizations want to back up recordings from cameras, using tape drives or similar.

Creating such backups based on the content of camera databases is not recommended; it may cause sharing violations or other malfunctions.

Instead, create such backups based on the content of archives. If you have not specified separate archiving locations for separate cameras, you could simply back up the default local archiving directory, *Archives*.

When scheduling a backup, make sure the backup job does not overlap with any scheduled archiving times.

- **Viewing Archived Recordings**

  You are able to view archived recordings via the Ocularis Client. All of the Ocularis Client's advanced features (video browsing , export, etc.) are available for archived recordings.

Archives Stored Locally

For archived recordings stored locally simply use the Ocularis Client's playback features for finding and viewing the required recordings; just like you would with recordings stored in a camera's regular database.

Exported Archives

For exported archives, for example archives stored on a CD, you also use the Ocularis Client.

- **Virus Scanning and Archiving**

  If allowed in your organization, disable any virus scanning of camera databases and archiving locations. For more information see Virus Scanning Information.

- **New Database if Archiving Fails**

  Under rare circumstances, archiving may fail, for example due to network problems. However, in RC-P this does not pose a threat. RC-P simply creates a new database and continues archiving in this new database. You can work with—and view—both this new database and the old one like any other databases.

CONFIGURE ARCHIVING LOCATIONS

Before configuring archiving locations, consider whether you want to use static or dynamic archiving paths:

- **Static** archiving paths mean that for a particular camera, archiving will take place to a particular location, and to that location only. Static archiving paths are in principle individual for each camera, but they do not have to be unique: several cameras can easily use the same path if required.

  You can configure static archiving paths for individual cameras, or as part of the general Recording & Archiving Paths properties.

  - **Individual cameras:** In the Management Application 's navigation pane, expand *Advanced Configuration*, expand *Cameras and Storage Information*, double-click the required camera, select *Recording & Archiving Paths*, and specify required properties.

  - **General Recording & Archiving Paths:** In the Management Application 's navigation pane, expand *Advanced Configuration*, double-click *Cameras and Storage Information*, and specify required properties.

Tip: If several cameras should use the same path, use the general Recording & Archiving Paths properties. There you get a template feature which lets you specify shared archiving locations in just a few clicks.

- **Dynamic** archiving paths allow greater flexibility, and are thus highly recommended. With dynamic archiving paths, you specify a number of different archiving paths, usually across several drives. If the path containing the camera database to be archived is on one of the drives you have selected for dynamic archiving, RC-P will always try to archive to that drive first. If not, RC-P automatically archives to the archiving drive with the most available space at any time, provided there is not a camera database using that drive. This fact will have no impact on how users find and view archived recordings. Dynamic archiving paths are general for all your cameras; you cannot configure dynamic archiving paths for individual cameras.

To configure archiving paths: In the Management Application 's navigation pane, expand *Advanced Configuration*, double-click *Cameras and Storage Information*, select *Dynamic Path Selection - Archives*, and specify required properties.

If configuring your cameras through the Configure Video & Recording Wizard, the wizard also lets you configure archiving paths.

CONFIGURE ARCHIVING SCHEDULES

RC-P automatically archives recordings if a camera's database becomes full (in earlier versions, this was an option configured individually for each camera).

You are furthermore able to schedule archiving at particular points in time up to 24 times per day, with minimum one hour between each one. This way, you can proactively archive recordings, so databases will never become full. As a rule of thumb, the more you expect to record, the more often you should archive.

There are two ways in which to configure archiving schedules:

- While configuring your cameras through the Configure Video & Recording Wizard, in which case you configure your archiving schedule on the wizard's *Drive selection* page.
- As part of the general Scheduling & Archiving Properties: In the Management Application's navigation pane, expand *Advanced Configuration*, right-click *Scheduling and Archiving*, select *Properties*, select *Archiving* in the dialog, and specify required properties.

Audio

ADD AUDIO SOURCES

You add cameras and other hardware devices, such as video encoders, to your RC-P system through the Add Hardware Devices... wizard. If microphones are attached to a hardware device, they are automatically added as well.

When managing microphones in RC-P, it is important to remember the basic concepts:

- **Microphones** are attached to hardware devices, and thus typically physically located next to cameras. They can typically record what people near a camera are saying. Operators, with the necessary rights, can then listen to these recordings through their Ocularis Clients (provided the computer running the Ocularis Client has speakers attached).

CONFIGURE MICROPHONES

Configuration of microphones in RC-P is very basic; settings such as volume, etc. are controlled on the microphone units themselves.

1. In the Management Application's navigation pane, expand *Advanced Configuration*, expand *Hardware Devices*, and expand the hardware device to which the required microphone is attached.
2. Right-click the required microphone, and select *Properties*.
3. Specify properties as required.
4. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

MICROPHONE (PROPERTIES)

When you configure microphones, properties are limited to:

- ***Enabled*****:** Microphones are enabled by default, meaning that they are able to transfer audio to RC-P. If required, you can disable an individual microphone, in which case no audio will be transferred from the microphone to RC-P.

- ***Microphone name*****:** Name of the microphone as it will appear in the Management Application as well as in clients. If required, you can overwrite the existing microphone name with a new one. Microphone names must be unique, and must not contain any of the following special characters: < > & ' " \ / : * ? | [ ]

On some hardware devices, audio can also be enabled/disabled on the hardware device itself, typically through the hardware device's own configuration web page. If audio on a hardware device does not work after enabling it in the Management Application, you should thus verify whether the problem may be due to audio being disabled on the hardware device itself.

Cameras & Recordings

ADD CAMERAS & OTHER HARDWARE DEVICES

Add cameras and other hardware devices, such as video encoders, to your RC-P system through the Add Hardware Devices... wizard. If microphones are attached to a hardware device, they are automatically added as well.

The wizard offers you four different ways of adding cameras:

- **Express (recommended):** Scans your network for relevant hardware devices, and helps you quickly add them to your system. To use the Express method, your RC-P server and your cameras must be on the same layer 2 network, that is a network where all servers, cameras, etc. can communicate without the need for a router. See Add Hardware Devices Wizard - Express.

- **Advanced:** Scans your network for relevant hardware devices based on your specifications regarding required IP ranges, discovery methods, drivers, and device user names and passwords. See Add Hardware Devices Wizard - Advanced.

- **Manual:** Lets you specify details about each hardware device separately. This is a good choice if you only want to add a few hardware devices, and you know their IP addresses, required user names and passwords, etc. See Add Hardware Devices Wizard - Manual.

- **Import from CSV file:** Lets you import data about cameras as comma-separated values from a file; this is an effective method if setting up several similar systems. See Add Hardware Devices Wizard - Import from CSV File.

CONFIGURE VIDEO & RECORDING

Once you have added hardware devices and attached cameras, you can configure video and recording settings in three ways:

- **Wizard-driven:** Guided configuration which lets you specify video, recording and archiving settings for all your cameras. See Configure Video & Recording Wizard and Adjust Motion Detection Wizard.

- **General:** Lets you specify video, recording and shared settings (such as dynamic archiving paths and whether audio should be recorded or not) for all your cameras.

1. In the Management Application 's navigation pane, expand *Advanced Configuration*, right-click *Cameras and Storage Information*, and select *Properties*.

2. Specify properties as required for Recording & Archiving Paths, Dynamic Path Selection, Video Recording, Manual Recording, Frame Rate - MJPEG, Frame Rate - MPEG, Audio Selection, Audio Recording and Storage Information. When ready, click *OK*.

3. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

- **Camera-specific:** Lets you specify video, recording and camera-specific settings (such as event notification, PTZ preset positions, and fisheye view areas) for each individual camera.

  1. In the Management Application 's navigation pane, expand *Advanced Configuration*, and expand *Cameras and Storage Information*.

  2. Right-click the required camera, and select *Properties*.

  3. Specify properties as required for General, Video, Audio, Recording, Recording Properties & Archiving Paths, Event Notification, Output, Motion Detection & Exclude Regions and—if applicable—Positions and PTZ on Event.

  4. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

VIEW VIDEO FROM CAMERAS IN MANAGEMENT APPLICATION

You can view live video from single cameras directly in the Management Application:

1. In the Management Application's navigation pane, expand *Advanced Configuration*, and expand *Cameras and Storage Information*.

2. Select the required camera to view live video from that camera. Above the live video, you will find a summary of the most important properties for the selected camera. Below the live video, you will find information about the camera's resolution and average image file size. For cameras using MPEG or H.264, you will also see the bit rate in Mbit/second.

IMPORTANT: Viewing of live video in the Management Application may under certain circumstances affect any simultaneous recording from the camera in question. Especially three scenarios are important to consider:

1) Some cameras supporting multistreaming may halve their frame rate or respond with other negative effects when a second stream is opened.

2) If a camera delivers live video in a very high quality, de-coding of images may increase the load on the Recording Server service, which may in turn affect ongoing recordings negatively.

3) Cameras that do not support multiple simultaneous video streams will not be able to connect to the surveillance server and the Management Application at the same time; therefore it is recommended to stop the Recording Server service when configuring such devices for motion detection and PTZ.

CONFIGURE WHEN CAMERAS SHOULD DO WHAT

Use the scheduling feature to configure when:

- Cameras should be online (that is transfer video to RC-P)

- Cameras should use speedup (that is use a higher than normal frame rate)

- You want to receive any e-mail notifications regarding cameras
- Archiving should take place

See Configure General Scheduling & Archiving and Configure Camera-specific Schedules.

Monitor Storage Space Usage

To view how much storage space you have on your RC-P system—as well as how much of it is free—do the following:

1. In the Management Application's navigation pane, expand *Advanced Configuration*, and select *Cameras and Storage Information*.
2. View the *Storage Usage Summary* for information about, which drives are available, what drives are used for, the size of each drive, as well as how much video data, other data, and free space exists in each drive.

Database Resizing

In case recordings for a camera get larger than expected, or the available drive space is suddenly reduced in another way, an advanced database resizing procedure will automatically take place:

If archives are present on the same drive as the camera's database, the oldest archive for all cameras archived on that drive will be moved to another drive (moving archives is only possible if you use dynamic archiving, with which you can archive to several different drives) or—if moving is not possible—deleted.

If no archives are present on the drive containing the camera's database, the size of all camera databases on the drive will be reduced by deleting a percentage of their oldest recordings, thus temporarily limiting the size of all databases

When the Recording Server service is restarted upon such database resizing, the original database sizes will be used. You should therefore make sure that the drive size problem is solved.

Should the database resizing procedure take place, you will be informed on-screen in the Ocularis Client, in log files, and (if set up) through an e-mail notification.

Disable or Delete Cameras

All cameras are enabled by default. This means video from the cameras can be transferred to RC-P—provided that the cameras are scheduled to be online.

To **disable** a camera:

1. In the Management Application's navigation pane, expand *Advanced Configuration*, expand *Cameras and Storage Information*, double-click the camera you want to disable, and clear the *Enabled* box.
2. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

To **delete** a camera, you technically have to delete the hardware device. Deleting the hardware device will also delete any attached microphones. If you do not want this, consider disabling the camera instead.

Wizards

CONFIGURE VIDEO & RECORDING WIZARD

The Configure Video and Recording wizard helps you quickly configure your cameras' video and recording properties. The wizard is divided into a number of pages:

- Video Settings and Preview
- Online Schedule
- Live and Recording Settings (Motion-JPEG Cameras)
- Live and Recording Settings (MPEG Cameras)
- Drive Selection
- Recording and Archiving Settings

ADJUST MOTION DETECTION WIZARD

The Adjust Motion Detection wizard helps you quickly configure your cameras' motion detection properties. The wizard is divided into two pages:

- Exclude Regions
- Motion Detection

Cameras that do not support multiple simultaneous video streams will not be able to connect to the surveillance server and the Management Application at the same time; therefore it is recommended to stop the Recording Server service when configuring such devices for motion detection and PTZ. See also View Video from Cameras in Management Application.

General Recording & Storage Properties

RECORDING & ARCHIVING PATHS

When you configure video and recording , you are able to specify certain properties for many cameras in one step. Either simply in order to speed up things, or because the properties in question are shared by all cameras rather than specific to individual cameras.

All properties on a white background are editable, properties on a light blue background cannot be edited. Note that all of the Recording and Archiving Paths properties can also be specified individually for each camera.

- ***Template*****:** The template can help you configure similar properties quickly. Say you have 20 cameras and you want to change the recording path, archiving path, and retention time for all of them. Instead of having to enter the same three pieces of information 20 times, you can simply enter them once in the template, and then apply the template to the 20 cameras with only two clicks.

- ***Apply Template*****:** Lets you select which cameras you want to apply the template for. You then use one of the two *Set* buttons (see descriptions in the following) to actually apply the template.

  Tip: To select all cameras in the list, click the *Select All* button.

- ***Camera Name*****:** Name of the camera as it will appear in the Management Application as well as in clients. If required, you can overwrite the existing camera name with a new one. Camera names must be unique, and must not contain any of the following special characters: `< > & ' " \ / : * ? | [ ]`

- ***Recording Path*****:** Path to the folder in which the camera's database should be stored. Default is C:\videodata. To browse for another folder, click the browse icon next to the required cell. You are only able to specify a path to a folder on a *local* drive. You cannot specify a path to a network drive. The reason for this limitation is that if you were using a network drive, it would not be possible to save recordings if the network drive became unavailable. If you change the recording path, and there are existing recordings at the old location, you will be asked whether you want to move the recordings to the new location (recommended), leave them at the old location, or delete them.

  Tip: If you have several cameras, and several local drives are available, you can improve performance by distributing individual cameras' databases across several drives.

- ***Archiving Path*****:** Only editable if not using dynamic paths for archiving. Path to the folder in which the camera's archived recordings should be stored. Default is C:\videodata. To browse for another folder, click the browse icon next to the required cell. If you change the archiving path, and there are existing archived recordings at the old location, you will be asked whether you want to move the archived recordings to the new location (recommended), leave them at the old location, or delete them. Note that if moving archived recordings, RC-P will also archive what is currently in the camera's database; in case you wonder why the camera database is empty just after you have moved archived recordings, this is the reason.

- ***Retention Time*****:** Total amount of time for which you want to keep recordings from the camera (that is recordings in the camera's database as well as any archived recordings). Default is 30 days.

  Note that the retention time covers the total amount of time you want to keep recordings for; in earlier RC-P versions time limits were specified separately for the database and archives.

- ***Camera*****:** Click the ***Open*** button to configure detailed and/or camera-specific settings (such as event notification, PTZ preset positions, and fisheye view areas) for the selected camera.

- ***Select All*****:** Click button to select all cameras in the *Apply Template* column.

- ***Clear All*****:** Click button to clear all selections in the *Apply Template* column

- ***Set selected template value on selected cameras*****:** Lets you apply one or more selected values from the template (rather than all values) to selected cameras.

- ***Set all template values on selected cameras*****:** Lets you apply all values from the template to selected cameras.

Dynamic Path Selection

When you configure video and recording , you can specify certain properties for many cameras in one step. In the case of Dynamic Path Selection, it is simply because the properties are shared by all cameras.

With dynamic archiving paths, you specify a number of different archiving paths, usually across several drives. If the path containing the RC-P database is on one of the drives you have selected for archiving, RC-P will always try to archive to that drive first. If not, RC-P automatically archives to the archiving drive with the most available space at any time, provided there is not a camera database using that drive. Which drive has the most available space may change during the archiving process, and archiving may therefore happen to several archiving drives during the same process. This fact will have no impact on how users find and view archived recordings.

Dynamic archiving paths are general for all your cameras; you cannot configure dynamic archiving paths for individual cameras.

All properties on a white background are editable, properties on a light blue background

General Recording & Storage Properties

When you configure video and recording , you can specify certain properties for many cameras in one step. Either simply in order to speed up things, or because the properties in question are shared by all cameras rather than specific to individual cameras.

In RC-P, the term *recording* means *saving video and, if applicable, audio from a camera in the camera's database on the surveillance system server*. Video/audio is often saved only when there is a reason to do so, for example as long as motion is detected, when an event occurs and until another event occurs, or within a certain period of time.

All properties on a white background are editable, properties on a light blue background cannot be edited. Note that all of the Video Recording properties can also be specified individually for each camera.

- ***Template*****:** The template can help you configure similar properties quickly. Say you have 20 cameras and you want 10 seconds of pre-recording on all of them. Instead of having to enter the same piece of information 20 times, you can simply enter it once in the template, and then apply the template to the 20 cameras with only two clicks.

- ***Apply Template*****:** Lets you select which cameras you want to apply the template for. You then use one of the two *Set* buttons (see descriptions in the following) to actually apply the template.

  Tip: To select all cameras in the list, click the *Select All* button.

- ***Camera Name:*** *Name of the camera as it will appear in the Management Application as well as in clients. If required, you can overwrite the existing camera name with a new one. Camera names must be unique, and must not contain any of the following special characters:* `< > & ' " \ / : * ? | [ ]`

- ***Record on*****:** Lets you select under which conditions video from the camera should be recorded:

  - ***Always:*** Record whenever the camera is enabled and scheduled to be online (the latter allows for time-based recording).

  - ***Never:*** Never record. Live video will be displayed, but—since no video is kept in the database—users will not be able to play back video from the camera.

  - ***Motion Detection*:** Select this to record video in which motion is detected. Unless post-recording (see the following) is used, recording will stop immediately after the last motion is detected.

  - ***Event*:** Select this to record video when an event occurs and until another event occurs. Use of recording on event requires that events have been defined, and that you select start and stop events in the neighboring columns.

    Tip: If you have not yet defined any suitable events, you can quickly do it: Use the *Configure events* list, located in the bottom left corner of the window.

  - ***Motion Detection & Event*:** Select this to record video in which motion is detected, or when an event occurs and until another event occurs. Remember to select start and stop events in the neighboring columns.

- ***Start Event*:** Use when recording on Event or Motion Detection & Event. Select required start event. Recording will begin when the start event occurs (or earlier if using pre-recording; see the following).

- ***Stop Event*:** Select required stop event. Recording will end when the stop event occurs (or later if using post-recording; see the following).

- ***Pre-recording*:** You can store recordings from periods preceding detected motion and/or start events. Select check box to enable this feature. Remember to specify required number of seconds in the neighboring column.

  How does pre- and post-recording work? RC-P receives video in a continuous stream from the camera whenever the camera is enabled and scheduled to be online. This is what lets you view live video, but it also means that RC-P can easily store received video for a number of seconds in its memory (also known as buffering). If it turns out that the buffered video is needed for pre- or post-recording, it is automatically appended to the recording. If not, it is simply discarded.

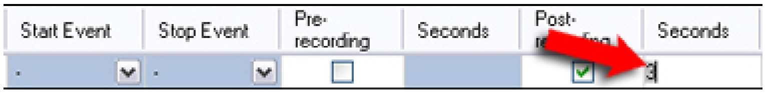
- ***Seconds [of pre-recording]*:** Specify the number of seconds for which you want to record video from before recording start conditions (that is motion or start event) are met. Usually, only some seconds of pre-recording is required, but you can specify up to 65535 seconds of pre-recording, corresponding to 18 hours, 12 minutes and 15 seconds. However, if specifying a very long pre-recording time, you can potentially run into a scenario where your pre-recording time spans scheduled or unscheduled archiving times. That can be problematic since pre-recording does not work well during archiving.

- ***Post-recording*:** You can store recordings from periods following detected motion and/or stop events. Select check box to enable this feature. Remember to specify required number of seconds in the neighboring column.

- ***Seconds [of post-recording]*:** Specify the number of seconds for which you want to record video from after recording stop conditions (that is motion or stop event) are met. Usually, only some seconds of post-recording is required, but you can specify up to 65535 seconds of post-recording, corresponding to 18 hours, 12 minutes and 15 seconds. However, if specifying a very long post-recording time, you can potentially run into a scenario where your post-recording time spans scheduled or unscheduled archiving times. That can be problematic since post-recording does not work well during archiving.

- ***Camera:*** Click the ***Open*** button to configure detailed and/or camera-specific settings (such as event notification, PTZ preset positions, and fisheye view areas) for the selected camera.

- ***Select All*:** Click button to select all cameras in the *Apply Template* column.
- ***Clear All*:** Click button to clear all selections in the *Apply Template* column
- ***Set selected template value on selected cameras*:** Lets you apply only a selected value from the template to selected cameras.



