BOSCH

Bosch Video Management System

Table of contents

1   Using the Help

Notice!

This document describes some functions that are not available for BVMS Viewer.

To find out more about how to do something in BVMS, access the online Help using any of the following methods.

To use the Contents, Index, or Search:

▸   On the **Help** menu, click **Help**. Use the buttons and links to navigate.

To get help on a window or dialog:

▸   On the toolbar, click   ?   .

OR

▸   Press F1 for help on any program window or dialog.

1.1   Finding information

You can find information in the Help in several ways.

To find information in the Online Help:

1.   On the **Help** menu, click **Help**.
2.   If the left-hand pane is not visible, click the **Show** button.
3.   In the Help window, do the following:

Click:	To:
Contents	Display the table of contents for the Online Help. Click each book to display pages that link to topics, and click each page to display the corresponding topic in the right-hand pane.
Index	Search for specific words or phrases or select from a list of index keywords. Double-click the keyword to display the corresponding topic in the right-hand pane.
Search	Locate words or phrases within the content of your topics. Type the word or phrase in the text field, press ENTER, and select the topic you want from the list of topics.

Texts of the user interface are marked **bold**.

▸   The arrow invites you to click on the underlined text or to click an item in the application.

Related Topics

▸   Click to display a topic with information on the application window you currently use.
This topic provides information on the application window controls.

Caution!

Medium risk (without safety alert symbol): Indicates a potentially hazardous situation.

If not avoided, this may result in property damage or risk of damage to the unit.

Cautionary messages should be heeded to help you avoid data loss or damaging the system.

Notice!

This symbol indicates information or a company policy that relates directly or indirectly to the safety of personnel or protection of property.

1.2   Printing the Help

While using the Online Help, you can print topics and information right from the browser window.

To print a Help topic:

1. Right-click in the right pane and select **Print**.
    The **Print** dialog box opens.
2. Click **Print**. The topic is printed to the specified printer.

2 Introduction

The BVMS Viewer is an IP video security application for live viewing and playback video of Bosch network attached cameras and recorders. The software package consists of an Operator Client for live viewing and playback of video and a Configuration Client. The BVMS Viewer supports the current Bosch IP video product portfolio as well as legacy Bosch video devices.

Click the link to access the Open Source Software licenses used by BVMS Viewer: http://www.boschsecurity.com/oss.
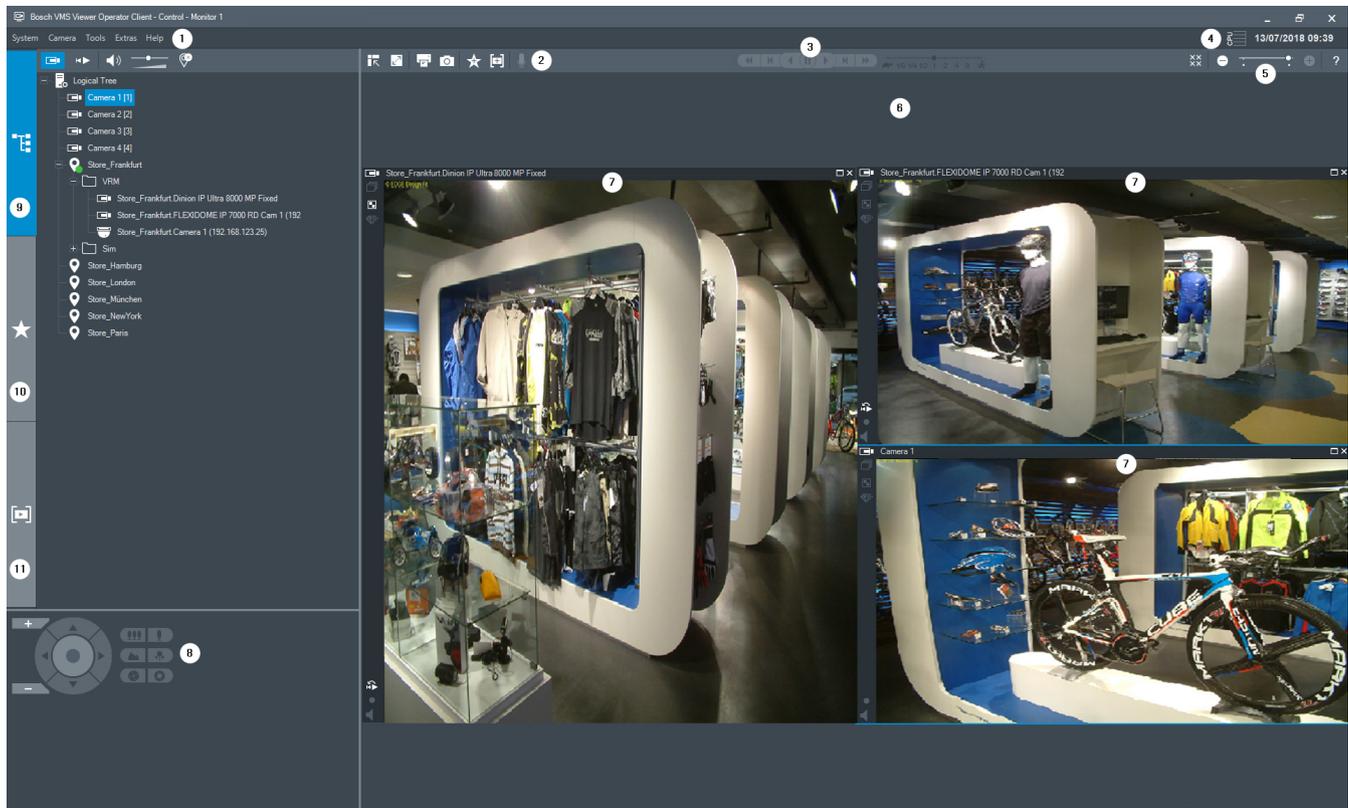
1	Menu bar
2	Toolbar
3	Instant playback control
4	Performance meter
5	Controls for Image panes
6	Image window
7	Image panes
8	PTZ Control window
9	Logical Tree window
10	Favorites Tree window
11	Bookmarks window

3   System overview

Notice!
This document describes some functions that are not available for BVMS Viewer.

Refer to the Release Notes of the current BVMS version for supported versions of firmware and hardware and other important information.
See data sheets on Bosch workstations and servers for information on computers where BVMS can be installed.
The BVMS software modules can optionally be installed on one PC.

3.1   Hardware requirements

See the data sheet for BVMS. Data sheets for platform PCs are also available.

3.2   Software requirements

Viewer cannot be installed where any other BVMS component is installed.

3.3   License requirements

See the data sheet for BVMS for the available licenses.

4   Concepts

This chapter provides background information on selected issues.

Notice!

This document describes some functions that are not available for BVMS Viewer.

4.1   Bosch VMS Viewer

BVMS Viewer is a free of charge variant of BVMS.

The BVMS Viewer system is an all in one BVMS solution for small to medium installations and gives the user of BVMS Viewer Operator Client access to live and recorded video data. Compared to a BVMS system, BVMS Viewer system supports only a subset of the BVMS features and devices. The software is designed for the basic video surveillance operations, like live viewing, playback video, search in recorded video and export of video data.

BVMS Viewer consists of a BVMS Operator Client and BVMS Configuration Client. Both applications show a reduced feature set compared to the two applications in BVMS.

BVMS Viewer Configuration Client is used to add devices to the system, to define the order of the device and to setup users and user preferences.

Device Configuration

Following device are supported:

–
–   Digital Video Recorders
–   Monitor / decoders (only digital monitor walls)
–   VRM devices
–   Live only and local storage cameras
–   unmanaged sites

BVMS Viewer does not overwrite the configuration of the devices, the devices are added with existing configuration to BVMS Viewer. If supported by devices, the configuration of the device can be changed with BVMS Viewer.

Structure of Logical Tree

Cameras, inputs and relays can be structured in the **Maps and Structure** page of BVMS Viewer. Devices can be grouped in folders and the order of devices can be configured.

User groups

In the user group settings, users can be configured, that are allowed to access BVMS Viewer. Depending on the user group settings, users have different rights in BVMS Viewer Operator Client.

Supported features

BVMS Viewer Operator Client supports the following features:

Live viewing:
–   PTZ cameras
–   Favorites
–   Sequences
–   Instant replay
–   Save and print images
–   Select stream
–   Bookmarks

Playback video:

- Smart Motion search
- Forensic Search
- Save and print images
- Export of video data
- Bookmarks

4.2   BVMS design concepts

Single Management Server System, page 13
A single BVMS Management Server System provides management, monitoring and control of up to 2000 cameras/encoders.

Unmanaged site, page 14
Devices can be grouped to unmanaged sites. Devices under unmanaged sites are not monitored by the Management Server. The Management Server provides a list of unmanaged sites to the Operator Client. The Operator can connect on demand to the site and gets access to live video data and recorded video data. Event and alarm handling is not available in the unmanaged site concept.

4.2.1   Single Management Server System

- A single BVMS Management Server can manage up to 2000 channels.
- A BVMS Management Server provides management, monitoring, and control of the entire system.
- The BVMS Operator Client is connected to the Management Server and receives events and alarms from the BVMS Management Server and shows live and playback.
- In most cases all devices are in one local area network with a high bandwidth and a low latency.

Responsibilities:

- Configuring data
- Event log (logbook)
- User profiles
- User priorities
- Licensing
- Event- and alarm-management
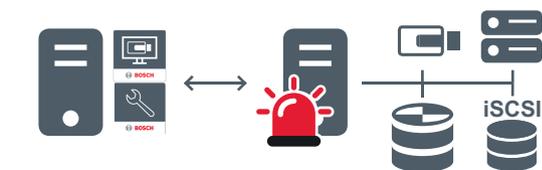
↔   Live, playback, events, alarms

	Management Server
	Operator Client / Configuration Client
	Cameras
	VRM

iSCSI	iSCSI
Other devices	Other devices

4.2.2   Unmanaged site

– A system design option in BVMS with a large number of small subsystems.
– It allows to configure up to 9999 locations in one BVMS Management Server
– Operators can access live and recorded video data from up to 20 sites simultaneously.
– For an easy navigation sites can be grouped in folders or can be placed on maps.
 Predefined username and password allow operators to quickly connect to a store.

The unmanaged site concept supports IP based BVMS system as well as analogue DVR solutions:

– Bosch DIVAR AN 3000 / 5000 analogue recorders
– DIP 3000/7000 units IP based recording
– Single BVMS Management Server System

Adding a site for central monitoring only requires a license per site and is independent of the number of channels in the site.
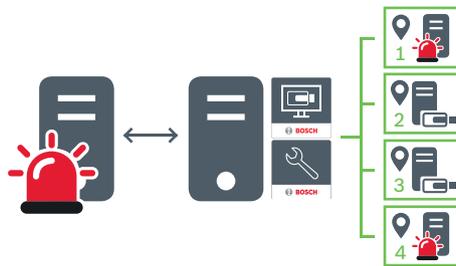
⟷   Live, playback, events, alarms

—   On demand live and playback video traffic

	Management Server
	Operator Client / Configuration Client
	Site
	DVR

See also
– *Adding an unmanaged site, page 30*

4.3   Viewing modes of a panoramic camera

This chapter illustrates the viewing modes of a panoramic camera which are available in BVMS.
The following viewing modes are available:

- Circle view
- Panorama view
- Cropped view

Panorama and cropped view modes are created by the dewarping process in BVMS. Edge dewarping is not used.

The administrator must configure the mounting position of a panoramic camera in Configuration Client.

You can resize the Image pane of a camera as required. The Image pane ratio is not restricted to the 4:3 or 16:9 aspect ratio.

4.3.1   360° panoramic camera - floor- or ceiling mounted

The following figure illustrates the dewarping of a 360° camera which is floor- or ceiling mounted.
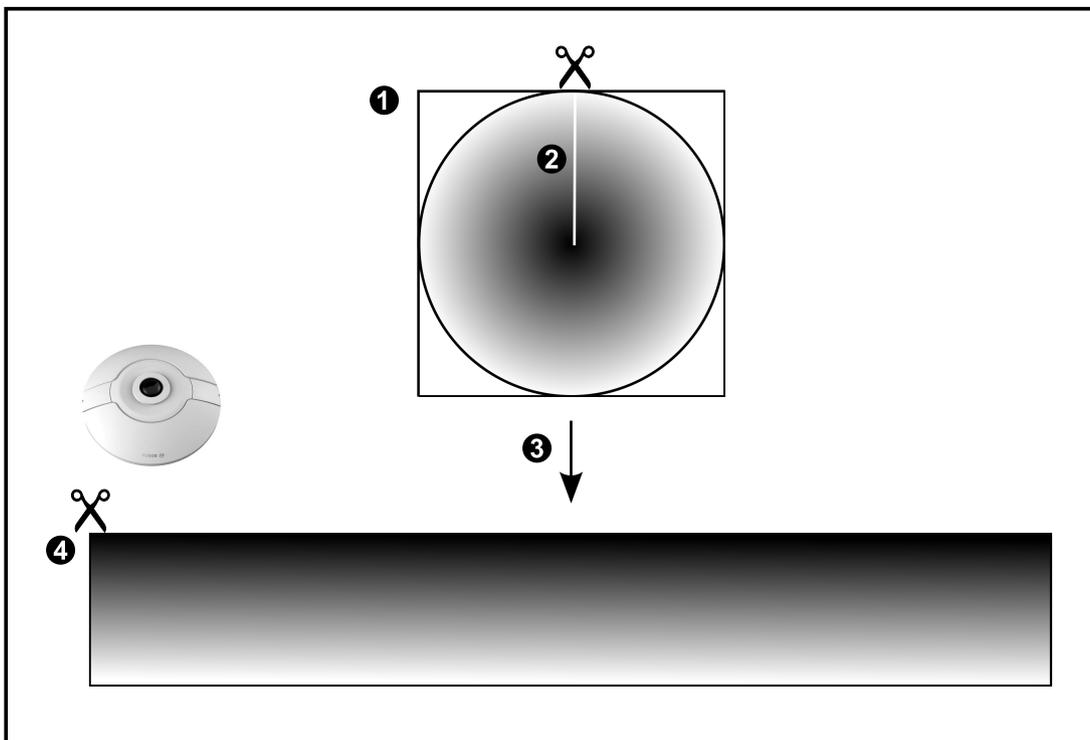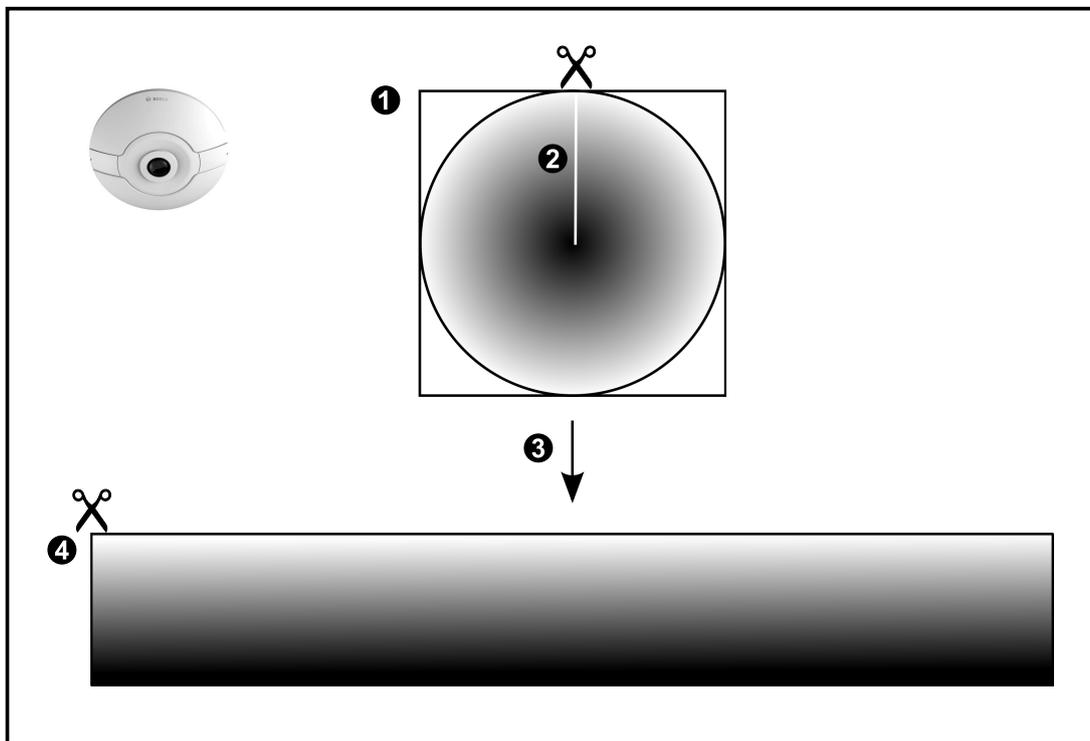
| 1 | Full circle image | 3 | Dewarping |
| 2 | Snipping line (operator can change its position when not zoomed in) | 4 | Panorama view |

4.3.2   **180° panoramic camera - floor- or ceiling mounted**

The following figure illustrates the dewarping of a 180° camera which is floor- or ceiling mounted.
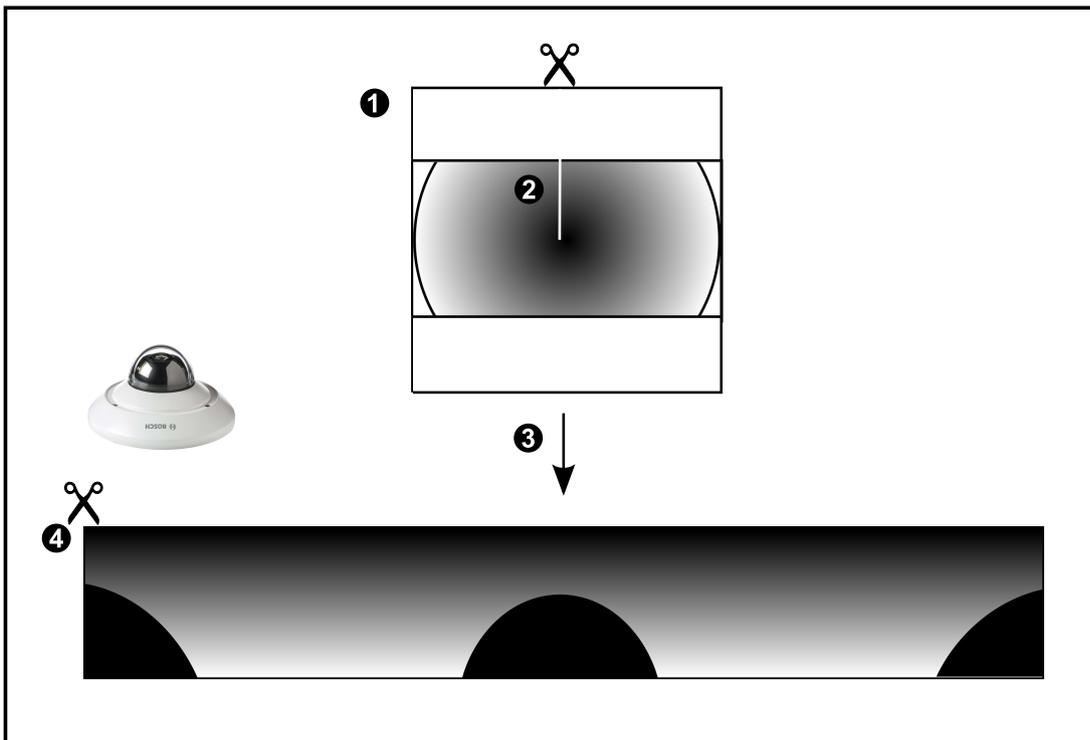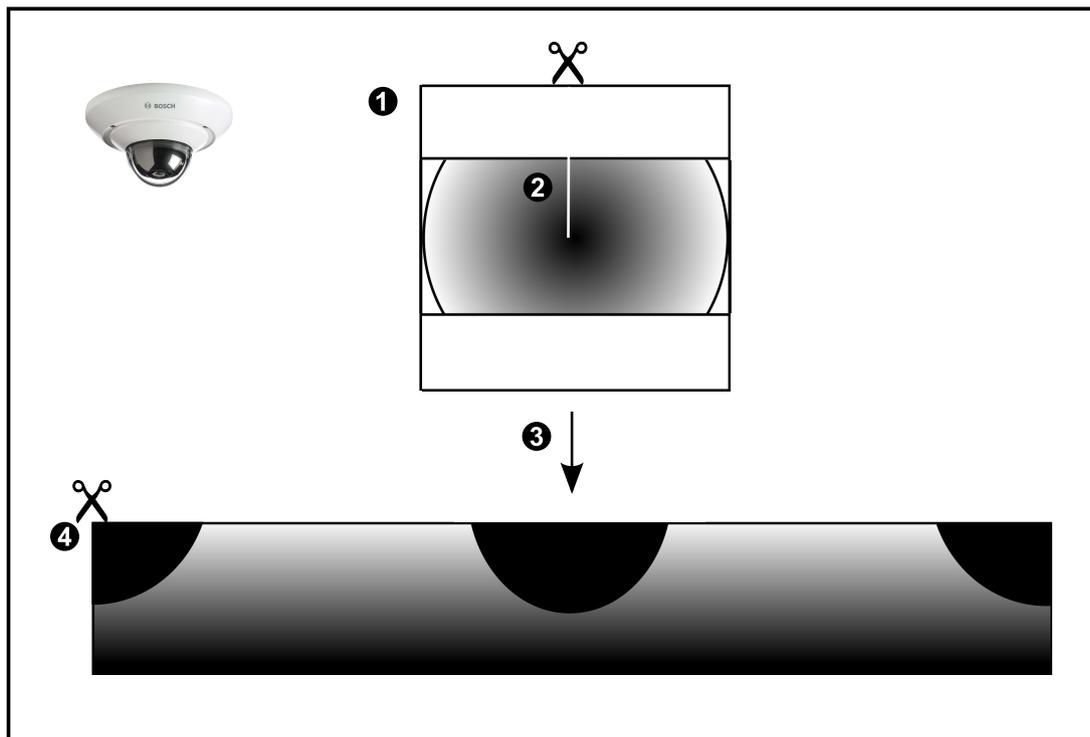
1	Full circle image	3	Dewarping
2	Snipping line (operator can change its position when not zoomed in)	4	Panorama view

4.3.3   **360° panoramic camera - wall mounted**

The following figure illustrates the dewarping of a 360° camera which is wall mounted.
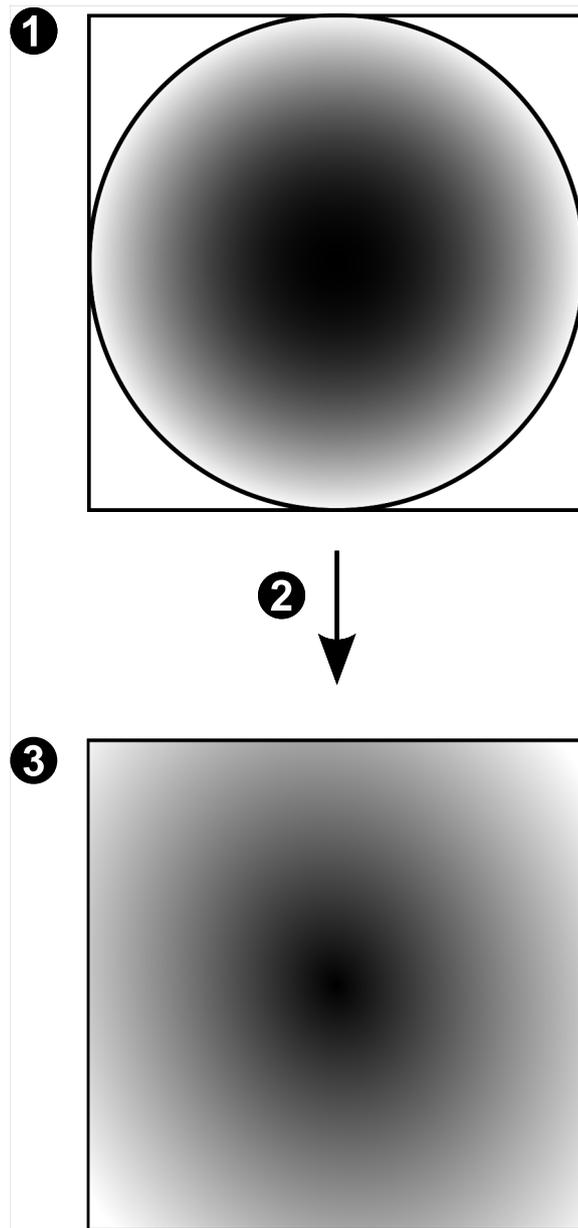
1	Full circle image	3	Panorama view
2	Dewarping		

4.3.4   **180° panoramic camera - wall mounted**

The following figure illustrates the dewarping of a 180° camera which is wall mounted.
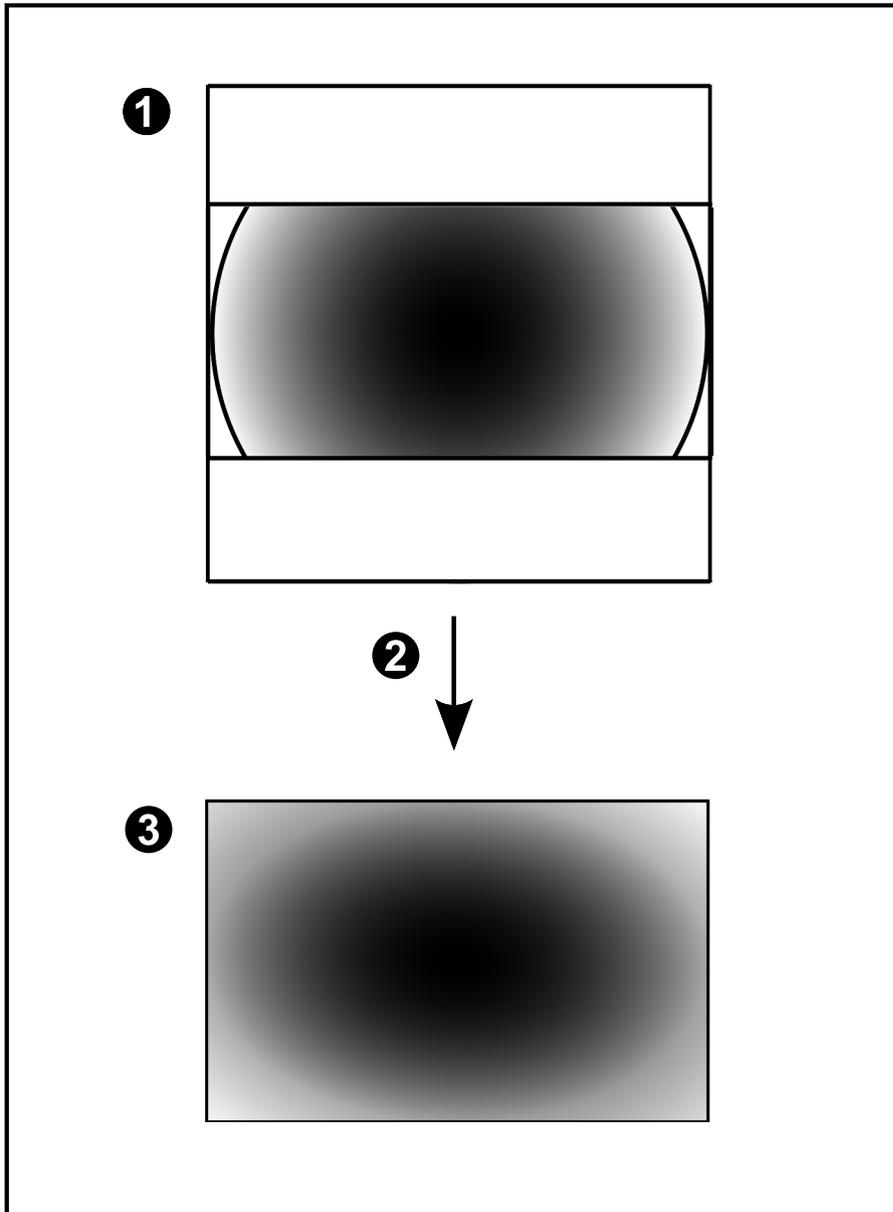
1	Full circle image	3	Panorama view
2	Dewarping		

4.3.5 **Cropped view on a panoramic camera**

The following example figure illustrates the cropping of a 360° camera which is floor- or ceiling mounted.