Start Event	Stop Event	Pre-recording	Seconds	Post-recording	Seconds
-	-	☐		☑	3

Example: Only the selected value is applied using this method

- ***Set all template values on selected cameras*:** Lets you apply all values from the template to selected cameras.

Manual Recording

When you configure video and recording , you can specify certain properties for many cameras in one step. In the case of Manual recording, it is simply because the properties are shared by all cameras.

When manual recording is enabled, Ocularis Client users with the necessary rights can manually start recording if they see something of interest while viewing live video from a camera which is not already recording.

If enabled, manual recording can thus take place even if recording for individual cameras is set to *Never* or *Conditionally*.

When started from the Ocularis Client, such user-driven recording will always take place for a fixed time, for example for five minutes.

- ***Enable manual recording: Select check box to enable manual recording and specify further details.***
- ***Default duration of manual recording*:** Period of time (in seconds) during which user-driven recording will take place. Default duration is 300 seconds, corresponding to five minutes.
- ***Maximum duration of manual recording*:** Maximum allowed period of time for user-driven recording. This maximum is not relevant in connection with manual recording started from the Ocularis Client, since such manual recording will always take place for a fixed time. In some installations it is, however, also possible to combine manual recording with third-party applications if integrating these with RC-P through an API or similar, and in such cases specifying a maximum duration may be relevant. If you are simply using manual recording in connection with the Ocularis Client, disregard this property.

FRAME RATE - MJPEG

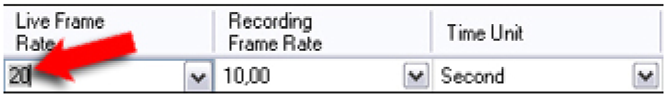
When you configure video and recording , you can specify certain properties for many cameras in one step. Either simply in order to speed up things, or because the properties in question are shared by all cameras rather than specific to individual cameras.

All properties on a white background are editable, properties on a light blue background cannot be edited. Note that all of the Frame Rate - MJPEG properties can also be specified individually for each camera using MJPEG.

- **Template and Common Properties**
    - ***Template*****:** The template can help you configure similar properties quickly. Say you have 20 cameras and you want a particular frame rate on all of them. Instead of having to enter the same piece of information 20 times, you can simply enter it once in the template, and then apply the template to the 20 cameras with only two clicks.
    - ***Apply Template*****:** Lets you select which cameras you want to apply the template for. You then use one of the two *Set* buttons (see descriptions in the following) to actually apply the template.

      Tip: To select all cameras in the list, click the *Select All* button.

    - ***Select All*****:** Click button to select all cameras in the *Apply Template* column.
    - ***Clear All*****:** Click button to clear all selections in the *Apply Template* column
    - ***Set selected template value on selected cameras*****:** Lets you apply only a selected value from the template to selected cameras.



Live Frame Rate	Recording Frame Rate	Time Unit
20	10,00	Second

Example: Only the selected value is applied using this method

-
    - ***Set all template values on selected cameras*****:** Lets you apply all values from the template to selected cameras.
    - ***Camera Name*****:** Name of the camera as it will appear in the Management Application as well as in clients. If required, you can overwrite the existing camera name with a new one. Camera names must be unique, and must not contain any of the following special characters: < > & ' " \ / : * ? | [ ]
- **Regular Frame Rate Properties**
    - ***Frame Rate:*** Required average frame rate for video from the camera. Select number of frames, then select required interval (per second, minute or hour) in the Time Unit column.
- **Speedup Frame Rate Properties**
    - ***Enable Speedup*****:** The speedup feature lets you use a higher than normal frame rate if motion is detected and/or an event occurs. When you enable speedup, further columns for specifying speedup details become available.
    - ***Frame Rate:*** Required average speedup frame rate for viewing video from the camera. Select number of frames, then select required interval (per second, minute or hour) in the Time Unit column. The frame rate must be higher than the frame rate specified under normal mode.

Frame Rate - MPEG

When you configure video and recording , you can specify certain properties for many cameras in one step. Either simply in order to speed up things, or because the properties in question are shared by all cameras rather than specific to individual cameras.

All properties on a white background are editable, properties on a light blue background cannot be edited. Note that all of the Frame Rate - MPEG properties can also be specified individually for each camera using MPEG.

- ***Template*:** The template can help you configure similar properties quickly. Say you have 20 cameras and you want a particular frame rate on all of them. Instead of having to enter the same piece of information 20 times, you can simply enter it once in the template, and then apply the template to the 20 cameras with only two clicks.

- ***Apply Template*:** Lets you select which cameras you want to apply the template for. You then use one of the two *Set* buttons (see descriptions in the following) to actually apply the template.

Tip: To select all cameras in the list, click the *Select All* button.

- ***Camera Name:*** *Name of the camera as it will appear in the Management Application as well as in clients. If required, you can overwrite the existing camera name with a new one. Camera names must be unique, and must not contain any of the following special characters:* < > & ' " \ / : * ? | [ ]
- ***Dual Stream:*** Allows you to check if dual streaming is enabled on the camera(s). Note that the information is read-only. For cameras that support dual streaming, this can be enabled/disabled as part of individual cameras' Video properties.

- ***Live FPS:*** Lets you select the camera's live frame rate per second (FPS).

- ***Camera:*** Click the Open button to configure detailed and/or camera-specific settings (such as event notification, PTZ preset positions, and fisheye view areas) for the selected camera.

- ***Select All:*** Click button to select all cameras in the Apply Template column.

- ***Clear All:*** Click button to clear all selections in the Apply Template column.

- ***Set selected template value on selected cameras*:** Lets you apply only a selected value from the template to selected cameras.

Audio Selection

When you configure video and recording , you can specify certain properties for many cameras in one step. Either simply in order to speed up things, or because the properties in question are shared by all cameras rather than specific to individual cameras.

With a default microphone selected for a camera, audio from the microphone will automatically be used when video from the camera is viewed. Note that all of the Audio Selection properties can also be specified individually for each camera.

- ***Template*:** The template can help you configure similar properties quickly. Say you have eight cameras and you want a particular default microphone for all of them. Instead of having to enter the same piece of information eight times, you can simply enter it once in the template, and then apply the template to the eight cameras with only two clicks.

- ***Apply Template*:** Lets you select which cameras you want to apply the template for. You then use one of the two *Set* buttons (see descriptions in the following) to actually apply the template.

  Tip: To select all cameras in the list, click the *Select All* button.

- ***Camera Name*****:** Name of the camera as it will appear in the Management Application as well as in clients. If required, you can overwrite the existing camera name with a new one. Camera names must be unique, and must not contain any of the following special characters: `< > & ' " \ / : * ? | [ ]`

- ***Default Microphone*****:** Select required default microphone.

  Tip: Note that you can select a microphone attached to another hardware device than the selected camera itself.

- ***Camera:*** Click the ***Open*** button to configure detailed and/or camera-specific settings (such as event notification, PTZ preset positions, and fisheye view areas) for the selected camera.

- ***Set selected template value on selected cameras*****:** Lets you apply only a selected value from the template to selected cameras.

- ***Set all template values on selected cameras*****:** Lets you apply all values from the template to selected cameras.

AUDIO RECORDING

When you configure video and recording for specific cameras, you can determine whether audio should be recorded or not. Your choice will apply for all cameras on your RC-P system.

- ***Always*****:** Always record audio on all applicable cameras.

- ***Never*****:** Never record audio on any cameras. Note that even though audio is never recorded, it will still be possible to listen to live audio in the Ocularis Client.

If you record audio, it is important that you note the following:

- **Audio recording affects video storage capacity:** Audio is recorded to the associated camera's database.

STORAGE INFORMATION

The storage information lets you view how much storage space you have on your recording component—and not least how much of it is free:

- ***Drive*: Letter representing the drive in question, for example C:.
- ***Path***: Path to the storage area, for example C:\ or \\OurServer\OurFolder\OurSubfolder\.
- ***Usage***: What the storage area is used for, for example recording or archiving.
- ***Drive Size***: Total size of the drive.
- ***Video Data***: Amount of video data on the drive.
- ***Other Data***: Amount of other data on the drive.
- ***Free Space***: Amount of unused space left on the drive.

Tip: To quickly view disk space usage in a pie chart format, select the line representing the drive you are interested in.

CAMERA ACCESS (PROPERTIES)

When adding or editing basic users , Windows users or groups , specify camera access settings:

In the list of cameras, select the camera(s) you want to work with. Note the last item in the list, *Rights for new cameras when added to the system*, with which you can allow the user/group access to any future cameras.

Tip: If the same features should be accessible for several cameras, you can select multiple cameras by pressing SHIFT or CTRL on your keyboard while selecting.

For the selected camera(s), in the ***Access*** check box, specify if the user/group should have access to live viewing and playback at all. If so, specify if they should have access to **both** live viewing and playback and—if this is the case—which sub-features should be available when working with the selected camera(s).

The sub-features are listed in two columns in the lower part of the window: the left column lists features related to live viewing, the right column lists features related to playback.

The *Camera access settings* check boxes work like a hierarchy of rights. If the *Access* check box is cleared, everything else is cleared and disabled. If the *Access* check box is selected, but, for example, the *Live* check box is cleared, everything under the *Live* check box is cleared and disabled.

In the *Live* column, the following features, all selected by default, are available:

- ***Live***: Ability to view live video from the selected camera(s).
    - ***PTZ***: Ability to use navigation features for PTZ (Pan/Tilt/Zoom) cameras. A user/group will only be able to use this right if having access to one or more PTZ cameras.
    - ***PTZ preset positions***: Ability to use navigation features for moving a PTZ camera to particular preset positions. A user/group will only be able to use this right if having access to one or more PTZ cameras with defined preset positions.
    - ***Output***: Ability to activate output (lights, sirens, door openers, etc.) related to the selected camera(s).
    - ***Events***: Ability to use manually triggered events related to the selected camera(s).

- ***Incoming audio*****:** Ability to listen to incoming audio from microphones related to the selected camera(s).
- ***Manual recording*****:** Ability to manually start recording for a fixed time (defined by the surveillance system administrator).
- ***Recorded audio*****:** Ability to listen to recorded audio from microphones related to the selected camera(s).

Why can I not select certain features? *Typically because the selected camera does not support the features. For example, you can only select PTZ-related features if the camera is a PTZ camera. Also, some of the features depend on the user's/group's General Access properties: For example, in order have access to PTZ or output features, the user/group must have access to viewing live video; in order to use AVI/JPEG export, the user/group must have access to playing back recorded video.*

Why are some feature check boxes filled with squares? *Square-filled check boxes can appear in the lower part of the window if you have selected several cameras and a feature applies for some but not all of the cameras. Example: For camera A you have selected that use of the* Events *is allowed; for camera B it is not allowed. If you select both camera A and camera B in the list, the* Events *check box in the lower part of the window will be square-filled. Another example: Camera C is a PTZ camera for which you have allowed the* PTZ preset positions *feature; camera D is not a PTZ camera. If you select both camera C and camera D in the list, the* PTZ preset positions *check box will be square-filled.*

VIDEO (CAMERA-SPECIFIC PROPERTIES)

When you configure video and recording for specific cameras, properties include:

- **If the Camera Uses the MJPEG Video Format**
  With MJPEG, you can define frame rates for regular as well as speedup modes. Furthermore, if the camera offers dual stream, you can enable this:

  Regular Frame Rate Mode:

  - ***Frame rate*****:** Frame rate for viewing video from the camera. Select number of frames in the first field, and required interval (per second, minute or hour) in the second field.

  Speedup Frame Rate Mode:

  - ***Frame rate*****:** Speedup frame rate for viewing video from the camera. Select number of frames in the first field, and required interval (per second, minute or hour) in the second field. The frame rate must be higher than the frame rate specified under normal mode.
  - ***On event*****:** Select this check box to use the speedup frame rates when an event occurs and until another event occurs. Use of speedup on event requires that events have been defined, and that you select start and stop events in the neighboring lists.

  Why are there three different places where I can configure frame rates for video? The first, **Live frame rate**, is for the regular recording stream. The second, **Live frame rate**, is for when speeding up recordings in connection with motion detection or similar. And the third, **FPS**, is for the additional stream used for live viewing.

- **If the Camera Uses the MPEG Video Format**

  With MPEG, you can define frame rate:

  - ***Frame rate per second*****:** Frame rate for viewing live and recorded video from the camera. Select number of frames per second.

GENERAL (CAMERA-SPECIFIC PROPERTIES)

When you configure video and recording for specific cameras, properties include:

- ***Enabled*****:** Cameras are enabled by default, meaning that provided they are scheduled to be online, they are able to transfer video to RC-P . If required, you can disable an individual camera, in which case no video/audio will be transferred from the camera source to RC-P .

- ***Camera name*****:** Name of the camera as it will appear in the Management Application as well as in clients. If required, you can overwrite the existing camera name with a new one. Camera names must be unique, and must not contain any of the following special characters: < > & ' " \ / : * ? | [ ]

  Tip: Camera names can be very long if required: the upper limit is more than 2000 characters, although such long camera names are hardly ever needed.

These properties are to a large extent camera-specific. Since such properties vary from camera to camera, descriptions in the following are for guidance only.

If the selected camera is accessible, a live preview is displayed. Click the *Camera Settings...* button to open a separate window with properties for the selected camera.

The video properties typically let you control bandwidth, brightness, compression, contrast, resolution, rotation, etc. by overwriting existing values of selecting new ones.

When adjusting video settings, you are—for most cameras—able to preview the effect of your settings in an image below the fields.

Video settings may feature an *Include Date and Time* setting. If set to *Yes*, date and time from the camera will be included in video. Note, however, that cameras are separate units which may have separate timing devices, power supplies, etc. Camera time and RC-P system time may therefore not correspond fully, and this may occasionally lead to confusion. As all frames are time-stamped by RC-P upon reception, and exact date and time information for each image is thus already known, it is recommended that the setting is set to *No*.

Tip: For consistent time synchronization, you may—if supported by the camera—automatically synchronize camera and system time through a time server.

AUDIO (CAMERA-SPECIFIC PROPERTIES)

When you configure video and recording for specific cameras, properties include the possibility of selecting a default microphone for the camera.

With a default microphone selected for a camera, audio from the microphone will automatically be used when video from the camera is viewed.

If a microphone is attached to the same hardware device as the camera, that microphone will be the camera's default microphone if you do not select otherwise.

Tip: Note that you can select a microphone attached to another hardware device than the selected camera itself.

- ***Default microphone*****:** Select required microphone.

The ability to select a default microphone for the camera requires that at least one microphone has been attached to a hardware device on the surveillance system.

RECORDING SETTINGS

In RC-P , the term *recording* means *saving video and, if applicable, audio from a camera in the camera's database on the surveillance system server*. Video/audio is often saved only when there is a reason to do so, for example as long as motion is detected, when an event occurs and until another event occurs, or within a certain period of time.

When you configure video and recording for specific cameras, recording properties include:

- ***Always*****:** Record whenever the camera is enabled and scheduled to be online (the latter allows for time-based recording).
- ***Never*****:** Never record. Live video will be displayed, but—since no video is kept in the database—users will not be able to play back video from the camera.
- ***Conditionally*****:** Record when certain conditions are met. When you select this option, specify required conditions (see the following).
- ***On built-in motion detection*****:** Select this check box to record video in which motion is detected. Unless post-recording (see the following) is used, recording will stop immediately after the last motion is detected.
- ***On event*****:** Select this check box to record video when an event occurs and until another event occurs. Use of recording on event requires that events have been defined, and that you select start and stop events in the neighboring lists.
- ***Start event*****:** Select required start event. Recording will begin when the start event occurs (or earlier if using pre-recording; see the following).
- ***Stop event*****:** Select required stop event. Recording will end when the stop event occurs (or later if using post-recording; see the following).

When the option *Conditionally* is selected, you can store recordings from periods preceding and following detected motion and/or specified events. Example: If you have defined that video should be stored when a door is opened, being able to see what happened immediately prior to the door being opened may also be important. Say you have specified that video should be stored conditionally on event, with a start event called Door Opened and a stop event called Door Closed. With three seconds of pre-recording, video will be recorded from three seconds before Door Opened occurs and until Door Closed occurs.

- ***Enable pre-recording*****:** Available only when the option *Conditional* is selected. Specify the number of seconds for which you want to record video from before recording start conditions (that is motion or start event) are met.
- ***Enable post-recording*****:** Available only when the option Conditional is selected. Specify the number of seconds for which you want to record video after recording stop conditions (that is motion end or stop event) are met.

How does pre- and post-recording work? *RC-P receives video in a continuous stream from the camera whenever the camera is enabled and scheduled to be online. This is what lets you view live video, but it also means that RC-P can easily store received video for a number of seconds in its memory (also known as buffering). If it turns out that the buffered video is needed for pre- or post-recording, it is automatically appended to the recording. If not, it is simply discarded.*

Note that manual recording may be enabled. With manual recording, Ocularis Client users with the necessary rights can manually start recording if they see something of interest while viewing live video from a camera which is not already recording. If enabled, manual recording can thus take place even if recording for individual cameras is set to *Never* or *Conditionally*.

Recording & Archiving Paths

When you configure video and recording for specific cameras, properties include:

- ***Recording path*****:** Path to the folder in which the camera's database should be stored. Default is C:\videodata. To browse for another folder, click the browse button next to the *Recording path* field. You are only able to specify a path to a folder on a *local* drive.

  If you change the recording path, and there are existing recordings at the old location, you will be asked whether you want to move the recordings to the new location (recommended), leave them at the old location, or delete them.

- ***Delete Database*****:** Click button to delete all recordings in the database for the camera. Archived recordings will not be affected.

  IMPORTANT: Use with caution; all recordings in the database for the camera will be permanently deleted. As a security measure, you will be asked to confirm the deletion.

- ***Archiving path:*** *Only available if not using dynamic paths for archiving. Path to the folder in which the camera's archived recordings should be stored. Default is C:\videodata\Archives. To browse for another folder, click the browse button next to the Archiving path field. You can specify a path to a local or a networked drive as required.* You can only specify a path to local drive. If you change the archiving path, and there are existing archived recordings at the old location, you will be asked whether you want to move the archived recordings to the new location (recommended), leave them at the old location, or delete them. Note that if moving archived recordings, RC-P will also archive what is currently in the camera's database; in case you wonder why the camera database is empty just after you have moved archived recordings, this is the reason.

- ***Delete Archives*****:** Click button to delete all archived recordings for the camera. Recordings in the camera's regular database will not be affected. The ability to delete is available regardless of whether you use a single archiving path or dynamic archiving paths.

  IMPORTANT: Use with caution; all archived recordings for the camera will be permanently deleted. As a security measure, you will be asked to confirm the deletion.

- ***Retention time*****:** Total amount of time for which you want to keep recordings from the camera (that is recordings in the camera's database as well as any archived recordings). Default is 30 days.

  Note that the retention time covers the **total** amount of time you want to keep recordings for; in earlier RC-P versions time limits were specified separately for the database and archives.

- ***Database repair action:*** *Select which action to take if the database becomes corrupted:*

  - *Repair, scan, delete if fails*: Default action. If the database becomes corrupted, two different repair methods will be attempted: a fast repair and a thorough repair. If both repair methods fail, the contents of the database will be deleted.

  - *Repair, delete if fails*: If the database becomes corrupted, a fast repair will be attempted. If the fast repair fails, the contents of the database will be deleted.

  - *Repair, archive if fails*: If the database becomes corrupted, a fast repair will be attempted. If the fast repair fails, the contents of the database will be archived.

  - *Delete (no repair)*: If the database becomes corrupted, the contents of the database will be deleted.

  - *Archive (no repair)*: If the database becomes corrupted, the contents of the database will be archived.

If you choose an action to repair a corrupt database, this corrupt database is closed while it is repaired. Instead, a new database is created to allow recordings to continue.

- ***Configure Dynamic Paths:*** *With dynamic archiving paths, you specify a number of different archiving paths, usually across several drives. If the drive containing the camera's database is among the path you have selected for dynamic archiving, RC-P will always try to archive to that path first. If not, RC-P automatically archives to the archiving drive with the most available space at any time, provided there is not a camera database using that drive.*

OUTPUT (CAMERA-SPECIFIC PROPERTIES)

When you configure video and recording for specific cameras, you are also able to associate a camera with particular hardware output, for example the sounding of a siren or the switching on of lights.

Associated output can then be activated automatically when motion is detected in video from the camera, or manually when Ocularis Client users with the necessary rights view live video from the camera.