The rectilinear section used for cropping is fixed. You can change the section in the cropped Image pane using the available PTZ controls.
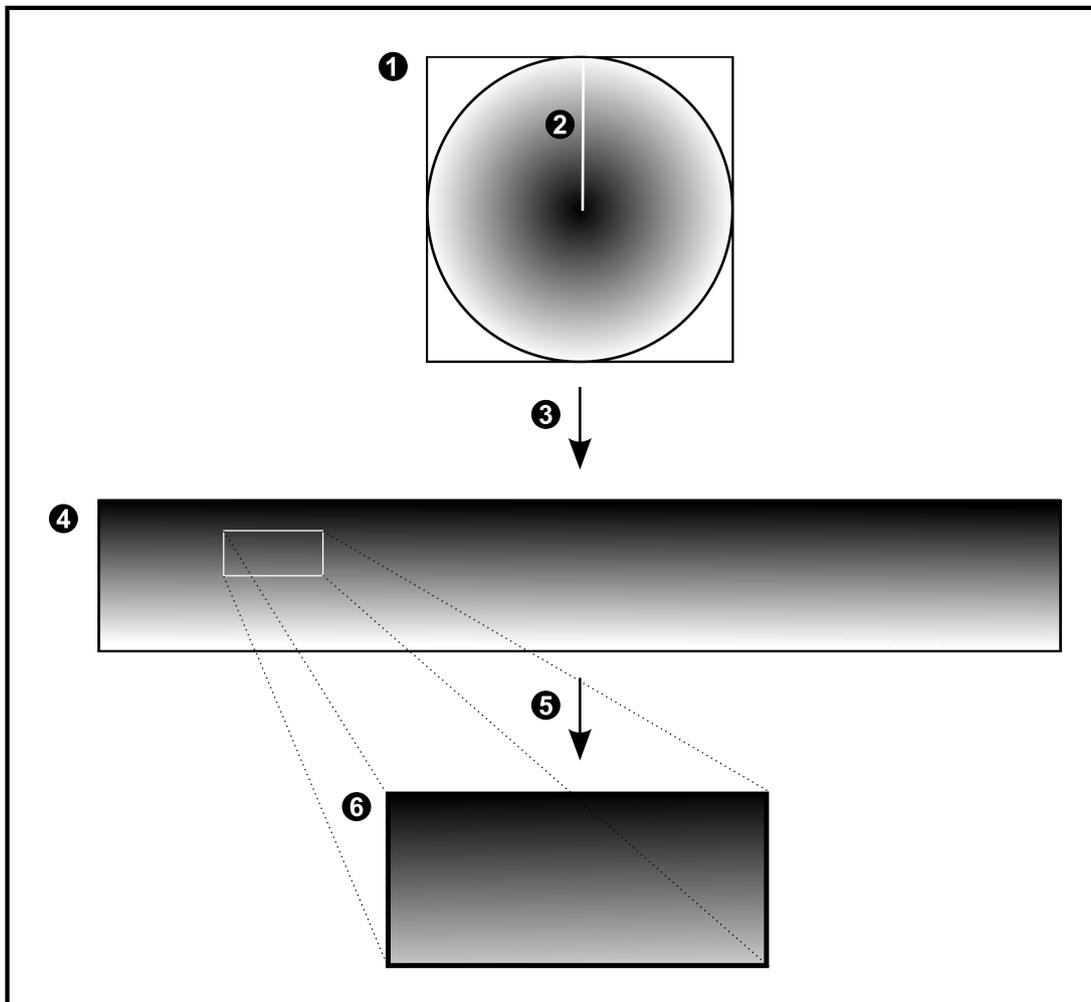
1	Full circle image	4	Panorama view
2	Snipping line (operator can change its position when not zoomed in)	5	Cropping
3	Dewarping	6	Cropped Image pane

4.4   SSH Tunneling

BVMS provides remote connectivity utilizing Secure Shell (SSH) tunneling.
SSH tunneling constructs an encrypted tunnel established by an SSH protocol/socket
connection. This encrypted tunnel can provide transport to both encrypted and un-encrypted
traffic. The Bosch SSH implementation also utilizes Omni-Path protocol, which is a high
performance low latency communications protocol developed by Intel.

Technical aspects and restrictions
–   SSH tunneling utilizes port 5322. This port cannot be modified.
–   The SSH Service must be installed on the same server as the BVMS Management Server.
–   User accounts must have a configured password. User accounts without a password
       cannot log on utilizing a SSH connection.
–   Configuration Client cannot connect remotely via SSH. Configuration Client connection
       must be done via port mapping.
–   Operator Client checks connection with SSH service every 15 seconds. If the connection
       is interrupted, Operator Client retests the connection every minute.

Port mapping
▸   Configure one port forwarding for the BVMS Management Server to utilize port 5322 for
     both internal and external connections.
     This is the only port mapping entry that you need to make for the entire system.
     BVMS port mapping is not required.

Encrypted communication
After the connection is established via a SSH tunnel, all communications between the BVMS
Management Server and a remote client are encrypted.

5   Getting started

This chapter provides information on how to get started with BVMS Viewer.

5.1   Installing BVMS Viewer

Notice!
Installing BVMS Viewer is only allowed on computers, where no other BVMS component is installed.

To install BVMS Viewer:
1.   Start the BVMS Viewer Setup with a double click on the Setup icon. The BVMS Viewer InstallShield Wizard is displayed.
2.   Click **Install** to install **Microsoft .NET Framework 4.6 Full**.
3.   On the Welcome screen click **Next** to continue.
4.   Accept End User License Agreement and click **Next** to continue.
5.   Select the desired installation folder and click **Next** to continue.
     Note: It is not recommended to change the default folder.
6.   Click **Install** to start the installation. BVMS Viewer Installation Wizard installs all components and shows a progress bar.
7.   Click **Finish** to finish the installation.
8.   Reboot workstation after the installation is finished.

5.2   Starting BVMS Viewer Configuration Client

To start BVMS Viewer Configuration Client:
1.   From the **Start** menu, select **Programs** > BVMS Viewer > Configuration Client or double click the Configuration Client icon.

The Login window of the BVMS Configuration Client is displayed.
2.   Fill in the following fields:
     –   **User Name:** type your user name.
         When you start the application for the first time, enter Admin as user name, no password is required.
     –   **Password:** type your password.
     –   **Connection:** select BVMS Viewer to log on to BVMS Viewer.
         Note: In the **Connection:** list, by default the local BVMS Viewer is selected.
         Select **<New...>** to add the IP address of a BVMS Management Server and log on directly to a BVMS Management Server.

5.3   Activating the software licenses

When you log on to BVMS Viewer Configuration Client for the first time, activation of the software licenses is mandatory.
Note: the Base package of BVMS Viewer is free of charge.

Prerequisites
–   Computer with internet access
–   Account for the Bosch Security Systems Software License Manager

Procedure

To activate the software licenses, you must perform following tasks:

1. Retrieving the computer signature
2. Obtaining the activation key
3. Activating the system

See also

–   *License Manager dialog box, page 65*

5.3.1   Retrieving the computer signature

To retrieve the computer signature:

1. Start BVMS Viewer Configuration Client.
2. On the **Tools** menu, click **License Manager...**.
    The **License Manager** dialog box is displayed.
3. Click to check the boxes for the software package, the features, and the expansions that
    you want to activate. For the expansions, enter the number of licenses.
4. Click **Activate**.
    The **License Activation** dialog box is displayed.
5. Copy the computer signature and paste it into a text file.

Notice!

The computer signature can change after exchanging hardware on the Management Server
computer. When the computer signature is changed, the license for the base package
becomes invalid.

To avoid licensing problems, finish the hardware and software configuration before you
generate the computer signature.

The following hardware changes can make the base license invalid:

Exchanging the network interface card.

Adding a VMWare or VPN virtual network interface.

Adding or activating a WLAN network interface.

5.3.2   Obtaining the Activation Key

To obtain the Activation Key**:**

1. On a computer with Internet access, enter the following URL into your browser:
    https://activation.boschsecurity.com.
2. Log on to Bosch Security Systems Software License Manager.
    If you do not have an account yet, create a new account.
3. Click Create Demo Licenses.
    The Create Demo License dialog box is displayed.
4. In the list of demo licenses, select the desired software version for which you want to
    create a demo license and click Submit.
    The License Activation dialog box is displayed.
5. In the License Activation dialog box, fill in the following fields:
    –   Computer Signature : copy the computer signature from the text file where you have
        saved it and paste it here.
    –   Installation Site: enter the installation site information.
    –   Comment: if desired, enter a comment (optional).
6. Click Submit.
    The License Activation dialog box is displayed, showing a summary of your license
    activation and the License Activation Key.

7.   Copy the activation key and paste it into a text file or send it via e-mail to a desired e-mail account.

5.3.3   Activating the system

To activate the system:
1.   Start BVMS Viewer Configuration Client.
2.   On the **Tools** menu, click **License Manager…**.
      The **License Manager** dialog box is displayed.
3.   Click to check the boxes for the software package, the features, and the expansions that you want to activate. For the expansions, enter the number of licenses.
4.   Click **Activate**.
      The **License Activation** dialog box is displayed.
5.   Copy the License Activation Key from the text file where you have saved it and paste it into the **License Activation Key:** field.
6.   Click **Activate**.
      The appropriate software packages are activated.
7.   Click **Close** to close the **License Manager** dialog box.

5.4   Preparing devices

Bosch video devices that shall be added to a BVMS Viewer must have an assigned fixed IP address and need to be preconfigured. To assign an IP address to the device, use the device configuration webpage or use Bosch tools to assign IP addresses. Recording relevant settings have to be done on the recorders via device configuration tools or device web pages.
For device specific configuration, please refer to the configuration or user manual of the desired device.

5.5   Configuring the language of Configuration Client

You configure the language of your Configuration Client independently of the language of your Windows installation.

To configure the language:
1.   On the **Settings** menu, click **Options…**.
      The **Options** dialog box is displayed.
2.   In the **Language** list, select the desired language.
      If you select the **System language** entry, the language of your Windows installation is used.
3.   Click **OK**.
      The language is switched after the next restart of the application.

5.6   Configuring the language of Operator Client

You configure the language of your Operator Client independently of the language of your Windows installation and of your Configuration Client. This step is performed in the Configuration Client.

To configure the language:
1.   Click **User Groups** > . Click the **User Group Properties** tab. Click the **Operating Permissions** tab.
2.   In the **Language** list, select the desired language.
3.   Click to save the settings.

4.   Click ![icon] to activate the configuration.
      Restart Operator Client.

5.7   Scanning for devices

Main window > ![icon] **Devices**

You can scan for the following devices to add them with the help of the **Bosch VMS Scan Wizard** dialog box:
–   VRM devices
–   Encoders
–   Live only encoders
–   Live only ONVIF encoders
–   Local storage encoders
–   Decoders
–   Video Streaming Gateway (VSG) devices
–   DVR devices
–   VIDOS NVRs

See also

To add VRM devices via scan:

1.   Right-click ![icon] and click **Scan for VRM Devices**.
      The **Bosch VMS Scan Wizard** dialog box is displayed.
2.   Select the desired check boxes for the devices that you want to add.
3.   In the **Role** list, select the desired role.
      It depends on the current type of the VRM device which new role you can select.
      If you select **Mirrored** or **Failover**, the next configuration step is additionally required.
4.   Click **Next >>**.
      The **Authenticate Devices** dialog box of the wizard is displayed.
5.   Type in the password for each device that is protected by a password.
      Password check is performed automatically, when you do not enter a further character in the password field for a few seconds or you click outside the password field.
      If the passwords of all devices are identical, you can enter it in the first **Password** field. Then right-click this field and click **Copy cell to column**.

      In the **Status** column, the successful logons are indicated with ![icon] .

      The failed logons are indicated with ![icon]
6.   Click **Finish**.
      The device is added to your BVMS.

To add encoders via scan:

1. Right-click ![icon] and click **Scan for Encoders**.
   The **Bosch VMS Scan Wizard** dialog box is displayed.
2. Select the required encoders, select the desired VRM pool and click **Assign** to assign
   them to the VRM pool.
3. Click **Next >>**.
   The **Authenticate Devices** dialog box of the wizard is displayed.
4. Type in the password for each device that is protected by a password.
   Password check is performed automatically, when you do not enter a further character in
   the password field for a few seconds or you click outside the password field.
   If the passwords of all devices are identical, you can enter it in the first **Password** field.
   Then right-click this field and click **Copy cell to column**.

   In the **Status** column, the successful logons are indicated with   .

   The failed logons are indicated with

   ![warning icon] indicates that the device requires an initial password.
   To set the initial password, enter it in the **Password** field.

   The status changes to   .
   Repeat this step for all devices that require an initial password.
   Note: As long as you have not set the initial password for all devices in the list that
   require an initial password, you cannot continue.
5. Click **Finish**.
   The device is added to the Device Tree.

To add Bosch live only devices via scan:

1. Right-click ![camera icon] and click **Scan for Live Only Encoders**.
   The **Bosch VMS Scan Wizard** dialog box is displayed.
2. Select the desired check boxes for the devices that you want to add.
3. Click **Next >>**.
   The **Authenticate Devices** dialog box of the wizard is displayed.
4. Type in the password for each device that is protected by a password.
   Password check is performed automatically, when you do not enter a further character in
   the password field for a few seconds or you click outside the password field.
   If the passwords of all devices are identical, you can enter it in the first **Password** field.
   Then right-click this field and click **Copy cell to column**.

   In the **Status** column, the successful logons are indicated with   .

   The failed logons are indicated with

   ![warning icon] indicates that the device requires an initial password.
   To set the initial password, enter it in the **Password** field.

   The status changes to   .

Repeat this step for all devices that require an initial password.

Note: As long as you have not set the initial password for all devices in the list that require an initial password, you cannot continue.

5. Click **Finish**.

The device is added to the Device Tree.

To add ONVIF live only devices via scan:

1. Right-click and click **Scan for Live Only ONVIF Encoders**.

The **Bosch VMS Scan Wizard** dialog box is displayed.

2. Select the desired check boxes for the devices that you want to add.

3. Click **Next >>**.

The **Authenticate Devices** dialog box of the wizard is displayed.

4. Type in the password for each device that is protected by a password.

Password check is performed automatically, when you do not enter a further character in the password field for a few seconds or you click outside the password field.

If the passwords of all devices are identical, you can enter it in the first **Password** field. Then right-click this field and click **Copy cell to column**.

In the **Status** column, the successful logons are indicated with   .

The failed logons are indicated with

5. Click **Finish**.

The device is added to your BVMS.

To add local storage encoders via scan:

1. In the Device Tree right-click and click **Scan for Local Storage Encoders**.

The **Bosch VMS Scan Wizard** dialog box is displayed.

2. Select the desired check boxes for the devices that you want to add.

3. Click **Next >>**.

The **Authenticate Devices** dialog box of the wizard is displayed.

4. Type in the password for each device that is protected by a password.

Password check is performed automatically, when you do not enter a further character in the password field for a few seconds or you click outside the password field.

If the passwords of all devices are identical, you can enter it in the first **Password** field. Then right-click this field and click **Copy cell to column**.

In the **Status** column, the successful logons are indicated with   .

The failed logons are indicated with

indicates that the device requires an initial password.

To set the initial password, enter it in the **Password** field.

The status changes to   .

Repeat this step for all devices that require an initial password.

Note: As long as you have not set the initial password for all devices in the list that require an initial password, you cannot continue.

5. Click **Finish**.

The device is added to the Device Tree.

To add VSG devices via scan:

1. Right-click ![icon] and click **Scan for Video Streaming Gateways**.
    The **Bosch VMS Scan Wizard** dialog box is displayed.
2. Select the required VSG devices, select the desired VRM pool and click **Assign** to assign
    them to the VRM pool.
3. Click **Next >>**.
    The **Authenticate Devices** dialog box of the wizard is displayed.
4. Type in the password for each device that is protected by a password.
    Password check is performed automatically, when you do not enter a further character in
    the password field for a few seconds or you click outside the password field.
    If the passwords of all devices are identical, you can enter it in the first **Password** field.
    Then right-click this field and click **Copy cell to column**.

    In the **Status** column, the successful logons are indicated with   .

    The failed logons are indicated with
5. Click **Finish**.
    The device is added to your BVMS.

To add DVR devices via scan:

1. Right-click ![icon] and click **Scan for DVR Devices**.
    The **Bosch VMS Scan Wizard** dialog box is displayed.
2. Select the desired check boxes for the devices that you want to add.
3. Click **Next >>**.
    The **Authenticate Devices** dialog box of the wizard is displayed.
4. Type in the password for each device that is protected by a password.
    Password check is performed automatically, when you do not enter a further character in
    the password field for a few seconds or you click outside the password field.
    If the passwords of all devices are identical, you can enter it in the first **Password** field.
    Then right-click this field and click **Copy cell to column**.

    In the **Status** column, the successful logons are indicated with   .

    The failed logons are indicated with
5. Click **Finish**.
    The device is added to your BVMS.

See also

6   Managing VRM storage

Main window > **Devices** >

This chapter provides information on how to configure the VRM storage in your system.

– Click to save the settings.

– Click to undo the last setting.

– Click to activate the configuration.

Notice!

This document describes some functions that are not available for BVMS Viewer.

6.1   Scanning for VRM devices

Main window > **Devices** >

In your network, you need a VRM service running on a computer, and an iSCSI device.

Caution!

When you add an iSCSI device with no targets and LUNs configured, start a default configuration and add the IQN of each encoder to this iSCSI device.

When you add an iSCSI device with targets and LUNs pre-configured, add the IQN of each encoder to this iSCSI device.

See Configuring an iSCSI device for details.

The system supports you with a scan for devices.

To add VRM devices via scan:

1. Right-click and click **Scan for VRM Devices**.
   The **Bosch VMS Scan Wizard** dialog box is displayed.
2. Select the desired check boxes for the devices that you want to add.
3. In the **Role** list, select the desired role.
   It depends on the current type of the VRM device which new role you can select.
   If you select **Mirrored** or **Failover**, the next configuration step is additionally required.
4. Click **Next >**.
5. In the **Master VRM** list, select the Master VRM for the selected Mirrored or Failover VRM.
6. Click **Next >>**.
   The **Authenticate Devices** dialog box of the wizard is displayed.
7. Type in the password for each device that is protected by a password.
   Password check is performed automatically, when you do not enter a further character in the password field for a few seconds or you click outside the password field.
   If the passwords of all devices are identical, you can enter it in the first **Password** field.

Then right-click this field and click **Copy cell to column**.

In the **Status** column, the successful logons are indicated with   .

The failed logons are indicated with

8. Click **Finish**.
   The device is added to your BVMS.

See also
– *BVMS Scan Wizard, page 75*
– *VRM Devices page, page 76*

6.2 Adding a Primary VRM manually

Main window >   **Devices** > Right-click   > Click **Add VRM** > **Add VRM** dialog box
You can add a Primary VRM device manually if you know the IP address and password.

To add a Primary VRM device:
1. Make the required settings for your VRM device.
2. In the **Type** list, select the **Primary** entry.
3. Click **OK**.
The VRM device is added.

See also
– *Add VRM dialog box, page 76*

6.3 Adding an unmanaged site

Main window >   **Devices** >

To create:

1. Right-click   and then click **Add Unmanaged Site**.
   The **Add Unmanaged Site** dialog box is displayed.
2. Type in a site name and a description.
3. In the **Time zone** list, select the appropriate entry.
4. Click **OK**.
   A new unmanaged site is added to the system.

> **i** **Notice!**
> This document describes some functions that are not available for BVMS Viewer.

See also
– *Unmanaged site, page 14*
– *Unmanaged Site page, page 77*

6.3.1   Adding an unmanaged network device

Main window > **Devices** > >

You can add a video network device to the **Unmanaged Sites** item of the Device Tree.
It is assumed that all unmanaged network devices of an unmanaged site are located in the same time zone.

1.   Right-click this item and then click **Add Unmanaged Network Device**.
      The **Add Unmanaged Network Device** dialog box is displayed.
2.   Select the desired device type.
3.   Type in a valid IP address or hostname and credentials for this device.
4.   Click **OK**.
      A new **Unmanaged Network Device** is added to the system.
      You can now add this unmanaged site to the Logical Tree.
      Please note that only the site is visible in the Logical Tree but not the network devices belonging to this site.
5.   Type in the valid user name for this network device if available.
6.   Type in the valid password if available.

See also
–   *Adding an unmanaged site, page 30*
–   *Unmanaged Network Device page, page 78*
–   *Unmanaged site, page 14*

6.3.2   Importing unmanaged sites

Main window > **Devices** >

You can import a CSV file containing a configuration of a DVR or another BVMS that you want to import in your BVMS as an unmanaged site.

To import:

1.   Right-click and then click **Import Unmanaged Sites**.
2.   Click the desired file and click **Open**.
      One or more new unmanaged site is added to the system.
      You can now add these unmanaged sites to the Logical Tree.
      Note: If an error occurs and the file cannot be imported, an error message informs you accordingly.

6.3.3   Configuring the time zone

Main window > **Devices** > Expand >

You can configure the time zone of an unmanaged site. This is useful when a user of Operator Client wants to access an unmanaged site using a computer with Operator Client located in another time zone than this unmanaged site.

To configure the time zone:

▶   In the **Time zone** list, select the appropriate entry.

See also
– *Unmanaged Site page, page 77*

7   Managing encoders / decoders

Main window > **Devices**

This chapter provides information on how to configure the devices in your system.

This chapter provides information on how to configure the encoders and decoders in your system.

– Click to save the settings.

– Click to undo the last setting.

– Click to activate the configuration.

> **Notice!**
>
> This document describes some functions that are not available for BVMS Viewer.

7.1   Adding an encoder to a VRM pool

Main window > **Devices** > Expand > Expand >

The system supports you with a scan for devices.

To add encoders via scan:

1. Right-click and click **Scan for Encoders**.
   The **Bosch VMS Scan Wizard** dialog box is displayed.
2. Select the required encoders, select the desired VRM pool and click **Assign** to assign them to the VRM pool.
3. Click **Next >>**.
   The **Authenticate Devices** dialog box of the wizard is displayed.
4. Type in the password for each device that is protected by a password.
   Password check is performed automatically, when you do not enter a further character in the password field for a few seconds or you click outside the password field.
   If the passwords of all devices are identical, you can enter it in the first **Password** field.
   Then right-click this field and click **Copy cell to column**.

   In the **Status** column, the successful logons are indicated with   .

   The failed logons are indicated with

   indicates that the device requires an initial password.
   To set the initial password, enter it in the **Password** field.

   The status changes to   .

Repeat this step for all devices that require an initial password.
Note: As long as you have not set the initial password for all devices in the list that require an initial password, you cannot continue.

5. Click **Finish**.
The device is added to the Device Tree.

See also
– *BVMS Scan Wizard, page 75*

7.2 Moving an encoder to another pool

Main window > **Devices** > Expand   > Expand   >   ,

You move a device from one pool to another within the same VRM device without any recording loss.

To move:

1. Right-click   and click **Change Pool ...**.
The **Change pool** dialog box is displayed.
2. In the **New Pool:** list, select the desired pool.
3. Click **OK**.
The device is moved to the selected pool.

7.3 Adding a live only encoder

Main window >   **Devices** >

The system supports you with a scan for devices.

To add Bosch live only devices via scan:

1. Right-click   and click **Scan for Live Only Encoders**.
The **Bosch VMS Scan Wizard** dialog box is displayed.
2. Select the desired check boxes for the devices that you want to add.
3. Click **Next >>**.
The **Authenticate Devices** dialog box of the wizard is displayed.
4. Type in the password for each device that is protected by a password.
Password check is performed automatically, when you do not enter a further character in the password field for a few seconds or you click outside the password field.
If the passwords of all devices are identical, you can enter it in the first **Password** field.
Then right-click this field and click **Copy cell to column**.

In the **Status** column, the successful logons are indicated with   .

The failed logons are indicated with

     indicates that the device requires an initial password.
To set the initial password, enter it in the **Password** field.

The status changes to   .

Repeat this step for all devices that require an initial password.

Note: As long as you have not set the initial password for all devices in the list that require an initial password, you cannot continue.

5.   Click **Finish**.

The device is added to the Device Tree.

To add ONVIF live only devices via scan:

1.   Right-click   and click **Scan for Live Only ONVIF Encoders**.

The **Bosch VMS Scan Wizard** dialog box is displayed.

2.   Select the desired check boxes for the devices that you want to add.

3.   Click **Next >>**.

The **Authenticate Devices** dialog box of the wizard is displayed.

4.   Type in the password for each device that is protected by a password.

Password check is performed automatically, when you do not enter a further character in the password field for a few seconds or you click outside the password field.

If the passwords of all devices are identical, you can enter it in the first **Password** field. Then right-click this field and click **Copy cell to column**.

In the **Status** column, the successful logons are indicated with   .

The failed logons are indicated with

5.   Click **Finish**.

The device is added to your BVMS.

See also

–   *BVMS Scan Wizard, page 75*
–   *Live Only page, page 77*

7.4   Adding a local storage encoder

Main window >   **Devices** >

The system supports you with a scan for devices.

To add local storage encoders via scan:

1.   In the Device Tree right-click   and click **Scan for Local Storage Encoders**.

The **Bosch VMS Scan Wizard** dialog box is displayed.

2.   Select the desired check boxes for the devices that you want to add.

3.   Click **Next >>**.

The **Authenticate Devices** dialog box of the wizard is displayed.

4.   Type in the password for each device that is protected by a password.

Password check is performed automatically, when you do not enter a further character in the password field for a few seconds or you click outside the password field.

If the passwords of all devices are identical, you can enter it in the first **Password** field. Then right-click this field and click **Copy cell to column**.

In the **Status** column, the successful logons are indicated with   .

The failed logons are indicated with

⚠ indicates that the device requires an initial password.

To set the initial password, enter it in the **Password** field.

The status changes to   .

Repeat this step for all devices that require an initial password.

Note: As long as you have not set the initial password for all devices in the list that require an initial password, you cannot continue.

5. Click **Finish**.

The device is added to the Device Tree.

See also
– *BVMS Scan Wizard, page 75*
– *Local Storage page, page 77*

7.5 Configuring an encoder / decoder

To configure an encoder:

Main window > **Devices** > Expand > Expand > >
or

Main window > **Devices** > Expand > Expand > Expand >
or

Main window > **Devices** > >
or

Main window > **Devices** > >

To configure a decoder:

Main window > **Devices** > Expand > Expand >

See the Online Help for the pages for details.

> ℹ **Notice!**
> IP devices can be connected that do not have all configuration pages that are described here.

See also
– *Bosch Encoder / Decoder page, page 79*

7.6   Updating the device capabilities

Main window > **Devices** > Expand > Expand > Expand > Right-click
 > Click **Edit Encoder** > **Edit Encoder** dialog box
or

Main window > **Devices** > Expand > Right-click > Click **Edit Encoder** >
Edit Encoder dialog box
or

Main window > **Devices** > Expand > Right-click > Click **Edit Encoder** >
Edit Encoder dialog box
or

Main window > **Devices** > Expand > Expand > Right-click > Click
Edit Encoder > **Edit Encoder** dialog box
or

Main window > **Devices** > Expand > Expand > Right-click > Click
Edit Decoder > **Edit Decoder** dialog box

After an upgrade of the device, you can update its device capabilities. A message text informs
you whether the retrieved device capabilities match the device capabilities stored in BVMS.

To update:
1.   Click **OK**.
      A message box is displayed with the following text:
      **If you apply the device capabilities, the recording settings and the event settings for
      this device may change. Check these settings for this device.**

2.   Click **OK**.
      The device capabilities are updated.

See also
–   *Edit Encoder / Edit Decoder dialog box, page 71*

7.7   Configuring failover recording mode on an encoder

Main window > **Devices** > Expand > Expand , ,
Prerequisites: On the **Pool** page, in the **Recording preferences mode** list, select **Failover**. If
Automatic is selected, the settings are performed automatically and cannot be configured.
If you want to use a secondary target for both automatic or failover mode: On the **Pool** page,
in the **Secondary target usage** list, select **On**.

It is recommended to configure at least 2 iSCSI devices for failover mode.

To configure:

1. Click **Advanced Settings**.
2. Click **Recording Preferences**.
3. Under **Primary target**, select the entry for the required target. All storage systems entered under **Storage Systems** will be shown in the list.
4. Under **Secondary target**, select the entry for the required target. All storage systems entered under **Storage Systems** are displayed in the list.
   The changes are active immediately. An activation is not required.

Related Topics

– Configuring automatic recording mode on a pool

7.8 Configuring multiple encoders / decoders

Main window

You can modify the following properties of multiple encoders and decoders at once:

– Display names
– IP addresses
– Firmware versions

Notice!

Changing the IP address of an IP device can make it unreachable.

To configure multiple IP addresses:

1. On the **Hardware** menu, click **IP Device Configuration...**. The **IP Device Configuration** dialog box is displayed.
2. Select the required devices. You can select multiple devices by pressing the CTRL- or the SHIFT-key.
3. Right-click the selected devices and click **Set IP Addresses...**. The **Set IP Addresses** dialog box is displayed.
4. In the **Start with:** field, type the first IP address.
5. Click **Calculate**. In the **End with:** field, the last IP address of the range for the selected devices is displayed.
6. Click **OK**.
7. In the **IP Device Configuration...** dialog box, click **Apply**.
   The new IP addresses are updated in the selected devices.

To configure multiple display names:

1. On the **Hardware** menu, click **IP Device Configuration...**. The **IP Device Configuration** dialog box is displayed.
2. Select the required devices. Multiple selection is possible by pressing the SHIFT key.
3. Right-click the selected devices and click **Set Display Names...** The **Set Display Names** dialog box is displayed.
4. In the **Start with:** field, type the first string.
5. Click **Calculate**. In the **End with:** field, the last string of the range for the selected devices is displayed.
6. Click **OK**.
7. In the **IP Device Configuration...** dialog box, click **Apply**.
   The calculated names are updated in the selected devices.

To update firmware for multiple devices:
1. On the **Hardware** menu, click **IP Device Configuration...**. The **IP Device Configuration** dialog box is displayed.
2. Select the required devices.
3. Click **Update Firmware**.
4. Select the file containing the update.
5. Click **OK**.

7.9   Changing the password of an encoder / decoder

Main window > **Devices** > Expand > Expand , ,

Main window > **Devices** > Expand > Expand ,

Main window > **Devices** > Expand > Expand > Expand ,

Main window > **Devices** > ,

Main window > **Devices** > ,
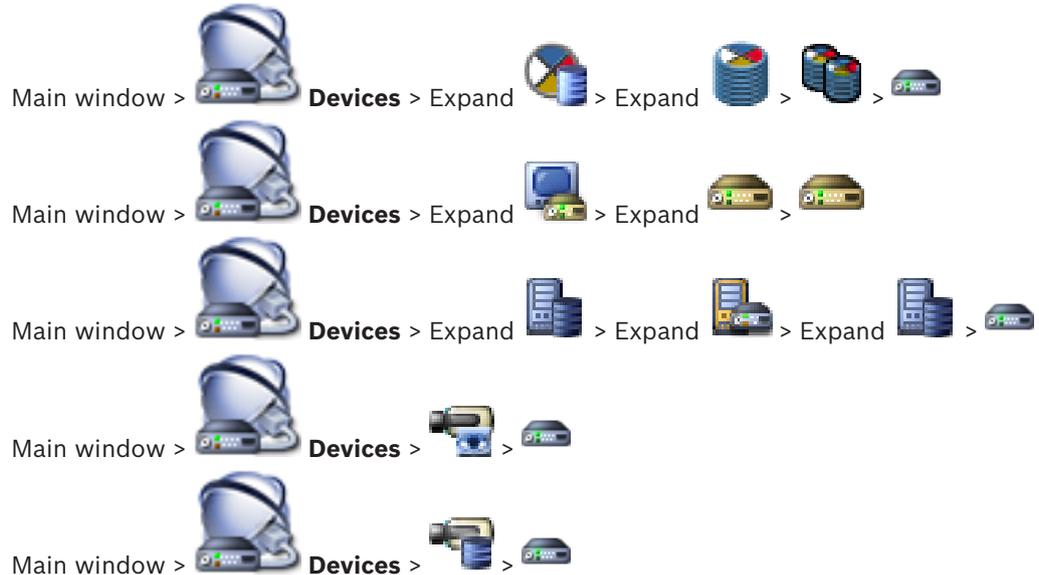
Define and change a separate password for each level. Enter the password (19 characters maximum; no special characters) for the selected level.

To change the password:

1. Right-click and click **Change password...**.
    The **Enter password** dialog box is displayed.
2. In the **Enter user name** list, select the desired user for which you want to change the password.
3. In the **Enter password for user** field, type in the new password.
4. Click **OK**.
✓ The password is changed immediately on the device.

See also
– *Enter password dialog box, page 72*

7.10   Providing the destination password for a decoder

Main window > **Devices** > Expand > Right-click > Click **Add Decoder** >
Add Decoder dialog box
To enable the access of a password protected encoder to a decoder, you must enter the password of the user authorization level of the encoder as the destination password in the decoder.

To provide:

1. In the **Enter user name** list, select destination password.
2. In the **Enter password for user** field, type in the new password.
3. Click **OK**.
✓ The password is changed immediately on the device.

See also
– *Enter password dialog box, page 72*

7.11   Encrypting live video

Main window > **Devices** > Expand > Expand > Right-click > Click
Edit Encoder > **Edit Encoder** dialog box

Main window > **Devices** > Right-click > Click **Edit Encoder** > **Edit Encoder**
dialog box

Main window > **Devices** > Right-click > Click **Edit Encoder** > **Edit Encoder**
dialog box

You can activate the encryption of live video transferred from an encoder to the following
devices if HTTPS port 443 is configured on the encoder:
– Operator Client computer
– Management Server computer
– Configuration Client computer
– VRM computer
– Decoder

Note:
When activated, the user of Operator Client cannot switch a stream to UDP and to UDP
multicast.
When activated, ANR does not work for the affected device.
When activated, encoder replay does not work on encoders with firmware earlier than 6.30.

To activate:
1. Click to enable **Secure connection (encryption)**.
2. Click **OK**.
   Encryption is enabled for this encoder.

See also
– *Network Access page, page 109*
– *Edit Encoder / Edit Decoder dialog box, page 71*

7.12   Managing the verification of authenticity

For activating the verification of authenticity on an encoder, you must perform the following
steps:
– Configure the authentication on the encoder.
– Download a certificate from the encoder.

– Install this encoder certificate on the workstation used for authenticity verification.

7.12.1 **Configuring the authentication**

Main window > ![icon] **Devices** > Expand ![icon] > Expand ![icon] > Expand ![icon] , ![icon]

or

Main window > ![icon] **Devices** > Expand ![icon] > ![icon]

You can activate the verification of authenticity on an encoder.

To configure:
1. Click **Camera**, and then click **Video Input**.
2. In the **Video authentication** list, select **SHA-256**.
3. In the **Signature intervals** list, select the desired value.
   A small value increases the security, a large value reduces the load for the encoder.
4. Click ![icon] .

See also
– *Video Input page, page 88*

7.12.2 **Downloading a certificate**

Main window > ![icon] **Devices** > Expand ![icon] > Expand ![icon] > Expand ![icon] , ![icon]

or

Main window > ![icon] **Devices** > Expand ![icon] > ![icon]

You can download a certificate from an encoder.

To download:
1. Click **Service**, and then click **Certificates**.
2. Select the desired certificate and click the `Save` icon.

![Usage - HTTPS server with save icon circled]
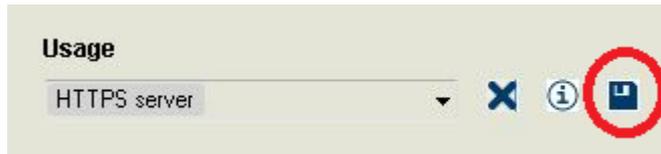
3. Select the appropriate directory for saving the certificate file.
4. Rename the file extension of the certificate file to `*.cer`.

You can now install this certificate on the workstation where you want to verify authenticity.

7.12.3 **Installing a certificate on a workstation**

You can install the certificate that you have downloaded from an encoder, on a workstation where you want to perform authenticity verification.
1. On the workstation, start `Microsoft Management Console`.
2. Add the `Certificates` snap-in on this computer with the `Computer account` option selected.

3.   Expand `Certificates (Local computer)`, expand `Trusted Root Certification Authorities`.
4.   Right-click `Certificates`, point to `All Tasks` and then and click `Import...`.
        The `Certificate Import Wizard` is displayed.
        The `Local Machine` option is preselected and cannot be changed.
5.   Click `Next`.
6.   Select the certificate file that you have downloaded from the encoder.
7.   Click `Next`.
8.   Leave the settings unchanged and click `Next`.
9.   Leave the settings unchanged and click `Finish`.

7.13   Recovering recordings from a replaced encoder

Main window > **Devices** > Expand > Expand > >

If replacing a defective encoder, the recordings of the replaced encoder are available for the new encoder when selecting the new encoder in the Operator Client.

> **Notice!**
> An encoder can only be replaced by an encoder with the same amount of channels.

To recover recordings from a replaced encoder

> **Notice!**
> Do not use the **Edit Encoder** command.

1.   Right-click > **Associate with recordings of predecessor ...** command.
2.   The **Associate with recordings of predecessor ...** dialog box is displayed.
3.   Type in the network address and a valid password for the new device.
4.   Click **OK**.
5.   Click to save the settings.
6.   Click to activate the configuration.

8   Managing various devices

Main window > ![icon] **Devices**

This chapter provides information on how to configure the devices in your system.

–   Click ![icon] to save the settings.

–   Click ![icon] to undo the last setting.

–   Click ![icon] to activate the configuration.

> **Notice!**
> This document describes some functions that are not available for BVMS Viewer.

8.1   Configuring the integration of a DVR

Main window > ![icon] **Devices** > Expand ![icon] > ![icon]

> **Caution!**
> Add the DVR using the administrator account of the device. Using a DVR user account with
> restricted permissions can result in features that are not usable in BVMS, for example using
> the control of a PTZ camera.

> **Notice!**
> You do not configure the DVR itself but only the integration of the DVR device into BVMS.

To add DVR devices via scan:

1.   Right-click ![icon] and click **Scan for DVR Devices**.
      The **Bosch VMS Scan Wizard** dialog box is displayed.
2.   Select the desired check boxes for the devices that you want to add.
3.   Click **Next >>**.
      The **Authenticate Devices** dialog box of the wizard is displayed.
4.   Type in the password for each device that is protected by a password.
      Password check is performed automatically, when you do not enter a further character in
      the password field for a few seconds or you click outside the password field.
      If the passwords of all devices are identical, you can enter it in the first **Password** field.
      Then right-click this field and click **Copy cell to column**.

      In the **Status** column, the successful logons are indicated with ![icon] .

      The failed logons are indicated with ![icon]

5.   Click **Finish**.
      The device is added to your BVMS.

To remove an item:
1.   Click the **Settings** tab, the **Cameras** tab, the **Inputs** tab, or the **Relays** tab.
2.   Right-click an item and click **Remove**. The item is removed.

Notice!

To restore a removed item, right-click the DVR device and click **Rescan DVR Device**.

To rename a DVR device:
1.   Right-click a DVR device and click **Rename**.
2.   Type the new name for the item.

See also
–   *BVMS Scan Wizard, page 75*
–   *DVR (Digital Video Recorder) page, page 67*

8.2   Adding a monitor wall

Main window > **Devices** > Right-click > Click **Add Monitor Wall**.

After having added the monitor wall, the user of Operator Client can control this monitor wall.
The user can change the monitor layout and assign encoders to monitors.

To add:
1.   Select the desired decoder.
2.   If required, enter the maximum number of cameras and configure thumbnails.
3.   Click .
4.   Click **Maps and Structure**.
5.   Drag the monitor wall to the Logical Tree.
6.   If required, configure the access to the monitor wall with corresponding user group permissions.

See also
–   *Add Monitor Wall dialog box, page 74*

8.3   Adding an analog monitor group

Main window > **Devices** > Right-click

1.   Click **Add Monitor Group**.
     The **Create New Analog Monitor Group** dialog box is displayed.
2.   Make the appropriate settings.
3.   Click **OK**.
     The analog monitor group is added to your system.
4.   Click **Maps and Structure**.

5.   Drag the monitor wall to the Logical Tree.

8.4   Configuring bypass of devices

Main window > **Maps and Structure**

It is possible to bypass certain encoders, cameras, inputs and relays, for example, during construction work. If an encoder, camera, input or relay is bypassed, recording is stopped, the BVMS Operator Client does not display any events or alarms and alarms are not recorded in the Logbook.

The bypassed cameras still show live video in the Operator Client and the Operator still has access to old recordings.

> **Notice!**
> If the encoder is bypassed, no alarms and events are generated for all cameras, relays and inputs of this encoder. If a certain camera, relay or input is bypassed separately and the certain device will be disconnected from the encoder, these alarms are still generated.

To bypass / unbypass a device in the Logical Tree or in the Device Tree:
1.   In the Logical Tree or in the Device Tree right-click the certain device.
2.   Click **Bypass** / **Unbypass**.

To bypass / unbypass a device on a map:
See Managing devices on a map

> **Notice!**
> It is possible to filter bypassed devices in the search text field.

9   Configuring the Logical Tree

This chapter provides information on how to configure the Logical Tree and how to manage resource files such as maps.

> **Notice!**
> If you move a group of devices in the Logical Tree, these devices loose their permission settings. You must set the permissions in the **User Groups** page again.

– Click ![save icon] to save the settings.

– Click ![undo icon] to undo the last setting.

– Click ![activate icon] to activate the configuration.

> **Notice!**
> This document describes some functions that are not available for BVMS Viewer.

See also
– *Adding a monitor wall, page 44*
– *Adding an analog monitor group, page 44*
– *Sequence Builder dialog box, page 119*
– *Add Sequence dialog box, page 120*
– *Add Sequence Step dialog box, page 120*

9.1   Configuring the Logical Tree

See also
– *Maps and Structure page, page 118*

9.2   Adding a device to the Logical Tree

Main window > ![Maps and Structure icon] **Maps and Structure**

To add a device:

▸ Drag an item from the Device Tree to the required location in the Logical Tree.
   You can drag a complete node with all sub-items from the Device Tree to the Logical Tree.
   You can select multiple devices by pressing the CTRL- or the SHIFT-key.

See also
– *Maps and Structure page, page 118*

9.3   Removing a tree item

Main window > ![Maps and Structure icon] **Maps and Structure**

To remove a tree item from the Logical Tree:

▶ Right-click an item in the Logical Tree and click **Remove**. If the selected item has sub-items, a message box is displayed. Click **OK** to confirm. The item is removed.
When you remove an item from a map folder of the Logical Tree, it is also removed from the map.

See also

– *Maps and Structure page, page 118*

9.4   Managing pre-configured camera sequences

Main window >   **Maps and Structure**

You can perform the following tasks for managing camera sequences:

– Create a camera sequence
– Add a step with a new dwell time to an existing camera sequence
– Remove a step from camera sequence
– Delete a camera sequence

Notice!

When the configuration is changed and activated, a camera sequence (pre-configured or automatic) usually is continued after restart of the Operator Client.

But in the following cases the sequence is not continued:

A monitor where the sequence is configured to be displayed has been removed.

The mode of a monitor (single/quad view) where the sequence is configured to be displayed has been changed.

The logical number of a monitor where the sequence is configured to be displayed is changed.

Notice!

After each of the following tasks:

Click to save the settings.

To create a camera sequence:

1. In the Logical Tree, select a folder where you want to create the camera sequence.

2. Click .
   The **Sequence Builder** dialog box is displayed.

3. In the **Sequence Builder** dialog box, click .
   The **Add Sequence** dialog box is displayed.

4. Enter the appropriate values.

For detailed information on the various fields, see the Online Help for the appropriate application window.

▶ Click **OK**.

A new camera sequence is added.

To add a step with a new dwell time to a camera sequence:

1. Select the desired camera sequence.

2.   Click **Add Step**.

The **Add Sequence Step** dialog box is displayed.

3.   Make the appropriate settings.

4.   Click **OK**.

A new step is added to the camera sequence.

To remove a step from a camera sequence:

▸   Right-click the desired camera sequence and click **Remove Step**.

The step with the highest number is removed.

To delete a camera sequence:

1.   Select the desired camera sequence.

2.   Click   . The selected camera sequence is removed.

See also

–   *Sequence Builder dialog box, page 119*
–   *Add Sequence dialog box, page 120*
–   *Add Sequence Step dialog box, page 120*

9.5   Adding a camera sequence

Main window >   **Maps and Structure**

You add a camera sequence to the root directory or to a folder of the Logical Tree.

To add a camera sequence:

1.   In the Logical Tree, select a folder where you want to add the new camera sequence.

2.   Click   . The **Sequence Builder** dialog box is displayed.

3.   In the list, select a camera sequence.

4.   Click **Add to Logical Tree**. A new   is added under the selected folder.

See also

–   *Sequence Builder dialog box, page 119*

9.6   Adding a folder

Main window >   **Maps and Structure**

To add a folder:

1.   Select a folder where you want to add the new folder.

2.   Click   . A new folder is added under the selected folder.

3.   Click   to rename the folder.

4.   Type the new name and press ENTER.

See also

–   *Maps and Structure page, page 118*

10   Configuring cameras and recording settings

Notice!
This document describes some functions that are not available for BVMS Viewer.

Main window > ![icon] **Cameras and Recording**

This chapter provides information on how to configure the cameras in your BVMS.
You configure various camera properties and the recording settings.

–   Click ![icon] to save the settings.

–   Click ![icon] to undo the last setting.

–   Click ![icon] to activate the configuration.

See also
–   *Cameras page, page 121*
–   *PTZ/ROI Settings dialog box, page 124*
–   *COM1, page 104*

10.1   Configuring PTZ port settings

Main window > ![icon] **Devices** > Expand ![icon] > Expand ![icon] > Expand ![icon] , ![icon] >
Interfaces tab > **Periphery** tab
or

Main window > ![icon] **Devices** > Expand ![icon] > Expand ![icon] > ![icon] > **Interfaces** tab >
Periphery tab
or

Main window > ![icon] **Devices** > ![icon] > ![icon] > **Interfaces** tab > **Periphery** tab

You can only configure port settings for an encoder where the control of the camera is
available and activated.
When the encoder or PTZ camera is exchanged, the port settings are not retained. You must
again configure them.
After a firmware update check the port settings.
To configure the port settings of an encoder:
▸   Make the appropriate settings.
       The settings are valid immediately after saving. You do not have to activate the
       configuration.
For detailed information on the various fields, see the Online Help for the appropriate
application window.

See also

– *Periphery page, page 104*

10.2   Configuring PTZ camera settings

Main window > **Cameras and Recording** >

First configure the port settings of your PTZ camera before you can configure the PTZ camera settings. Otherwise the PTZ control is not working in this dialog box.

You can remove menu items of the context menu displayed on a PTZ camera hot spot on a map.

To configure the control of a camera:

1.   In the Camera Table, select the required encoder.

2.   To activate the control of a camera: In the column, select the check box.

3.   Click the button.
     The dialog box for configuring PTZ settings is displayed.

4.   Remove the prepositions that you do not want to be displayed as context menu items on a map.

5.   Make the appropriate settings.

6.   Click **OK**.

For detailed information on the various fields, follow the link to the appropriate application window below.

See also

– *PTZ/ROI Settings dialog box, page 124*
– *Configuring PTZ port settings, page 49*

11   Configuring users, permissions and Enterprise Access

Main window >   **User Groups**

This chapter provides information on how to configure user groups, Enterprise User Groups and Enterprise Access. You configure all device permissions and operating permissions per user group and not per user.

A user can only be the member of one user group or Enterprise User Group.

You cannot change the settings of a default user group.

This user group has access to all the devices of the Full Logical Tree and is assigned the **Always** schedule.

For accessing the Windows user groups of a domain, LDAP user groups are used.

> **Notice!**
> Enterprise User Groups and Enterprise Access are not available for BVMS Viewer.

– Click   to save the settings.

– Click   to undo the last setting.

– Click   to activate the configuration.

> **Notice!**
> This document describes some functions that are not available for BVMS Viewer.

Strong password policy

To enhance the protection of your computer against unauthorized access, it is recommended to use strong passwords for user accounts.

Hence a strong password policy is enabled by default for all newly created user groups. This includes admin user group as well as standard user groups, Enterprise user groups and Enterprise Access.

The following rules apply:

– Minimum password length as set on the **Account policies** page for the appropriate user group.
– At least one upper-case letter (A through Z).
– At least one number (0 through 9).
– At least one special character (for example: ! $ # %).
– Previous password must not be used.

When the Admin user starts Configuration Client for the first time, the **Password policy is violated** dialog box is displayed asking him to set a password for the Admin user account. We highly recommend to keep this setting and to set a strong password for the Admin user account according to the password policy rules.

When creating new user groups in Configuration Client the strong password policy setting is enabled by default. If you do not set passwords for the new user accounts of the appropriate user group, you cannot activate the configuration. The **Password policy is violated** dialog box is displayed listing all users for whom no password has been set.
To activate the configuration, set the missing passwords.

See also
– *Account policies page, page 136*
– *User Group Properties page, page 127*
– *User Properties page, page 128*
– *Logon Pair Properties page, page 129*
– *Camera Permissions page, page 130*
– *Copy User Group Permissions dialog box, page 131*
– *LDAP Server Settings dialog box, page 131*
– *Logical Tree page, page 133*
– *Operator Features page, page 134*
– *User Interface page, page 135*

11.1   Creating a group or account

Main window >   **User Groups**

You can create a standard user group, an Enterprise User Group or an Enterprise Account.
For adapting the user group permissions to your requirements, create a new user group and change its settings.

> **Notice!**
> Enterprise User Groups and Enterprise Access are not available for BVMS Viewer.

11.1.1   Creating a standard user group

Main window >   **User Groups**

To create a standard user group:
1. Click the **User Groups** tab.
2. Click   .
    The **New User Group** dialog box is displayed.
3. Type in the name and a description.
4. Click **OK**.
    A new group is added to the corresponding tree.
5. Right-click the new user group and click **Rename**.
6. Enter the desired name and press ENTER.

See also
– *User Group Properties page, page 127*
– *Operator Features page, page 134*
– *User Interface page, page 135*

11.2 Creating a user

Main window > **User Groups** > **User Groups** tab
or

Main window > **User Groups** > **Enterprise User Group** tab

> **Notice!**
> Enterprise User Groups and Enterprise Access are not available for BVMS Viewer.

You create a user as a new member of an existing standard user group or Enterprise User Group.

> **Notice!**
> A user who wants to operate a Bosch IntuiKey keyboard connected to a decoder, must have a number-only user name and password. The user name can have maximum 3 numbers; the password can have maximum 6 numbers.

To create a user:

1. Select a group and click or right-click the desired group and click **New User**.
   A new user is added to the **User Groups** tree.
2. Right-click the new user and click **Rename**.
3. Enter the desired name and press ENTER.
4. On the **User Properties** page, type the user name and a description.
5. The **User must change password at next logon** check box is pre-selected for all newly created user accounts.
   Type the password according to the password policy rules and confirm this password.
6. Click **Apply** to apply the settings.
7. Click to activate the password.