1. In the *Available output* list, select the required output. It is only possible to select one output at a time.

2. Click the >> button to copy the selected output to:

    - the *On manual activation* list, in which case the output will be available for manual activation in the Ocularis Client.

    - and/or -

    - the *On motion detected* list, in which case the output will be activated when motion is detected in video from the camera.

   If required, the same output can appear on both lists.

3. Repeat for each required output.

If you later want to remove an output from the one of the lists, simply select the output in question, and click the << button.

MOTION DETECTION & EXCLUDE REGIONS

When you configure video and recording for specific cameras, adjusting motion detection is important since it may determine when video from the camera is recorded, when e-mail notifications are generated, when hardware output (such as lights or sirens) is activated, etc. Time spent on finding the best possible motion detection settings for each camera may help you later avoid unnecessary recordings, notifications, etc. Depending on the physical location of the camera, it may be a very good idea to test motion detection under different physical conditions (day/night, windy/calm weather, etc.).

Before you configure motion detection for a camera, it is highly recommended that you have configured the camera's video properties, such as compression, resolution, etc.

Cameras that do not support multiple simultaneous video streams will not be able to connect to the surveillance server and the Management Application at the same time; therefore it is recommended to stop the Recording Server service when configuring such devices for motion detection and PTZ.

- **How to Configure Motion Detection Properties**

    1. Determine whether there are any areas which should be excluded from motion detection (for example if the camera view covers an area where a tree is swaying in the wind or where cars regularly pass in the background). If so, you can avoid detection of irrelevant motion by following the points below. If not, continue to step 2.

        - ***Enable:*** Lets you enable or disable the built-in motion detection.

          Motion detection is enabled as default. Disabling it will improve CPU and RAM performance of your RC-P system, but will—depending on your system settings—also affect your motion detection, event and alarm management. In the following two tables, the differences between enabling (table 1) and disabling (table 2) built-in motion detection for a camera are listed:

Camera's recording settings:	**Enabled motion detection: Will you get...**			
	...recordings?	**...motion based events?**	**...non-motion based events?**	**...sequences?**
Always	Yes	Yes	Yes	Yes
Never	No	Yes	Yes	No
Built-in Motion Detection	Yes	Yes	Yes	Yes
Built-in Motion Detection & Event **or** ***Event*** **only**	Yes	Yes	Yes	Yes

Camera's recording settings:	**Disabled motion detection: Will you get...**			
	...recordings?	**...motion based events?**	**...non-motion based events?**	**...sequences?**
Always	Yes	No	Yes	No
Never	No	No	Yes	No
Built-in Motion Detection	No	No	Yes	No
Built-in Motion Detection & Event **or** ***Event*** **only**	Yes (depending on settings)	No	Yes (depending on settings)	No

- ***Show grid*:** Lets you toggle the grid on and off. Toggling the grid off may provide a less obscured view of the preview image; selection of areas which should be excluded from motion detection takes place the same way as when the grid is visible. When on, the preview image will be divided into small sections by a grid. To define areas which should be excluded from motion detection, drag the mouse pointer over the required areas in the preview image while pressing the mouse button down. Left mouse button selects a grid section; right mouse button clears a grid section. Selected areas are highlighted in blue.

- ***Include All*:** Lets you quickly select all grid sections in the preview image. This may be advantageous if you want to exclude motion detection in most areas of the image, in which case you can simply clear the few sections in which you do not want to exclude motion detection.

- ***Exclude All*:** Lets you quickly clear all grid sections in the preview image.

2. Use the two sliders for configuring motion detection:

- ***Sensitivity*:** Determines how much each pixel must change before it is regarded as motion. With a high sensitivity, very little change in a pixel is required before it is regarded as motion. Areas in which motion is detected are highlighted in green in the preview image. Select a slider position in which only detections you consider motion are highlighted. As an alternative to using the slider, you may specify a value between 0 and 256 in the field next to the slider to control the sensitivity setting.

Tip: If you find the concept of sensitivity difficult to grasp, try dragging the slider to its leftmost position: The more you drag the slider to the left, the more of the preview image becomes highlighted. This is because with a high sensitivity even the slightest change in a pixel will be regarded as motion.

- ***Motion:*** *Determines how many pixels must change in the image before it is regarded as motion. The selected level is indicated by the black vertical line in the motion level indication bar below the preview image. The black vertical line serves as a threshold: When detected motion is above (that is to the right of) the selected sensitivity level, the bar changes color from green to red, indicating a positive detection. As an alternative to using the slider, you may specify a value between 0 and 10000 in the field next to the slider to control the motion setting.*

3. Specify your requirements for the following:

   - ***Detection interval:*** Determines how often motion detection analysis should be carried out on video from the camera. The interval is measured in milliseconds; default is 240 milliseconds (that is close to once every quarter of a second). The interval is applied regardless of the camera's frame rate settings.

   - ***Detection resolution:*** Determines settings for how much of the image should be analyzed. Should it be the full image or only a selected percentage of the image? By analyzing, for example 25%, only every fourth pixel in the image is analyzed instead of all pixels. Using optimized detection will reduce the amount of processing power used, but will also mean a less accurate motion detection.

- **Motion Detection and PTZ Cameras**
  Motion detection generally works the same way for PTZ (Pan/Tilt/Zoom) cameras as it does for regular cameras. However:

  - It is not possible to configure motion detection separately for each of a PTZ camera's preset positions.

PRIVACY MASKING

Determine if there are any areas of the camera image that must be masked from viewing. For example, if the camera points in a way so that it catches the window of a private building, the privacy of the residents must be respected. In that case, you can mask areas of the image by configuring the settings below.

- ***Enable:*** Lets you enable the *Privacy Masking* feature.

- ***Show grid*****:** Lets you toggle the grid on and off. Toggling the grid off may provide a less obscured view of the preview image; selection of areas which should be excluded from privacy masking takes place the same way as when the grid is visible. When on, the preview image will be divided into small sections by a grid. To define areas which should be excluded from privacy masking, drag the mouse pointer over the required areas in the preview image while pressing the mouse button down. Left mouse button selects a grid section; right mouse button clears a grid section. Selected areas are highlighted in red.

- ***Show privacy mask:*** Lets you toggle the red area indicating privacy masking on and off. Toggling the red area off may provide a less obscured view of the preview image.

- ***Clear***: Lets you clear the privacy masking.

360° LENS

360° lens technology allows viewing of 360° panoramic video through an advanced lens. If a camera is going to use 360° lens technology, you must enable the technology and, in some cases, enter a special license key.

- ***Enable 360° lens*****:** Select check box to enable use of the 360° lens technology and to be able to specify further properties.

- ***Enable panomorph support:*** Select to enable panomorph support. Panomorph is an advanced technology can provide high resolution in zones of interest, while at the same time using fewer pixels than conventional fisheye solutions. In the list, also select whether the camera is located in the ceiling, on a wall or on ground level.

- ***Immervision Enables® panomorph RPL number*:** In the drop down, select the type of 360° lens you require. If you, at some point, want to add additional types of lenses, go to *File* and select *Import new lens types.* Locate the .xml file that contains information about the lens type and press *OK.*

- ***Enable fisheye support:*** Select to enable fisheye support. Fisheye technology uses a wide-angle lens to capture a hemispherical image, which can then be de-warped through configured fisheye settings for the camera in question.

- ***License key*:** If required, enter your special fisheye license key and click *OK*, after which it will be possible to configure fisheye settings for camera(s) attached to the hardware device.

Do I need the special license key, and where do I get it? *Contact your OnSSI vendor for further information.*

PTZ PRESET POSITIONS

PTZ-related properties are only available when you are dealing with a PTZ (Pan/Tilt/Zoom) camera. PTZ preset positions can be used for making the PTZ camera automatically go to a particular position when particular events occur. Preset positions also become selectable in clients, allowing users with required rights to move the PTZ camera between preset positions.

Names of preset positions must contain only the characters A-Z, a-z and the digits 0-9. If you import preset positions from cameras (see the following), verify that their names do not contain other characters; if they do, change the preset position names before importing them.

Restart services after having made changes to PTZ settings.

Cameras that do not support multiple simultaneous video streams will not be able to connect to the surveillance server and the Management Application at the same time; therefore it is recommended to stop the Recording Server service when configuring such devices for motion detection and PTZ.

- ***PTZ type*:** Your configuration options depend on the type of PTZ camera in question:

  - Type 1 (stored on server): You define preset positions by moving the camera using the controls in the upper half of the window, then storing each required position on the RC-P server. You can define up to 25 preset positions this way.

  - Type 2 (imported from camera): You import preset positions which have previously been defined and stored on the PTZ camera itself through the camera's own configuration interface. The number of allowed preset positions depends on the PTZ camera and driver used.

  - Type 3 (stored on camera): You define preset positions by moving the camera with the controls in the upper half of the window, then storing each required position in the camera's own memory. You are able to define up to 25 preset positions this way. If preset positions have already been defined for the camera, you can simply import them for use with RC-P.

For PTZ types 1 and 3, you can move the PTZ camera to required positions:

  - By simply clicking the required position in the camera preview (if supported by the camera).

  - By using the sliders located near the camera preview to move the PTZ camera along each of its axes: the X-axis (for panning left/right), the Y-axis (for tilting up/down), and the Z-axis (for zooming in and out; to zoom in, move the slider towards *Tele;* to zoom out, move the slider towards *Wide*).

- By using the navigation buttons:

↖	Moves the PTZ camera up and to the left
↑	Moves the PTZ camera up
↗	Moves the PTZ camera up and to the right
←	Moves the PTZ camera to the left
⌂	Moves the PTZ camera to its home position (that is default position)
→	Moves the PTZ camera to the right
↙	Moves the PTZ camera down and to the left
↓	Moves the PTZ camera down
↘	Moves the PTZ camera down and to the right
🔍−	Zooms out (one zoom level per click)
🔍+	Zooms in (one zoom level per click)

- ***Import / Refresh*****:** Only available when you have selected PTZ type 2 or 3. Lets you import already defined preset positions from the camera's memory for use with RC-P. If you have already imported preset positions this way, and preset positions have since then been added or changed on the camera, you can use this button to refresh the imported preset positions.

- ***Add New*****:** Only available when you have selected PTZ type 1. When you have move the camera to a required position using the controls in the upper half of the window, type a name for the position in the blank field, then click the button to add the position to the list of defined preset positions.

Remember that names of preset positions must contain only the characters A-Z, a-z and the digits 0-9.

- ***Set New Position*****:** Only available when you have selected PTZ type 1 or 3. Lets you change an already defined preset position. In the list, select the preset position you want to change. Then move the camera to the new required position using the controls in the upper half of the window. Then click the button to overwrite the old position with the new one.

- ***Delete*****:** Only available when you have selected PTZ type 1 or 3. Lets you delete an already defined preset. In the list, select the preset position you want to delete, then click the button.

Before you delete a preset position, make sure it is not used in PTZ on event. Since the preset positions are stored on the camera, you can bring a deleted preset position back into RC-P by clicking the *Import / refresh* button. If you bring back a preset position this way, and the preset position is to be used in PTZ on event, you must manually configure PTZ on event to use the preset position again.

- ***Test*****:** Lets you try out a preset position. In the list, select the preset position you want to test, then click the button to view the camera move to the selected position.

- ⬆ ***and*** ⬇**:** Lets you move a preset position selected in the list up and down respectively. The selected preset position is moved one step per click. By moving preset positions up or down, you can control the sequence in which preset positions are presented in clients.

PTZ ON EVENT

PTZ-related properties are only available when you are dealing with a PTZ (Pan/Tilt/Zoom) camera. When a PTZ camera supports preset positions, it is possible to make the PTZ camera automatically go to a particular preset position when a particular event occurs.

When associating events with preset positions on a PTZ camera, you are able to select between **all** events defined on your RC-P system; you are not limited to selecting events defined on a particular hardware device.

1. In the *Events* list in the left side of the window, select the required event.
2. In the *PTZ Preset Position* list in the right side of the window, select the required preset position.

For this purpose, you can only use an event once per PTZ camera. However, different events can be used for making the PTZ camera go to the same preset position. Example:

- Event 1 makes the PTZ camera go to preset position A
- Event 2 makes the PTZ camera go to preset position B
- Event 3 makes the PTZ camera go to preset position A

If you later want to end the association between a particular event and a particular preset position, simply clear the field containing the event.

Restart services after having made changes to PTZ settings.

Cameras that do not support multiple simultaneous video streams will not be able to connect to the surveillance server and the Management Application at the same time; therefore it is recommended to stop the Recording Server service when configuring such devices for motion detection and PTZ. See also View Video from Cameras in Management Application.

Events, Input & Output

OVERVIEW OF EVENTS, INPUT & OUTPUT

Hardware input, such as door sensors, etc. can be attached to input ports on hardware devices. Input from such external hardware input units can be used for generating events in RC-P.

Events of various types (see the following for details) can be used for automatically triggering actions in RC-P. Examples of actions: starting or stopping recording on cameras, switching to a particular video frame rate, triggering e-mail notifications, making PTZ cameras move to specific preset positions, etc. Events can also be used for activating hardware output.

Hardware output units can be attached to output ports on many hardware devices, allowing you to activate lights, sirens, etc. from RC-P. Such hardware output can be activated automatically by events, or manually from clients.

- **Event Types**
  - **Hardware input events:** Events based on input from hardware input units attached to hardware devices are called hardware input events.

    Some hardware devices have their own capabilities for detecting motion, for detecting moving and/or static objects, etc. (configured in the hardware devices' own software; typically by accessing a browser-based configuration interface on the hardware device's IP address). When this is the case, RC-P considers such detections as input from the hardware, and you can use such detections as input events as well.

Lastly, hardware input events can be based on RC-P detecting motion in video from a camera, based on RC-P's motion detection settings. This type of hardware input events is also called system motion detection events or VMD (Video Motion Detection) events. In earlier RC-P versions, VMD events were an event type of their own; now they are simply considered a type of hardware input event.

- **Manual events:** Events may be generated manually by users selecting them in their clients. These events are called manual events.
- **Timer events:** Timer events are separate events, triggered by the hardware input event or manual event under which they are defined. Timer events occur a specified number of seconds or minutes after the event under which they are defined has occurred. Timer events may be used for a wide variety of purposes, typically for stopping previously triggered actions. Examples:
  - A camera starts recording based on a hardware input event, for example when a door is opened; a timer event stops the recording after 15 seconds
  - Lights are switched on and a camera starts recording based on a manual event; a timer event stops the recording after one minute, and another timer event switches the lights off after two minutes

- **Consider the Following**

  Before you specify use of hardware input and hardware output units on a hardware device, verify that sensor operation is recognized by the hardware device. Most hardware devices are capable of showing this in their configuration interfaces, or via CGI script commands. Also check the RC-P release notes to verify that input and output controlled operations are supported for the hardware device and firmware used.

- **Moving on**

  You do not have to configure hardware input units separately, any hardware input units connected to hardware devices are automatically detected when you add the hardware devices to RC-P. The same goes for hardware output, but hardware output does require some simple configuration in RC-P.

  Before configuring events of any type, **configure general event handling**, such as which ports RC-P should use for event data. Normally, you can just use the default values, but it is a good idea to verify that your organization is not already using the ports for other purposes. See Configure General Event Handling.

  When you are ready to **configure events**, see Add a Hardware Input Event and Add a Manual Event. If you want to use timer events with your other events, see Add a Timer Event.

Configure General Event Handling

Before configuring events of any type, configure general event handling, such as which ports RC-P should use for event data. Normally, you can just use the default values, but it is a good idea to verify that your organization is not already using the ports for other purposes.

1. In the Management Application's navigation pane, expand *Advanced Configuration*, right-click *Events and Output*, and select *Properties.*

2. Specify required properties. When ready, click *OK.*

3. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

ADD A HARDWARE INPUT EVENT

With hardware input events, you can turn input received from input units attached to hardware devices into events in RC-P.

Before you specify input for a hardware device, verify that sensor operation is recognized by the hardware device. Most hardware devices are capable of showing this in their configuration interfaces, or via CGI script commands. Also check the release notes to verify that input-controlled operation is supported for the hardware device and firmware used.

To add and/or configure a hardware input event, do the following:

1. In the Management Application's navigation pane, expand *Advanced Configuration,* then expand *Events and Output.* Right-click *Hardware Input Events* and select *Enable New Input Event*.

2. In the *Hardware Input Event Properties* window's list of hardware devices, expand the required hardware device to see a list of pre-defined hardware input.

3. Select the required types of input to use them as events. The types of input often vary from camera to camera. If motion detection is enabled in RC-P for the camera in question, note the input type *System Motion Detection*, which lets you turn detected motion in the camera's video stream into an event. In earlier RC-P versions, this was known as a VMD event.

   Note that some types of input are mutually exclusive. When you select one type of input, you may therefore note that other types of input become unavailable for selection.

4. For each selected type of input, select required properties. When ready, click *OK*, or click the *Add button* to add a timer event to the event you have just created.

5. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

ADD A MANUAL EVENT

With manual events, your users with required rights can trigger events manually from their clients. Manual events can be global (shared by all cameras) or tied to a particular camera (only available when the camera is selected). You can use manual events for a wide variety of purposes, for example:

- As start and stop events for use when scheduling cameras' online periods. For example, you can make a camera start or stop transferring video to the surveillance system based on a manual event.

- As start and stop events for controlling other camera settings. For example, you can make a camera use a higher frame rate based on a manual event or you can use a manual event for triggering PTZ on event.

- For triggering output. Particular output can be associated with manual events.

- For triggering event-based e-mail notifications.

- In combinations. For example, a manual event could make a camera start transferring video to the surveillance system while an output is triggered and an e-mail notification is sent to relevant people.

To add a manual event, do the following:

1. In the Management Application's navigation pane, expand *Advanced Configuration,* then expand *Events and Output.* Right-click *Manual Events* and select *Add New Manual Event*
2. In the list in the left side of the *Manual Event Properties*, select global or a camera as required.
3. Click the *add* button and specify required properties. When ready, click *OK*, or click the *Add* button again to add a timer event to the event you have just created.
4. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

ADD A TIMER EVENT

Timer events are separate events, triggered by the **hardware input event** or **manual event** under which they are defined. Timer events occur a specified number of seconds or minutes after the event under which they are defined has occurred. Timer events may be used for a wide variety of purposes, typically for stopping previously triggered actions. Examples:

- A camera starts recording based on a hardware input event, for example when a door is opened; a timer event stops the recording after 15 seconds
- Lights are switched on and a camera starts recording based on a manual event; a timer event stops the recording after one minute, and another timer event switches the lights off after two minutes

To add a timer event, select any event you have previously configured, click the *Add* button, and specify required properties. When ready, click *OK*, and save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

ADD A HARDWARE OUTPUT

With hardware output, you can add external output units, such as lights, sirens, door openers, etc., to your RC-P system. Once added, output can be activated automatically by events or detected motion, or manually by client users.

Before you specify output, verify that sensor operation is recognized by the hardware device with which you are going to use the output. Most hardware devices are capable of showing this in their configuration interfaces, or via CGI script commands. Also check the release notes to verify that output-controlled operation is supported for the hardware device and firmware used.

To add a hardware output event, do the following:

1. In the Management Application's navigation pane, expand *Advanced Configuration,* then expand *Events and Output.* Right-click *Hardware Output* and select *Add New Output*.
2. In the *Hardware Output Properties* window's list of hardware devices, select the required hardware device, and click the *Add* button below the list.
3. Specify required properties.
4. Click *OK*.
5. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

Configure Hardware Output on Event

Once you have added hardware output, such as lights, sirens, door openers, etc., you can associate the hardware output with events. This way, particular hardware output can be activated automatically when events occur. Example: When a door is opened (hardware input event), lights are switched on (hardware output).

When making the associations, you can select between **all** output and events defined on your RC-P server; you are not limited to selecting output or events defined on particular hardware devices.

1. In the Management Application's navigation pane, expand *Advanced Configuration,* then expand *Events and Output.* Right-click *Output Control on Event* and select *Properties*.
2. In the *Event* column, select the required event.
3. In the *Output* column, select the hardware output you want to be activated by the event.
4. Click *OK*.
5. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

You can use a single event for activating more than one output.

You cannot delete associations, but you can change your selections or select *None* in both columns as required.

General Event Properties

Ports & Polling - General Event Properties

The *General Event Properties* window lets you specify network settings to be used in connection with event handling.

- ***Alert port*****:** Lets you specify port number to use for handling events. Default port is port 1234.
- ***SMTP event port*****:** Lets you specify port number to use for sending event information from hardware devices to RC-P via SMTP. Default port is port 25.
- ***FTP event port*****:** Lets you specify port number to use for sending event information from hardware devices to RC-P via FTP. Default port is port 21.
- ***Polling interval [1/10] second*****:** For a small number of hardware devices, primarily dedicated input/output devices, it is necessary for RC-P to regularly check the state of the hardware devices' input ports in order to detect input. Such state checking at regular intervals is called polling. You can specify (in tenths of a second) the interval between state checks. Default value is 10 tenths of a second (that is one second). For dedicated input/output devices, it is highly recommended that the polling frequency is set to the lowest possible value (one tenth of a second between state checks). For information about which hardware devices require polling, see the release note.

Event- & Output-specific Properties

Hardware Input Event

When adding hardware input events, some properties depend on the selected type of input:

- ***Enable*****:** Select check box to use selected type of input as an event in RC-P, and specify further properties.
- ***Event name*****:** Specify a name for the event. Hardware input event names must be unique, and must not contain the following characters: < > & ' " \ / : * ? | [ ]

Some cameras only support event names of a certain length and/or with a certain structure. Refer to the camera's documentation for exact details.

- ***Images from camera*****:** Only relevant if using pre- and post-alarm images, a feature available for selected cameras only; it enables sending of images from immediately before an event took place from the camera to the surveillance system via e-mail. Pre- and post-alarm images should not be confused with RC-P's own pre- and post-recording feature. Lets you select which camera you want to receive pre- and/or post-alarm images from.
- ***Number of pre-alarm images*****:** Only relevant if using pre-alarm images, a feature available for selected cameras only. Specify required number of pre-alarm images. Allowed number may differ from camera to camera; allowed range is displayed to the right of the field.
- ***Frames per second*****:** Only relevant if using pre-alarm images, a feature available for selected cameras only. Specify required frame rate. Used in combination with the *Number of pre-alarm images* field, this field indirectly allows you to control how long before the event you want to receive pre-alarm images from.
- ***Send e-mail if this event occurs*****:** Only available if e-mail notification is enabled. Select if RC-P should automatically send an e-mail when the event occurs. Recipients are defined as part of the e-mail notification configuration. When using e-mail notifications, also keep in mind individual cameras' scheduling.
- ***Attach image from camera*****:** Only available if e-mail notification is enabled. Select to include an image—recorded at the time the event is triggered—in the e-mail notification, then select the required camera in the list next to the check box.
- ***Delete*****:** Lets you delete a selected timer event.
- ***Add*****:** When a specific hardware input event is selected, clicking *Add* will add a timer event to the selected hardware input event.

Manual Event

When adding manual events , specify the following properties:

- ***[List of defined global events and cameras]*****:** Contains a *Global* node and a list of all defined cameras. You can configure as many manual events as required, no matter whether they are global or camera-specific. A + sign next to the *Global* node indicates that one or more global manual events have already been configured. A + sign next to a camera indicates that one or more manual events have already been configured for that camera.
- ***Event name*****:** Specify a name for the event; this is the name that client users will see. Manual event names must be unique, and must not contain the following characters: < > & ' " \ / : * ? | [ ]

Some cameras only support event names of a certain length and/or with a certain structure. Refer to the camera's documentation for exact details.

- ***Send e-mail if this event occurs*:** Only available if e-mail notification is enabled. Select if RC-P should automatically send an e-mail when the event occurs. Recipients are defined as part of the e-mail notification configuration. When using e-mail notifications, also keep in mind individual cameras' scheduling.

- ***Attach image from camera*:** Only available if e-mail notification is enabled. Select to include an image—recorded at the time the event is triggered—in the e-mail notification, then select the required camera in the list next to the check box.

- ***Delete*:** Lets you delete a selected event.

TIMER EVENT

When adding timer events , specify the following properties:

- ***Timer event name*:** Specify a name for the event. Timer event names must be unique, and must not contain the following characters: < > & ' " \ / : * ? | [ ]

> Some cameras only support event names of a certain length and/or with a certain structure. Refer to the camera's documentation for exact details.

- ***Timer event occurs after*:** Lets you specify the amount of time that should pass between the main event occurring and the timer event (in seconds or minutes).

HARDWARE OUTPUT

When adding hardware output , specify the following properties:

- ***Output name*:** Specify a name for the event. If you are going to make the hardware output available for manual activation in clients, this is the name that client users will see. Hardware output names must be unique, and must not contain the following characters: < > & ' " \ / : * ? | [ ]

> Some hardware devices only support hardware output names of a certain length and/or with a certain structure. Refer to the hardware device's documentation for exact details.

- ***Output connected to*:** Lets you select which of the hardware device's output ports the output is connected to. Many hardware devices only have a single output port; in that case simply select *Output 1*.

- ***Keep output for*:** Lets you specify the amount of time for which the output should be applied. Specify the required amount of time in either 1/10 seconds or seconds.

> Some hardware devices are only able to apply output for a relatively short time, for example for up to five seconds. Refer to the documentation for the hardware device in question for exact information.

Hardware Devices

ADD HARDWARE DEVICES

You add cameras and other hardware devices, such as video encoders, to your RC-P system through the Add Hardware Devices... wizard. If microphones are attached to a hardware device, they are automatically added as well.

RC-P You are allowed to use up to 26 cameras. You are allowed to use up to 48 cameras. Note that, if required, it is possible to *add* more cameras than you are allowed to use. If using video encoder devices on your system, keep in mind that many video encoder devices have more than one camera connected to them. For example, a fully used four-port video encoder will count as four cameras.

The wizard offers you four different ways of adding cameras:

- **Express (recommended):** Quickly scans your network for devices, and helps you quickly add them to your system. This method is quick and easy since it only scans for devices supporting device discovery, and only on the part of your network (subnet) where the RC-P server itself is located. Device discovery is a method with which hardware devices make information about themselves available on the network. Based on such information, RC-P can recognize relevant hardware devices on your network, and thus include, for example, cameras, but not printers, in the scan. To use the Express method, your RC-P server and your cameras must be on the same layer 2 network, that is a network where all servers, cameras, etc. can communicate without the need for a router. See Add Hardware Devices Wizard - Express.

- **Advanced:** Scans your network for hardware devices based on your specifications regarding required IP ranges, discovery methods, drivers, and device user names and passwords. See Add Hardware Devices Wizard - Advanced.

- **Manual:** Lets you specify details about each hardware device separately. A good choice if you only want to add a few hardware devices, and you know their IP addresses, required user names and passwords, etc. See Add Hardware Devices Wizard - Manual.

- **Import from CSV file:** Lets you import data about cameras as comma-separated values from a file; an effective method if setting up several similar systems. See Add Hardware Devices Wizard - Import from CSV File.

Configure Hardware Devices

Once you have added hardware devices, you can specify/edit device-specific properties, such as the IP address, which video channels to use, which COM ports to use for controlling attached PTZ (Pan/Tilt/Zoom) cameras, whether to use 360° lens technology, etc.

1. In the Management Application's navigation pane, expand *Advanced Configuration*, expand *Hardware Devices*, right-click the required hardware device, and select *Properties*

2. Specify Name & Video Channels, Network, Device Type & License, PTZ Device, and 360° Lens properties as required.

3. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

Use Dedicated Input/Output Devices

It is possible to add a number of dedicated input/output (I/O) hardware devices to RC-P (see Add Hardware Devices). For information about which I/O hardware devices are supported, see the release notes.

When such I/O hardware devices are added, input on them can be used for generating events in RC-P, and events in RC-P can be used for activating output on the I/O hardware devices. This means that I/O hardware devices can be used in your events-based system setup in the same way as a camera.

When using some I/O hardware devices it is necessary for the surveillance system to regularly check the state of the hardware devices' input ports in order to detect whether input has been received. Such state checking at regular intervals is called *polling*. The interval between state checks, called a *polling frequency*, is specified as part of RC-P's general ports & polling properties. For such I/O hardware devices, the polling frequency should be set to the lowest possible value (one tenth of a second between state checks). For information about which I/O hardware devices require polling, see the release notes.

Replace a Hardware Device

If required, you can replace a hardware device—which you have previously added to and configured on your surveillance system—with a new one. This can typically be relevant if you replace a physical camera on your network.

The Replace Hardware Device wizard helps you through the entire replacement process on the surveillance system server, including:

- Detecting the new hardware device
- Specifying license for the new hardware device
- Deciding what to do with existing recordings from the old hardware device

You access the Replace Hardware Device wizard from the Management Application's navigation pane: Expand *Advanced Configuration*, expand *Hardware Devices*, right-click the hardware device you want to replace, and select *Replace Hardware Device*.

You can access also the wizard when dealing with a hardware device's Network, Device Type & License properties.

DELETE HARDWARE DEVICES

IMPORTANT: Deleting a hardware device will not only delete all cameras and microphones attached to the hardware device. It will also delete any recordings from cameras on the hardware device.

1. In the Management Application's navigation pane, expand *Advanced Configuration*, expand *Hardware Devices*, right-click the hardware device you want to delete, and select *Delete Hardware device*.
2. Confirm that you want to delete the hardware device and all its recordings.
3. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.
4. Restart the Recording Server service.

If you find that deleting a hardware device is not the right thing to do, consider disabling the individual cameras or microphones connected to the hardware device instead:

1. In the Management Application's navigation pane, expand *Advanced Configuration*, expand *Hardware Devices*, and expand the hardware device in question.
2. Right-click the camera or microphone you want to disable, and select *Disable*.
3. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.
4. Restart the Recording Server service.

Wizard

ADD HARDWARE DEVICES WIZARD: EXPRESS

The Express option scans your network for relevant hardware devices, and helps you quickly add them to your system. With the Express option, the wizard only scans for hardware devices supporting device discovery, and only on the part of your network (subnet) where the RC-P server itself is located.

What is device discovery? *Device discovery is a method with which hardware devices make information about themselves available on the network. Based on such information, RC-P can quickly recognize relevant hardware devices, such as cameras and video encoders, and include them in the scan.*

To use the Express method, **your RC-P server and your cameras must be on the same layer 2 network**; that is a network where all servers, cameras, etc. can communicate without the need for a router. The reason for this is that device discovery relies on direct communication between the RC-P server and the cameras. If you know that routers are used on your network, use the advanced or manual method instead.

When using the Express option, the wizard is divided into a number of pages:

- Hardware Detection and Verification
- Overview and Names

ADD HARDWARE DEVICES WIZARD: ADVANCED

The Advanced option scans your network for relevant hardware devices based on your specifications regarding required IP ranges, discovery methods, drivers, and device user names and passwords.

When using the Advanced option, the wizard is divided into a number of pages:

- Device Discovery, IP Ranges, Drivers and Authentication
- Detected and Verified Hardware Devices
- Overview and Names

ADD HARDWARE DEVICES WIZARD: MANUAL

The Manual option lets you specify details about each hardware device separately. A good choice if you only want to add a few hardware devices, and you know their IP addresses, required user names and passwords, etc.

When using the Manual option, the wizard is divided into a number of pages:

- Hardware Device Information, Driver Selection and Verification
- Overview and Names

ADD HARDWARE DEVICES WIZARD: IMPORT FROM CSV FILE

This option lets you import data about hardware devices and cameras as comma-separated values (CSV) from a file; a highly effective method if setting up several similar systems.

First select whether cameras and the RC-P server is online (that is having working network connections) or offline.

Then point to the CSV file, and click *Next*.

- **CSV File Format and Requirements**

  The CSV file must have a header line (determining what each value on the subsequent lines is about), and subsequent lines must each contain information about one hardware device only. A minimum of information is always required for each hardware device, but note that the minimum required information is different depending on whether your server and cameras are online or offline.

  Cameras and Server Are Online
  If cameras and server are **online**, required information is:

  - ***HardwareAddress***
    IP address of the hardware device.
  - ***HardwarePort***
    Port to use for HTTP communication with the hardware device. Default is port 80.

- ***HardwarePassword***
  Password for the hardware device's administrator account. Most organizations use their own passwords rather than device manufacturers' passwords.

Camera and Server Are Offline
If cameras and server are **offline**, required information is:

- ***HardwareAddress***
  IP address of the hardware device.
- ***HardwareMacAddress***
  MAC address of the hardware device. Examples of valid MAC address formats: 0011D81187A9, 0011d81187a9, 00:11:D8:11:87:A9, 00-11-D8-11-87-A9
- ***HardwareDriverID***
  A numerical ID used for identifying which video device driver to use for the hardware device in question. For information about how to find the right ID for your devices, see Hardware Driver IDs.
- ***HardwarePort***
  Port to use for HTTP communication with the hardware device. Default is port 80.
- ***HardwarePassword***
  Password for the hardware device's administrator account. For security reasons most organizations use their own passwords rather than device manufacturers' passwords.

Optional Parameters
You can furthermore include these optional parameters, regardless whether cameras and server are online or offline:

- ***HardwareUserName*** and ***HardwarePassword***
  User name for the hardware device's administrator account. If you do not specify a user name, RC-P will use the device manufacturer's default user name for each hardware device. Many organizations use the hardware device manufacturers' default user names for their hardware devices. If that is the case in your organization, there is no need to painstakingly type hardware device manufacturers' default user names as this can be a source of error; trust that RC-P will know the manufacturers' default user names. Note that you must always specify a password (the *HardwarePassword* parameter) even when it is not necessary to specify user name.

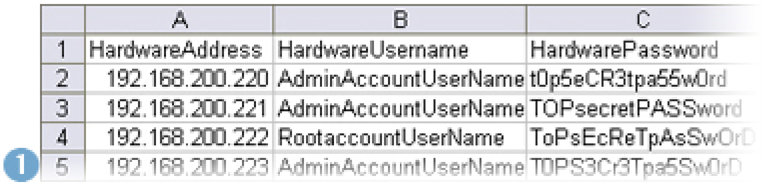
  If the extremely rare cases where the user name for a hardware device is [blank], you cannot use the CSV method, since the method interprets no password as “use the hardware device manufacturer's default password.” If the user name for a hardware device is [blank], use the wizard's *Manual* method instead; with the *Manual* method you can use a [blank] user name.

- ***HardwareDeviceName***
  Name of the hardware device. Name must unique, and must not contain any of the following special characters: < > & ' " \ / : * ? | [ ]
- ***CameraName[number]***
  Name of the camera. Must appear as *CameraName1*, *CameraName2*, etc. in the header line since a hardware device can potentially have more than one camera attached. Names must unique, and must not contain any of the following special characters: < > & ' " \ / : * ? | [ ]
- ***CameraShortcut[number]***
  Number for keyboard shortcut access to the camera in the Ocularis Client . Must appear as *CameraShortcut1*, *CameraShortcut2*, etc. in the header line since a hardware device can potentially have more than one camera attached. A camera shortcut number must not contain any letters or special characters, and must not be longer than eight digits.
- ***PreBufferLength[optional number]***
  Required length (in seconds) of pre-recording. If specified as, for example, *PreBufferLength1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
- ***PostBufferLength[optional number]***
  Required length (in seconds) of post-recording. If specified as, for example,

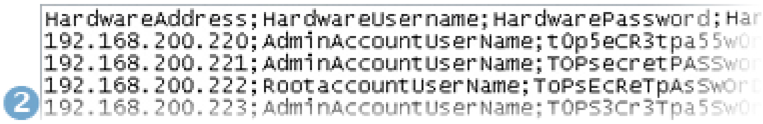
PostBufferLength1, information relates to a specific camera, otherwise to all cameras attached to the hardware device.

- ***RecordingPath[optional number]***
  Path to the folder in which a camera's database should be stored. If specified as, for example, *RecordingPath1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
- ***ArchivePath[optional number]***
  Path to the folder in which the camera's archived recordings should be stored. Remember that an archiving path is only relevant if not using dynamic paths for archiving. If specified as, for example, *ArchivePath1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
- ***RetentionTime[optional number]***
  Required retention time (in minutes). Remember that retention time is the total of recording time plus archiving time. If specified as, for example, *RetentionTime1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
- ***MjpegLiveFrameRate[optional number]***
  Required MJPEG live frame rate (in number of frames; depending on what has been configured on the camera, it will then know whether it is frames per second, minute, or hour). If specified as, for example, *MjpegLiveFrameRate1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
- ***MjpegRecordingFrameRate[optional number]***
  Required MJPEG recording frame rate (in number of frames; depending on what has been configured on the camera, it will then know whether it is frames per second, minute, or hour). If you need to specify a value which includes a decimal separator, use the full stop character (example: 7.62). If specified as, for example, *MjpegRecordingFrameRate1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
- ***MotionSensitivity[optional number]***
  A value between 0-256; corresponds to using the *Sensitivity* slider when configuring motion detection settings in the Management Application . If specified as, for example, *MotionSensitivity1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
- ***MotionDetectionThreshold[optional number]***
  A value between 0-10000; corresponds to using the *Motion* slider when configuring motion detection settings in the Management Application . If specified as, for example, *MotionDetectionThreshold1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
- ***MotionDetectionInterval[optional number]***
  Lets you specify how often motion detection analysis should be carried out on video from the camera. Specified in milliseconds. The interval is applied regardless of the camera's frame rate settings. If specified as, for example, *MotionDetectionInterval1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.

Most system integrators store hardware device information in spreadsheets like Microsoft Excel, from which they can save the information as comma-separated values in a CSV file. These examples show hardware information in Excel (1) and when exported to a CSV file (2); note the header lines:



	A	B	C
1	HardwareAddress	HardwareUsername	HardwarePassword
2	192.168.200.220	AdminAccountUserName	t0p5eCR3tpa55w0rd
3	192.168.200.221	AdminAccountUserName	TOPsecretPASSword
4	192.168.200.222	RootaccountUserName	ToPsEcReTpAsSwOrD
5	192.168.200.223	AdminAccountUserName	T0PS3Cr3Tpa5Sw0rD



```
HardwareAddress;HardwareUsername;HardwarePassword;Har
192.168.200.220;AdminAccountUserName;tOp5eCR3tpa55wOr
192.168.200.221;AdminAccountUserName;TOPsecretPASSwor
192.168.200.222;RootaccountUserName;ToPsEcReTpAsSwOrD
192.168.200.223;AdminAccountUserName;TOPS3Cr3Tpa5SwOr
```

Whichever method is used, the following applies:

- The first line of the CSV file must contain the headers, and subsequent lines must contain information about one hardware device each
- Separators can be commas, semicolons or tabs, but cannot be mixed
- All lines must contain valid values—pay special attention to the fact that camera names, user names, etc. must be unique, and must not contain any of the following special characters: < > & ' " \ / : * ? | [ ]
- There is no fixed order of values, and optional parameters can be omitted entirely
- Boolean fields are considered true unless set to 0, false or no
- Lines containing only separators are ignored
- Empty lines are ignored
- Even though the CSV file format is generally ASCII only, Unicode identifiers are allowed; even without Unicode identifiers, the entire file or even individual characters are allowed to be Unicode strings

If you need to include separator characters in a value—for example if a camera name is Reception; Camera 1—you can encapsulate the value in quotes to indicate that the separator should not be interpreted as separating values in the file. Such quote-encapsulated values are interpreted as they appear. If a separator, a quote or a space is needed in a value, the whole value has to be encapsulated in quotes. Leading and trailing spaces outside the quote-encapsulated value are removed, while spaces inside the quote-encapsulated value are maintained. No characters (except spaces) are allowed outside the quote-encapsulated value. A double quote inside a quote-encapsulated value is interpreted as a single quote. Nested quotes (quotes inside quotes) are not allowed.