See also
– *User Properties page, page 128*
– *Strong password policy , page 51*
– *User Groups page, page 126*

11.3 Creating a dual authorization group

Main window > **User Groups** > **User Groups** tab
or

Main window > **User Groups** > **Enterprise User Group** tab

You can create a dual authorization for a standard user group or for an Enterprise User Group.

For Enterprise Access, a dual authorization is not available.

You select two user groups. The members of these user groups are the members of the new dual authorization group.

Notice!

Enterprise User Groups and Enterprise Access are not available for BVMS Viewer.

To create a dual authorization group:

1.   Click .

The **New Dual Authorization Group** dialog box respectively the **New Enterprise Dual Authorization Group** dialog box is displayed.
2.   Type in a name and a description.
3.   Click **OK**.

A new dual authorization group is added to the corresponding tree.
4.   Right-click the new dual authorization group and click **Rename**.
5.   Enter the desired name and press ENTER.

See also

–   *Adding a logon pair to dual authorization group, page 54*
–   *User Group Properties page, page 127*
–   *Operator Features page, page 134*
–   *User Interface page, page 135*

11.4   Adding a logon pair to dual authorization group

Main window >   **User Groups** > **User Groups** tab >   **New Dual Authorization Group**

To add a logon pair to a dual authorization group:

1.   Select the desired dual authorization group and click   or right-click the group and click **New Logon Pair**.

The appropriate dialog box is displayed.
2.   Select a user group in each list.

The users of the first user group are the users that must log on in the first dialog box for logging on, the users of the second user group confirm the logon.

It is possible to select the same group in both lists.
3.   For each group, select **Force dual authorization** if required.

When this check box is selected, each user of the first group can only log on together with a user of the second group.

When this check box is cleared, each user of the first group can log on alone but he only has the access rights of his group.
4.   Click **OK**.

A new logon pair is added tot he appropriate dual authorization group.
5.   Right-click the new logon pair and click **Rename**.
6.   Enter the desired name and press ENTER

Notice!

Enterprise User Groups and Enterprise Access are not available for BVMS Viewer.

See also
– *Creating a dual authorization group, page 53*
– *Logon Pair Properties page, page 129*

11.5   Configuring Admin Group

Main window > **User Groups** > **User Groups** tab Admin Group

Allows you to add new admin users to the Admin Group, to rename admin users and to remove them from the Admin Group.

To add a new admin user to the Admin Group:

1.   Click or right-click the Admin Group and click **New User**.
      A new admin user is added to the Admin Group.
2.   On the **User Properties** page, type the user name and a description.
3.   The **User must change password at next logon** check box is pre-selected for all newly created user accounts.
      Type the password according to the password policy rules and confirm this password.
4.   Click **Apply** to apply the settings.
5.   Click to activate the password.

To rename an admin user:
1.   Right-click the desired admin user and click **Rename**.
2.   Enter the desired name and press ENTER.

3.   Click to activate the user name changes.

To remove an admin user from the Admin Group:
▶   Right-click the desired admin user and click **Remove**.
      The admin user is removed from the Admin Group.

Note:

You can remove an admin user from the Admin Group only if other admin users exist.

If there is a single admin user in the Admin group it cannot be removed.

See also
– *User Groups page, page 126*
– *User Properties page, page 128*
– *Strong password policy , page 51*

11.6   Configuring LDAP settings

Main window >   **User Groups** > **User Groups** tab >   > **Operating Permissions** tab

or

Main window >   **User Groups** > **Enterprise User Group** tab >   > **Operating Permissions** tab

> **Notice!**
> Enterprise User Groups and Enterprise Access are not available for BVMS Viewer.

> **Caution!**
> Do not assign an LDAP group to different BVMS user groups. This can result in not intended permissions for these users.

> **Notice!**
> Type the search paths accurately. Wrong paths can make the search on an LDAP server very slow.

You configure LDAP groups in standard user groups or Enterprise User Groups.

To configure LDAP settings:
1.   Click the **User Group Properties** tab.
2.   In the **LDAP Properties** field, make the appropriate settings.
For detailed information on the various fields, see the Online Help for the appropriate application window.

11.7   Associating an LDAP group

Main window >   **User Groups** > **User Groups** tab >   > **Operating Permissions** tab

or

Main window >   **User Groups** > **Enterprise User Group** tab >   > **Operating Permissions** tab

You associate an LDAP group with a BVMS user group to give the users of this LDAP group access to the Operator Client. The users of the LDAP group have the access rights of the user group where you configure the LDAP group.
You probably need the help of the IT administrator who is responsible for the LDAP server.
You configure LDAP groups in standard user groups or Enterprise User Groups.

To associate an LDAP group:
1.   Click the **User Group Properties** tab.

2.   In the **LDAP Properties** field, click **Settings**.
     The **LDAP Server Settings** dialog box is displayed.
3.   Enter the settings of your LDAP server and click **OK**.
For detailed information on the various fields, see the Online Help for the appropriate application window.

▸   In the **LDAP groups** list, double-click an LDAP group.
    This LDAP group is entered in the **Associated LDAP group** field.

11.8   Configuring operating permissions

Main window >   ![key icon]   **User Groups** > **User Groups** tab > ![icon] > **Operating Permissions** tab
or

Main window >   ![key icon]   **User Groups** > **Enterprise User Group** tab > ![icon] > **Operating Permissions** tab

![info icon]	**Notice!** Enterprise User Groups and Enterprise Access are not available for BVMS Viewer.

You can configure operating permissions like Logbook access or user interface settings.
You cannot change these settings for a default user group.
You configure operating permissions in standard user groups or Enterprise User Groups.
For detailed information on the various fields, see the Online Help for the appropriate application window.

See also
–   *User Group Properties page, page 127*
–   *Operator Features page, page 134*
–   *User Interface page, page 135*

11.9   Configuring device permissions

Main window >   ![key icon]   **User Groups** > **User Groups** tab > **Device Permissions** tab
or

Main window >   ![key icon]   **User Groups** > **Enterprise Access** tab > **Device Permissions** tab

![info icon]	**Notice!** Enterprise User Groups and Enterprise Access are not available for BVMS Viewer.

You can set the permissions for all devices of the Logical Tree independently.

In an Enterprise System, these permissions are valid for the access of Enterprise User Group users to the devices of a local Management Server, controlled by Enterprise Accounts.
After you have moved permitted devices to a folder that is not permitted for this user group, you must set the permissions for the folder to grant access to its devices.
You cannot change these settings for a default user group.
You configure device permissions in standard user groups or Enterprise Accounts.
For detailed information on the various fields, see the Online Help for the appropriate application window.

See also
– *Logical Tree page, page 133*
– *Camera Permissions page, page 130*

12   Managing configuration data

Main window

You must activate the current configuration to make it valid for the Management Server and Operator Client. The system reminds you to activate when exiting the Configuration Client. Every activated configuration is saved with the date and with a description if required.

At every point in time you can restore a recently activated configuration. All configurations saved in the meantime get lost.

You can export the current configuration in a configuration file and import this file later. This restores the exported configuration. All configurations saved in the meantime get lost.

–   Click to save the settings.

–   Click to undo the last setting.

–   Click to activate the configuration.

> **Notice!**
> This document describes some functions that are not available for BVMS Viewer.

12.1   Activating the working configuration

Main window

You activate the currently working configuration. The Operator Client uses the activated configuration after the next start if the user accepted it. If the activation is enforced, all open instances of the Operator Client in the network exit and start again. The user of each Operator Client instance usually does not have to log on again.

You can configure a delayed activation time. If you configure a delayed activation time, the working configuration is not activated at once but at the time configured. If you configure another activation time later (delayed or not does not matter), this time is active now. The first configured activation time is removed.

When you exit the Configuration Client the system reminds you to activate the current working copy of the configuration.

You cannot activate a configuration that contains a device without password protection.

> **Notice!**
> If the activation is enforced, each instance of Operator Client restarts when the configuration is activated. Avoid unnecessary activations. Perform activations preferably in the night or during time periods with low activities.

> **Notice!**
> If your system contains devices that are not protected by a password, you must secure these devices before you can activate. You can deactivate this password enforcement.

To activate the currently working configuration:

1.   Click   .

The **Activate Configuration** dialog box is displayed.

If your configuration contains devices that are not protected by a password, you cannot activate. In this case the **Protect Devices with Default Password...** dialog box is displayed.

Follow the instructions in this dialog box and click **Apply**.

The **Activate Configuration** dialog box is displayed again.

2.   If appropriate, enter a delayed activation time. By default, the present point in time is configured as activation time. If you do not change the delayed activation time, the activation is performed immediately.

If appropriate, click to check **Force activation for all Operator Clients**.

3.   Type a description and click **OK**.

The current configuration is activated.

Each Operator Client workstation is instantly restarted, if connected to the network and the activation is enforced. If a workstation is not connected, it is restarted as soon it is connected again.

If you configured a delayed activation time, the configuration will be activated later.

See also

–   *Activate Configuration dialog box, page 65*

12.2 Activating a configuration

Main window

You can activate a previous version of the configuration that you have saved earlier.

To activate a configuration:

1.   On the **System** menu, click **Activation Manager...**.

The **Activation Manager** dialog box is displayed.

2.   In the list, select the configuration you want to activate.

3.   Click **Activate**.

A message box is displayed.

4.   Click **OK**.

The **Activate Configuration** dialog box is displayed.

5.   If appropriate, click to check **Force activation for all Operator Clients**. Each Operator Client workstation is automatically restarted to activate the new configuration. The user cannot refuse the new configuration.

If **Force activation for all Operator Clients** is not checked, on each Operator Client workstation a dialog box appears for some seconds. The user can refuse or accept the new configuration. The dialog box is closed after a few seconds without user interaction. In this case the new configuration is not accepted.

See also

–   *Activate Configuration dialog box, page 65*
–   *Activation Manager dialog box, page 64*

12.3 Exporting configuration data

Main window

You can export the device configuration data of BVMS in a .zip file. This .zip file contains the database file (`Export.bvms`) and the user data (`.dat` file).

You can use these files for restoring a system configuration that has been exported before on the same (Enterprise) Management Server or for importing it on another (Enterprise) Management Server. The user data file cannot be imported but you can use it to manually restore the user configuration.

To export configuration data:
1.   On the **System** menu, click **Export Configuration....**
      The **Export Configuration File** dialog box is displayed.

      Note: If your current working copy configuration is not activated (is active), you export this working copy and not the activated configuration.
2.   Click **Save**.
3.   Enter a filename.
      The current configuration is exported. A .zip file with database and user data is created.

See also
–   *Importing configuration data, page 61*

12.4   Importing configuration data

Main window

The following use cases are covered:
–   Importing a configuration that has been exported (backup has been performed) before on the same server
–   Importing a configuration template that has been prepared and exported on another server
–   Importing the configuration of an earlier BVMS version.

You can only import a configuration if the latest changes of the current working copy are saved and activated.

For importing the configuration data you need the appropriate password.

You cannot import user data.

To import the configuration:
1.   On the **System** menu, click **Import Configuration....**.
      The **Import Configuration File** dialog box is displayed.
2.   Select the desired file for import and click **Open**.
      The **Import Configuration...** dialog box is displayed.
3.   Enter the appropriate password and click **OK**.
      The Configuration Client is restarted. You must logon again.
      The imported configuration is not activated but editable in Configuration Client.

Notice!

If you want to continue editing the configuration that has been activated for your Management Server, perform a rollback in the **Activate Configuration** dialog box.

See also
–   *Exporting configuration data, page 60*

12.5 Checking the status of your encoders/decoders

Main window > **Hardware** menu > **Device Monitor...** command > **Device Monitor** dialog box
You can check the status of all activated encoders/decoders in the Device Tree.

13 Global Configuration Client windows

This chapter contains information on some basic application windows available in BVMS Configuration Client.

Notice!
This document describes some functions that are not available for BVMS Viewer.

13.1 Menu commands

System menu commands	
Save Changes	Saves all changes made on this page.
Undo All Changes on Page	Restores the settings of this page since the last saving.
Activation Manager...	Displays the **Activation Manager** dialog box.
Export Configuration...	Displays the **Export Configuration File** dialog box.
Import Configuration...	Displays the **Import Configuration File** dialog box.
Export Device Information for OPC...	Displays a dialog box for creating a configuration file that you can import in a 3rd party management system.
Exit	Exits the program.

Tools menu commands	
Command Script Editor...	Displays the **Command Script Editor** dialog box
Resource Manager...	Displays the **Resource Manager** dialog box.
Sequence Builder...	Displays the **Sequence Builder** dialog box.
Resource Converter	Displays the **Resource Converter** dialog box if old map resources in DWF format are available.
RRAS Configuration...	Displays the **RRAS Configuration** dialog box.
License Manager...	Displays the **License Manager** dialog box.
License Inspector...	Displays the **License Inspector** dialog box.

Settings menu commands	
Alarm Settings...	Displays the **Alarm Settings** dialog box.
SNMP Settings...	Displays the **SNMP Settings** dialog box.
Set Recording Qualities...	Displays the **Stream Quality Settings** dialog box.
Options...	Displays the **Options** dialog box.
Remote Access Settings...	Displays the **Remote Access Settings** dialog box.

Help menu commands	

	Display help	Displays the BVMS Application Help.
	Help	Displays a dialog box containing information on the installed system, e.g., the version number.

Hardware menu commands		
	Initial Device Scan...	Displays the **Initial Device Scan** dialog box.
	Protect Devices with Default Password...	Displays the **Protect Devices with Global Default Password** dialog box.
	IP Device Configuration...	Displays the **IP Device Configuration** dialog box.
	Device Monitor...	Displays the **Device Monitor** dialog box.

13.2   Activation Manager dialog box

Main window > **System** menu > **Activation Manager...** command

Allows you to activate the current configuration or to rollback to a previous configuration.
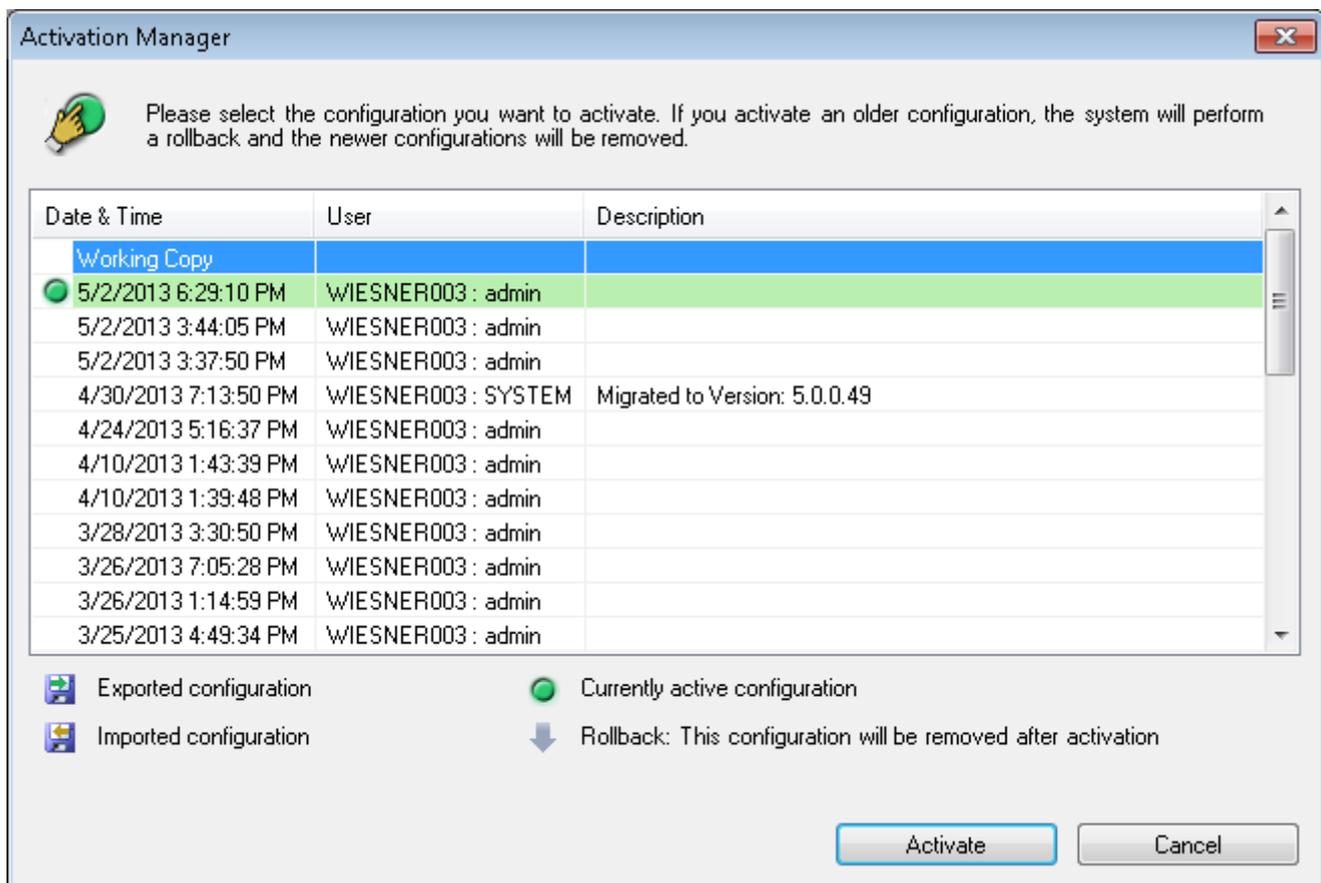
Activate

Click to display the **Activate Configuration** dialog box.

See also

–   *Activating the working configuration, page 59*
–   *Activating a configuration, page 60*

13.3   Activate Configuration dialog box

Main window >

Allows you to type a description for the working copy of the configuration to be activated.

Set Delayed Activation time
Click to select a delayed activation time.

Force activation for all Operator Clients
If checked, each Operator Client workstation is automatically restarted to activate the new configuration. The user cannot refuse the new configuration.
If not checked, on each Operator Client workstation a dialog box appears for some seconds. The user can refuse or accept the new configuration. The dialog box is closed after a few seconds without user interaction. In this case the new configuration is not accepted.

Configure RRAS service before Activation
Only available if you have enabled the **Enable Port Mapping** option in the **Remote Access Settings** dialog box.
If checked, the **RRAS Configuration** dialog box is displayed before activation is performed.

See also
– *Activating the working configuration, page 59*

13.4   License Manager dialog box

Main window > **Tools** menu > **License Manager...** command
Allows you to license the BVMS package that you have ordered and to upgrade with additional features.

Base Packages
Displays the available base packages.

Type Number
Displays the Commercial Type Number (CTN) of the selected package, feature or expansion.

Status
Displays the licensing status if applicable.

Optional Features
Displays the available features.

Expansion
Displays the available expansions and their count. To change the count point right from a check box and click the up or down arrow.

Activate
Click to display the **License Activation** dialog box.

Import Bundle Info
Click to import an XML file containing a Bundle Information that you received from Bosch.

Add New Package
Click to display a dialog box for selecting a new license file.

13.5   Options dialog box

Main window > **Settings** menu > **Options...** command

Language
Allows you to configure the language of your Configuration Client. If you select **System Language** the language of your Windows installation is used.
This setting is enabled after restarting Configuration Client.

Scan Options
Allows you to configure if it is possible to scan for devices in the respective subnet or across the subnet.

Disable hot spot coloring in maps
Allows you to configure disabling blinking hot spots in maps.

Enable advanced state display (hot spot coloring in maps depending on state)
Allows you to configure for all state events that the hot spots of the devices belonging to this event, are displayed with a background color and blink when the configured event occurs.

Automatic Logoff

Enforce automatic logoff of Configuration Client after this time of inactivity
Allows you to configure the automatic logoff of Configuration Client. Configuration Client will log off after the configured time period.
Changes in the configuration pages of the following devices in the **Devices** page are not saved automatically and are lost after inactivity logoff:
–   Encoders
–   Decoders
–   VRM devices
–   iSCSI devices
–   VSG devices
All other pending configuration changes are saved automatically.
Note: Changes in dialog boxes that were not confirmed by clicking **OK**, are not saved.

Allow multiple logons with the same user name
Allows you to configure that a user of Bosch VMS SDK, BVMS Web Client, BVMS Mobile App, or Operator Client can perform multiple synchronous logons with the same user name.

Global iSCSI connection password (CHAP password):
Type the iSCSI CHAP password which is necessary to authenticate at the iSCSI storage device and to enable a direct playback from the iSCSI.

Show password
Click to enable that the entered password is displayed. Be careful that nobody can spy out this password.

13.6   License Investigator dialog box

Main window > **Tools** menu > **License Inspector...** command > **License Inspector** dialog box
You can check whether the number of installed BVMS licenses exceeds the number of purchased licenses.

14   Devices page

> **Notice!**
> This document describes some functions that are not available for BVMS Viewer.

Main window > **Devices**

Displays the Device Tree and the configuration pages.

The count of items below an entry is displayed in square brackets.

Allows you to configure the available devices, such as mobile video services, ONVIF encoders, Bosch Video Streaming Gateway devices, encoders, decoders, VRMs, local storage encoders, analog matrices, or peripheral devices like ATM / POS bridges.

Note:

Devices are represented in a tree and grouped by the physical network structure and the device categories.

Video sources like encoders are grouped under VRMs. Digital video recorders such as DiBos are listed separately.

 IP Device Configuration

Click to display the **IP Device Configuration** dialog box.

Type in a string and press the ENTER key to filter the displayed items. Only items containing the string and their corresponding parent items (only in trees) are displayed. The count of filtered items and the total count of items is provided. An active filter is indicated by   . Enclose strings with double quotes to find them exactly, for example "Camera 1" exactly filters the cameras with this name, not camera 201.

To cancel filtering, click   .

‣   Click a tree item to display the corresponding page.

14.1   Initial Device Scan dialog box

Main window > **Hardware** menu > **Initial Device Scan...** command

Displays the devices which have duplicate IP addresses or a default IP address (192.168.0.1).

Allows you to change such IP addresses and subnet masks.

You must enter the correct subnet mask before changing an IP address.

14.2   DVR (Digital Video Recorder) page

Main window > **Devices** > >

Displays the property pages of a selected DVR.

Allows you to integrate a DVR into your system.

‣   Click a tab to display the corresponding property page.

> **Notice!**
> You do not configure the DVR itself but only the integration of the DVR device into BVMS.

Caution!
Add the DVR using the administrator account of the device. Using a DVR user account with restricted permissions can result in features that are not usable in BVMS, for example using the control of a PTZ camera.

See also
– *Configuring the integration of a DVR, page 43*

14.2.1 Add DVR dialog box

Main window > **Devices** > Expand > > **Add DVR Recorder**
Allows you to manually add a DVR device.

Network address / port
Type the IP address of your DVR. If required, change the port number.

User name:
Type the user name for connecting to the DVR.

Password:
Type the password for connecting to the DVR.

Security
The **HTTPS** check box is selected by default.
If a connection via HTTPS is not possible, a message appears. Click to remove the checkmark.

Notice!
If the **HTTPS** check box is selected, command and control connections are encrypted. Video data streaming is not encrypted.

Click below to get step-by-step instructions:
– Adding a device

14.2.2 Settings tab

Main window > **Devices** > > > **Settings** tab
Displays the network settings of the DVR connected to your system. Allows you to change the settings if required.

14.2.3 Cameras tab

Main window > **Devices** > > > **Cameras** tab
Displays all video channels of the DVR as cameras. Allows you to remove cameras.
A video input that is disabled in a DVR device is displayed as an active camera in BVMS because earlier recordings could exist for this input.

14.2.4 Inputs tab

Main window > **Devices** > > > **Inputs** tab
Displays all inputs of the DVR.
Allows you to remove items.

14.2.5   Relays tab

Main window > **Devices** > [icon] > [icon] > **Relays** tab

Displays all relays of the DVR. Allows you to remove items.

14.3   Workstation page

Main window > [icon] **Devices** > Expand [icon] > [icon]

Allows you to configure the following settings for a workstation:

– Add a CCTV keyboard connected to a Bosch Video Management System workstation.
– Assign a Command Script that is executed on startup of the workstation.
– Select the default stream for live display.
– Enable Forensic Search.

A workstation must have the Operator Client software installed.

To add a Bosch IntuiKey keyboard that is connected to a decoder, expand [icon] , click [icon] .

14.3.1   Settings page

Main window > [icon] **Devices** > Expand [icon] > [icon] > **Settings** tab

Allows you to configure a script that is executed when the Operator Client on the workstation is started.

Allows you to configure TCP or UDP as transmission protocol used for all cameras that are displayed in Live Mode on your workstation.

Allows you to configure which stream of an IP device is used for live display.

Allows you to enable Forensic Search for this workstation.

And you can configure the keyboard that is connected to this workstation.

Default camera protocol:

Select the default transmission protocol used for all cameras that are assigned to the Logical Tree of this workstation.

When a camera is displayed in Live Mode then the default stream set for the workstation is used. If the camera has no stream 2 or the transcoding service (SW and HW) is not available then stream 1 will be used even though another setting is configured in the workstation settings.

Keyboard type:

Select the type of the keyboard that is connected to your workstation.

Port

Select the COM port that is used to connect your keyboard.

Baudrate:

Select the maximum rate, in bits per second (bps), that you want data to be transmitted through this port. Usually, this is set to the maximum rate supported by the computer or device you are communicating with.

Data bits:

Displays the number of data bits you want to use for each character that is transmitted and received.

Stop bits:

Displays the time between each character being transmitted (where time is measured in bits).

Parity:

Displays the type of error checking you want to use for the selected port.

Port type:

Displays the connection type that is used to connect the Bosch IntuiKey keyboard with the workstation.

14.4 Decoders page

Main window > **Devices** > Expand >

Allows you to add and configure decoders.

See *Bosch Encoder / Decoder page, page 79* for details.

> **Notice!**
> If you want to use decoders in your system, make sure that all encoders use the same password for the user authorization level.

See also

– *Scanning for devices, page 25*

14.4.1 Add Encoder / Add Decoder dialog box

Main window > **Devices** > Expand > Expand > Right-click > Click **Add Encoder** > **Add Encoder** dialog box

or

Main window > **Devices** > Right-click > Click **Add Encoder** > **Add Encoder** dialog box

or

Main window > **Devices** > Right-click > Click **Add Encoder** > **Add Encoder** dialog box

or

Main window > **Devices** > Expand > Expand > Right-click > Click **Add Encoder** > **Add Encoder** dialog box

or

Main window > **Devices** > Expand > Right-click > Click **Add Decoder** > **Add Encoder** dialog box

Allows you to add an encoder or decoder manually. This is especially useful when you want to add any Video IP device from Bosch (only for VRM).

IP address:
Type in a valid IP address.