Some examples (using semicolon as the separator):

- "camera"; is interpreted as camera
- "cam;""era"; is interpreted as cam;"era
- """camera"""; is interpreted as "camera"
- ""; is interpreted as an empty string
- ...; "   cam"" era "   ;... is interpreted as | cam" era | (where | is not part of the interpretation but only used to show the start and end of the interpretation)
- ""camera; is not valid as there are characters outside the quote-encapsulated value
- "cam" "era"; is not valid as the two quotes are separated with a space and quotes cannot be nested
- "cam"er"a"; is not valid as you cannot nest quotes
- cam"era"; is not valid as there are characters outside the quotes

REPLACE HARDWARE DEVICE WIZARD

The Replace Hardware Device wizard helps you replace a hardware device—which you have previously added to and configured on your surveillance system—with a new one. The wizard is divided into two pages:

- New Hardware Device Information
- Database Action

Properties

NAME & VIDEO CHANNELS

When configuring hardware devices , specify the following properties:

- ***Hardware name*****:** Name of the hardware device as it will appear in the Management Application. If required, you can overwrite the existing hardware device name with a new one. Hardware device names must be unique, and must not contain any of the following special characters: < > & ' " \ / : * ? | [ ]

- ***Video channel # enabled*****:** Lets you enable/disable each of the selected hardware device's video channels. Many hardware devices only have a single video channel, in which case only one channel will be listed. Other hardware devices—typically video encoder devices—have several video channels.

Why are some of the channels unavailable? *This will be the case if you are not licensed to use all of a video encoder device's channels. Example: You have a video encoder device with four channels, but your license for the device only allows you to use two of them. In that case, you will only be able to have two channels enabled at a time; the two other channels will be disabled. Note that you are free to select which two channels you want to enable.*

NETWORK, DEVICE TYPE & LICENSE

When configuring hardware devices , specify the following properties:

- ***Address*****:** IP address or host name of the hardware device.

- ***HTTP port*****:** Port to use for HTTP communication with the hardware device. Default is port 80. To use the default port, select ***Use default HTTP port***.

- ***FTP port*****:** Port to use for FTP communication with the hardware device. Default is port 21. To use the default port, select ***Use default FTP port***.

- ***User name*****:** User name for the hardware device's administrator account. Many organizations use the hardware device manufacturer's default user names for their hardware devices. If that is the case in your organization, select <*default*> (do not type a manufacturer's default user name as this can be a source of error; trust that RC-P will know the manufacturer's default user name). Other typical user names, such as *admin* or *root* are also selectable from the list. If requiring a user name which is not on the list, simply type the required user name.

- ***Password*****:** Password for the hardware device's administrator account, also known as the root password.

- ***Hardware type*****:** Read-only field displaying the type of video device driver used for communication with the hardware device.

- ***Serial number (MAC address)*****:** Read-only field displaying the serial number of device. The serial number is usually identical to the 12-character hexadecimal MAC address of the hardware device (example: 0123456789AF).

- ***License information:*** The current license status for the hardware.

- ***Replace Hardware Device*****:** Opens a wizard, with which you—if required—can replace the selected hardware device with another one. This can typically be relevant if you replace a physical camera on your network. The wizard helps you take all relevant issues into account: for example, deciding what to do with recordings from cameras attached to the old hardware device, etc.

PTZ DEVICE

The *PTZ Device* tab is only available if configuring video encoder hardware devices on which the use of PTZ (Pan/Tilt/Zoom) cameras is possible:

- ***Connected cameras have Pan/tilt/Zoom capabilities*****:** Select check box if any of the cameras attached to the video encoder device is a PTZ camera.

- ***PTZ type on COM#*****:** If a PTZ camera is controlled through the COM port (also known as serial port) in question, select the required option. Options are device-specific, depending on which PTZ protocols are used by the device in question. If no PTZ cameras are controlled through the COM port in question, select *None*.

  Some of the options concern absolute and relative positioning. What is that? *Absolute positioning is when the PTZ camera is controlled based on a single fixed position, against which all other positions are measured. Relative positioning is when the PTZ camera is controlled relative to its current position.*

The table in the lower half of the dialog contains a row for each video channel on the hardware device. First row from the top corresponds to video channel 1, second row from the top corresponds to video channel 2, etc.

- ***Name*****:** Name of the camera attached to the video channel in question.

- ***Type*****:** Lets you select whether the camera on the selected camera channel is fixed or moveable:

  - ***Fixed*****:** Camera is a regular camera mounted in a fixed position

  - ***Moveable*****:** Camera is a PTZ camera

- ***Port*****:** Available only if *Moveable* is selected in the *Type* column. Lets you select which COM port on the video encoder to use for controlling the PTZ camera.

- ***Port Address*****:** Available only if *Moveable* is selected in the *Type* column. Lets you specify port address of the camera. The port address will normally be *1*. If using daisy chained PTZ cameras, the port address will identify each of them, and you should verify your settings with those recommended in the documentation for the camera.

Licenses

OVERVIEW OF LICENSES

When you purchase RC-P, you also purchase a certain number of licenses for device channels. Device channels are typically cameras but could also be dedicated input/output boxes.

When you have installed the various RC-P components, configured the system, and added recording servers and cameras through the Management Application, the surveillance system initially runs on temporary licenses that need to be activated before a certain period ends. This is called the grace period.

If grace periods have expired on one or more of your devices **and** no licenses have been activated, recording servers and cameras will not send data to the surveillance system. We therefore recommend that you activate your licenses before you make final adjustments to your system and its devices.

Tip: When short of licenses—until you get additional ones—you can disable some less important cameras to allow some of the new cameras to run instead. To disable or enable a camera, expand Hardware Devices in the Management Application's navigation pane. Select the required hardware device, right-click the relevant camera, and then select Enable or Disable.

- **Which Devices Require a License?**

  You need licenses for the number of device channels—typically cameras or dedicated input/out boxes—you want to run on your RC-P system. One device channel license enables you to run one camera or one dedicated input/output box. You can use and define an unlimited number of microphones, inputs, and outputs.

  Depending on your current number of licenses you might be able to get more licenses as your surveillance system grows. See *Getting Additional Licenses* in the following.

- **Replacing Cameras**

  You can replace a camera licensed in the RC-P system with a new camera and have the new camera activated and licensed instead.

  The total number of purchased device channels corresponds to the total number of cameras able to run on the surveillance system simultaneously. If you remove a camera from a recording server, you also free a license.

  When replacing a camera, you must use the Management Application's *Replace Hardware Device* wizard to map all relevant databases of cameras, microphones, inputs, outputs, etc. When done, remember to activate the license.

- **Viewing Your License Information**

  You get an excellent overview of your RC-P licenses from the Management Application's navigation pane. Expand *Advanced Configuration* and select *Hardware Devices.* This presents you with the *Hardware Device Summary* table:

  - **Hardware Device Name:** Hardware devices (typically cameras but could also be dedicated input/output boxes).
  - **License:** Licensing status of your hardware devices. Can be either *Licensed*, *[number of] day(s) grace, Trial,* or *Expired*.
  - **Video Channels:** Number of available video channels on your hardware devices.
  - **Licensed Channels:** Number of video channels—on each of your hardware devices—for which you have a license.

- **Microphone Channels:** Number of available microphone channels on your hardware devices.
- **Address:** http addresses of your hardware devices.
- **WWW:** Links to http addresses of your hardware devices.
- **Port:** Port used by your hardware devices.
- **Device Driver:** Names of device drivers associated with your hardware devices.

You can activate licenses online or offline. On the Management Application's toolbar, click *File* and either *Activate License Online* or *Manage License Offline.*

- **Getting Additional Licenses**
  Want to add—or have already added—more device channels than you currently have licenses for? In that case, you must buy additional licenses before the cameras will be able to send data to your RC-P system.

  To get additional licenses for your RC-P system, contact your integrator or dealer.

  When your license file (.lic) is updated, you can activate your licenses. See Activate Licenses for more information on activating.

MANAGE LICENSES

When you purchase your surveillance system, you will receive a temporary license file (.lic) for the recorder, a recorder Software License Code (SLC) and a Base SLC. You must use the temporary license file when installing the recording component software.

License activation can be done in two ways: **online** or **offline**.

Tip: If the computer running the Management Application has internet access, use online activation for a quick and convenient activation procedure.

You cannot activate more licenses than you have purchased. If you have added more cameras than you have licenses for, you must buy additional licenses before you can activate them.

Tip: To get an overview of your licenses, go to the Management Application's navigation pane, expand *Advanced Configuration,* select *Hardware Devices* and view your *Hardware Device Summary* table.

In the following examples, it is assumed that the recording component is installed with a temporary license (.lic) file.

- **Activate License - Online**

  Precondition: Add at least one device to your RC-P system.

  This will start the grace period of 30 days for the device in question. You must activate a license for the device before the end of the grace period.

  Activate a License
  On the Management Application's menu, click *File*, *Activate License Online*.

  1. Specify how many licenses you want for each device, and click *OK.*
  2. Next:
     - If you are **an existing user**, enter your user name and password to log in to the licensing portal.
     - If you are **a new user,** click the *Create new user...* link to set up a new user account in the licensing portal and follow the registration procedure.

3. When done, click *Activate*.

4. When your temporary license file (.lic) is successfully updated, click *Close*.

5. Your license file (.lic) is now updated and permanent (updates are visible in your *Hardware Device Summary* table).

Activate using this process each time you add a new device.

o If You Receive an Online Activation Error Message

Under rare circumstances, you may receive one of the following error messages during online activation. Should you receive one, the following list of *Problems* and *What to do* will help you identify the problem:

Unable to access license server, Error activating license, License not allowed, Feature not registered, Feature already in use, Failed to login.

- **Problem:** Online activation was not possible, either due to a problem on the online activation server itself, a problem with your connection to the online activation server, or to a problem with the specified information (such as username or password).

- **What to do:** Contact OnSSI Support (support@onssi.com), who will investigate the issue for you. If activation has already taken place on another system, activation should not be necessary, as another system is already running with your activated licenses. If you believe that this is wrong, contact OnSSI Support (support@onssi.com), who will investigate the issue for you.

• Activate License - Offline

Precondition: Add at least one device to your RC-P system.

This will start the grace period of 30 days for the device in question. You must activate a license for the device before the end of the grace period.

Step 1: Export License for Activation (Offline)
To export a license file with your currently added devices for activation, do the following:

1. On the Management Application's toolbar, click *File*, *Manage License Offline, Export License for Activation.*

2. Specify how many licenses you want for each device, and click *OK.*

3. Specify a file name and location for the license request (.lrq) file (automatically generated by RC-P). If the computer you are working from does not have internet access, use external, removable data storage.

4. Email the .lrq file as an attachment to: support@onssi.com.

How long will this process take? *After sending the .lrq file, turn around time may be up to one hour during regular business hours.*

5. Next, you will receive the updated permanent license file (.lic) via e-mail. Save it to a location accessible from the Management Application.

Step 2: Import License (Offline)
When you have received your permanent license file (.lic) via e-mail and saved it to a location accessible from the Management Application, you are ready to import it to your surveillance system.

1. On the Management Application's toolbar, click *File*, *Manage License Offline*, *Import License*, and select your saved .lic file to import it.

2. When the permanent license file is successfully imported, click *OK.*

Activate using both step 1 and 2 in this process each time you add a new device.

- **Activate License after Grace Period**

  If the grace period is exceeded before activation, all cameras that are not activated within the given period will become unavailable and will not be able to send data to the surveillance system.

  If you exceed the grace period before you activate a license, the license is not lost. You can activate the license as usual.

  Configuration, added cameras, and other settings will not be removed from the Management Application if a license is activated too late.

- **Change SLC**

  If—for some reason—you need to change your SLC and have received a new permanent license file (.lic) via e-mail and saved it to a location accessible from the Management Application, you are ready to import it to your surveillance system.

  1. On the Management Application's toolbar, click *File*, *Manage License Offline*, *Import License*, and select your saved .lic file to import it.

  2. When the new permanent license file is successfully imported, click *OK.*

Logging

OVERVIEW OF RECORDER LOGS

The recording component is able to generate various logs:

- **Log Types**

  - **Management Application log files.** These files log activity in the Management Application. A new log file is created for each day the Management Application is used. You cannot disable this type of logging. Management Application log files are named according to the structure AdminYYYYMMDD.log, for example Admin20091231.log.

  - **Recording Server service log files.** These files log Recording Server service activity. A new log file is created for each day the service is used. You cannot disable this type of logging. Recording Server service log files are named according to the structure RecordingServerYYYYMMDD.log, for example RecordingServer20091231.log.

  - **Image Server service log files.** These files log activity on the Image Server service. A new log file is created for each day the service is used. You cannot disable this type of logging. Image Server service log files are named according to the structure ISLog_YYYYMMDD.log, for example ISLog_20091231.log.

  - **Image Import service log files.** These files log activity regarding the Image Import service, when this service is used for fetching pre-alarm images, and storing the fetched images in camera databases. Pre-alarm images is a feature available for selected cameras only; it enables sending of images from immediately before an event took place from the camera to the surveillance system via e-mail. A new log file is created for each day the service is used. You cannot disable this type of logging. Image Import service log files are named according to the structure ImageImportLog_YYYMMDD.log, for example ImageImportLog20091231.log.

- **Event log files.** These files log information about registered events in the recorder. A new log file is created for each day on which events occur. You cannot disable this type of logging.

- **Audit log files:** These files log Ocularis Client user activity provided audit logging is enabled. A new log file is created for each day with audit logging enabled and client user activity. Audit log files are named according to the structure is_auditYYYMMDD.log, for example is_audit20091231.log. The _is prefix is due to the fact that the audit log files are generated by the Image Server service. When using Ocularis, remember that the same user account for the recorder is used for all Base users.

- **Log Locations**

  All log files are by default placed in the appropriate *All Users* folder for the operating system used , for example C:\ProgramData\OnSSI\RC-X if running Windows Vista . By default, they are stored there for seven days. Note, however, that log file locations as well as the number of days to store the logs can be changed as part of the logging configuration.

- **Log Structures**

  Most log files generated by RC-P use a shared structure complying with the W3C Extended Log File Format. Each log file consists of a header and a number of log lines:

  - The header outlines the information contained in the log lines.

  - The log lines consist of two main parts: the log information itself as well as an encrypted part. The encrypted part makes it possible—through decryption and comparison—to assert that a log file has not been tampered with.

- **Log Integrity Checks**

  All log files, except Management Application log files, are subjected to an integrity check once every 24 hours. The integrity check is performed by RC-P's Log Check service.

  The result of the integrity check is automatically written to a file named according to the structure LogCheck_YYYYMMDD.log, for example LogCheck_20091231.log. Like the log files themselves, the log check files are by default placed in the appropriate All Users folder for the operating system used, for example C:\ProgramData\OnSSI if running Windows Vista.

  Any inconsistencies will be reported in the form of error messages written in the log check file. Possible error messages (other, non-error, messages may also appear in the log check file):

  - ***Log integrity information was not found. Log integrity can't be guaranteed.*:** The log file could not be checked for integrity.

  - ***Log information does not match integrity information. Log integrity can't be guaranteed.*:** The log file exists, but does not contain the expected information. Thus, log integrity cannot be guaranteed.

  - ***[Log file name] not found*:** The log file was not present.

  - ***[Log file name] is empty*:** The log file was present, but empty.

  - ***Last line changed/removed in [log file name]*:** The last line of the log file did not match validation criteria.

- ***Encrypted data missing in [log file name] near line [#]*****:** The encrypted part of the log line in question was not present.
- ***Inconsistency found in [log file name] near line [#]*****:** The log line does not match the encrypted part.
- ***Inconsistency found in [log file name] at beginning of log file*****:** The log file header is not correct. This situation is most likely to occur if a user has attempted to delete the beginning of a log file.

CONFIGURE SYSTEM, EVENT & AUDIT LOGGING

To configure recorder logging, do the following:

1. In the Management Application's Navigation pane, expand *Advanced Configuration*, right-click *Logs* and select *Properties*.
2. Specify required properties for:
   - General system logs (Management Application log, Recording Server service log, Image Server service log, Image Import service log)
   - The event log
   - The audit log

   Note that only audit logging can be disabled/enabled by administrators; all other logs are compulsory. When ready, click *OK*.
3. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

Properties

LOG PROPERTIES

When you configure logging , you can define the following:

Logs (that is Management Application log, Recording Server service log, Image Server service log, Image Import service log)

- ***Path*****:** These system log files are by default placed in the appropriate *All Users* folder for the operating system used , for example C:\ProgramData\OnSSI\RC-X if running Windows Vista . To specify another location for your log files, type the path to the required folder in the *Path* field, or click the browse button next to the field to browse to the required folder.
- ***Days to log*****:** A new log file is created each day the Management Application and/or the services are used. A log file older than the number of days specified in the field is automatically deleted. By default, the log file will be stored for seven days. To specify another number of days (max. 9999), simply overwrite the value in the field. The current day's activity is always logged, even with a value of 0 in the field. Therefore, if you specify 0, you will log current day's activity; if you specify 1, you will keep one day plus the current day's activity, and so on.

Event Log

- ***Path*****:** Event log files are by default placed in the appropriate *All Users* folder for the operating system used. To specify another location for your event log files, type the path to the required folder in the *Path* field, or click the browse button next to the field to browse to the required folder.

- ***Days to log*****:** A new log file is created for each day on which events occur. A log file older than the number of days specified in the field is automatically deleted. By default, the log file will be stored for seven days. To specify another number of days (max. 9999), simply overwrite the value in the field. The current day's activity is always logged, even with a value of 0 in the field. Therefore, if you specify 0, you will log current day's activity; if you specify 1, you will keep one day plus the current day's activity, and so on.

Audit Log

- ***Enable audit logging*****:** Audit logging is the only type of RC-P logging which is not compulsory. Select/clear the check box to enable/disable audit logging.

- ***Path*****:** Audit log files are by default placed in the appropriate *All Users* folder for the operating system used. To specify another location for your audit log files, type the path to the required folder in the *Path* field, or click the browse button next to the field to browse to the required folder.

- ***Days to log*****:** A new log file is created for each day with audit logging enabled and client user activity. A log file older than the number of days specified in the field is automatically deleted. By default, the log file will be stored for seven days. To specify another number of days (max. 9999), simply overwrite the value in the field. The current day's activity is always logged (provided audit logging is enabled and there is user activity). Therefore, if you specify 1, you will keep one day plus the current day's activity. Note that if you specify 0 (zero), audit log files will be kept indefinitely (disk space permitting).

- ***Minimum logging interval*****:** Minimum number of seconds between logged events. Specifying a high number of seconds between logged events may help reduce the size of the audit log. Default is 60 seconds.

- ***In sequence timespan*****:** Number of seconds to pass for viewed images to be considered to be within the same sequence. Specifying a high number of seconds may help limit the number of viewed sequences logged, and thus reduce the size of the audit log. Default is ten seconds.

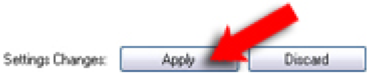
Management Application

APPLY OR SAVE CONFIGURATION CHANGES

Whenever you make changes in your RC-P configuration, you will be asked to apply them:

- If you made the changes in one of the Management Application's dialogs, simply apply them by clicking *OK*.

- If you made the changes in one of the Management Application's summary tables, click the *Apply* button below the summary table.



Applying a configuration change means that the change is stored by RC-P in a restore point (so that you can return to a working configuration if something goes wrong), but **applying a configuration change does not mean that the changes will take immediate effect** on the surveillance system.

- To actually store your configuration change in RC-P's configuration file, click the *Save Configuration* button in the Management Application's toolbar (or select *File* > *Save* from the menu). Your configuration changes will then take effect the next time RC-P's services are restarted.

- If you want your configuration changes to have immediate effect, RC-P's services must be restarted: Click the *Save Changes and Restart Surveillance Services* button in the Management Application's toolbar (or select *File* > *Save Changes and Restart Services* from the menu).

IMPORTANT: While services are restarted, it will not be possible to view or record video. Restarting the services typically only takes some seconds, but in order to minimize disruption you may want to restart services at a time when you do not expect important incidents. Users connected to RC-P through clients will typically remain logged in during the services restart, but they will experience a short video outage.

Change or Reset Management Application Behavior

You can change the way the Management Application behaves. For example, the Management Application will ask you to confirm many of your actions by default. If you find this annoying, you can change the Management Application's behavior, so it will not ask you again.

1. In the Management Application's menu bar, select *Application Settings* > *Application Behavior...*
2. For each action, you can now select how the Management Application should behave. Examples:
   - When you attempt to delete a hardware device, should the Management Application ask you to confirm that you want to delete the hardware device, or should it delete the hardware device straight away without asking?
   - If you add more cameras than allowable, should the Management Application warn you or not?

   Note that selectable behavior may vary, depending on the type of action.
3. Click *OK*.
4. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

Scheduling

Configure General Scheduling and Archiving

The general Scheduling and Archiving feature lets you configure when:

- Cameras should be online (that is transfer video to RC-P)
- Cameras should use speedup (that is use a higher than normal frame rate)
- You want to receive any e-mail notifications regarding cameras
- Archiving should take place

Do the following:

1. In the Management Application's navigation pane, expand *Advanced Configuration*, right-click *Scheduling and Archiving*, and select *Properties*.
2. Specify properties as required for Scheduling All Cameras, Scheduling Options, and Archiving. When ready, click *OK*.
3. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

CONFIGURE CAMERA-SPECIFIC SCHEDULES

With camera-specific scheduling, you can configure when:

- A camera should be online (that is transfer video to RC-P)
- A camera should use speedup (that is use a higher than normal frame rate)
- You want to receive any e-mail notifications regarding the camera

Do the following:

1. In the Management Application's navigation pane, expand *Advanced Configuration*, expand *Scheduling and Archiving*, right-click the required camera, and select *Properties*.
2. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

General Scheduling Properties

SCHEDULING ALL CAMERAS

When you configure general scheduling and archiving, you can specify certain properties for many cameras in one step. Either simply in order to speed up things, or because the properties in question are shared by all cameras rather than specific to individual cameras.

All properties on a white background are editable, properties on a light blue background cannot be edited. Note that the properties Online Period, Speedup, E-mail Notification can also be specified individually for each camera.

- ***Template*****:** The template can help you configure similar properties quickly. Say you have 20 cameras and you want to change the online schedule profile for all of them. Instead of having to select the same profile 20 times, you can simply enter them once in the template, and then apply the template to the 20 cameras with only two clicks.
- ***Apply Template*****:** Lets you select which cameras you want to apply the template for. You then use one of the two *Set* buttons (see descriptions in the following) to actually apply the template.
- ***Camera*****:** Name of each camera as it will appear in the Management Application as well as in clients.
- ***Online*****:** Lets you select the required profile (for example *Always on*) for the online schedule for the camera(s) in question.
- ***Speedup*****:** Lets you select the required profile for the speedup schedule for the camera(s) in question.
- ***E-mail*****:** Lets you select the required profile for the e-mail notification schedule for the camera(s) in question.

SCHEDULING OPTIONS

When you configure general scheduling and archiving, you can specify certain properties for many cameras in one step. In the case of Scheduling Options, it is simply because the properties are shared by all cameras.

Is it possible to view live and even record video from a camera outside its online recording schedule? *Yes, you simply select the* Start cameras on client requests *and, if needed, the* Enable recording when started on client request *options in the following when setting up your scheduling properties for the camera in question.*

- ***Start cameras on client requests*:** Cameras may be offline, for example because they have reached the end of an online recording schedule, in which case client users will not be able to view live video from the cameras. However, if you select *Start cameras on client requests*, client users will be able to view live video from the camera outside online schedule—but without recording (technically: force the camera to be online outside its online schedule).

  You must select *Enable recording when started on client request* (see the following), if you want recording to take place.

- ***Enable recording when started on client request:*** Lets you enable recording on the camera when *Start cameras on client requests* (see the previous) is also selected.

  If a user does not have access to manual recording, selecting *Enable recording when started on client request*, will **not** enable the user to do manual recording.

- ***Schedule profile for new cameras*:** Lets you select which online schedule profile to use as default for cameras you subsequently add to your RC-P system. Note that your selection only applies for the online schedule, not for any other schedules. Default selection is *Always on*, meaning that new cameras will always be online, that is transferring video to the RC-P server for live viewing and further processing.

- ***Maximum delay between reconnect attempts*:** Lets you control the aggressiveness of reconnection attempts. If RC-P loses the connection to a camera, it will by default attempt to re-establish the connection after ten seconds. In some environments, for example if using vehicle-mounted cameras through wireless connections, camera connections may frequently be lost, and you may want to change the aggressiveness of such reconnection attempts.

ARCHIVING (GENERAL SCHEDULING PROPERTIES)

The recorder automatically archives recordings if a camera's database becomes full (in earlier versions, this was an option configured individually for each camera).

You are furthermore able to schedule archiving at particular points in time every day. This way, you can proactively archive recordings, so databases will never become full. As a rule of thumb, the more you expect to record, the more often you should archive.

- **Archiving Time**

  The *Archiving Times* list shows the times at which you want to automatically archive the content of all camera databases on your RC-P server. You can do this up to 24 times per day, with minimum one hour between each one.

  To add archiving times to the list:

  1. Specify required time in the time box to the right of the *Archiving Times* list. You specify the required time by selecting the hour, minute and second values respectively, then clicking the *up* and *down* buttons to increase or decrease values. Alternatively, you can simply overwrite selected hour, minute or second values.

  2. Click the *Add* button.

- **Archive Failure Notification**

  You can automatically get notified if archiving fails:

  - ***Send e-mail on archiving failure*:** If selected, RC-P will automatically send an e-mail to selected recipients if archiving fails. This requires that the e-mail notification feature is enabled. Recipients are defined as part of the e-mail notification properties.

E-mail notifications are normally only sent during scheduled periods. However, archiving failures are considered to be so serious that, if enabled, e-mail notifications regarding archiving failures are sent regardless of schedules.

Camera-specific Scheduling Properties

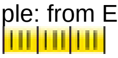
Online Period

When you configure scheduling for specific cameras, your *Online Period* settings are probably the most important, since they determine when each camera should transfer video to RC-P.

By default, cameras added to RC-P will automatically be online, and you will only need to modify the online period settings if you require cameras to be online only at specific times or events. Note, however, that this default may be changed as part of the general scheduling options, in which case subsequently added cameras will not automatically be online.

The fact that a camera transfers video to RC-P does not necessarily mean that video from the camera is recorded. Recording is configured separately; see Configure Video & Recording.

You specify a camera's online periods by creating schedule profiles based on:

- Periods of time (example: Mondays from 08.30 until 17.45), shown in pink:
- Events within periods of time (example: from Event A occurs until Event B occurs Mondays from 08.30 until 17.45), shown in yellow: 

The two options can be combined , but they cannot overlap in time.

Two simple schedule profiles are available: ***Always on*** and ***Always off***, which cannot be edited or deleted. If these do not meet your needs, you can create any number of customized schedule profiles for each camera. When you create a customized schedule profile for one camera, you can reuse it with other cameras if required. To create a customized schedule profile:

1. In the field below the ***Schedule profiles*** list, specify a name for the new schedule profile. Schedule profile names must not contain any of the following special characters: < > & ' " \ / : * ? | [ ]

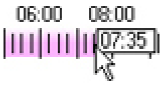
2. Click the ***Add New*** button (which becomes available when you specify a name).

3. In the top right corner of the dialog, select ***Set camera to start/stop on time*** (to base subsequent settings on periods of time) or ***Set camera to start/stop on event*** (to base subsequent settings on events within periods of time).

   Tip: You can combine the two, so you may return to this step in order to toggle between the two options.

4. In the calendar section, place your mouse pointer at a required start point, then hold down the left mouse button, drag the mouse pointer and release at the required end point.

   - You specify each day separately.
   - You specify time in increments of five minutes; RC-P helps you by showing the time over which your mouse pointer is positioned:

   - If you base your schedule profile—or parts of it—on events within periods of time, remember to select ***Start event*** and ***Stop event*** from the lists below the calendar section.

- To delete an unwanted part of a schedule profile, right-click it and select *Delete*.
- To quickly fill or clear an entire day, double-click the name of the day.
- As an alternative to dragging inside the calendar section, use the ***Start time***, ***End time*** and ***Day*** fields, then the ***Change Period*** or ***Set Period*** button as required. When using the *Start time* and *End time* fields, remember that time is specified in increments of five minutes. You cannot specify a period shorter than five minutes, and you can only use times like 12:00, 12.05, 12:10, 12:15, etc. If you specify a time outside of the five-minute intervals, such as 12:13, you will get an error message.

SPEEDUP

When you configure scheduling for specific MJPEG cameras, you can specify speedup periods. Before you can define this type of schedule, speedup must be enabled. You specify a camera's speedup periods by creating schedule profiles based on:

- Periods of time (example: Mondays from 08.30 until 17.45), shown in olive green: 🟩

Speedup may also take place based on events, but that is configured elsewhere: See Frame Rate - MJPEG (General Recording & Storage Properties) and Video (Camera-specific Properties).

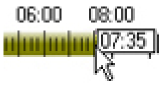
Two simple schedule profiles are available: ***Always on*** and ***Always off***, which cannot be edited or deleted. If these do not meet your needs, you can create any number of customized schedule profiles for each camera. When you create a customized schedule profile for one camera, you can reuse it with other cameras if required. To create a customized schedule profile:

1. In the field below the ***Schedule profiles*** list, specify a name for the new schedule profile. Schedule profile names not contain any of the following special characters: `< > & ' " \ / : * ? | [ ]`

2. Click the ***Add New*** button (which becomes available when you specify a name).

3. In the calendar section, place your mouse pointer at a required start point, then hold down the left mouse button, drag the mouse pointer and release at the required end point.

   - You specify each day separately.
   - You specify time in increments of five minutes; RC-P helps you by showing the time over which your mouse pointer is positioned:

   - To delete an unwanted part of a schedule profile, right-click it and select *Delete*.
   - To quickly fill or clear an entire day, double-click the name of the day.
   - As an alternative to dragging inside the calendar section, use the ***Start time***, ***End time*** and ***Day*** fields, then the ***Change Period*** or ***Set Period*** button as required. When using the *Start time* and *End time* fields, remember that time is specified in increments of five minutes. You cannot specify a period shorter than five minutes, and you can only use times like 12:00, 12.05, 12:10, 12:15, etc. If you specify a time outside of the five-minute intervals, such as 12:13, you will get an error message.

E-MAIL NOTIFICATION

When you configure scheduling for specific cameras, you can specify e-mail notification periods. Before you can define this type of schedule, e-mail notification must be enabled. You specify a camera's e-mail notification periods by creating schedule profiles based on:

- Periods of time (example: Mondays from 08.30 until 17.45), shown in blue:

Two simple schedule profiles are available: ***Always on*** and ***Always off***, which cannot be edited or deleted. If these do not meet your needs, you can create any number of customized schedule profiles for each camera. When you create a customized schedule profile for one camera, you can reuse it with other cameras if required. To create a customized schedule profile:

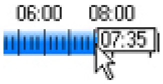
1. In the field below the ***Schedule profiles*** list, specify a name for the new schedule profile. Schedule profile names must not contain any of the following special characters: `< > & ' " \ / : * ? | [ ]`

2. Click the ***Add New*** button (which becomes available when you specify a name).

3. In the calendar section, place your mouse pointer at a required start point, then hold down the left mouse button, drag the mouse pointer and release at the required end point.

    - You specify each day separately.

    - You specify time in increments of five minutes; RC-P helps you by showing the time over which your mouse pointer is positioned:

    - To delete an unwanted part of a schedule profile, right-click it and select *Delete*.

    - To quickly fill or clear an entire day, double-click the name of the day.

    - As an alternative to dragging inside the calendar section, use the ***Start time***, ***End time*** and ***Day*** fields, then the ***Change Period*** or ***Set Period*** button as required. When using the *Start time* and *End time* fields, remember that time is specified in increments of five minutes. You cannot specify a period shorter than five minutes, and you can only use times like 12:00, 12.05, 12:10, 12:15, etc. If you specify a time outside of the five-minute intervals, such as 12:13, you will get an error message.

Services

OVERVIEW OF SERVICES

The following services are all automatically installed on the recorder server:

- **Recording Server service:** A vital part of the surveillance system; video streams are only transferred to RC-P while the Recording Server service is running.

- **Image Server service:** Provides access to the surveillance system for users logging in with the Ocularis Client.

Note: If the Image Server service is configured in Windows *Services* to log in with another account than the *Local System* account, for example as a domain user, Ocularis Clients on other computers than the surveillance server itself will not be able to log in to the server using the server's host name. Instead, those users must enter the server's IP address.

- **Image Import service:** Used for fetching pre- and post-alarm images, and storing the fetched images in camera databases. Pre- and post-alarm images is a feature available for selected cameras only; it enables sending of images from immediately before and after an event took place from the camera to the surveillance system via e-mail. Pre- and post-alarm images should not be confused with RC-P's own pre- and post-recording feature.

- **Log Check service:** Performs integrity checks on RC-P log files. For more information, see Overview of Logs.

The services by default run transparently in the background on the RC-P server. If required, you are able to start and stop each service separately from the Management Application; see Start & Stop Services.

Start and Stop Services

On an RC-P server, four services run in the background by default. If required, you can start and stop each service separately:

1. In the Management Application's Navigation pane, expand *Advanced Configuration* and select *Services*. This will display the status of each service.

2. You can now stop each service by clicking the *Stop* button. When a service is stopped, the button changes to *Start*, allowing you to start the service again when required.

   Tip: Occasionally, you may want to stop a service and start it again immediately after. The *Restart* button allows you to do just that with a single click.

System

Configure Default File Paths

The recorder supports the following default file paths:

- ***Default recording path for new cameras*:** All new cameras you add will by default use this path for storing recordings. If required, you can change individual cameras' recording paths as part of their individual configuration, but you can also change the default recording path so all new cameras you add will use a path of your choice.

- ***Default archiving path for new cameras*:** All new cameras you add will by default use this path for archiving. If required, you can change individual cameras' archiving paths as part of their individual configuration, but you can also change the default recording path so all new cameras you add will use a path of your choice. Note that camera-specific archiving paths are not relevant if using dynamic path selection for archiving.

- ***Configuration path*:** The path by default used for storing your RC-P system's configuration.

To change any of the default file paths:

1. If changing the configuration path, stop all services. This step is not necessary if changing the default recording or archiving path.

2. In the Management Application's menu bar, select *Application Settings* > *Default File Paths...*

3. You can now overwrite required paths. Alternatively, click the browse button next to the required field and browse to the required location.

   For the default recording path, you are only able to specify a path to a folder on a *local* drive. If using a network drive, it would not be possible to save recordings if the network drive became unavailable.

If you change the default recording or archiving paths, and there are existing recordings at the old locations, you will be asked whether you want to move the recordings to the new locations (recommended), leave them at the old locations, or delete them.

4. Click *OK*.

5. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

6. Restart all services.

FIND VERSION AND LICENSE INFORMATION

Knowing the exact version of your software can be important if you require technical support, want to upgrade your system, etc.

To view such information, select *About...* in the Management Application's *Help* menu.

RESTORE RECORDER CONFIGURATION FROM RESTORE POINT

Restore points allow you to return to a previous configuration state. Each time a configuration change is applied in the Management Application—either by clicking *OK* in a properties dialog or by clicking the *Apply* button in a summary pane—a new restore point is created.

All restore points in the current and previous five sessions are stored and can be selected again. A new session begins each time the Management Application is started as well as each time you save the whole configuration, for example by clicking the *Save Configuration* button in the Management Application's toolbar. For sessions older than the last five sessions, only the latest restore point of each session is stored. With the *Number of old sessions to keep* field you can control how many old sessions are kept.

When selecting to restore a configuration from a restore point, the configuration from the selected restore point will be applied and used once the services are restarted (see Start & Stop Services).

If you have added new cameras or other devices to RC-P after the restore point was created, they will be missing if you load the restore point. This is due to the fact that they were not in the system when the restore point was created. In such cases, you will be notified and must decide what to do with recordings from the affected devices.

1. From the Management Application's *File* menu, select *Load Configuration from Restore Point...*

2. In the left part of the *Restore Points* dialog, select the required restore point.

   Tip: When you select a restore point, you will in the right part of the dialog see information about the configuration state at the selected point in time. This can help you select the best possible restore point.

3. Click the *Load Restore Point* button.

4. If you are sure that you want to overwrite the current configuration with the one from the selected restore point, click *OK*.

5. Only relevant if the current configuration contains cameras or other devices which were not present in the selected restore point: You will be asked whether you want to delete or keep recordings from affected devices. If keeping the recordings, note that they will not be accessible until you add the affected devices to RC-P again. Select the required option, and click *OK*.

6. Click *OK* in the Restore Points dialog.

7. In the Management Application's navigation pane, expand *Advanced Configuration*, and select *Services*.

8. For the Recording Server and Image Server services respectively, click the *Restart* button. When the two services are restarted, the configuration from the selected restore point is applied.

EXPORT AND IMPORT RECORDER CONFIGURATION

You can export the current configuration of your RC-P Management Application, either as a safety measure in order to have a backup file of your configuration, or as a clone allowing you to use a similar Management Application configuration elsewhere. You are subsequently able to import previously exported Management Application configurations.

- **Export Management Application Configuration as Backup**

  With this option, all relevant RC-P Management Application configuration files will be combined into one single .xml file, which can then be saved at a location specified by you. Note that if there are unsaved changes to your configuration, they will automatically be saved when you export the configuration.

  1. In the Management Application's *File* menu, select *Export Configuration - Backup*.

  2. Browse to the location at which you want to store the exported configuration, specify a suitable file name, and click *Save*.

  If you intend to set up an identical version of your surveillance system elsewhere, **do not** export your configuration as *backup*, since this may lead to the same device information being used twice, in which case clients may get the following error message: *Application is not able to start because two (or more) cameras are using the same name or id.* Instead, export your configuration as a *clone*. When you export as a clone, the export takes into account the fact that you will not use the exact same physical cameras, etc. even though your new system may otherwise be identical to your existing one.

- **Export Management Application Configuration as Clone**

  With this option, all relevant RC-P Management Application configuration files will be collected, and GUIDs (Globally Unique IDentifiers; unique 128-bit numbers used for identifying individual system components, such as cameras) will be marked for later replacement.

  Why are GUIDs marked for replacement? GUIDs are marked for later replacement because they refer to specific components (cameras, etc.). Even though you wish to use the cloned configuration for setting up a new similar system using similar types of cameras, the new system will not use the exact same physical cameras as the cloned system. When the cloned configuration is later used in a new system, the GUIDs will therefore be replaced with GUIDs representing the specific components of the new system.

  After GUIDs have been marked for replacement, the configuration files will be combined into one single .xml file, which can then be saved at a location specified by you. Note that if there are unsaved changes to your configuration, they will automatically be saved when you export the configuration.

  1. In the Management Application's *File* menu, select *Export Configuration - Clone*.

  2. Browse to the location at which you want to store the exported configuration, specify a suitable file name, and click *Save*.

- **Import Previously Exported Management Application Configuration**

  The same import method is used regardless of whether the RC-P Management Application configuration was exported as a backup or a clone.

  1. In the Management Application's *File* menu, select *Import Configuration*.

2. Browse to the location from which you want to import the configuration, select the required configuration file, and click *Open*.

3. Only relevant if the system into which you import the configuration contains devices (cameras, etc.) which are not present in the imported configuration: You will be asked whether you want to delete or keep recordings from affected devices. If keeping the recordings, note that they will not be accessible until you add the affected devices to RC-P again. Select the required option, and click *OK*.

4. In the Management Application's navigation pane, expand *Advanced Configuration*, and select *Services*.

5. For the Recording Server and Image Server services respectively, click the *Restart* button. When the two services are restarted, the imported Management Application configuration is applied.

IMPORT CHANGES TO CONFIGURATION

It is possible to import changes to a configuration. This can be relevant if installing many similar RC-P systems, for example in a chain of retail establishments where the same types of server, hardware devices, and cameras are used in each location. In such cases, you can use an existing configuration—typically a cloned configuration—as a template for the other installations. However, since the shops' installations are not exactly the same (the hardware devices and cameras are of the same type, but they are not physically the same, and thus they have different MAC addresses), there needs to be an easy way of importing changes to the template configuration.

This is why RC-P lets you import changes about hardware devices and cameras as comma-separated values (CSV) from a file:

1. From RC-P's menu bar, select *File* > *Import Changes to Configuration...*

2. Select *Online verification* if the new hardware devices and cameras listed in your CSV file are connected to the server and you want to verify that they can be reached.

3. Then point to the CSV file, and click the *Import Configuration from File* button.

- ### CSV File Format and Requirements

  The CSV file must have a header line (determining what each value on the subsequent lines is about), and subsequent lines must each contain information about one hardware device only.

  A minimum of information is always required for each hardware device:

  - ***HardwareOldMacAddress***
    The MAC address of the hardware device used in the template configuration. Required format: 12 hex characters without spaces or six groups of two hex characters separated with dashes (-) or colons (:).