Encoder type: / Decoder type:
For a device with known device type, select the appropriate entry. It is not necessary that the device is available in the network.
If you want to add any Video IP device from Bosch, select **<Auto Detect>**. The device must be available in the network.

14.4.2 Edit Encoder / Edit Decoder dialog box

Main window > **Devices** > Expand > Expand > Expand > Right-click > Click **Edit Encoder** > **Edit Encoder** dialog box
or

Main window > **Devices** > Expand > Right-click > Click **Edit Encoder** > **Edit Encoder** dialog box
or

Main window > **Devices** > Expand > Right-click > Click **Edit Encoder** > **Edit Encoder** dialog box
or

Main window > **Devices** > Expand > Expand > Right-click > Click **Edit Encoder** > **Edit Encoder** dialog box
or

Main window > **Devices** > Expand > Expand > Right-click > Click **Edit Decoder** > **Edit Decoder** dialog box

Allows you to check and update the device capabilities of a device. On opening this dialog box the device is connected. The password is checked and the device capabilities of this device are compared with the device capabilities stored in BVMS.

Name
Displays the device name. When you add a Video IP device from Bosch, the device name is generated. If required change the entry.

Network address / port
Type the network address of the device. If required, change the port number.

 i	**Notice!** The port can only be changed, if the **HTTPS** check box is selected.

User name

Displays the user name used for authenticating at the device.

Password

Type the valid password for authenticating at the device.

Show password

Click to enable that the entered password is displayed. Be careful that nobody can spy out this password.

Authenticate

Click to authenticate at the device with the credentials entered above.

Secure connection (encryption)

You can activate the encryption of live video transferred from an encoder to the following devices if HTTPS port 443 is configured on the encoder:

– Operator Client computer

– Management Server computer

– Configuration Client computer

– VRM computer

– Decoder

Note:

When activated, the user of Operator Client cannot switch a stream to UDP and to UDP multicast.

When activated, ANR does not work for the affected device.

When activated, encoder replay does not work on encoders with firmware earlier than 6.30.

Device Capabilities

You can sort the displayed device capabilities per category or alphabetically.

A message text informs you whether the detected device capabilities match the current device capabilities.

Click **OK** to apply the changes of the device capabilities after an upgrade of the device.

See also

– *Encrypting live video, page 40*

– *Updating the device capabilities, page 37*

14.4.3   Enter password dialog box

Main window > **Devices** > Expand > Expand > > Right-click > **Change password...** command

Main window > **Devices** > Expand > Right-click > **Change password...** > **Enter password** dialog box

Main window > ![icon] **Devices** > Expand ![icon] > Expand ![icon] > Expand ![icon] > Right-click ![icon] > **Change password...** command

Main window > ![icon] **Devices** > ![icon] > Right-click ![icon] > **Change password...** command

Main window > ![icon] **Devices** > ![icon] > Right-click ![icon] > **Change password...** command

A password prevents unauthorized access to the device. You can use different authorization levels to limit access.

Proper password protection is only guaranteed when all higher authorization levels are also protected with a password. Therefore, you must always start from the highest authorization level when assigning passwords.

You can define and change a password for each authorization level if you are logged into the "service" user account.

The device has three authorization levels: service, user, and live.

– service is the highest authorization level. Entering the correct password gives access to all the functions and allows all configuration settings to be changed.
– user is the middle authorization level. At this level you can operate the device, play back recordings, and also control camera, for example, but you cannot change the configuration.
– live is the lowest authorization level. At this level you can only view the live video image and switch between the different live image displays.

For a decoder the following authorization level replaces the live authorization level:

– destination password (only available for decoders)
Used for access to an encoder.

See also
– *Changing the password of an encoder / decoder, page 39*
– *Providing the destination password for a decoder, page 39*

14.5   Monitor Wall page

Main window > ![icon] **Devices** > ![icon]

Allows you to add a monitor wall application. This application allows for controlling the monitor wall hardware from within Operator Client. No server is involved in controlling the monitor wall. This ensures that the user of Operator Client is always able to control the monitor wall even if the Management Server is offline.

Name
Type in a display name for your monitor wall.

Monitor
Select a monitor that is connected to a decoder.
If you add a decoder that has 2 monitors connected, you must display the **Edit Decoder** dialog box of the decoder and update the device capabilities of this decoder. For each monitor add a further monitor wall.

Maximum number of cameras to connect

Type in the maximum number of cameras that are allowed to be displayed in the monitor wall. If you leave the field empty, the operator can display as many cameras as Image panes on the monitor wall layout are available.

Enable thumbnails

Click to check if you want to display a snapshot in Operator Client for each monitor. This snapshot is regularly updated.

Initial sequence

Select a camera sequence for initial display on the monitor wall when the operator starts this monitor wall.

> **Notice!**
> When you delete a sequence in the **Sequence Builder** dialog box, this sequence is automatically removed from the **Initial sequence** list of a monitor wall if configured there.

See also

14.5.1 Add Monitor Wall dialog box

Main window > **Devices** > Right-click > Click **Add Monitor Wall**.

Add the required decoder to your BVMS before you add the monitor wall.

Name

Type in a display name for your monitor wall.

Monitor

Select a monitor that is connected to a decoder.

If you add a decoder that has 2 monitors connected, you must display the **Edit Decoder** dialog box of the decoder and update the device capabilities of this decoder. For each monitor add a further monitor wall.

Maximum number of cameras to connect

Type in the maximum number of cameras that are allowed to be displayed in the monitor wall. If you leave the field empty, the operator can display as many cameras as Image panes on the monitor wall layout are available.

Enable thumbnails

Click to check if you want to display a snapshot in Operator Client for each monitor. This snapshot is regularly updated.

Initial sequence

Select a camera sequence for initial display on the monitor wall when the operator starts this monitor wall.

See also

14.6   BVMS Scan Wizard

Main window > **Devices** > Expand > Right-click > Click **Scan for Encoders** > **Bosch VMS Scan Wizard** dialog box

Main window > **Devices** > Expand > Right-click > Click **Scan for Video Streaming Gateways** > **Bosch VMS Scan Wizard** dialog box

Main window > **Devices** > Right-click > Click **Scan for Live Only Encoders**> **Bosch VMS Scan Wizard** dialog box

Main window > **Devices** > Right-click > Click **Scan for Local Storage Encoders** > **Bosch VMS Scan Wizard** dialog box

This dialog box allows you to scan for available devices in your network, configure them and add them to your system in one process.

Use
Click to select a device for adding to the system.

Type (not available for VSG devices)
Displays the type of the device.

Display Name
Displays the device name that was entered in the Device Tree.

Network Address
Displays the IP address of the device.

User Name
Displays the user name that is configured on the device.

Password
Type in the password for authenticating with this device.

Status
Displays the status of authentication.

 : Succeeded

 : Failed

Main window > **Devices** > Right-click > Click **Scan for VRM Devices**> BVMS Scan Wizard dialog box

Notice!
For configuring a Secondary VRM you must first install the appropriate software on the desired computer. Run Setup.exe and select **Secondary VRM**.

Master VRM

In the list, select the desired entry.

User Name

Displays the user name that is configured on the VRM device.

You can type in another user name if required.

See also

14.7 VRM Devices page

Main window > **Devices** > Expand >

Allows you to add and configure VRM devices. A VRM device needs at least an encoder, an iSCSI device, and a LUN assigned to the iSCSI device, and a storage pool. See the Release Notes and the data sheet for current firmware versions.

14.7.1 Add VRM dialog box

Main window > **Devices** > Right-click > Click **Add VRM** > **Add VRM** dialog box

Allows you to add a VRM device. You can select the type of the device and enter the credentials.

You can effectively assign a Failover VRM to a Master VRM only when both are online and are successfully authenticated. The passwords are then synchronized.

Name

Type in a display name for the device.

Network address / port

Type in the IP address of your device.

Type

Select the desired device type.

User name

Type in the user name for authentication.

Password

Type in the password for authentication.

Show password

Click to enable that the password is visible.

Test

Click to check whether the device is connected and authentication is successful.

Properties

If required, change the port numbers for the HTTP port and for the HTTPS port. This is only possible when you add or edit a VRM that is not connected. If the VRM is connected, the values are retrieved and you cannot change them.

The **Master VRM** table row shows the selected device if applicable.

See also
– *Adding a Primary VRM manually, page 30*

14.8 Live Only page

Main window > **Devices** > Expand >

Allows you to add and configure encoders used for live only. You can add Bosch encoders and ONVIF network video transmitters.

See also
– *Adding a live only encoder, page 34*
– *Scanning for devices, page 25*
– *Bosch Encoder / Decoder page, page 79*

14.9 Local Storage page

Main window > **Devices** > Expand >

Allows you to add and configure encoders with local storage.

See also
– *Adding a local storage encoder, page 35*
– *Bosch Encoder / Decoder page, page 79*
– *Scanning for devices, page 25*

14.10 Unmanaged Site page

Main window > **Devices** > Expand >

You can add a video network device to the **Unmanaged Sites** item of the Device Tree.
It is assumed that all unmanaged network devices of an unmanaged site are located in the same time zone.

Site name
Displays the name of the site that was entered during creation of this item.

Description
Type in a description for this site.

Time zone
Select the appropriate time zone for this unmanaged site.

See also
– *Unmanaged site, page 14*
– *Adding an unmanaged site, page 30*
– *Importing unmanaged sites, page 31*
– *Configuring the time zone, page 31*

14.11   Unmanaged Network Device page

Main window > **Devices** > Expand > Expand >

You can add a video network device to the **Unmanaged Sites** item of the Device Tree.

It is assumed that all unmanaged network devices of an unmanaged site are located in the same time zone.

See also
–   *Unmanaged site, page 14*

14.11.1   Add unmanaged Network Device Dialog Box

Device type:

Select the entry that is applicable for this device.

Available entries:

–   **DIVAR AN / DVR**
–   **DIVAR IP 3000/7000 / Bosch VMS**
–   **Bosch IP camera / encoder**

Network address:

Type an IP address or hostname. If required, change the port number.

Note: If you use a SSH connection, enter the address in the following format:

ssh://IP or servername:5322

Security

The **HTTPS** check box is selected by default.

Notice!

If adding DVR and the **HTTPS** check box is selected, command and control connections are encrypted. Video data streaming is not encrypted.

User name:

Type the valid user name for this network device if available. See *Unmanaged site, page 14* for details.

Password:

Type the valid password if available. See *Unmanaged site, page 14* for details on user credentials.

See also
–   *Unmanaged site, page 14*

15   Bosch Encoder / Decoder page

The count of items below an entry is displayed in square brackets.

To configure an encoder / decoder:

Main window > **Devices** > Expand > Expand > Expand >

or

Main window > **Devices** > Expand > Expand > Expand >

or

Main window > **Devices** > Expand >

or

Main window > **Devices** > Expand >

Main window > **Devices** > Expand > Expand >
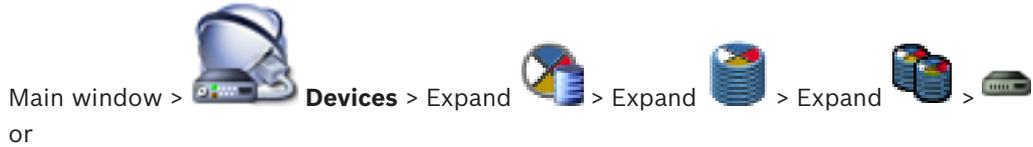
Most of the settings on the encoder / decoder pages are active immediately after you click

 . If you click another tab without clicking and changes have occurred, two corresponding message boxes are displayed. Confirm them both if you want to save.

To change the passwords of an encoder right-click the device icon and click **Change password...**.

To display the device in a Web browser right-click the device icon and click **Show Webpage in Browser**.

Note:

Depending on the selected encoder or camera, not all pages described here are available for each device. The wording used here for describing the field labels can deviate from your software.

▸   Click a tab to display the corresponding property page.

 Notice!

This document describes some functions that are not available for BVMS Viewer.

See also

–   *Scanning for devices, page 25*
–   *Configuring an encoder / decoder, page 36*

15.1   Enter password dialog box

Main window > **Devices** > Expand > Expand > > Right-click > **Change password...** command

Main window > **Devices** > Expand > Right-click > **Change password...** > **Enter password** dialog box

Main window > **Devices** > Expand > Expand > Expand > Right-click > **Change password...** command

Main window > **Devices** > > Right-click > **Change password...** command

Main window > **Devices** > > Right-click > **Change password...** command

A password prevents unauthorized access to the device. You can use different authorization levels to limit access.

Proper password protection is only guaranteed when all higher authorization levels are also protected with a password. Therefore, you must always start from the highest authorization level when assigning passwords.

You can define and change a password for each authorization level if you are logged into the "service" user account.

The device has three authorization levels: service, user, and live.

– service is the highest authorization level. Entering the correct password gives access to all the functions and allows all configuration settings to be changed.
– user is the middle authorization level. At this level you can operate the device, play back recordings, and also control camera, for example, but you cannot change the configuration.
– live is the lowest authorization level. At this level you can only view the live video image and switch between the different live image displays.

For a decoder the following authorization level replaces the live authorization level:

– destination password (only available for decoders)
  Used for access to an encoder.

See also
– *Changing the password of an encoder / decoder, page 39*
– *Providing the destination password for a decoder, page 39*

15.2   Unit Access page

15.2.1   Identification / Camera identification

Device name
Type the name of the device.

The name simplifies the management of multiple devices in large systems. The name is used for identification of a device. Use a name that makes it as easy as possible to identify its location.

Do not use any special characters in the name. Special characters are not supported and may cause problems, e.g. with playback.

Click to update the name in the Device Tree.

Each device should be assigned a unique identifier that can be entered here as an additional means of identification.

Initiator name
Displays the iSCSI initiator name. The initiator name is automatically displayed after a connection is established.

Initiator extension
Type your own text to make the unit easier to identify in large iSCSI systems. This text is added to the initiator name, separated from it by a full stop.

15.2.2   Camera name

Camera
Type the name of the camera. Ensure that Camera 1 is allocated to Video Input 1, Camera 2 to Video Input 2, etc.

The camera name facilitates the identification of the remote camera location, for example in case of an alarm. Use a name that makes it as easy as possible to identify the location.

Do not use any special characters in the name. Special characters are not supported and may cause problems, for example the play back of recordings. The settings on this page apply to all camera inputs.

Click to update the name in the Device Tree.

15.2.3   Version information

Hardware version
Displays the version of the hardware.

Firmware version
Displays the version of the firmware.

15.3   Date/Time page

Device date format Device date Device time
If there are multiple devices operating in your system or network, it is important to synchronize their internal clocks. For example, it is only possible to identify and correctly evaluate simultaneous recordings when all devices are operating on the same time.

1. Enter the current date. Since the device time is controlled by the internal clock, it is not necessary to enter the day of the week – it is added automatically.
2. Enter the current time or click **Sync to PC** to apply the system time from your computer to the device.

Note:
It is important that the date/time is correct for recording. An incorrect date/time setting could prevent correct recording.

Device time zone
Select the time zone in which the system is located.
Daylight saving time
Set by BVMS Management Server.

Time server IP address
Set by BVMS Management Server.

Time server type
Set by BVMS Management Server. Default setting is SNTP.

15.4   Initialization page

15.4.1   Application variant
The camera has a choice of application variants that set up the camera for optimum performance in a specific environment. Select the application variant best suited to your installation.
The application variant must be selected before any other changes are made, as the camera reboots automatically and resets the factory defaults when the application variant is changed.

15.4.2   Base frame rate
Select the base frame rate for the camera.
Note: Shutter times, frame rates, and the analog output (if present) are affected by this value.

15.4.3   Camera LED
Disable the **Camera LED** on the camera to switch it off.

15.4.4   Mirror image
Select **On** to output a mirror image of the camera picture.

15.4.5   Flip image
Select **On** to output an upside down camera image.

15.4.6   Menu button
Select **Disabled** to prevent access to the install wizard via the menu button on the camera itself.

15.4.7   Heater
Select **Auto** to let the camera determine when the heater should be switched on.

15.4.8   Reboot device

15.4.9   Factory defaults
Click **Defaults** to restore the factory defaults for the camera. A confirmation screen appears. Allow several seconds for the camera to optimize the picture after a reset.

15.4.10   Lens Wizard
Click **Lens Wizard...** to open a separate window which can be used to focus the camera lens (not for all cameras).

15.5   Camera Calibration page

15.5.1   Positioning
The **Positioning** feature describes the location of the camera and the perspective in the camera's field of view.

Perspective information is essential to Video Analytics, as it enables the system to compensate for the illusory smallness of distant objects.

Only through use of perspective information is it possible to distinguish objects such as persons, bicycles, cars and trucks, and accurately compute their real size and speeds as they move through 3D space.

However, to calculate perspective information accurately, the camera must be directed at a single, flat horizontal plane. Multiple and inclined planes, hills, stairs can falsify perspective information and produce incorrect object information such as size and speed.

Mounting position

The mounting position describes the perspective information that is also often called calibration.

In general, the mounting position is determined by the parameters of the camera such as height, roll angle, tilt angle, and focal length.

The height of the camera must always be entered manually. Whenever possible, roll angle and tilt angle are provided by the camera itself. The focal length is provided, if the camera has a built-in lens.

Select the appropriate mounting position of the camera. Options that appear depend on the type of camera.

Custom	Select to configure the calibration of the DINION and FLEXIDOME cameras. Cameras on CPP7 and CPP7.3 platform have an integrated 6-axis-gyro sensor to determine the tilt and roll angle.
Standard	Select to configure a global calibration of the AUTODOME and MIC cameras. And then, enter the height of the camera. Tilt angle and focal length are provided automatically by the camera to complete the calibration for every potential field of view of the camera. Optionally, set the calibration manually for prepositions with video analytics assigned.
Ceiling	Select to configure the calibration of FLEXIDOME IP panoramic cameras with ceiling mount. The calibration assistants **AutoSet** and **Sketch** are not available.
Wall	Select to configure the calibration of FLEXIDOME IP panoramic cameras with wall mount. The calibration assistants **AutoSet** and **Sketch** are not available.

Tilt angle [°]

The tilt angle describes the angle between the horizontal and the camera.

A tilt angle of 0° means that the camera is mounted parallel to the ground.

A tilt angle of 90° means that the camera is mounted vertically in bird's eye view perspective.

The flatter the tilt angle is set, the less accurate the estimate of object sizes and speeds will be. The settings must be between 0° and 90°. Estimates are no longer possible when you have reached 0°.

Enter the tilt angle if the value is not determined by the camera.

Roll angle [°]

The roll angle describes the angle between the roll axis and the horizontal plane. The angle can deviate from the horizontal by up to 45°.

Enter the roll angle if the value is not determined by the camera.

Height [m]

The height describes the vertical distance from the camera to the ground plane of the captured image. Typically the elevation of the mounted camera above the ground.

Enter the height in meters of the position of the camera.

Focal length

The focal length is determined by the lens. The shorter the focal length, the wider the field of view. The longer the focal length, the narrower the field of view and the higher the magnification.

Enter the focal length in meters of the position of the camera if the value is not determined by the camera.

Coordinate system

The **Coordinate system** feature describes the position of the camera in a local **Cartesian** or the global **WGS 84** coordinate system. The camera and the objects tracked by the video analytics are displayed on a map.

Select the coordinate system and enter the appropriate values in the additional input fields that appear depending on the coordinate system selected.

Cartesian

The Cartesian coordinate system describes each point in the space by a combination of the position on three orthogonal axes X, Y and Z. A right-handed coordinate system is used, where X and Y span the ground plane and Z describes the elevation of the ground plane.

X [m]	The location of the camera on the ground on the X-axis.
Y [m]	The location of the camera on the ground on the Y-axis.
Z [m]	The elevation of the ground plane. To determine the elevation of the camera, add the **Z [m]** value and the **Height [m]** value of the camera.

WGS 84

The WGS 84 coordinate system is a spherical coordinate system description of the world and used in many standards including GPS.

Latitude	Latitude is the north-south position of the camera in the spherical coordinate system WGS 84.
Longitude	Longitude is the east-west position of the camera in the spherical coordinate system WGS 84.
Ground level [m]	The elevation of the ground above sea level. To determine the elevation of the camera, add the **Ground level [m]** value and the **Height [m]** value of the camera.

Azimuth [°]	The orientation of the camera in a counter-clockwise angle starting with 0° in the east (WGS 84) or on the X-axis (Cartesian). If the camera is directed towards the north (WGS 84) or the Y-axis (Cartesian), the azimuth is 90°.

15.5.2 Sketch Calibration

The **Sketch** functionality offers an additional, half-automatic calibration method. This calibration method allows you to describe the perspective in the camera's field of view by drawing vertical lines, ground lines, and ground angles in the camera image and entering the correct size and angle. Use the **Sketch** functionality if the result of the automatic calibration is not sufficient.

You can also combine this manual calibration with the values for roll angle, tilt angle, height and focal length calculated by the camera or entered manually.

> **Notice!**
> The **Sketch** functionality is not available for FLEXIDOME IP panoramic cameras.

> **Notice!**
> The **Sketch** functionality is only available for configured and assigned pre-positions.
> For AUTODOME and MIC cameras, configure the pre-positions of the camera and assign the pre-positions to one of the available 16 VCA profiles before calibration with **Sketch**. Applications are pre-positions of cameras directed towards different ground planes, an optimized calibration for inclined ground planes or large focal lengths. A local pre-position calibration does not change the global calibration.
> It is also possible to calibrate pre-positions without entering a global calibration.

VCA Profile

Select the appropriate profile.

Select the **Global** check box to use the global, overall calibration for all AUTODOME and MIC cameras.

Alternatively, clear the **Global** check box to obtain a local calibration and overwrite the global calibration for the selected profile. To do this, select the VCA profile before.

Calculate

Select the **Calculate** check box to obtain the roll angle, tilt angle, height and focal length from the sketched calibration elements - vertical lines, ground lines and angles - you have placed in the camera.

Clear the **Calculate** check box to enter a value manually or to refresh to the values provided by the camera itself.

Tilt angle [°] / Roll angle [°]	Enter the angle manually, or click the refresh icon to obtain values provided by any sensors that the camera may have. Alternatively, select the **Calculate** check box to obtain values based on the calibration elements marked on the image.
Height [m]	Enter the height manually, or click the refresh icon to obtain values provided by any sensors that the camera may have. Alternatively, select the **Calculate** check box to obtain values based on the calibration elements marked on the image.

Focal length [mm]	Enter the focal length manually, or click the refresh icon to obtain values provided by any sensors that the camera may have. Alternatively, select the **Calculate** check box to obtain values based on the calibration elements marked on the image.

Calibrating cameras using the Sketch Calibration window
To determine non-automatically set values:
1. Enter the value for tilt angle, roll angle, height and focal length if the value is known, for example, by measuring the height of the camera above the ground, or reading the focal length from the lens.
2. For each value that is still unknown, select the **Calculate** check box, then place a calibration element on the camera image. Use these calibration elements to trace individual outlines of the displayed environment in the camera image and define the position and size of these lines and angles.

    –   Click   to place a vertical line across the image.
        A vertical line corresponds to a line that is perpendicular to the ground plane, such as a door frame, edge of a building or a lamp post.

    –   Click   to place a line across the ground in the image.
        A line on ground corresponds to a line that is on the ground plane, such as a road marking.

    –   Click   to place an angle on the ground in the image.
        The angle on ground represents an angle lying on the horizontal ground plane, such as the corner of a carpet or parking bay markings.
3. Adjust the calibration elements to the situation:
    –   Enter the real size of a line or angle. To do this, select the line or angle, then enter the size in the corresponding box.
        Example: You have placed a line on ground across the lower side of an automobile. You know that the automobile is 4 m long. Enter 4 m as the length of the line.
    –   Adjust the position or length of a line or angle. To do this, drag the line or angle or move the end points to the desired position in the camera image.
    –   Remove a line or angle. To do this, select the line or angle, then click the trash can icon.
    Note:
    Blue lines indicate calibration elements added by you.
    White lines represent the element as it should be positioned on the camera image based on the current calibration results or the determined calibration data.

15.5.3   Verify

Here you can verify your camera calibration.

15.6   Privacy Masks page

Privacy masking is used to block a specific area of a scene from being viewed. Four privacy mask areas can be defined. The activated masked areas are filled with the selected pattern in live view.
1. Select the pattern to be used for all masks.
2. Check the box of the mask you wish to activate.
3. Use the mouse to define the area for each of the masks.

	Notice!
i	Draw the mask at 50% optical zoom or less for improved masking performance. Draw the mask 10% larger than the object to ensure that the mask completely covers the object as the camera zooms in and out.

Active masks

To activate a mask, select the appropriate check box.

Privacy masks

Select the privacy mask number. The preview window displays a gray rectangle in the scene.

Enabled

Select the check box to activate the privacy mask. After saving, the content inside the privacy mask is no longer visible in the preview. This area is blocked out from being viewing and recording.

Pattern

Pattern of the privacy mask.

Preview window

If necessary, change the size of the privacy mask area and move it to the position you want.

15.7 Recording Management page

Active recordings are indicated by .

Point to the icon. Detailed information about the active recordings are displayed.

Recordings manually managed

The recordings are managed locally on this encoder. All relevant settings must be carried out manually. The encoder / IP camera acts as a live only device. It is not be removed from VRM automatically.

Recording 1 managed by VRM

The recordings of this encoder are managed by the VRM system.

Dual VRM

Recording 2 of this encoder is managed by a secondary VRM.

iSCSI Media tab

Click to display the available iSCSI storage connected to this encoder.

Local Media tab

Click to display the available local storage on this encoder.

Add

Click to add a storage device to the list of managed storage media.

Remove

Click to remove a storage device from the list of managed storage media.

15.8 Recording preferences page

The **Recording preferences** page is displayed for each encoder. This page only appears if a device is assigned to a VRM system.

Primary target

Only visible if the **Recording preferences mode** list on the **Pool** page is set to **Failover**.
Select the entry for the required target.

Secondary target
Only visible if the **Recording preferences mode** list on the **Pool** page is set to **Failover** and if the **Secondary target usage** list is set to **On**.
Select the entry for the required target for configuring failover mode.

15.9   Video Input page

Camera name stamping
This field sets the position of the camera name overlay. It can be displayed at the **Top**, at the **Bottom**, or at a position of your choice that you can then specify using the **Custom** option. Or it can be set to **Off** for no overlay information.
1.   Select the desired option from the list.
2.   If you select the **Custom** option, additional fields are displayed where you can specify the exact position (**Position (XY)**).
3.   In the **Position (XY)** fields, enter the values for the desired position.

Logo
Click **Choose File** to select a file. Heed the restrictions for file format, logo size, and color depth. **Click** Upload to load the file to the camera.
If no logo is selected, Configuration displays the message, "No file chosen."