  You can furthermore include these optional parameters:

  - ***HardwareNewMacAddress***
    The MAC address of the new hardware device to be used in the real configuration. Required format: 12 hex characters without spaces or six groups of two hex characters separated with dashes (-) or colons (:).
  - ***HardwareAddress***
    IP address of the hardware device.
  - ***HardwareUsername***
    User name for hardware device's administrator account.

    In the extremely rare cases where a particular user name has previously been required for a device, but you now want the user name to be <blank>, you cannot use the CSV file to specify <blank>. The reason is that no information is interpreted as “leave the user name as it currently is.” If you need the new user name to be <blank>, you should not change it through the CCV file. Instead, change it as part of the hardware device's Network, Device Type & License properties after you have imported the other changes through the CSV file.

- ***HardwarePassword***
  Password for hardware device's administrator account.

  In the extremely rare cases where a particular password has previously been required for a device, but you now want the password to be <blank>, you cannot use the CSV file to specify <blank>. The reason is that no information is interpreted as “leave the password as it currently is.” If you need the new password to be <blank>, you should not change it through the CSV file. Instead, change it as part of the hardware device's Network, Device Type & License properties after you have imported the other changes through the CSV file.

- ***HardwareDeviceName***
  Name of the hardware device. Name must unique, and must not contain any of the following special characters: < > & ' " \ / : * ? | [ ]

- ***CameraName[number]***
  Name of the camera. Must appear as *CameraName1*, *CameraName2*, etc. in the header line since a hardware device can potentially have more than one camera attached. Names must be unique, and must not contain any of the following special characters: < > & ' " \ / : * ? | [ ]

- ***CameraShortcut[number]***
  Number for keyboard shortcut access to the camera in the Ocularis Client. Must appear as *CameraShortcut1*, *CameraShortcut2*, etc. in the header line since a hardware device can potentially have more than one camera attached. A camera shortcut number must not contain any letters or special characters, and must not be longer than eight digits.

- ***GenerateNewCameraGuid[optional number]***
  Lets you specify whether to generate a new GUID for a camera; this is especially relevant if using a cloned configuration as your template, since all GUIDs are removed from cloned configurations. If specified as, for example, *GenerateNewCameraGuid1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device. Any character means “yes, generate a new GUID.”

- ***PreBufferLength[optional number]***
  Required length (in seconds) of pre-recording. If specified as, for example, *PreBufferLength1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.

- ***PostBufferLength[optional number]***
  Required length (in seconds) of post-recording. If specified as, for example, *PostBufferLength1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.

- ***RecordingPath[optional number]***
  Path to the folder in which a camera's database should be stored. If specified as, for example, *RecordingPath1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.

- ***ArchivePath[optional number]***
  Path to the folder in which the camera's archived recordings should be stored. Remember that an archiving path is only relevant if not using dynamic paths for archiving. If specified as, for example, *ArchivePath1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.

- ***OldRecordingsNewPath[optional number]***
  Lets you specify what to do with old recordings in case *RecordingPath* or *ArchivePath* have been changed. If this parameter is not specified, default behavior is *Leave* (see the following). If specified as, for example, *OldRecordingsNewPath1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device. Valid options are: *Delete* (deletes old recordings), *Leave* (leaves old recordings for offline investigation but unavailable for online system), or *Move* (moves old recordings to archive).

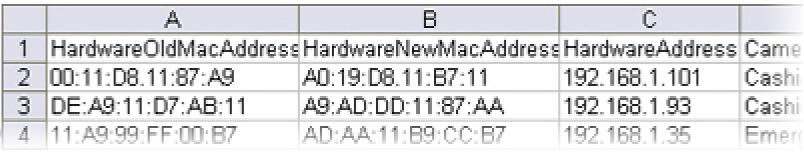
- ***OldRecordingsNewMac[optional number]***
  Lets you specify what to do with old recordings in case a new MAC address has been

specified for the hardware device. If this parameter is not specified, default behavior is Leave (see the following). If specified as, for example, *OldrecordingsNewMac1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device. Valid options are: Delete (deletes old recordings), Leave (leaves old recordings for offline investigation but unavailable for online system), or Inherit (renames all old recording folders according to the new MAC address, thus making them available for the online system).

- ***RetentionTime[optional number]***
  Required retention time (in minutes). Remember that retention time is the total of recording time plus archiving time. If specified as, for example, *RetentionTime1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
- ***MjpegLiveFrameRate[optional number]***
  Required MJPEG live frame rate (in number of frames; depending on what has been configured on the camera, it will then know whether it is frames per second, minute, or hour). If specified as, for example, *MjpegLiveFrameRate1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
- ***MjpegRecordingFrameRate[optional number]***
  Required MJPEG recording frame rate (in number of frames; depending on what has been configured on the camera, it will then know whether it is frames per second, minute, or hour). If you need to specify a value which includes a decimal separator, use the full stop character (example: 7.62). If specified as, for example, *MjpegRecordingFrameRate1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
- ***MotionSensitivity[optional number]***
  A value between 0-256; corresponds to using the *Sensitivity* slider when configuring motion detection settings in the Management Application. If specified as, for example, *MotionSensitivity1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
- ***MotionDetectionThreshold[optional number]***
  A value between 0-10000; corresponds to using the *Motion* slider when configuring motion detection settings in the Management Application. If specified as, for example, *MotionDetectionThreshold1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
- ***MotionDetectionInterval[optional number]***
  Lets you specify how often motion detection analysis should be carried out on video from the camera. Specified in milliseconds. The interval is applied regardless of the camera's frame rate settings. If specified as, for example, *MotionDetectionInterval1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
- ***ServerName***
  Name with which the RC-P will appear when listed in clients. Name must be unique, and must not contain any of the following special characters: `< > & ' " \ / : * ? | [ ]`
- ***ServerPort***
  Port number to use for communication between the RC-P server and clients.
- ***OnlineVerification***
  If this parameter is used, all online hardware devices found using *HardwareOldMacAddress* are updated. All other hardware devices are not updated. Any character means “yes, use online verification.”

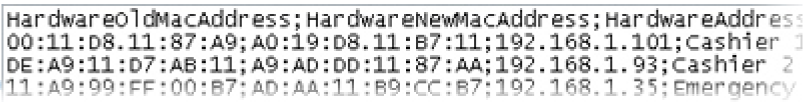
Existing configuration parameters that are not specified in CSV file will remain unchanged. If a parameter value for an individual camera in the CSV file is empty, the existing parameter value will remain unchanged on that camera.

Most system integrators store hardware device information in spreadsheets like Microsoft Excel, from which they can save the information as comma-separated values in a CSV file. These examples show hardware information in Excel (**1**) and when exported to a CSV file (**2**); note the header lines:



1

	A	B	C	
1	HardwareOldMacAddress	HardwareNewMacAddress	HardwareAddress	Came
2	00:11:D8.11:87:A9	A0:19:D8.11:B7:11	192.168.1.101	Cashi
3	DE:A9:11:D7:AB:11	A9:AD:DD:11:87:AA	192.168.1.93	Cashi
4	11:A9:99:FF:00:B7	AD:AA:11:B9:CC:B7	192.168.1.35	Emer



2

```
HardwareOldMacAddress;HardwareNewMacAddress;HardwareAddres
00:11:D8.11:87:A9;A0:19:D8.11:B7:11;192.168.1.101;Cashier 1
DE:A9:11:D7:AB:11;A9:AD:DD:11:87:AA;192.168.1.93;Cashier 2
11:A9:99:FF:00:B7;AD:AA:11:B9:CC:B7;192.168.1.35;Emergency
```

Whichever method is used, the following applies:

- The first line of the CSV file must contain the headers, and subsequent lines must contain information about one hardware device each
- Separators can be commas, semicolons or tabs, but cannot be mixed
- All lines must contain valid values—pay special attention to the fact that camera names, user names, etc. must be unique, and must not contain any of the following special characters: < > & ' " \ / : * ? | [ ]
- There is no fixed order of values, and optional parameters can be omitted entirely
- Boolean fields are considered true unless set to 0, false or no
- Lines containing only separators are ignored
- Empty lines are ignored
- Even though the CSV file format is generally ASCII only, Unicode identifiers are allowed; even without Unicode identifiers, the entire file or even individual characters are allowed to be Unicode strings

If you need to include separator characters in a value—for example if a camera name is Reception; Camera 1—you can encapsulate the value in quotes to indicate that the separator should not be interpreted as separating values in the file. Such quote-encapsulated values are interpreted as they appear. If a separator, a quote or a space is needed in a value, the whole value has to be encapsulated in quotes. Leading and trailing spaces outside the quote-encapsulated value are removed, while spaces inside the quote-encapsulated value are maintained. No characters (except spaces) are allowed outside the quote-encapsulated value. A double quote inside a quote-encapsulated value is interpreted as a single quote. Nested quotes (quotes inside quotes) are not allowed.

Some examples (using semicolon as the separator):

- "camera"; is interpreted as camera
- "cam;""era"; is interpreted as cam;"era
- """camera"""; is interpreted as "camera"
- ""; is interpreted as an empty string
- ...; "   cam"" era "   ;... is interpreted as | cam" era | (where the character | is not part of the interpretation but only used to show the start and end of the interpretation)
- ""camera; is not valid as there are characters outside the quote-encapsulated value
- "cam" "era"; is not valid as the two quotes are separated with a space and quotes cannot be nested
- "cam"er"a"; is not valid as you cannot nest quotes
- cam"era"; is not valid as there are characters outside the quotes

Daylight Savings Time

Daylight saving time (DST) is the practice of advancing clocks in order for evenings to have more daylight and mornings to have less. Typically, clocks are adjusted forward one hour sometime during the spring season and adjusted backward sometime during the fall season, hence the saying *spring forward, fall back*. Note that use of DST varies between countries/regions.

When working with a surveillance system, which is inherently time-sensitive, it is important to know how the system handles DST.

Spring: Switch from Standard Time to DST

The change from standard time to DST is not much of an issue since you jump one hour forward. Typically, the clock jumps forward from 02:00 standard time to 03:00 DST, and the day thus has 23 hours. In that case, there is simply no data between 02:00 and 03:00 in the morning since that hour, for that day, did not exist.

Fall: Switch from DST to Standard Time

When you switch from DST to standard time in the fall, you jump one hour back. Typically, the clock jumps backward from 02:00 DST to 01:00 standard time, repeating that hour, and the day thus has 25 hours. In that case, you will reach 01:59:59, then immediately revert back to 01:00:00. If the system did not react, it would essentially re-record that hour, so the first instance of, for example, 01:30 would be overwritten by the second instance of 01:30.

Because of this, the recorder will forcefully archive the current video in the event that the system time changes by more than five minutes. The first instance of the 01:00 hour will not be viewable directly from clients. However, the data is recorded and safe, and it can be browsed using the Ocularis Client application by opening the archived database directly.

PROTECT RECORDING DATABASE FROM CORRUPTION

In the Management Application you can select which action to take if a camera database becomes corrupted. The actions include several database repair options. While being able to select such actions is highly valuable, it is of course even better to take steps to ensure that your camera databases do not become corrupted:

- **Power Outages: Use a UPS**

  The single biggest reason for corrupt databases is the surveillance system server being shut down abruptly, without files being saved and without the operating system being closed down properly. This may happen due to power outages, due to somebody accidentally pulling out the server's power cable, or similar.

  The best way of protecting your surveillance system server from being shut down abruptly is to equip your surveillance system server with a UPS (Uninterruptible Power Supply).

  The UPS works as a battery-driven secondary power source, providing the necessary power for saving open files and safely powering down your system in the event of power irregularities. UPSs vary in sophistication, but many UPSs include software for automatically saving open files, for alerting system administrators, etc.

  Selecting the right type of UPS for your organization's environment is an individual process. When assessing your needs, however, do keep in mind the amount of runtime you will require the UPS to be able to provide if the power fails; saving open files and shutting down an operating system properly may take several minutes.

- **Windows Task Manager: Be Careful when Ending Processes**

  When working in Windows Task Manager, be careful not to end any processes which affect the surveillance system. If you end an application or system service by clicking *End Process* in the Windows Task Manager, the process in question will not be given the chance to save its state or data before it is terminated. This may in turn lead to corrupt camera databases.

  Windows Task Manager will typically display a warning if you attempt to end a process. Unless you are absolutely sure that ending the process will not affect the surveillance system, make sure you click the *No* button when the warning message asks you if you really want to terminate the process.

- **Hard Disk Failure: Protect Your Drives**

  Hard disk drives are mechanical devices, and as such they are vulnerable to external factors. The following are examples of external factors which may damage hard disk drives and lead to corrupt camera databases:

  - Vibration (make sure the surveillance system server and its surroundings are stable)
  - Strong heat (make sure the server has adequate ventilation)
  - Strong magnetic fields (avoid)
  - Power outages (make sure you use a UPS; see more information in the previous)
  - Static electricity (make sure you ground yourself if you are going to handle a hard disk drive).
  - Fire, water, etc. (avoid)

Users

Overview of Users and Groups

To get an overview of your recorder's user accounts, expand *Advanced Configuration* in the Management Application's navigation pane, then expand *Users*.

The term *users* primarily refers to users who are able to connect to the surveillance system using the Ocularis Client. You can configure such users in two ways:

- As **basic users**, authenticated by a user name/password combination.
- As **Windows users**, authenticated based on their Windows login

You can add both types of users through the Configure User Access wizard or individually (see Add Basic Users and Add Windows Users).

By grouping users, you can specify rights for all users within a **group** in one step. If you have many users performing similar tasks, this can save you significant amounts of work. User groups are logical groups created and used for practical purposes in the Management Application only. They are not in any way connected with user groups from central directory services such as, for example, Active Directory®. If you want to use groups, make sure you add groups before you add users: You cannot add existing users to groups.

Finally, the **Administrators** group is also listed under *Users*. This is a default Windows user group for administration purpose which automatically has access to the Management Application.

Configure User Access Wizard

The Configure User Access wizard helps you quickly configure access to the RC-P server.

When using the wizard, all user accounts added will have access all to cameras, including any new cameras added at a later stage. If this is not acceptable, specify access settings, users and user rights separately; see Configure Server Access. Also note that you cannot add users to groups through the wizard.

The wizard is divided into a number of pages:

- Server Access Settings
- Basic and Windows Users
- Access Summary

ADD BASIC USERS

When adding a basic user, create a dedicated surveillance system user account with basic user name and password authentication for the individual user. Note that adding the user as a Windows user will provide better security.

Note: with Ocularis only one user account is needed. This account should have full access rights to the recording component.

If you want to include users in groups, make sure you add required groups before you add users: You cannot add existing users to groups.

You can add basic users in two ways: One is through the Configure User Access Wizard, the other is described here:

1. In the Management Application's navigation pane, expand *Advanced Configuration*, right-click *Users*, and select *Add New Basic User*.
2. Specify a user name. User names must be unique, and must not contain the following characters: < > & ' " \ / : * ? | [ ]

   Then specify a password, and repeat it to be sure you have specified it correctly.
3. Click *OK*.
4. Specify General Access and Camera Access properties. These properties will determine the rights of the user.
5. Click *OK*
6. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

ADD WINDOWS USERS

When adding Windows users, you import users defined locally on the server and authenticate them based on their Windows login. This generally provides better security than the basic user concept, and is the recommended method.

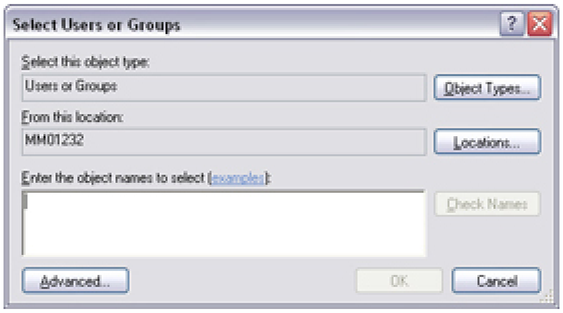
If you want to include users in groups, make sure you add required groups before you add users: You cannot add existing users to groups.

You can add Windows users in two ways: One is through the Configure User Access Wizard, the other is described here:

The users you want to add must have been defined as local PC users on the server. Simple file sharing must be disabled on the server. To disable simple file sharing, right-click Windows' *Start* button and select *Explore*. In the window that opens, select the *Tools* menu, then select *Folder Options...* , then the *View* tab. Scroll to the bottom of the tab's *Advanced Settings* list, and make sure that the *Use simple files sharing* check box is cleared. When ready, click *OK* and close the window.

Adding Local Users

1. In the Management Application's navigation pane, expand *Advanced Configuration*, right-click *Users*, and select *Add New Windows User*. This will open the S*elect Users or Groups* dialog.

   Select Users or Groups

   Select this object type:
   Users or Groups

   From this location:
   MM01232

   Enter the object names to select (examples):

   Note that you will only be able to make selections from the local computer, even if you click the *Locations...* button.

2. In the *Enter the object names to select* box, type the required user name(s), then use the *Check Names* feature to verify that the user name(s) you have entered are correct. If typing several user names, separate each name with a semicolon. Example: *Brian; Hannah; Karen; Wayne*

3. When ready, click *OK* .

Any prerequisites for adding users from a local database? *The users must have been defined as local PC users on the server. Simple file sharing must be disabled on the server. Depending on your operative system, this is done in different ways:*

Windows 7: click the Windows logo and type file sharing *in the search results window and press* Enter*. Under* File and Printer Sharing*, make sure that* Turn off file and printer sharing *is selected. Under* Public Folder Sharing*, make sure that* Turn off public folder sharing *is cleared.*

Windows Vista: click Start > Control Panel*. Under* Network and Internet*, select* Set up file sharing*. The* Network and Sharing Center *window appears. Under* Sharing and Discovery*, set the option for file sharing to* Off *by clicking the down arrow next to* File Sharing *and select the radio button to* Turn off file sharing*. Click* Apply *and continue through the warning messages.*

Windows XP: click Start > My Computer*. In the* My Computer *window, select* Tools *and in the top menu, select* Folder Options*. A new* Folder Options *window opens. Click on the* View *tab and scroll down to find* Use simple file sharing (recommended)*. Clear the box to disable file sharing. Click* OK*.*

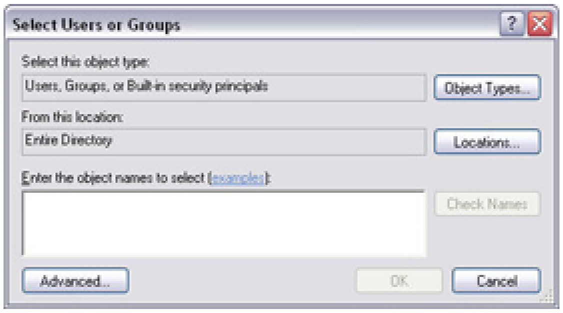
What is Active Directory? *Active Directory is a distributed directory service included with several Windows Server operating systems; users are specified centrally in Active Directory. In short, the benefits of importing user data from Active Directory are that administrators do not have to create separate user accounts for accessing the surveillance system because user authentication will be handled centrally by Active Directory, and that users can use their Windows login when accessing the surveillance system; no need to memorize separate user names and passwords.*

Any prerequisites for adding users from Active Directory? *RC-P verifies client users' identities using NTLM challenge handshake with a Microsoft Domain Controller. In order to be able to import users and groups through Active Directory, a server with Active Directory installed and acting as domain controller must be available on your network. Consult your network administrator if in doubt.*

Can I add groups from Active Directory? *You can only add individual users from Active Directory to RC-P. Active Directory also supports groups of users, but you cannot add such groups to RC-P. You can, however, group individual users in RC-P, and quickly assign common user rights for all users within such groups.*

Adding AD Users

1. In the Management Application's navigation pane, expand *Advanced Configuration*, right-click *Users*, and select *Add New Windows User*. This will open the *Select Users or Groups* window.



Select Users or Groups

Select this object type:

Users, Groups, or Built-in security principals

From this location:

Entire Directory

Enter the object names to select (examples):

   By default, you will be able to make selections from your entire directory. If you want to narrow this, click the *Select Users and Groups* window's *Locations...* button, and select the location you require.

2. In the *Enter the object names to select* box, type the required user names, then use the *Check Names* feature to verify that the user names you have entered are recognized. Example: *Brian; Hannah; Karen; Wayne*

3. When ready, click *OK* .

4. Specify General Access and Camera Access properties. These properties will determine the rights of the user.

5. Click *OK*

6. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

When a user who has been added from a local database logs in with a client, the user should not specify any server name, PC name, or IP address as part of the user name. When a user who has been added from a **local database** logs in with a client, the user should not specify any server name, PC name, or IP address as part of the user name. Example of a correctly specified user name: USER001. Example of an incorrectly specified user name: PC001/USER001. The user should of course still specify a password and any required server information.

ADD USER GROUPS

User groups are logical groups created and used for practical purposes in the Management Application only. They are not in any way connected with user groups from central directory services such as, for example, Active Directory®.

By grouping users, you can specify rights for all users within a group in one step. If you have many users performing similar tasks, this can save you significant amounts of work.

Make sure you add groups before you add users: You cannot add existing users to groups.

1. In the Management Application's navigation pane, expand *Advanced Configuration*, *right-click Users*, and select *Add New User Group*.

2. Specify a name for the group. Group names must be unique, and must not contain the following characters: < > & ' " \ / : * ? | [ ]

3. Click *OK*.

4. Specify General Access and Camera Access properties. These properties will determine the rights of the group's future members.

5. Click *OK*.

6. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

7. Now you can add users to the group: In the navigation pane, right-click the group you just created, and Add Basic Users or Add Windows Users as required.

CONFIGURE USER AND GROUP RIGHTS

User/group rights are configured during the process of adding users/groups, see Add Basic Users, Add Windows Users and Add User Groups.

Note that you can also add basic and Windows users through the Configure User Access wizard. However, when using the wizard all users you add will have access all to cameras, including any new cameras added at a later stage.

If you at a later stage want to edit the rights of a user or group:

1. In the Management Application's navigation pane, expand *Advanced Configuration*, expand *Users*, right-click the required user or group, and select *Properties*.

2. Edit General Access and Camera Access properties. These properties will determine the rights of the user/group.

3. Click *OK*

4. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

Properties

USER INFORMATION (PROPERTIES)

- ***User name*****:** Only editable if the selected user is of the type basic user. Lets you edit the user name. User names must be unique, and must not contain the following characters: < > & ' " \ / : * ? | [ ]

- ***Password*****:** Only editable if the selected user is of the type basic user. Lets you edit the password. Remember to repeat the password to be sure you have specified it correctly.

- ***User type*****:** Non-editable field, displaying whether the selected user is of the type basic user or Windows user group.

GROUP INFORMATION (PROPERTIES)

- ***Group name*****:** Lets you edit the group name. Group names must be unique, and must not contain the following characters: < > & ' " \ / : * ? | [ ]

GENERAL ACCESS (PROPERTIES)

When adding or editing basic users , Windows users or groups , specify general access settings:

- ***Live*****:** Ability to view Live video in the Ocularis Client.

- ***Playback*****:** Ability to view video in Browse mode in the Ocularis Client.
- ***Setup*****:** Ability to access the *Setup* function when using Ocularis Client in Limited Mode.
- ***Edit shared views*****:** Ability to create and edit views in shared groups when operating the Ocularis Client in Limited Mode . Views placed in shared groups can be accessed by every user.
- ***Edit private views*****:** Ability to create and edit views in private groups when operating the Ocularis Client in Limited Mode. Views placed in private groups can only be accessed by the user who created them.
- ***Administrator Access:*** Ability to access and work with the Management Application. Selected and non-editable for Administrators. Cleared and selectable for all other users.

CAMERA ACCESS (PROPERTIES)

When adding or editing basic users , Windows users or groups , specify camera access settings:

In the list of cameras, select the camera(s) you want to work with. Note the last item in the list, *Rights for new cameras when added to the system*, with which you can allow the user/group access to any future cameras.

For the selected camera(s), in the ***Access*** check box, specify if the user/group should have access to live viewing and playback at all. If so, specify if they should have access to **both** live viewing and playback and—if this is the case—which sub-features should be available when working with the selected camera(s).

The sub-features are listed in two columns in the lower part of the window: the left column lists features related to live viewing, the right column lists features related to playback.

The *Camera access settings* check boxes work like a hierarchy of rights. If the *Access* check box is cleared, everything else is cleared and disabled. If the *Access* check box is selected, but, for example, the *Live* check box is cleared, everything under the *Live* check box is cleared and disabled.

In the *Live* column, the following features, all selected by default, are available:

- ***Live*****:** Ability to view live video from the selected camera(s).
  - ***PTZ*****:** Ability to use navigation features for PTZ (Pan/Tilt/Zoom) cameras. A user/group will only be able to use this right if having access to one or more PTZ cameras.
  - ***PTZ preset positions*****:** Ability to use navigation features for moving a PTZ camera to particular preset positions. A user/group will only be able to use this right if having access to one or more PTZ cameras with defined preset positions.
  - ***Output*****:** Ability to activate output (lights, sirens, door openers, etc.) related to the selected camera(s).
  - ***Events*****:** Ability to use manually triggered events related to the selected camera(s).
  - ***Incoming audio*****:** Ability to listen to incoming audio from microphones related to the selected camera(s).
  - ***Manual recording*****:** Ability to manually start recording for a fixed time (defined by the surveillance system administrator).
  - ***Recorded audio*****:** Ability to listen to recorded audio from microphones related to the selected camera(s).

Why can I not select certain features? *Typically because the selected camera does not support the features. For example, you can only select PTZ-related features if the camera is a PTZ camera. Also, some* *of the features depend on the user's/group's General Access properties: For example, in order have access to PTZ or output features, the user/group must have access to viewing live video; in order to use AVI/JPEG export, the user/group must have access to playing back recorded video.*

Why are some feature check boxes filled with squares? *Square-filled check boxes can appear in the lower part of the window if you have selected several cameras and a feature applies for some but not all of the cameras. Example: For camera A you have selected that use of the* Events *is allowed; for camera B it is not allowed. If you select both camera A and camera B in the list, the* Events *check box in the lower part of the window will be square-filled. Another example: Camera C is a PTZ camera for which you have allowed the* PTZ preset positions *feature; camera D is not a PTZ camera. If you select both camera C and camera D in the list, the* PTZ preset positions *check box will be square-filled.*

Drivers

Update Video Device Drivers

Video device drivers are small programs used for controlling/communicating with the camera devices connected to the recording component. Video device drivers are installed automatically during the initial installation of the recorder software. However, new versions of video device drivers—called Device Packs—are released and made available for free on the OnSSI website from time to time.

We recommend that you always use the latest version of video device drivers. When updating video device drivers, there is no need to remove the old video device drivers first; simply install the latest version on top of any old version you may have.

IMPORTANT: When you install new video device drivers, your system will not be able to communicate with camera devices from the moment you begin the installation until the moment installation is complete and you have restarted the Recording Server service. Usually, the process takes no longer than a few minutes, but it is highly recommended that you perform the update at a time when you do not expect important incidents to take place.

1. On the recording component machine on which you want to install the new video device drivers version, shut down any running surveillance software, including any running Recording Server service.

2. Double-click the downloaded video device driver file *DeviceInstaller.exe* to begin installation.

   Depending on your security settings, one or more Windows security warnings may appear after you click the link. If such security warnings appear, accept security warnings by clicking the *Run* button (button may have other name; exact button name depends on your operating system version).

3. Select required language, and click *OK*. This will open the *Video Device Driver Setup Wizard*, which will guide you through the installation. Click the *Next* button and follow the wizard prompts.

4. When the wizard is complete, remember to start the Recording Server service again.

Hardware Drivers IDs

If using the Add Hardware Devices Wizard's Import from CSV File option, you must—if cameras and server are offline—specify a *HardwareDriverID* for each hardware device you want to add.

IDs are subject to change without notice. More devices may be supported by the time you read this, as new versions of video device drivers—are released at regular intervals. To view a current list of IDs, view the release notes for the Device Pack used in your organization. Alternatively visit the OnSSI website for the latest information.

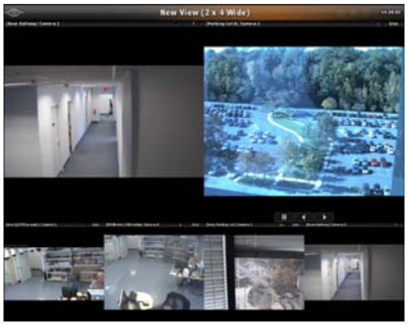
Clients & Ancillary Applications

OCULARIS CLIENT

Users can get access to the RC-P surveillance system in different ways:

- With ***Ocularis Client*** users may:
    - Monitor live video from an unlimited number of cameras at multiple sites
    - Use instant investigation utilities
    - Easily access and investigate alerts generated by motion or external systems
    - Export video clips and still images for further event handling or as course evidence
    - View sites maps to observe cameras from a geographical perspective
    - Push video to a video wall
    - Be alerted to important events that occur
    - Bookmark video clips for easy retrieval and sharing
    - ...and much more!

  Ocularis Client is accessed by logging into Ocularis Base in order to view video from RC-P.



Example: Ocularis Client

- You may also use Ocularis Client to log directly in to the recorder. In this case, the functionality is more restricted. This is called operating ***Ocularis Client in Limited Mode***. Certain features, such as maps and video walls, are not available in this mode.

Recording Server Manager

RECORDING SERVER MANAGER

The Recording Server service is a vital part of the surveillance system; video streams are only transferred to RC-P while the Recording Server service is running. The Recording Server Manager informs you about the state of the Recording Server service. It also lets you manage the service.

In the notification area (also known as Windows system tray), the Recording Server Manager's icon indicates whether the Recording Server service is running or not. Green indicates running (default), red indicates not running.

By right-clicking the icon you can start and stop the Recording Server service, view log files, etc.:

- **Start the Recording Server Service**

  1. Right-click the notification area's Recording Server icon.
  2. In the menu that appears, select *Start Recording Server Service.*
  3. The icon in the notification area changes to green.

- **Stop the Recording Server Service**

  1. Right-click the notification area's Recording Server icon.
  2. In the menu that appears, select *Stop Recording Server Service.*
  3. The icon in the notification area changes to red.

- **Open the Management Application**

  1. Right-click the notification area's Recording Server icon.
  2. In the menu that appears, select *Open Management Application.*

- **Show System Status**

  By right-clicking the notification area's Recording Server icon and then selecting *Show System Status*, you get access to the *Status* window.

  The *Status* window lets you view the status of the image server(s) and connected cameras. The status of each server/camera is indicated by a color:

  - ***Green*** indicates that the server or camera is running correctly.
  - ***Gray*** indicates that the *camera* (not the server) is not running. Typically, a camera will be indicated in gray in the following situations:
    - the camera is not online (as defined in the camera's online period schedule).
    - the Recording Server service has been stopped.

- ***Red*** indicates that the server or camera is not running. This may because it has been unplugged or due to a network or hardware error. Errors are listed in the Recording Server log file.

Place your mouse pointer over a camera in the status window to view details about the camera in question. The information updates approximately every 10 seconds.

- ***Resolution*****:** The resolution of the camera.
- ***FPS*****:** The number of frames per second (also known as frame rate) currently used by the camera. The number updates each time the camera has received 50 frames.
- ***Frame count*****:** The number of frames received from the camera since the Recording Server service was last started.
- ***Received KB*****:** The number of kilobytes sent the by camera since the Recording Server service was last started.
- ***Offline*****:** Indicates the number of times the camera has been offline due to an error.

- **View the Recording Server Service Log File**

  1. Right-click the notification area's Recording Server icon.
  2. In the menu that appears, select *Open Recording Server Log File...*.

- **View the Image Server Service Log File**

  1. Right-click the notification area's Recording Server icon.
  2. In the menu that appears, select *Open Image Server Log File...*.

  For more information about log files, see Configure Audit, Event & System Logging.

- **Access the Built-in Help System**

  1. Right-click the notification area's Recording Server icon.
  2. In the menu that appears, select *Help*.

  For more information, see Use the Built-in Help System.

- **View Version Information**

  Knowing the exact version number can be useful in case you require technical support.

  1. Right-click the notification area's Recording Server icon.
  2. In the menu that appears, select *About...*

- **Exit the Recording Server Manager**
  1. Right-click the notification area's Recording Server icon.
  2. In the menu that appears, select *Exit Recording Server Manager.*

     Tip: If you later want to re-open the Recording Server Manager, go to Windows' Start menu and select *All Programs* > *Startup* > *Recording Server Manager*.

Backup

Back Up System Configuration

We recommend that you make regular backups of your RC-P configuration (cameras, schedules, views, etc.) as a disaster recovery measure. While it is rare to lose your configuration, it can happen under unfortunate circumstances. Luckily, it takes only a minute to back up your existing configuration.

The following describes backup of the configuration in RC-P version 1.0 and onwards.

In the following, we assume that you have not changed the RC-P default configuration path, which is *C:\Documents and Settings\All Users\Application Data\OnSSI\RC-P* on servers running Windows® XP or Windows Server 2003, and *C:\Program Data\OnSSI\RC-P* on servers running all other supported operating systems. If you have changed the default configuration path, you must take your changes into consideration when using the method described in the following.

To Back Up:

1. If RC-P is used on a server running Windows XP or Windows Server 2003, make a copy of the folder *C:\Documents and Settings\All Users\Application Data\OnSSI\RC-P* and all of its content.

   If RC-P is used on a server running any other supported operating system, make a copy of the folder *C:\Program Data\OnSSI\RC-P* and all of its content.

2. Open the folder *C:\Program Files\OnSSI\RC-P\devices*, and verify if the file *devices.ini* exists. If the file exists, make a copy of it. The file will exist if you have configured video properties for certain types of cameras; for such cameras, changes to the properties are stored in the file rather than on the camera itself.

3. Store the copies away from the RC-P server, so that they will not be affected if the server is damaged, stolen or otherwise affected.

   Remember that a backup is a snapshot of your RC-P system configuration at the time of backing up. If you later change your configuration, your backup will not reflect the most recent changes. Therefore, back up your system configuration regularly.

   Tip: When you back up your configuration as described, the backup will include restore points. This allows you to not only restore the backed-up configuration, but also to revert to an earlier point in that configuration if required.

To Restore Your Backed-up Configuration:

1. If RC-P is used on a server running Windows XP or Windows Server 2003, copy the content of the backed-up folder into *C:\Documents and Settings\All Users\Application Data\OnSSI\RC-P*.

   If RC-P is used on a server running any other supported operating system, copy the content of the backed-up folder into *C:\Program Data\OnSSI\RC-P.*

2. If you backed up the file *devices.ini*, copy the file into *C:\Program Files\OnSSI\RC-P\devices.*

Upgrade from a Previous Version

Upgrading your entire RC-P system configuration is a fairly easy task.

- **Back Up Your Current Configuration**

  When you install the new version of RC-P , it will inherit the configuration from your old version.

However, we recommend that you make regular backups of your server configuration as a disaster recovery measure. Upgrading your server is no exception. While it is rare to lose your configuration (cameras, schedules, views, etc), it *can* happen under unfortunate circumstances. Luckily, it takes only a minute to back up your existing configuration:

1. Create a folder called *Backup* on a network drive, or on removable media.
2. On the recorder machine, navigate to the recorder installation folder.
3. Copy the following files and folders into your *Backup* folder:
    - All configuration (.ini) files
    - All scheduling (.sch) files
    - The file *users.txt* (only present in a few installations)
    - Folders with a name ending in *...ViewGroups*

   Note that some of the files/folders may not exist if upgrading from old software versions.

- **Remove the Current Version**

  In most cases, you do not need to manually remove the old version of old recorder before you install the new version. The old version is removed when you install the new version. In fact, manual removal of some versions may cause problems. Please refer to the *Upgrading to Ocularis Guide* for more specific information.

- **Install the New Version**

  Run the installation file for the new software version. Select the installation options that best fit your needs.

- **Restore a Configuration Backup (if Required)**

  If for some reason, after installing the new software version, you have lost your configuration, you can restore your configuration, provided you have followed the previous instructions.

  If for some reason after installing the new software version you have lost your configuration, you can easily restore your configuration, provided you have followed the previous instructions in this chapter.

1. Close the *Management Application* if it is open.
2. Stop the Recording Server Service.
3. Make a copy of the contents of the following directory (RC-P is used in this example):

   C:\ProgramData\OnSSI\RC-P

   Note: on Windows 2003 Server, the location is: C:\Documents and Settings\All Users\Application Data\OnSSI.

   These directories may be hidden from view. If you cannot see the folder, be sure to modify folder options to display hidden files and folders.

4. Delete the <u>contents</u> of the folder:

   C:\ProgramData\OnSSI\RC-P

   Do not delete the folder.

5. Make sure the RC-P installation folder contains a folder named ConfigurationBackup, and that the folder contains the .ini and .sch files from your old configuration. If not, create the folder, and copy your backed-up configuration files into the folder.

6. In Windows' *Start* menu, select *Run…*

7. Type *cmd* and click *OK*.

8. Change directories to: C:\Program Files\Onssi\ProSight

9. In the command line window, type the following TWICE:

10. `Configurationupgrader.exe C:\ProgramData\OnSSI\RC-P` Press [ENTER]
11. `Configurationupgrader.exe C:\ProgramData\OnSSI\RC-P` Press [ENTER]

    This should copy the necessary older configuration files as well as create a configuration.xml to the C:\ProgramData\OnSSI\RC-P directory. It may take a few moments for the configuration.xml file to appear.

12. Close the command line window.

13. Open the Management Application again.

Tip: Once the configuration has been converted, your entire configuration will be contained in a single file. When you later want to back up your configuration, you can simply make a copy of the file configuration.xml.

- ### Upgrade Video Device Drivers

Video device drivers are small programs used for controlling/communicating with the hardware devices connected to an RC-P system.

Video device drivers are installed automatically during the installation of your RC-P system. However, new versions of the video device drivers—called Device Packs—are released and made available for free on the OnSSI website from time to time.

We therefore recommend that you visit the OnSSI website and download the latest Device Pack.

When updating video device drivers, there is no need to remove the old video device drivers first; simply install the latest version on top of any old version you may have. For detailed information, see Update Video Device Drivers.

Removal

REMOVE THE RECORDING COMPONENT

To remove the entire RC-P surveillance system (that is the recording component software and related installation files and video device drivers) from your server, do the following:

1. Shut down all RC-P components.

> The following procedure describes standard system component removal in recent Windows versions; the procedure may be slightly different in older Windows versions:

2. In Windows' *Start* menu, select *Control Panel*, and then...
   - If using Category view, find the Programs category, and click *Uninstall a program*.
   - If using Small icons or Large icons view, select *Programs and Features*.
3. In the list of currently installed programs, right-click the RC-X entry (e.g. RC-P 1.0).
4. Select *Uninstall* and follow the removal instructions.

What happens to my recordings and configuration files? *Your recordings will not be removed; they will remain on the server even after the server software has been removed. Likewise, the RC-P configuration files will remain on the server; this allows you to reuse your configuration if you later install RC-P again.*

REMOVE VIDEO DEVICE DRIVERS

Video device drivers are small programs used for controlling/communicating with the camera devices connected to an RC-P system. To remove the video device drivers, do the following:

1. In Windows' *Start* menu, select *Control Panel*, and then...
   - If using Category view, find the Programs category, and click *Uninstall a program*.
   - If using Small icons or Large icons view, select *Programs and Features*.
2. In the list of currently installed programs, right-click the *Video Device Pack V. [version number]* entry.
3. Select *Uninstall* and follow the removal instructions.

REMOVE OCULARIS CLIENT

To remove the Ocularis Client do the following on the computer on which the Ocularis Client is installed:

1. In Windows' *Start* menu, select *Control Panel*, and then...

- If using Category view, find the Programs category, and click *Uninstall a program*.
- If using Small icons or Large icons view, select *Programs and Features*.

2. In the list of currently installed programs, right-click the Ocularis Client entry.
3. Select *Uninstall* and follow the removal instructions.

Contact Information

On-Net Surveillance Systems (OnSSI)

One Blue Plaza
7th Floor
P.O. Box 1555
Pearl River, NY 10965

Website:	www.onssi.com	
General:	info@onssi.com	845.732.7900
Fax:		845.732.7999
Sales Support:	sales@onssi.com	845.732.7900 x 1
PreSales Support	salesengineering@onssi.com	845.732.7900 x 2
Technical Support:	support@onssi.com	845.732.7900 x 3
Training:	training@onssi.com	845.732.7900 x 4
Marketing:	marketing@onssi.com	845.732.7900 x 5