Logo position
Select the position for the logo on the OSD: **To the left of the name**, **To the right of the name**, or **Logo only**.
Select **Off** (the default value) to disable logo positioning.

Time stamping
This field sets the position of the time overlay. It can be displayed at the **Top**, at the **Bottom** or at a position of your choice that you can then specify using the **Custom** option. Or it can be set to **Off** for no overlay information.
1.   Select the desired option from the list.
2.   If you select the **Custom** option, additional fields are displayed where you can specify the exact position (**Position (XY)**).
3.   In the **Position (XY)** fields, enter the values for the desired position.
If necessary, display milliseconds for **Time stamping**. This information can be useful for recorded video images; however, it does increase the processor's computing time. Select **Off** if displaying milliseconds is not needed.

Alarm mode stamping
Select **On** to display a text message overlay in the image in the event of an alarm. It can be displayed at a position of your choice that you can then specify using the **Custom** option. Or it can be set to **Off** for no overlay information.
1.   Select the desired option from the list.
2.   If you select the **Custom** option, additional fields are displayed where you can specify the exact position (**Position (XY)**).
3.   In the **Position (XY)** fields, enter the values for the desired position.

Alarm message
Enter the message to be displayed in the image in the event of an alarm. The maximum text length is 31 characters.
Check this box to make transparent the stamp background on the image.

Camera OSD
Select **On** to momentarily display camera response information, such as Digital Zoom, Iris open/close, and Focus near/far overlays in the image. Select **Off** to display no information.

1.   Select the desired option from the list.
2.   Specify the exact position (**Position (XY)**).
3.   In the **Position (XY)** fields, enter the values for the desired position.

Title OSD

OSD titles can be displayed at a position of your choice.

Select **On** to display sector or pre-position title overlays continuously in the image.

Select **Momentary** to display sector or pre-position title overlays for a few seconds.

1.   Select the desired option from the list.
2.   Specify the exact position (**Position (XY)**).
3.   In the **Position (XY)** fields, enter the values for the desired position.

Select **Off** to deactivate the display of overlay information.

Video authentication

Select from the **Video authentication** drop-down box a method for verifying the integrity of the video.

If you select **Watermarking**, all images are marked with an icon. The icon indicates if the sequence (live or saved) has been manipulated.

If you want to add a digital signature to the transmitted video images to ensure their integrity, select one of the cryptographic algorithms for this signature.

Signature interval [s]

For certain **Video authentication** modes, enter the interval (in seconds) between insertions of the digital signature.

See also

–   *Managing the verification of authenticity, page 40*

15.10   Picture settings - Scene mode

A scene mode is a collection of image parameters that are set in the camera when that particular mode is selected (installer menu settings are excluded). Several pre-defined modes are available for typical scenarios. After a mode has been selected, additional changes can be made through the user interface.

15.10.1   Current mode

Select the mode you wish to use from the drop-down menu.

15.10.2   Mode ID

The name of the selected mode is displayed.

15.10.3   Copy mode to

Select the mode from the drop-down menu to which you wish to copy the active mode.

15.10.4   Restore Mode Defaults

Click **Restore Mode Defaults** to restore the factory default modes. Confirm you decision.

15.10.5   Scene mode factory defaults

Outdoor

This mode covers most situations. It should be used in applications where the lighting changes from day to night. It takes into account sun highlights and street (sodium vapor) lighting.

Motion

This mode is used for monitoring the traffic movement on roads or parking lots. It can also be used for industrial applications where fast moving objects are to be monitored. Motion artifacts are minimized. This mode should be optimized for a sharp and detailed picture in color and black/white mode.

Low light

This mode is optimized for sufficient details at low light. It requires more bandwidth and can introduce motion judder.

BLC

This mode is optimized for scenes with people moving in front of a bright background.

Indoor

This mode is similar to the outdoor mode but it avoids the limitations imposed by the sun or street lighting.

Vibrant

This mode has enhanced contrast, sharpness and saturation.

15.10.6 Scene mode factory defaults

Outdoor

This mode covers most situations. It should be used in applications where the lighting changes from day to night. It takes into account sun highlights and street (sodium vapor) lighting.

Motion

This mode is used for monitoring the traffic movement on roads or parking lots. It can also be used for industrial applications where fast moving objects are to be monitored. Motion artifacts are minimized. This mode should be optimized for a sharp and detailed picture in color and black/white mode.

Low light

This mode is optimized for sufficient details at low light. It requires more bandwidth and can introduce motion judder.

Indoor

This mode is similar to the outdoor mode but it avoids the limitations imposed by the sun or street lighting.

Vibrant

This mode has enhanced contrast, sharpness and saturation.

15.10.7 Scene mode factory defaults

Indoor

This mode is similar to the outdoor mode but it avoids the limitations imposed by the sun or street lighting.

Outdoor

This mode covers most situations. It should be used in applications where the lighting changes from day to night. It takes into account sun highlights and street (sodium vapor) lighting.

Low light

This mode is optimized for sufficient details at low light. It requires more bandwidth and can introduce motion judder.

Night-optimized

This mode is optimized for sufficient details at low light. It requires more bandwidth and can introduce motion judder.

Low bit rate

This mode reduces the bitrate for installations with restricted network bandwidth and storage.

BLC

This mode is optimized for scenes with people moving in front of a bright background.

Vibrant

This mode has enhanced contrast, sharpness and saturation.

Sports and gaming

This mode is for high-speed capture, and improved color rendition and sharpness.

Motion

This mode is used for monitoring the traffic movement on roads or parking lots. It can also be used for industrial applications where fast moving objects are to be monitored. Motion artifacts are minimized. This mode should be optimized for a sharp and detailed picture in color and black/white mode.

Traffic

This mode is used for monitoring the traffic movement on roads or parking lots. It can also be used for industrial applications where fast moving objects are to be monitored. Motion artifacts are minimized. This mode should be optimized for a sharp and detailed picture in color and black/white.

Retail

This mode has improved color rendition and sharpness with reduced bandwidth requirements.

15.11 Picture settings - Color

Contrast (0...255)

Adjust the contrast with the slider from 0 to 255.

Saturation (0...255)

Adjust the color saturation with the slider from 0 to 255.

Brightness (0...255)

Adjust the brightness with the slider from 0 to 255.

15.11.1 White balance

– **Indoor**: Allows the camera to continually adjust for optimal color reproduction in an indoor environment.
– **Outdoor**: Allows the camera to continually adjust for optimal color reproduction in an outdoor environment.
– In **Manual** mode the Red, Green, and Blue gain can be manually set to a desired position.

Hold

Click **Hold** to put ATW on hold and save the current color settings. The mode changes to manual.

R-gain

In **Manual** white balance mode, adjust the red gain slider to offset the factory white point alignment (reducing red introduces more cyan).

G-gain

In **Manual** white balance mode, adjust the green gain slider to offset the factory white point alignment (reducing green introduces more magenta).

B-gain

In **Manual** white balance mode, adjust the blue gain slider to offset the factory white point alignment (reducing blue introduces more yellow).

Note:

It is only necessary to change the white point offset for special scene conditions.

Default

Click **Default** to set all video values to their factory setting.

15.11.2   White balance

– **Basic auto** mode allows the camera to continually adjust for optimal color reproduction using an average reflectance method. This is useful for indoor light sources and for colored LED light illumination.
– **Standard auto** mode allows the camera to continually adjust for optimal color reproduction in an environment with natural light sources.
– Sodium vapor auto mode allows the camera to continually adjust for optimal color reproduction in an environment with sodium vapor light sources (street lighting).
– In **Manual** mode the Red, Green, and Blue gain can be manually set to a desired position.

Hold

Click **Hold** to put ATW on hold and save the current color settings. The mode changes to manual.

R-gain

In **Manual** white balance mode, adjust the red gain slider to offset the factory white point alignment (reducing red introduces more cyan).

G-gain

In **Manual** white balance mode, adjust the green gain slider to offset the factory white point alignment (reducing green introduces more magenta).

B-gain

In **Manual** white balance mode, adjust the blue gain slider to offset the factory white point alignment (reducing blue introduces more yellow).

Note:

It is only necessary to change the white point offset for special scene conditions.

Default

Click **Default** to set all video values to their factory setting.

15.11.3   White balance

– **Standard auto** mode allows the camera to continually adjust for optimal color reproduction in an outdoor environment.
– In **Manual** mode the Red, Green, and Blue gain can be manually set to a desired position.

Hold

Click **Hold** to put ATW on hold and save the current color settings. The mode changes to manual.

R-gain

In **Manual** white balance mode, adjust the red gain slider to offset the factory white point alignment (reducing red introduces more cyan).

G-gain

In **Manual** white balance mode, adjust the green gain slider to offset the factory white point alignment (reducing green introduces more magenta).

B-gain

In **Manual** white balance mode, adjust the blue gain slider to offset the factory white point alignment (reducing blue introduces more yellow).

Note:

It is only necessary to change the white point offset for special scene conditions.

Default

Click **Default** to set all video values to their factory setting.

15.11.4   White balance

- – **Basic auto** mode allows the camera to continually adjust for optimal color reproduction using an average reflectance method. This is useful for indoor light sources and for colored LED light illumination.
- – **Standard auto** mode allows the camera to continually adjust for optimal color reproduction in an environment with natural light sources.
- – Sodium vapor auto mode allows the camera to continually adjust for optimal color reproduction in an environment with sodium vapor light sources (street lighting).
- – **Dominant color auto** mode takes into account any dominant color in the image (for example, the green of a football pitch or of a gaming table) and uses this information to obtain a well balanced color reproduction.
- – In **Manual** mode the Red, Green, and Blue gain can be manually set to a desired position.

Hold

Click **Hold** to put ATW on hold and save the current color settings. The mode changes to manual.

RGB-weighted white balance

In an auto mode, **RGB-weighted white balance** can be switched On or Off. When On, additional fine tuning of the automatic color reproduction can be made with the R, G and B weight sliders.

R-gain

In **Manual** white balance mode, adjust the red gain slider to offset the factory white point alignment (reducing red introduces more cyan).

G-gain

In **Manual** white balance mode, adjust the green gain slider to offset the factory white point alignment (reducing green introduces more magenta).

B-gain

In **Manual** white balance mode, adjust the blue gain slider to offset the factory white point alignment (reducing blue introduces more yellow).

Note:

It is only necessary to change the white point offset for special scene conditions.

Default

Click **Default** to set all video values to their factory setting.

15.12   Picture settings - ALC

15.12.1   ALC mode

Select the mode for automatic light-level control:

- – Fluorescent 50 Hz
- – Fluorescent 60 Hz
- – Outdoor

15.12.2   ALC level

Adjust the video output level (-15 to 0 to +15).

Select the range within which the ALC will operate. A positive value is more useful for low-light conditions; a negative value is more useful for very bright conditions.

15.12.3   Saturation (av-pk)

The saturation (av-pk) slider configures the ALC level so that it controls mainly on scene average level (slider position -15) or on scene peak level (slider position +15). Scene peak level is useful for capturing images that contain car headlights.

15.12.4   Exposure/frame rate

Automatic exposure

Select to let the camera automatically set the optimum shutter speed. The camera tries to maintain the selected shutter speed as long as the light level of the scene permits.

▸   Select the minimum frame rate for automatic exposure. (The values available depend on the value set for the **Base frame rate** in the **Installer Menu**.)

Fixed exposure

Select to set a fixed shutter speed.

▸   Select the shutter speed for fixed exposure. (The values available depend on the value set for the ALC mode.)

▸   Select a default shutter speed. The default shutter improves the motion performance in auto exposure mode.

15.12.5   Day/night

Auto - the camera switches the IR cut-off filter on and off depending on the scene illumination level.

Monochrome - the IR cut-off filter is removed, giving full IR sensitivity.

Color - the camera always produces a color signal regardless of light levels.

Switch level

Set the video level at which the camera in **Auto** mode switches to monochrome operation (-15 to 0 to +15).

A low (negative) value means that the camera switches to monochrome at a lower light level. A high (positive) value means that the camera switches to monochrome at a higher light level.

Note:

To ensure stability when using IR illuminators, use the alarm interface for reliable Day/Night switching.

Switch level

Set the video level at which the camera in **Auto** mode switches to monochrome operation (-15 to 0 to +15).

A low (negative) value means that the camera switches to monochrome at a lower light level. A high (positive) value means that the camera switches to monochrome at a higher light level.

IR function

(only for cameras with built-in IR illuminators)

Select the control setting for IR illumination:

–   **Auto**: the camera automatically switches the IR illumination.

–   **On**: the IR illumination is always on.

–   **Off**: the IR illumination is always off.

Intensity level

Set the intensity of the IR beam (0 to 30).

Day-to-night switchover

Adjust the slider to set the video level at which the camera in **Auto** mode switches from color to monochrome operation (-15 to +15).

A low (negative) value means that the camera switches to monochrome at a lower light level. A high (positive) value means that the camera switches to monochrome at a higher light level.

Night-to-day switchover

Adjust the slider to set the video level at which the camera in **Auto** mode switches from monochrome to color operation (-15 to +15).

A low (negative) value means that the camera switches to color at a lower light level. A high (positive) value means that the camera switches to color at a higher light level.

(The actual switch-over point might change automatically to avoid instable switching.)

Note:

To ensure stability when using IR illuminators, use the alarm interface for reliable Day/Night switching.

15.13 Encoder Regions page

1. Select one of the eight available regions from the drop-down box.
2. Use the mouse to define the area for that region by dragging the center or sides of the shaded window.
3. Select the encoder quality to be used for the defined area.
   (Object and background quality levels are defined on the **Expert Settings** section of the **Encoder Profile** page.)
4. If required, select another region and repeat steps 2 and 3.
5. Click **Set** to apply the region settings.

Preview

Click to open a viewing window where a 1:1 live image and the bit rate for the region settings can be previewed.

15.14 Camera page

AE-response speed

Select the speed of the response of auto exposure. Options are Super slow, Slow, Medium (default), Fast.

Backlight compensation

Optimizes the video level for the selected area of the image. Parts outside this area may be underexposed or overexposed. Select On to optimize the video level for the central area of the image. The default setting is Off.

Blue Gain

The blue gain adjustment offsets the factory white point alignment (reducing blue introduces more yellow). It is only necessary to change the white point offset for special scene conditions.

Color hue

The degree of color in the video image (HD only). Values range from -14° to 14°; the default is 8°.

Fixed Gain

Use the slide to select the desired number for fixed gain. The default is 2.

Gain control

Adjusts the automatic gain control (AGC). Automatically sets the gain to the lowest possible value needed to maintain a good picture.

–   **AGC** (default): electronically brightens dark scenes, which may cause graininess in low light scenes.
–   **Fixed**: no enhancement. This setting disables the Max. Gain Level option.
    If you select this option, the camera makes the following changes automatically:
    –   **Night Mode**: switches to Color
    –   **Auto Iris**: switches to Constant

High sensitivity

Adjusts the level of intensity or lux within the image. Select from **Off** or **On**.

Maximum Gain Level

Controls the maximum value the gain can have during AGC operation. To set the maximum gain level, choose from:

–   **Normal**
–   **Medium**
–   **High** (default)

Night mode

Selects night mode (B/W) to enhance lighting in low light scenes. Select from the following options:

–   **Monochrome**: Forces the camera to stay in Nigh Mode and transmit monochrome images.
–   **Color**: The camera does not switch to Night Mode regardless of ambient light conditions.
–   **Auto** (default): The camera switches out of Night Mode after the ambient light level reaches a pre-defined threshold.

Night mode threshold

Adjusts the level of light at which the camera automatically switches out of night mode (B/W) operation. Select a value between 10 and 55 (in increments of 5; default 30). The lower the value, the earlier the camera will switch to color mode.

Noise Reduction

Turns on the 2D and 3D noise reduction feature.

Red Gain

The red gain adjustment offsets the factory white point alignment (reducing red introduces more cyan).

Saturation

The percentage of light or color in the video image. Values range from 60% to 200%; the default is 110%.

Sharpness

Adjusts the sharpness of the picture. To set the sharpness, use the slider to select a number. The default is 12.

Current mode

Shutter

Adjusts the electronic shutter speed (AES). Controls the time period for which light is gathered by the collecting device. The default setting is 1/60 second for NTSC and 1/50 for PAL cameras. The range of settings is from 1/1 to 1/10000.

Shutter Mode
–   **Fixed**: The shutter mode is fixed to a selectable shutter speed.
–   **Automatic exposure**: increases camera sensitivity by increasing the integration time on the camera. This is accomplished by integrating the signal from a number of consecutive video frames to reduce signal noise.
    If you select this option, the camera disables **Shutter** automatically.

Stabilization
This feature is ideal for cameras mounted on a pole or mast, or on another location that shakes frequently.
Select On to activate the video stabilization feature (if available on your camera) that reduces camera shake in both the vertical and horizontal axis. The camera compensates for the movement of the image by up to 2% of the image size.
Select Auto to activate the feature automatically when the camera detects vibration.
Select Off to deactivate the feature.
Note: This feature is not available on 20x models.

White Balance
Adjusts the color settings to maintain the quality of the white areas of the image.

15.14.1   ALC

ALC mode
Select the mode for automatic light-level control:
–   Fluorescent 50 Hz
–   Fluorescent 60 Hz
–   Outdoor

ALC level
Adjust the video output level (-15 to 0 to +15).
Select the range within which the ALC will operate. A positive value is more useful for low-light conditions; a negative value is more useful for very bright conditions.
The saturation (av-pk) slider configures the ALC level so that it controls mainly on scene average level (slider position -15) or on scene peak level (slider position +15). Scene peak level is useful for capturing images that contain car headlights.

Exposure

Automatic exposure
Select to let the camera automatically set the optimum shutter speed. The camera tries to maintain the selected shutter speed as long as the light level of the scene permits.
▸   Select the minimum frame rate for automatic exposure. (The values available depend on the value set for the **Base frame rate** in the **Installer Menu**.)

Fixed exposure
Select to set a fixed shutter speed.
▸   Select the shutter speed for fixed exposure. (The values available depend on the value set for the ALC mode.)
▸   Select a default shutter speed. The default shutter improves the motion performance in auto exposure mode.

Day/night
Auto - the camera switches the IR cut-off filter on and off depending on the scene illumination level.
Monochrome - the IR cut-off filter is removed, giving full IR sensitivity.
Color - the camera always produces a color signal regardless of light levels.

Note:
To ensure stability when using IR illuminators, use the alarm interface for reliable Day/Night switching.

Night-to-day switchover
Adjust the slider to set the video level at which the camera in **Auto** mode switches from monochrome to color operation (-15 to +15).
A low (negative) value means that the camera switches to color at a lower light level. A high (positive) value means that the camera switches to color at a higher light level.
(The actual switch-over point might change automatically to avoid instable switching.)

Day-to-night switchover
Adjust the slider to set the video level at which the camera in **Auto** mode switches from color to monochrome operation (-15 to +15).
A low (negative) value means that the camera switches to monochrome at a lower light level. A high (positive) value means that the camera switches to monochrome at a higher light level.

IR function
(only for cameras with built-in IR illuminators)
Select the control setting for IR illumination:
– **Auto**: the camera automatically switches the IR illumination.
– **On**: the IR illumination is always on.
– **Off**: the IR illumination is always off.

Intensity level
Set the intensity of the IR beam (0 to 30).

15.14.2   Scene mode
A scene mode is a collection of image parameters that are set in the camera when that particular mode is selected (installer menu settings are excluded). Several pre-defined modes are available for typical scenarios. After a mode has been selected, additional changes can be made through the user interface.
Current mode
Select the mode you wish to use from the drop-down menu.
Mode ID
The name of the selected mode is displayed.

15.14.3   Scene Mode Scheduler
The scene mode scheduler is used to determine which scene mode should be used during the day and which scene mode should be used during the night.
1. Select the mode you wish to use during the day from **Marked range** drop-down box.
2. Select the mode you wish to use during the night from **Unmarked range** drop-down box.
3. Use the two slider buttons to set the **Time ranges**.

Outdoor
This mode covers most situations. It should be used in applications where the lighting changes from day to night. It takes into account sun highlights and street (sodium vapor) lighting.

Vibrant
This mode has enhanced contrast, sharpness and saturation.

Motion

This mode is used for monitoring the traffic movement on roads or parking lots. It can also be used for industrial applications where fast moving objects are to be monitored. Motion artifacts are minimized. This mode should be optimized for a sharp and detailed picture in color and black/white mode.

Low light

This mode is optimized for sufficient details at low light. It requires more bandwidth and can introduce motion judder.

Indoor

This mode is similar to the outdoor mode but it avoids the limitations imposed by the sun or street lighting.

BLC

This mode is optimized for scenes with people moving in front of a bright background.

15.14.4 WDR

Select **Auto** for automatic Wide Dynamic Range (WDR); select **Off** to disable WDR.

Note:

WDR can only be active if Auto exposure is selected, and there is a match between the base frame rate selected in the installer menu and the ALC fluorescent mode frequency. If there is a conflict, a pop-up window will suggest a solution and adjust the appropriate settings.

15.14.5 Sharpness level

The slider adjusts the sharpness level between -15 and +15. Zero position of the slider corresponds to the factory default level.

A low (negative) value makes the picture less sharp. Increasing sharpness brings out more detail. Extra sharpness can enhance the details of license plates, facial features and the edges of certain surfaces but can increase bandwidth requirements.

15.14.6 Backlight Compensation

Select **Off** to switch off backlight compensation.

Select **On** to capture details in high-contrast and extremely bright-dark conditions.

Select **Intelligent AE** to capture object detail in scenes with people moving in front of a bright background

15.14.7 Contrast enhancement

Select **On** to increase the contrast in low contrast conditions.

15.14.8 Intelligent DNR

Select **On** to activate intelligent Dynamic Noise Reduction (DNR) which reduces noise based on motion and light levels.

Temporal noise filtering

Adjusts the **Temporal noise filtering** level between -15 and +15. The higher the value, the more noise filtering.

Spatial noise filtering

Adjusts the **Spatial noise filtering** level between -15 and +15. The higher the value, the more noise filtering.

15.15   Lens page

15.15.1   Focus

Autofocus

Continuously adjusts the lens automatically to the correct focus for the sharpest picture.
– **One push** (default): Activates the Auto Focus feature after the camera stops moving. Once focused, Auto Focus is inactive until the camera is moved again.
– **Auto focus**: Auto Focus is always active.
– **Manual**: Auto Focus is inactive.

Focus polarity
– **Normal** (default): Focus controls operate normally.
– **Reverse**: Focus controls are reversed.

Focus speed

Controls how fast the Auto focus will readjust when the focus becomes blurred.

15.15.2   Iris

Auto iris

Automatically adjusts the lens to allow the correct illumination of the camera sensor. This type of lens is recommended for use when there are low light or changing light conditions.
– **Constant** (default): Camera constantly adjusts to varying light conditions.
  If you select this option, for example the AutoDome Junior HD makes the following changes automatically:
  – **Gain control**: switches to AGC
  – **Shutter mode**: switches to Normal
– **Manual**: Camera must be manually adjusted to compensate for varying light conditions.

Iris polarity

Capability to reverse the operation of the iris button on the controller.
– **Normal** (default): Iris controls operate normally.
– **Reverse**: Iris controls are reversed.

Auto iris level

Increases or decreases brightness according to the amount of light. Type a value between 1 and 15, inclusive. The default setting is 8.

Iris speed

Controls how fast the Iris will adjust the opening according to the illumination of the scene. Type a value between 1 and 10, inclusive. The default setting is 5.

15.15.3   Zoom

Maximum zoom speed

Controls the zoom speed. Default setting: **Fast**

Zoom polarity

Capability to reverse the operation of the zoom button on the controller.
– **Normal** (default): Zoom controls operate normally.
– **Reverse**: Zoom controls are reversed.

Digital zoom

Digital zoom is a method of decreasing (narrowing) the apparent angle of view of a digital video image. It is accomplished electronically, without any adjustment of the camera's optics, and no optical resolution is gained in the process.
– **Off** (default): Enables the Digital Zoom feature.

– **On**: Disables the Digital Zoom feature.

15.16 PTZ page

Auto pan speed
Continuously pans the camera at a speed between right and left limit settings. Type a value between 1 and 60 (expressed in degrees), inclusive. The default setting is 30.

Inactivity
Selects the time period the dome must be not controlled until the inactivity event will be executed.
– **Off** (default): Camera remains on a current scene indefinitely.
– **Scene 1**: Camera returns to Preset 1.
– **Previous Aux**: Camera returns to the previous activity.

Inactivity period
Determines the behavior of the dome when the control for dome is inactive. Select a time period from the pull-down list (3 sec. - 10 min.). The default setting is 2 minutes.

Auto pivot
The Auto Pivot tilts the camera through the vertical position as the camera is rotated to maintain the correct orientation of the image.
Set the Auto Pivot to **On** (default) to automatically rotate the camera 180º when following a subject traveling directly beneath the camera. To disable this feature, click **Off**.

Freeze frame
Select **On** (default) to freeze the image while the camera moves to a predetermined scene position.

Tilt up limit
Click **Set**, to set the upper tilt limit of the camera.

Tilt limits
Click **Reset** to clear the upper tilt limit.

15.17 Prepositions and Tours page

Allows you to define the individual scenes and a preposition tour comprised of the defined scenes.

To add scenes:
Click ➕.

To delete scenes:
Select the scene, then click ✕.

To overwrite (save) scenes:
Click 💾.

To view scenes:
Select the scene, then click 👁.

Include in standard tour (marked with *)
Select the check box if the scene should be part of the preposition tour. The asterisk (*) on the left of the scene name indicates this.

15.18 Sectors page

Sector

The pan capability (for example for the AutoDome Junior HD camera) is 360° and is divided into eight equal sectors. This allows you to apply a title for each sector and to designate any sectors as a Blanked Sector.

To define a title for sectors:

1. Place the pointer in the input box to the right of the sector number.
2. Type a title for the sector, up to 20 characters long.
3. To blank the sector, click the check box to the right of the sector title.

15.19 Misc page

Address

Allows the appropriate device to be operated via the numerical address in the control system. Type a number between 0000 and 9999, inclusive, to identify the camera.

15.20 Logs page

This page allows you to display and to save log files.

Download

Click to obtain the log file information. The log files are displayed in the overview.

Save

Click to save the log files.

15.21 Audio page

This function allows you to set the gain of the audio signals to suit your specific requirements. The current video image is shown in the small window next to the slide controls to help you check the selected audio source and improve assignments. Your changes are effective immediately.

The numbering of the audio inputs follows the labeling on the device and the assignment to the respective video inputs. The assignment cannot be changed for Web browser connections.

Audio

The audio signals are sent in a separate data stream parallel to the video data, and so increase the network load. The audio data are encoded according to G.711 and require an additional bandwidth of approximately 80 kbps for each connection.

– **On**: Transmits audio data.
– **Off**: No transmission of audio data.

Line In 1 - Line In 4

Enter the value of the gain of the audio signal. Make sure that the display of the slider remains green.

Line Out

Enter the value of the gain. Make sure that the display of the slider remains green.

Microphone (MIC)

Enter the value of the gain for the microphone.

Line Out/Speaker (SPK)

Enter the value of the gain of the line and the loudspeaker.

Recording format

Select a format for audio recording.

G.711: default value.

L16: Select L16 if you want better audio quality with higher sampling rates. This requires approximately eight times the G.711 bandwidth.

AAC: Select AAC if you want high-fidelity audio but lower data rates than G.711 and L16. It is the best choice when quality is the primary consideration.

15.22   Relay page

This function allows you to configure the switching behavior of the relay outputs.

You can configure the switching behavior of the relay outputs. For each relay, you can specify an open switch relay (normally closed contact) or a closed switch relay (normally open contact).

You can also specify whether an output should operate as a bistable or monostable relay. In bistable mode, the triggered state of the relay is maintained. In monostable mode, you can set the time after which the relay returns to the idle state.

You can select different events that automatically activate an output. It is possible, for example, to turn on a floodlight by triggering a motion alarm and then turning the light off again when the alarm has stopped.

Idle state

Select **Open** if you want the relay to operate as an NO contact, or select **Closed** if the relay is to operate as an NC contact.

Operating mode

Select an operating mode for the relay.

For example, if you want an alarm-activated lamp to stay on after the alarm ends, select the **Bistable** entry. If you wish an alarm-activated siren to sound for ten seconds, select the 10 s entry.

Relay follows

If required, select a specific event that will trigger the relay. The following events are possible triggers:

Off: Relay is not triggered by events

Connection: Trigger whenever a connection is made

Video alarm: Trigger by interruption of the video signal at the corresponding input

Motion alarm: Trigger by motion alarm at the corresponding input, as configured on the VCA page.

Local input: Trigger by the corresponding external alarm input

Remote input: Trigger by remote station's corresponding switching contact (only if a connection exists)

Note:

The numbers in the lists of selectable events relate to the corresponding connections on the device, Video alarm 1, for example to the Video In 1 connection.

Trigger output

Click the relay button to trigger the relay manually (for example, for testing purposes or to activate a door opener).

The relay button displays the state of each relay.

Red: Relay is activated.

Blue: Relay is not activated.

15.23   Periphery page

15.23.1   COM1

This function allows you to configure the serial interface parameters according to your requirements.

If the device is working in multicast mode, the first remote location to establish a video connection to the device is also assigned the transparent data connection. However, after about 15 seconds of inactivity the data connection is automatically terminated and another remote location can exchange transparent data with the device.

Serial port function

Select a controllable device from the list. Select Transparent data to transmit transparent data via the serial port. Select Terminal to operate the device from a terminal.

After selecting a device, the remaining parameters in the window are set automatically and should not be changed.

Baud rate (bps)

Select the value for the transmission rate.

Stop bits

Select the number of stop bits per character.

Parity check

Select the type of parity check.

Interface mode

Select the protocol for the serial interface.

15.24   VCA page

The device contains an integrated Video Content Analysis (VCA), which can detect and analyze changes in the signal using image processing algorithms. Such changes are triggered by motion in the camera's field of view.

If there is not enough computing power, priority is given to live images and recordings. This can lead to impairment of the VCA system. Observe the processor load and optimize the settings of the device or the VCA settings, if necessary.

You can configure profiles with different VCA configurations. You can save profiles on your computer's hard drive and load saved profiles from there. This can be useful if you want to test a number of different configurations. Save a functioning configuration and test new settings. You can use the saved configuration to restore the original settings at any time.

‣   Select a VCA profile and change the settings if necessary.

To rename the VCA profile:

‣   Click 🖉. The **Edit** dialog box is displayed. Type the new name, and then click **OK**.

Alarm status

Displays the current alarm state to check the effects of your settings immediately.

Aggregation time [s]

Set an aggregation time of between 0 and 20 seconds. The aggregation time always starts when an alarm event occurs. It extends the alarm event by the value set. This prevents alarm events that occur in quick succession from triggering several alarms and successive events in a rapid sequence. No further alarm is triggered during the aggregation time.

The post-alarm time set for alarm recordings only starts once the aggregation time has expired.

Analysis type

Select the required analysis type from the drop-down menu. Different analysis types offer varying levels of control over alarm rules, object filters and tracking modes.

Refer to the VCA documentation for more information on using these.

Motion detector

See *Motion detector (MOTION+ only), page 105*.

Motion detection is available for the Motion+ analysis type. For the detector to function, the following conditions must be met:

– Analysis must be activated.
– At least one sensor field must be activated.
– The individual parameters must be configured to suit the operating environment and the desired responses.
– The sensitivity must be set to a value greater than zero.

Note:

Reflections of light (from glass surfaces, etc.), lights switching on and off, or changes in the light level caused by cloud movement on a sunny day can trigger unintended responses from the motion detector and generate false alarms. Run a series of tests at different times of the day and night to ensure that the video sensor is operating as intended. For indoor surveillance, ensure constant lighting of the areas during the day and at night.

Tamper detection

See *Tamper detection, page 106*

Load...

Click to load a saved profile. The **Open** dialog box is displayed. Select the filename of the profile you want to load, and then click **OK**.

Save...

Click to save the profile settings to another file. The **Save** dialog box is displayed. Type the filename, select the folder where to save the file, and then click **OK**.

Default

Click to return all settings to their default values.

15.24.1   Motion detector (MOTION+ only)

Motion detector

For the detector to function, the following conditions must be met:

– Analysis must be activated.
– At least one sensor field must be activated.
– The individual parameters must be configured to suit the operating environment and the desired responses.
– The sensitivity must be set to a value greater than zero.

Caution!

Reflections of light (off glass surfaces, etc.), switching lights on or off or changes in the light level caused by cloud movement on a sunny day can trigger unintended responses from the motion detector and generate false alarms. Run a series of tests at different times of the day and night to ensure that the video sensor is operating as intended.

For indoor surveillance, ensure constant lighting of the areas during the day and at night.

Debounce time 1 s

The debounce time prevents very brief alarm events from triggering individual alarms. If the **Debounce time 1 s** option is activated, an alarm event must last at least 1 second to trigger an alarm.

Selecting the area

Select the areas of the image to be monitored by the motion detector. The video image is subdivided into square sensor fields. Activate or deactivate each of these fields individually. To exclude particular regions of the camera's field of view from monitoring due to continuous movement (by a tree in the wind, for example), the relevant fields can be deactivated.

1. Click **Mask...** to configure the sensor fields. A new window opens.
2. If necessary, click **Clear All** first to clear the current selection (fields marked red).
3. Left-click the fields to be activated. Activated fields are marked red.
4. If necessary, click **Select All** to select the entire video- frame for monitoring.
5. Right-click any fields to deactivate.
6. Click **OK** to save the configuration.
7. Click the close button (**X**) in the window title bar to close the window without saving the changes.

Sensitivity

Sensitivity is available for the Motion+ analysis type. The basic sensitivity of the motion detector can be adjusted for the environmental conditions to which the camera is subject. The sensor reacts to variations in the brightness of the video image. The darker the observation area, the higher the value that must be selected.

Minimum object size

Specify the number of sensor fields that a moving object must cover to generate an alarm. This setting prevents objects that are too small from triggering an alarm. A minimum value of 4 is recommended. This value corresponds to four sensor fields.

15.24.2   Tamper detection

You can detect tampering of cameras and video cables by means of various options. Run a series of tests at different times of the day and night to ensure that the video sensor is operating as intended.

Tamper detection is usually used for fixed cameras. For dome cameras or other motorized cameras you first have to define a pre-position for which you then can configure the tamper detection. As long as you have not defined and selected a pre-position, you cannot configure tamper detection.

Scene quality

Current brightness	Shows the value of the current brightness of the scene.
Scene too bright	Select this check box if too bright light conditions should trigger an alarm. The current brightness of the scene provides a basis for recognition.
Threshold*	Use the slider to set the threshold of the alarm trigger. The value is displayed to the right of the slider.
Scene too dark	Select this check box if you want to detect camera covering, for example. The current brightness of the scene provides a basis for recognition.

Threshold*	Use the slider to set the threshold of the alarm trigger. The value is displayed to the right of the slider.
Scene too noisy*	Activate this function if tampering associated with EMC interference (noisy scene as the result of a strong interference signal in the vicinity of the video lines) should trigger an alarm.
* Option is not applicable for all encoders.	

Global change I: Sudden scene changes

Global scene change	Select this check box if a global change in the video image should trigger an alarm.
Sensitivity	Move the slider to set how large the global change in the video image must be for an alarm to be triggered. Set a high value if fewer sensor fields need to change to trigger an alarm. With a low value, it is necessary for changes to occur simultaneously in a large number of sensor fields to trigger an alarm.

Global change II: Reference image check
Here you can save a reference image that can be continuously compared with the current video image. If the current video image in the marked areas differs from the reference image, an alarm is triggered. This detects tampering that would otherwise not be detected, for example, if the camera is turned.

Reference image check	Select this check box to activate the on-going check.
Seconds to alarm	Counts down the time set under **Trigger delay** before the alarm is triggered.

Reference image	1. Click **Set** to save the currently visible video image as a reference.
	The reference image is displayed.
	2. Right-click in the image and select **Create VCA Mask**
	3. Use the mouse button to create the desired VCA mask.
	Note: The area inside the mask is excluded from monitoring.
	4. Edit the VCA mask:
	  – To change the mask size:
	    Select the mask, and then drag the line or the corners (nodes) of the mask to the desired position in the camera image.
	  – To move the mask:
	    Select the mask, and then drag the field as a whole to the desired position in the camera image.
	  – To insert a corner (node):
	    Select the mask, and then double-click a line
	    or
	    Select the mask, right-click a line and select **Insert Node**

	– To delete a corner (node): Select the mask, right-click a corner and select **Delete Node** – To delete a mask: Select the mask, and then press DELETE.
Trigger delay	Set delayed alarm triggering here. The alarm is only triggered after a set time interval in seconds has elapsed and then only if the triggering condition still exists. If the original condition has been restored before this time interval elapses, the alarm is not triggered. This avoids false alarms triggered by short-term changes, for example, cleaning activities in the direct field of vision of the camera. ▸ Move the **Trigger delay** slider to the left to decrease the delay or move the slider to the right to increase the delay.
Sensitivity	The basic sensitivity of the tamper detection can be adjusted for the environmental conditions to which the camera is subject. The algorithm reacts to the differences between the reference image and the current video image. The darker the observation area, the higher the value that must be selected. ▸ Move the **Sensitivity** slider to the left to decrease the sensitivity or move the slider to the right to increase the sensitivity.
Edge check	**Appearing edges** Select this option if the selected area of the reference image includes a largely homogenous surface. If structures appear in this area, then an alarm is triggered.
	Disappearing edges The area selected in the reference image should contain a prominent structure. If this structure is concealed or moved, the reference check triggers an alarm. If the selected area is too homogenous, so that concealing and moving the structure would not trigger an alarm, then an alarm is triggered immediately to indicate the inadequate reference image.

Select Area dialog box

> **Notice!**
> This dialog box is only available for encoders with firmware version earlier than 6.10.

This dialog box displays the camera image. Within this window you can activate the areas of the image to be monitored.

To activate an area:
In the camera image, drag over the area you want to activate. Activated areas are marked yellow.

To deactivate an area:
In the camera image, press the SHIFT key and click the area you want to deactivate.

To obtain commands in the window:

To see the commands for activating or deactivating the areas, right-click anywhere in the window. The following commands are available:

– **Undo**

  Undoes the last command.

– **Set All**

  Activates the entire camera image.

– **Clear All**

  Deactivates the entire camera image.

– **Tool**

  Defines the shape of the mouse pointer.

– **Settings**

  Displays the Editor Settings dialog box. In this dialog box you can change the sensitivity and the minimum object size.

15.25   Network Access page

The settings on this page are used to integrate the device into an existing network.

DHCP

If the network has a DHCP server for the dynamic assignment of IP addresses, select **On** or **On plus Link-Local** to automatically accept the DHCP-assigned IP address.

If no DHCP server is available select **On plus Link-Local** to automatically assign a Link-Local (Auto-IP) address.

For certain applications, the DHCP server must support the fixed assignment between IP address and MAC address, and must be appropriately set up so that, once an IP address is assigned, it is retained each time the system is rebooted.

Subnet mask

Enter the appropriate subnet mask for the set IP address.

Gateway address

For the device to establish a connection to a remote location in a different subnet, enter the IP address of the gateway here. Otherwise, this field can remain empty (0.0.0.0).

Prefix length

Enter the appropriate prefix length for the set IP address.

DNS server address

The device is easier to access if it is listed on a DNS server. For example, to establish an Internet connection to the camera, it is sufficient to enter the name given to the device on the DNS server as a URL in the browser. Enter the DNS server's IP address. Servers are supported for secure and dynamic DNS.

Video transmission

If the device is used behind a firewall, TCP (Port 80) should be selected as the transmission protocol. For use in a local network, choose UDP.

Multicast operation is only possible with the UDP protocol. The TCP protocol does not support multicast connections.

TCP rate control

Select **On** if you want to allow Adaptive Bit Rate encoding.

HTTP browser port

Select a different HTTP browser port from the list if required. The default HTTP port is 80. To limit connection to HTTPS, deactivate the HTTP port. To do this, activate the **Off** option.

HTTPS browser port

To limit browser access to encrypted connections, choose an HTTPS port from the list. The standard HTTPS port is 443. Select the **Off** option to deactivate HTTPS ports and limit connections to unencrypted ports.

The camera uses the TLS 1.0 protocol. Ensure that the browser has been configured to support this protocol. Also ensure that Java application support is activated (in the Java Plug-in Control Panel of the Windows Control Panel).

To limit connections to SSL encryption, set the **Off** option in the HTTP browser port, the RCP+ port, and Telnet support. This deactivates all unencrypted connections allowing connections on the HTTPS port only.

Configure and activate encryption for media data (video, audio, metadata) on the **Encryption** page.

HSTS

Select **On** to use the web security policy HTTP Strict Transport Security (HSTS) to provide secure connections.

RCP+ port 1756

Activating RCP+ port 1756 allows unencrypted connections on this port. To allow only encrypted connections, set the **Off** option to deactivate the port.

Telnet support

Activating Telnet support allows unencrypted connections on this port. To allow only encrypted connections, set the **Off** option to deactivate telnet support, making telnet connections impossible.

Interface mode ETH 1 - **Interface mode ETH 2** - **Interface mode ETH 3**

If necessary, select the Ethernet link type for interface ETH. Depending on the device connected, it may be necessary to select a special operation type.

Network MSS [Byte]

Set the maximum segment size for the IP packet's user data here. This gives the option to adjust the size of the data packets to the network environment and to optimize data transmission. In UDP mode, comply with the MTU value set below.

iSCSI MSS [Byte]

Enter the Maximum Segment Size (MSS) for a connection to the iSCSI system.

The maximum segment size for a connection to the iSCSI system can be higher than for the other data traffic via the network. The size depends on the network structure. A higher value is only useful if the iSCSI system is located in the same subnet as the device.

MAC address

Displays the MAC address.

15.25.1   JPEG posting

This function allows you to save individual JPEG images on an FTP server at specific intervals. Then, retrieve these images at a later date to reconstruct alarm events, if required.

Image size

Select the resolution for the JPEG images.

File name

Select how file names are created for the individual images that are transmitted.

–   **Overwrite**

The same file name is always used. An existing file is overwritten by the current file.

–   **Increment**

A number from 000 to 255 is added to the file name and automatically incremented by 1. When the number reaches 255, the number starts again from 000.

– **Date/time suffix**
The date and time are automatically added to the file name. Ensure that the date and time of the device are always set correctly. For example, the file snap011008_114530.jpg was stored on October 1, 2008 at 11.45 and 30 seconds.

Posting interval (s; 0 = Off)
Enter the interval in seconds at which the images is sent to an FTP server. Enter zero for no images to be sent.

15.25.2 FTP server

FTP server IP address
Type the IP address of the FTP server on which to save the JPEG images.

FTP server login
Type your login name for the FTP server.

FTP server password
Type the password for the FTP server.

Path on FTP server
Type the exact path where to save the images on the FTP server.

Post JPEG from camera
Select the check box to activate the camera input for the JPEG image. The numbering follows the labeling of the video inputs on the device.

Max. bit rate
You can limit the bit rate for FTP posting.

15.26 DynDNS

15.26.1 Enable DynDNS

A dynamic Domain Name Service (DNS) allows you to select the unit via the Internet using a host name, without having to know the current IP address of the unit. You can enable this service here. To do this, you must have an account with one of the dynamic DNS providers and you must register the required host name for the unit on that site.

Note:
For information about the service, registration process and available host names refer to the provider.

15.26.2 Provider

Select your dynamic DNS Provider from the drop-down list.

15.26.3 Host name

Enter the host name registered for the unit.

15.26.4 User name

Enter the user name you registered.

15.26.5 Password

Enter the password you registered.

15.26.6   Force registration now

Force the registration by transferring the IP address to the DynDNS server. Entries that change frequently are not provided in the Domain Name System. It is a good idea to force the registration when setting up the device for the first time. Only use this function when necessary and no more than once a day, to avoid the possibility of being blocked by the service provider. To transfer the IP address of the device, click the **Register** button.

15.26.7   Status

The status of the DynDNS function is displayed here for information purposes; these settings cannot be changed.

15.27   Network Management

15.27.1   SNMP

The camera supports the SNMP V1 (Simple Network Management Protocol) for managing and monitoring network components, and can send SNMP messages (traps) to IP addresses. It supports SNMP MIB II in the unified code.

If **On** is selected for the SNMP parameter and a SNMP host address is not entered, the device does not send the traps automatically and will only reply to SNMP requests. If one or two SNMP host addresses are entered, SNMP traps are sent automatically. Select **Off** to deactivate the SNMP function.

SNMP host addresses

To send SNMP traps automatically, enter the IP address of one or two target devices here.

SNMP traps

To choose which traps are sent:
1.   Click **Select**. A dialog box appears.
2.   Click the check boxes of the appropriate traps.
3.   Click **Set** to close the window and send all of the checked traps.

15.27.2   UPnP

Select **On** to activate UPnP communication. Select **Off** to deactivate it.

When the Universal Plug-and-Play (UPnP) function is activated, the unit responds to requests from the network and is automatically registered on the requesting computers as a new network device. This function should not be used in large installations due to the large number of registration notifications.

Note:

To use the UPnP function on a Windows computer, both the Universal Plug-and-Play Device Host and the SSDP Discovery Service must be activated.

15.27.3   Quality of Service

The priority of the different data channels can be set by defining the DiffServ Code Point (DSCP). Enter a number between 0 and 252 as a multiple of four. For alarm video you can set a higher priority than for regular video and you can define a Post Alarm Time over which this priority is maintained.

15.28   Advanced page

15.28.1   SNMP

The device supports the SNMP V2 (Simple Network Management Protocol) for managing and monitoring network components, and can send SNMP messages (traps) to IP addresses. The device supports SNMP MIB II in the unified code.

SNMP

Select **On** to activate the SNMP function.

1. SNMP host address / 2. SNMP host address

Type the IP addresses of one or two target units. The device (for example encoder, camera) sends SNMP traps automatically to the target units.

If you do not enter IP addresses, the device only replies to SNMP requests and does not send SNMP traps to the target units.

SNMP traps

Allows you to select which traps the device sends to the target units. To do this, click **Select**. The **SNMP traps** dialog box is displayed.

SNMP traps dialog box

Select the check boxes of the appropriate traps, and then click **OK**.

15.28.2   802.1x

IEEE 802.1x allows you to communicate with the device if a RADIUS server is used in a network.

Authentication

Select **On** to activate 802.1x.

Identity

Type the user name that the RADIUS server uses for identifying the device.

Password

Type the password that the RADIUS server uses for identifying the device.

15.28.3   RTSP

RTSP port

If necessary, select a different port for the exchange of the RTSP data. The default port is 554. **Off** disables the RTSP function.

15.28.4   UPnP

You can activate the universal plug and play function (UPnP). When activated the camera reacts on requests from the network and will be registered automatically as a new network device on the inquiring computers. The access to the camera is then possible using the Windows file explorer, and without knowledge of the camera's IP address.

Note:

In order to use the UPnP function on a computer with Windows XP or Windows Vista, the Universal Plug and Play Device Host and the SSDP Discovery services must be activated.

15.28.5   TCP metadata input

This feature allows a device to receive data from an external TCP sender, for example an ATM or POS device, and store it as metadata.

TCP port

Select the port for TCP communication. Select **Off** to deactivate the TCP metadata function.

Sender IP address
Type the IP address of the TCP metadata sender here.

15.29   Multicast page

In addition to a 1:1 connection between an encoder and a single receiver (unicast), the device enables multiple receivers to receive the video signal from an encoder simultaneously.
The device either duplicates the data stream itself and then distributes it to multiple receivers (Multi-unicast) or it sends a single data stream to the network, where the data stream is simultaneously distributed to multiple receivers in a defined group (Multicast). You can enter a dedicated multicast address and port for each stream.
The prerequisite for multicast operation is a multicast-capable network that uses the UDP and IGMP protocols. Other group management protocols are not supported. The TCP protocol does not support multicast connections.
A special IP address (class D address) must be configured for multicast operation in a multicast-enabled network. The network must support group IP addresses and the Internet Group Management Protocol (IGMP V2). The address range is from 225.0.0.0 to 239.255.255.255. The multicast address can be the same for multiple streams. However, it is then necessary to use a different port in each case so that multiple data streams are not sent simultaneously using the same port and the same multicast address.
Note: The settings must be done for each encoder (video input) and for each stream individually. The numbering follows the labeling of the video inputs on the device.

Enable
To enable simultaneous data reception on several receivers you need to activate the multicast function. To do this, select the check box. Then enter the multicast address.

Multicast Address
Enter a valid multicast address for each stream from the relevant encoder (video input) to be operated in multicast mode (duplication of the data streams in the network).
With the setting 0.0.0.0 the encoder for the relevant stream operates in multi-unicast mode (copying of data streams in the device). The device supports multi-unicast connections for up to five simultaneously connected receivers.
Note: Duplication of data places a heavy demand on the device and can lead to impairment of the image quality under certain circumstances.

Port
Assign a different port to each data stream if there are simultaneous data streams at the same multicast address.
Enter the port address of the required stream here.

Streaming
Select the check box to activate multicast streaming mode for the relevant stream. The device even streams multicast data if no connection is active.
For normal multicast operation, streaming is typically not required.

Packet TTL (only for Dinion IP, Gen4 and FlexiDome)
Enter a value to specify how long the multicast data packets are active on the network. If multicast is to be run via a router, the value must be greater than 1.

15.30   Accounts

Four separate accounts can be defined for posting and recording export.

Type

Select either FTP or Dropbox for the account type.

Before using a Dropbox account ensure that the time settings of the device have been correctly synchronized.

Account name

Enter an account name to be shown as the target name.

FTP server IP address

For an FTP server, enter the IP address.

FTP server login

Enter your login name for the account server.

FTP server password

Enter the password that gives access to the account server. Click Check to confirm that it is correct.

Path on FTP server

Enter an exact path to post the images on the account server. Click Browse... to browse to the required path.

Maximum bit rate

Enter the maximum bit rate in kbps that will be allowed when communicating with the account.

15.31   IP v4 Filter

To restrict the range of IP addresses within which you can actively connect to the device, fill-in an IP address and mask. Two ranges can be defined.

▸   Click **Set** and confirm to restrict access.

If either of these ranges are set, no IP V6 addresses are allowed to actively connect to the device.

The device itself may initiate a connection (for example, to send an alarm) outside the defined ranges if it is configured to do so.

15.32   Licenses page

You can enter the activation key to release additional functions or software modules.

> **i** | **Notice!**
> The activation key cannot be deactivated again and is not transferable to other units.

15.33   Certificates page

How to get here: **Configuration** window > expand **System** > click **Certificates**

This page displays all available and used certificates. You can also create and upload new certificates and delete certificates that are no longer needed.

Common name column

Displays the common name you must enter in case of generating a signing request to create a new certificate.

Issuer column

Displays the issuer signed the certificate.

Expires column

Displays when the certificate date expires.

Key column

Displays that a key is available for the certificate.

Usage column

Displays the respective certificates in the system. Click the list to select more certificates if necessary.

Note: Trusted certificates are .displayed separately.

🗑 **trashcan icon (Delete)**

Click to delete the selected certificate.

📥 **icon (Download)**

Click to download the certificate file.

Set

Click to save your actions.

Add

Click to upload existing certificates or to generate a signing request to obtain new certificates.

15.34   Maintenance page

Update server

The address of the firmware update server appears in the address box.

15.35   Decoder page

15.35.1   Decoder profile

Allows you to set the various options for the display of video images on an analog monitor or VGA monitor.

Monitor name

Type the name of the monitor. The monitor name facilitates the identification of the remote monitor location. Use a name that makes it as easy as possible to identify the location.

Click 💾 to update the name in the Device Tree.

Standard

Select the video output signal of the monitor you are using. Eight pre-configured settings for the VGA monitors are available in addition to the PAL and NTSC options for analog video monitors.

 Caution!

 Selecting a VGA setting with values outside the technical specification of the monitor can result in severe damage to the monitor. Refer to the technical documentation of the monitor you are using.

Window layout

Select the default image layout for the monitor.

VGA screen size

Type the aspect ratio of the screen (for example 4 x 3) or the physical size of the screen in millimeters. The device uses this information to accurately scale the video image for distortion-free display.

15.35.2   Monitor display

The device recognizes transmission interruptions and displays a warning on the monitor.

Display transmission disturbance

Select **On** to display a warning in case of transmission interruption.

Disturbance sensitivity

Move the slider to adjust the level of the interruption that triggers the warning.

Disturbance notification text

Type the text of the warning the monitor displays when connection is lost. The maximum text length is 31 characters.

Delete decoder logo

Click to delete the logo that has been configured on the Web page of the decoder.

16   Maps and Structure page

> **Notice!**
> This document describes some functions that are not available for BVMS Viewer.

The count of items below an entry is displayed in square brackets.

Main window >   **Maps and Structure**

Permissions can get lost. If you move a group of devices, these devices loose their permission settings. You must set the permissions on the **User Groups** page again.

Displays the Device Tree, the Logical Tree, and the map window.

Allows you to introduce a structure for all the devices in your BVMS. Your structure is displayed in the Logical Tree.

Allows you to perform the following tasks:

– Configuring the Full Logical Tree
– Managing resource files, assigning them to nodes
– Creating hot spots on a map
– Creating a malfunction relay

Resource files can be:

– Site map files
– Document files
– Web files
– Audio files
– Command Scripts
– Camera sequence files

Hot spots can be:

– Cameras
– Inputs
– Relays
– Command Scripts
– Sequences
– Links to other maps

Displays a dialog box for managing resource files.

Displays a dialog box for adding or managing Command Scripts to the Logical Tree.

Displays a dialog box for adding or editing a camera sequence file.

Creates a folder in the Logical Tree.

Displays a dialog box for adding map resource files.

Displays a dialog box for adding a document file (HTML, HTM, TXT, URL, MHT).

Displays a dialog box for adding a link to an external application.

Displays a dialog box for adding a malfunction relay.

: Device was added to the Logical Tree.

Type in a string and press the ENTER key to filter the displayed items. Only items containing the string and their corresponding parent items (only in trees) are displayed. The count of filtered items and the total count of items is provided. An active filter is indicated by . Enclose strings with double quotes to find them exactly, for example "Camera 1" exactly filters the cameras with this name, not camera 201.

To cancel filtering, click .

16.1   Sequence Builder dialog box

Main window >   **Maps and Structure** >

Allows you to manage camera sequences.

Click to display the **Add Sequence** dialog box.

Click to rename a camera sequence.

Click to remove the selected camera sequence.

> **Notice!**
> When you delete a sequence in the **Sequence Builder** dialog box, this sequence is automatically removed from the **Initial sequence** list of a monitor wall if configured there.

Add Step

Click to display the **Add Sequence Step** dialog box.

Remove Step

Click to remove selected steps.

Step

Displays the number of the step. All cameras of a particular step have the same dwell time.

Dwell

Allows you to change the dwell time (seconds).

Camera Number

Click a cell to select a camera via its logical number.

Camera

Click a cell to select a camera via its name.

Camera Function

Click a cell to change the function of the camera in this row.

Data

Type the time for the duration of the selected camera function. To configure this, you must have selected an entry in the **Camera** column and an entry in the **Camera Function** column.

Data Unit

Select the unit for the selected time, for example seconds. To configure this, you must have selected an entry in the **Camera** column and an entry in the **Camera Function** column.

Add to Logical Tree

Click to add the selected camera sequence to the Logical Tree and to close the dialog box.

See also

– *Monitor Wall page, page 73*
– *Managing pre-configured camera sequences, page 47*

16.2   Add Sequence dialog box

Main window > **Maps and Structure** > > **Sequence Builder** dialog box >

Allows you to configure the properties of a camera sequence.

Sequence name:

Type an appropriate name for the new camera sequence.

Logical number:

For using with a Bosch IntuiKey keyboard, enter a logical number for the sequence.

Dwell time:

Enter the appropriate dwell time.

Cameras per step:

Enter the number of cameras in each step.

Steps:

Enter the appropriate number of steps.

See also

– *Managing pre-configured camera sequences, page 47*

16.3   Add Sequence Step dialog box

Main window > **Maps and Structure** > > **Add Step** button

Allows you to add a step with a new dwell time to an existing camera sequence.

Dwell time:

Enter the appropriate dwell time.

See also

– *Managing pre-configured camera sequences, page 47*

17   Cameras and Recording page

Notice!
This document describes some functions that are not available for BVMS Viewer.

Main window > **Cameras and Recording**

Displays the Camera Table page or a Recording Table page.

Allows you to configure camera properties and recording settings.

Allows you to filter the cameras that are displayed according to their type.

Click to copy recording settings from one Recording Schedule to another.

Click to display the **Stream Quality Settings** dialog box.

Click to display the **Scheduled Recording Settings** dialog box.

Click to display the dialog box for configuring a selected PTZ camera.

Displays all available cameras regardless of their storage device.

Click to change the Camera Table according to the selected storage device.

Displays the corresponding Camera Table. No recording settings are available because these cameras are not recorded in BVMS.

Type in a string and press the ENTER key to filter the displayed items. Only items containing the string and their corresponding parent items (only in trees) are displayed. The count of filtered items and the total count of items is provided. An active filter is indicated by ✗ . Enclose strings with double quotes to find them exactly, for example "Camera 1" exactly filters the cameras with this name, not camera 201.

To cancel filtering, click ✗ .

17.1   Cameras page

Main window > **Cameras and Recording** > Click an icon to change the Cameras page according to the desired storage device, for example

Displays various information on the cameras available in your BVMS.

Allows you to change the following camera properties:
– Camera name
– Assignment of an audio source
– Logical number
– PTZ control, if available
– Live quality (VRM and Live / Local Storage)

- Recording settings profile
- Minimum and maximum storage time
- Region of Interest (ROI)
- Automated Network Replenishment
- Dual Recording

▸ Click a column title to sort the table by this column.

Camera - Encoder

Displays the device type.

Camera - Camera

Displays the name of the camera.

Camera - Network Address

Displays the IP address of the camera.

Camera - Location

Displays the location of the camera. If the camera is not assigned to a Logical Tree yet, **Unassigned Location** is displayed.

Camera - Device Family

Displays the name of the device family to which the selected camera belongs.

Camera - Number

Click a cell to edit the logical number that the camera received automatically when it was detected. If you enter an already used number, a corresponding error message is displayed. The logical number is "free" again when the camera is removed.

Audio

Click a cell to assign an audio source to the camera.

If an alarm occurs with low priority and with a camera that has audio configured, this audio signal is played even when an alarm with higher priority is currently being displayed. But this is only true, if the high priority alarm has no audio configured.

Stream 1 - Codec / Stream 2 - Codec (only VRM and Local Storage)

Click a cell to select the desired codec for encoding the stream.

Stream 1 - Quality / Stream 2 - Quality

Select the desired quality of the stream used for live or recording. You configure quality settings in the **Stream Quality Settings** dialog box.

Stream 1 - Active platform / Stream 2 - Active platform

Shows the name of the platform settings within the **Stream Quality Settings** dialog box. This column is read only and indicates which profile settings will be written to the encoder.

---

i **Notice!**

Applicable only if the stream quality profiles quiet, standard or busy are selected:
The value **Active platform** changes if you change the codec of the selected camera. The target bit rate is adjusted automatically and the name of the platform settings is displayed.

Live Video - Stream (only VRM and Live Only and Local Storage)

Click a cell to select the stream for a VRM or a local storage / live only encoder.

Live Video - Profile (only available for ONVIF cameras)

Click a cell to browse for the available live profile tokens of this ONVIF camera.

If you select the **<Automatic>** entry, the stream with the highest quality is automatically used.

Live Video - ROI

Click to enable Region of Interest (ROI). This is only possible if in the **Quality** column the H.264 MP SD ROI or H.265 MP SD ROI item is selected for stream 2 and stream 2 is assigned to Live Video.

Note: If stream 1 is used for Live for a specific workstation then the Operator Client running on this workstation cannot enable ROI for this camera.

is automatically enabled in the   table.

Recording - Setting

Click a cell to select the required recording setting. You configure the available recording settings in the **Scheduled Recording Settings** dialog box.

Recording - Profile (only available for ONVIF cameras)

Click a cell to browse for the available recording profile tokens of this ONVIF camera. Select the desired entry.

Recording - ANR

Select a check box to enable the ANR function. You can only enable this function, if the encoder has an appropriate firmware version and an appropriate device type.

Recording - Max Pre-Alarm Duration

Displays the calculated maximum pre-alarm duration for this camera. This value can help you in calculating the required storage capacity of the local storage medium.

> **Notice!**
>
> If a Mirrored VRM is already configured for an encoder, you cannot change any settings for this encoder in the **Secondary Recording** columns.

Secondary Recording - Setting (only available if a Secondary VRM is configured)

Click a cell to assign a scheduled recording setting to the dual recording of this encoder. Depending on your configuration it can happen that the configured stream quality for secondary recording is not valid. The stream quality configured for primary recording is then used instead.

Secondary Recording - Profile (only available for ONVIF cameras)

Click a cell to browse for available recording profile tokens of this ONVIF camera.

(Only visible when you click   **All**)

Select a check box to activate PTZ control.

Note:

For port settings refer to *COM1, page 104*.

Port (Only visible when you click   **All**)

Click a cell to specify which encoder serial port is used for PTZ control. For a PTZ camera connected to a Bosch Allegiant system, you can select **Allegiant**. For such a camera you do not need to use a trunk line.

Protocol (Only visible when you click   **All**)

Click a cell to select the appropriate protocol for the PTZ control.

PTZ Address (Only visible when you click   **All**)

Type the address number for the PTZ control.

Recording - Storage Min Time [days]

Secondary Recording - Storage Min Time [days] (only VRM and Local Storage)

Click a cell to edit the minimum number of days that video data from this camera is retained. Recordings younger than this number of days are not deleted automatically.

Recording - Storage Max Time [days]

Secondary Recording - Storage Max Time [days] (only VRM and Local Storage)

Click a cell to edit the maximum number of days that video data from this camera is retained. Only recordings older than this number of days are deleted automatically. 0 = unlimited.

See also

17.2 PTZ/ROI Settings dialog box

Main window > ![icon] **Cameras and Recording** > ![icon] > Select a PTZ camera > ![icon]

Allows you to configure a PTZ camera or a ROI camera.

For a ROI camera no auxiliary commands are available.

Note:

First configure the port settings of your PTZ camera before you can configure the PTZ camera settings. Otherwise the PTZ control is not working in this dialog box.

![icon] Click to move the camera to the predefined position or to execute the command.

![icon] Click to save the predefined position or command.

![icon] Click to rename the predefined position or command.

![icon] Click to remove the predefined position or command.

Predefined Positions tab

Click to display the table with the predefined positions.

Nr

Displays the number of the predefined position.

Name

Click a cell to edit the name of the predefined position.

Aux Commands tab (only for PTZ cameras)

Click to display the table with the auxiliary commands.

Nr

Displays the number of the auxiliary command.

Name

Click a cell to edit the name of the command.

Code

Click a cell to edit the command´s code.

See also

– *Configuring PTZ camera settings, page 50*

18 User Groups page

Notice!
This document describes some functions that are not available for BVMS Viewer.

Main window > **User Groups**

Allows you to configure user groups, Enterprise User Groups and Enterprise Access.
The following user group is available by default:
– Admin Group (with one Admin user).

User Groups tab
Click to display the pages available for configuring the rights of the standard user group.

Enterprise User Group tab (only available with valid Enterprise license)
Click to display the pages available for configuring the permissions of an Enterprise User Group.

Enterprise Access tab (only available with valid Enterprise license)
Click to display the pages available for adding and configuring Enterprise Access.

User/user group options

 Click to delete a selected entry.

 Click to add a new group or account.

 Click to add a new user to the selected user group. Change the default user name if desired.

 Click to add a new dual authorization group.

 Click to add a new logon pair for dual authorization.

 Displays a dialog box for copying permissions from a selected user group to another user group.

 Click to display the pages available for configuring the permissions of this group.

 Click to display the page available for configuring the properties of this user.

 Click to display the page available for configuring the properties of this logon pair.

 Click to display the pages available for configuring the permissions of this dual authorization group.

Activating user name changes and password changes

 Click to activate password changes.

Click to activate user name changes.

Notice!
User name changes and password changes are reverted after a configuration rollback.

Notice!
Enterprise User Groups and Enterprise Access are not available for BVMS Viewer.

Permissions on a single Management Server
For managing the access to one of the Management Servers, use the standard user group. You configure all permissions on this Management Server in this user group.
You can configure dual authorization user groups for standard user groups and for Enterprise User Groups.

Type in a string and press the ENTER key to filter the displayed items. Only items containing the string and their corresponding parent items (only in trees) are displayed. The count of filtered items and the total count of items is provided. An active filter is indicated by ✗ . Enclose strings with double quotes to find them exactly, for example "Camera 1" exactly filters the cameras with this name, not camera 201.

To cancel filtering, click ✗ .

18.1 User Group Properties page

Main window > **User Groups** > **User Groups** tab > **> Operating Permissions** tab > **User Group Properties** tab
or

Main window > **User Groups** > **Enterprise User Group** tab > **> Operating Permissions** tab > **User Group Properties** tab

Notice!
Enterprise User Groups and Enterprise Access are not available for BVMS Viewer.

Allows you to configure the following settings for the selected user group:
– Logon schedule
– Association of an LDAP user group

Description:
Type an informative description for the user group.

Language
Select the language of the Operator Client.

Associated LDAP group

Type the name of the LDAP user group that you want to use for your system.

You can also double-click an item in the **LDAP groups** list.

Settings

Click to display the **LDAP Server Settings** dialog box.

Associate Group

Click to associate the selected LDAP group with this user group.

Clear Group

Click to clear the **Associated LDAP group** field. The association of the LDAP group to the BVMS user group is removed.

See also
– *Configuring LDAP settings, page 56*
– *Associating an LDAP group, page 56*

18.2   User Properties page

Main window > **User Groups** > **User Groups** tab >

Allows you to configure a new user in a standard user group or in an Enterprise User Group.

 Notice!

Enterprise User Groups and Enterprise Access are not available for BVMS Viewer.

If you change the password for a user or delete a user while this user is logged on, this user can still continue working with Operator Client after password change or deletion. If after password change or deletion the connection to Management Server is interrupted (for example after activating the configuration), the user cannot automatically reconnect to the Management Server again without logoff/logon at Operator Client.

Account is enabled

Select check box to activate a user account.

Full name

Type the full name of the user.

Description:

Type an informative description for the user.

User must change password at next logon

Select check box to enforce users to set a new password at next logon.

Enter new password

Type the password for the new user.

Confirm password

Type the new password again.

Notice!

We highly recommend to assign a specific password to all new users, and have the user change this at logon.

Notice!

Clients of Mobile Video Service, Web Client, Bosch iOS App and SDK clients are not able to change the password on logon.

Apply

Click to apply the settings.

Click to activate the password.

Additional information

After upgrading to BVMS 9.0.0.x the **User Properties** settings are the following:

–   **Account is enabled** is set.

–   **User must change password at next logon** is not set.

18.3   Logon Pair Properties page

Main window >   **User Groups** > **User Groups** tab >   **New Dual Authorization**

Group >

or

Main window >   **User Groups** > **Enterprise User Group** tab >   **New Enterprise**

Dual Authorization Group >

Notice!

Enterprise User Groups and Enterprise Access are not available for BVMS Viewer.

Allows you to modify a pair of user groups to a dual authorization group. The users of the first user group are the users that must log on in the first dialog box for logging on, the users of the second user group confirm the logon.

Select Logon Pair

In each list, select a user group.

Force dual authorization

Select the check box to force each user to log on only together with a user of the second user group.

See also

–   *Adding a logon pair to dual authorization group, page 54*

18.4   Camera Permissions page

Main window > [icon] **User Groups** > **User Groups** tab > [icon] > **Device Permissions** tab >
Camera Permissions tab
or

Main window > [icon] **User Groups** > **Enterprise Access** tab > [icon] > **Device Permissions**
tab > **Camera Permissions** tab

> **Notice!**
> Enterprise User Groups and Enterprise Access are not available for BVMS Viewer.

Allows you to configure the access rights for the features of a selected camera or camera
group for the selected user group.
If new components are added, camera permissions must be configured afterwards.
You can recall the access to a camera on the **Camera** page.

Camera
Displays the camera name as configured on the **Cameras and Recording** page.

Location
Displays the location of the camera as configured on the **Maps and Structure** page.

Access
Select a check box to allow access to this camera.

Live Video
Select a check box to allow using live video.

Live Audio
Select a check box to allow using live audio.

Playback Video
Select a check box to allow using playback video.
You can select or clear this check box only when playback is enabled on the **Operator
Features** page.

Playback Audio
Select a check box to allow using playback audio.
You can select or clear this check box only when playback is enabled on the **Operator
Features** page.

Export
Select a check box to allow exporting video data.
You can select or clear this check box only when the export of video data is enabled on the
Operator Features page.

PTZ/ROI
Select a check box to allow using the PTZ control or the ROI of this camera.
You can select or clear this check box only when the PTZ control or ROI of this camera is
enabled on the **Operator Features** page. Additionally you must configure PTZ or ROI in the
Camera Table.

Aux

Select a check box to allow executing auxiliary commands.

You can select or clear this check box only when the PTZ control of a camera is enabled on the **Operator Features** page.

Set Presets

Select a check box to allow the user to set prepositions of this PTZ camera.

You can also set prepositions for the Region of Interest feature, if enabled and authorized.

You can select or clear this check box only when the PTZ control of a camera is enabled on the **Operator Features** page.

18.5   Copy User Group Permissions dialog box

Main window >   **User Groups** > **User Groups** tab > >

or

Main window >   **User Groups** > **Enterprise User Group** tab > >

Allows you to select user group permissions to be copied to selected user groups.

Copy from:

Displays the selected user group. Its permissions are to be copied to another user group.

Settings to Copy

Select a check box to select the desired user group permissions for copying.

Copy to:

Select a check box to specify the user group where to copy the selected user group permissions to.

18.6   LDAP Server Settings dialog box

Main window >   **User Groups** > **User Groups** tab > > **Operating Permissions** tab > **User Group Properties** tab > **Settings** button

or

Main window >   **User Groups** > **Enterprise User Group** tab > > **Operating Permissions** tab > **User Group Properties** tab > **Settings** button

You enter the LDAP server settings that are configured outside of BVMS. You will need the assistance of your IT administrator who set up the LDAP server for the following entries.

All fields are mandatory except the fields in the **Test User / User Group** group box.

LDAP Server Settings

LDAP Server:

Type the name of the LDAP server.

Port

Type the port number of the LDAP server (default unencrypted: 389, encrypted: 636)

Secure connection

Select the check box to activate encrypted data transmission.

LDAP basis for user:

Type the unique name (DN = distinguished name) of the LDAP path in which you can search for a user. Example for a DN of the LDAP basis:CN=Users,DC=Security,DC=MyCompany,DC=com

Filter for user:

Select a filter used to search for a unique user name. Examples are predefined. Replace %username% with the actual user name.

LDAP basis for group:

Type the unique name of the LDAP path in which you can search for groups. Example for a DN of the LDAP basis: CN=Users,DC=Security,DC=MyCompany,DC=com

Filter for group member search:

Select a filter used to search for a group member.

Examples are predefined. Replace %usernameDN% with the actual user name and his DN.

Proxy User

User name (DN):

Type the unique name of the proxy user. This user is required to allow the users of this BVMS user group to access the LDAP server.

Password:

Type the proxy user password.

Test

Click to test whether the proxy user has access to the LDAP server.

Test User / User Group

The entries in this group box are not saved after clicking **OK**. They only serve for testing.

User name:

Type the name of a test user. Omit the DN.

Password:

Type the test user password.

Test User

Click to test whether the combination of user name and password is correct.

Group (DN):

Type the unique group name with which the user is associated.

Test Group

Click to test the association of the user with the group.

Group search filter:

Do not leave this field empty. If there is no entry, you cannot assign an LDAP group to a BVMS user group.

Select a filter to find a user group.

Examples are predefined.

See also

– *Configuring LDAP settings, page 56*

18.7 Logical Tree page

Main window > **User Groups** > **User Groups** tab > > **Device Permissions** tab > **Logical Tree** tab

or

Main window > **User Groups** > **Enterprise Access** tab > > **Device Permissions** tab > **Logical Tree** tab

Notice!

Enterprise User Groups and Enterprise Access are not available for BVMS Viewer.

Allows you to configure the Logical Tree for each user group.

To configure permissions:

▸   Select or clear the check boxes as appropriate.

      Selecting an item below a node, automatically selects the node.

      Selecting a node, automatically selects all items below.

Camera

Select a check box to give the users of the selected user group access to the corresponding devices.

You can recall the access to a camera on the **Camera Permissions** page.

Analog Monitor Group

Select the check box to give the users of the selected user group access to this analog monitor group.

See also

–   *Configuring device permissions, page 57*

18.8   Operator Features page

Main window >   **User Groups** > **User Groups** tab >   > **Operating Permissions** tab > **Operator Features** tab

or

Main window >   **User Groups** > **Enterprise User Group** tab   > **Operating Permissions** tab > **Operator Features** tab

---

ⓘ   **Notice!**

Enterprise User Groups and Enterprise Access are not available for BVMS Viewer.

Allows you to configure various permissions for the selected user group.

PTZ control of dome cameras

Select the check box to allow the control of a camera.

Control Priorities page: In the **Control Priorities** field, you can set the priority for acquiring the control of a camera.

Print and save

Select the check box to allow printing and saving video, maps and documents.

Playback

Select the check box to allow various playback features.

Export video

Select the check box to allow exporting video data.

Export MOV / ASF video

Select the check box to allow exporting video data in ASF and MOV format.

Protect video

Select the check box to allow protecting video data.

Unprotect video
Select the check box to allow both protecting and unprotecting video data.

Delete video
Select the check box to allow deleting video data.

Close Operator Client
Select the check box to allow closing the Operator Client.

Minimize Operator Client
Select the check box to allow minimizing the Operator Client.

Audio Intercom
Select the check box to allow the user to speak on the loudspeakers of an encoder with audio-in and audio-out function.

18.9 User Interface page

Main window >   **User Groups** > **User Groups** tab >   > **Operating Permissions** tab > **User Interface** tab

Allows you to configure the user interface of 4 monitors used by Operator Client.
You can configure a multi monitor mode with up to 4 monitors. You set for every monitor what is displayed on it, e.g. monitor 2 only displays Live Image panes or Monitor 1 and Monitor 2 use the 16:9 aspect ratio for HD cameras.

Control Monitor
Select the monitor which should be used as a control monitor.

Max. rows of image panes in playback
Select the maximum rows of Image panes displayed in the Playback Image window on the Control monitor.

Monitor 1 - 4
In the corresponding list of each monitor, select the required entry.

– For the Control monitor the entry **Control** is preselected and cannot be changed.
– For the Alarm monitor you can select one of the following entries:
  – **Live video and alarm content**
  – **Alarm content only**
– For the remaining monitors you can select one of the following entries:
  – **Live only Image window**
  – **Map and document window**
  – **Two maps and document**
  – **Fullscreen Live Image window**
  – **Quad Live Image window**

Max. rows of image panes
Select the maximum rows of Image panes displayed in the Image window on the appropriate monitor.
Note: This option is only available for the following views:
– **Control**
– **Alarm content only**
– **Live video and alarm content**
– **Live only Image window**

The remaining views have a fixed layout with a fixed number of Image pane rows and cannot be changed.

Image panes aspect ratio

For each monitor select the required aspect ratio for the initial startup of Operator Client. Use 16:9 for HD cameras.

Save settings when shutting down

Select the check box to activate that the system remembers the last state of the user interface when the user logs off from the Operator Client. If the check box is not selected, the Operator Client starts always with the configured user interface.

Restore Default

Click to restore the default settings of this page. All list entries are reset to their default settings.

18.10   Account policies page

Main window > **User Groups** > **User Groups** tab > > **Security** tab > **Account policies** tab
or

Main window > **User Groups** > **Enterprise User Group** tab > > **Security** tab > **Account policies** tab

Allows you to configure settings for users and passwords.

Strong password policy

Select the check box to enable the password policy.

For more information see: *Configuring users, permissions and Enterprise Access, page 51*

Notice!

The **Strong password policy** setting is only applied to the users if the check box is selected in the corresponding user group.

We highly recommend to keep this setting to enhance the protection of your computer against unauthorized access.

Minimum password length

This setting determines the least number of characters that can make up a password for a user account.

Select the check box to enable the setting and enter the minimum value.

Maximum password age in days

This setting determines the period of time (in days) that a password can be used before the system requires the user to change it.

Select the check box to enable the setting and enter the minimum value.

Number of used passwords in history

This setting determines the number of unique new passwords that must be associated with a user account before an old password can be reused.

Select the check box to enable the setting and enter the minimum value.

Maximum invalid logon attempts

This setting enables blocking an account after a specific number of logon attempts.

Select the check box to enable the setting and enter the minimum value.

Notice!

If the maximum value of invalid logon attempts is exceeded, the account is disabled and has to be activated again.

Notice!

The count of invalid logon attempts get reset upon successful login.

Notice!

The **Maximum invalid logon attempts** check box is disabled for the Admin Group.

Disable offline client

Select the check box to disable logon to an offline client.

The **Disable offline client** check box is automatically selected, if the **Maximum invalid logon attempts** check box is selected.

Additional information

From BVMS 9.0 on the following **Account policies** settings apply as default:

– The **Strong password policy** check box is pre-selected.
– The **Minimum password length** check box is pre-selected. The default value is 10.
– The **Maximum password age in days** check box is not pre-selected. The default value is 90.
– The **Number of used passwords in history** check box is not pre-selected. The default value is 10.
– The **Maximum invalid logon attempts** check box is not pre-selected. The default value is 1.
– The **Disable offline client** check box is not pre-selected.

See also

Glossary

802.1x

The IEEE 802.1x standard provides a general method for authentication and authorization in IEEE-802 networks. Authentication is carried out via the authenticator, which checks the transmitted authentication information using an authentication server (see RADIUS server) and approves or denies access to the offered services (LAN, VLAN or WLAN) accordingly.

Activation Key

Number that the user needs to activate the purchased licenses. You receive the Activation Key after entering the Authorization Number in the Bosch Security System Software License Manager.

alarm

Event that is configured to create an alarm. This is a particular situation (motion detected, doorbell rung, signal lost, etc.) that requires immediate attention. An alarm can display live video, playback video, an action plan, a web page, or a map.

analog monitor group

A set of analog monitors connected to decoders. The analog monitor group can be used for alarm processing in a given physical area. For example, an installation with three physically separated control rooms might have three monitor groups. The monitors in an analog monitor group are logically configured into rows and columns and can be set to full-screen or quad view.

ANR

Automated Network Replenishment. Integrated process that copies missing video data from a video transceiver to the network video recorder after a network failure. The copied video data exactly fills the gap that occurred after the network failure. Hence the transceiver needs any kind of local storage. The recording capacity on this local storage is calculated with the following formula: (network bandwidth x estimated network downtime + safety margin) x (1 + 1/backup speed). The resulting recording capacity is required because the continuous recording must continue during the copy process.

ASF

Advanced Systems Format; Microsoft Windows media audio and video format.

ATM

Automatic Teller Machine

bypass/unbypass

To bypass a device means to ignore any alarms that it may generate, usually for the duration of some extenuating circumstances such as maintenance. To unbypass means to stop ignoring them.

Command Script

Macro, that the administrator can program to build an automatic action like positioning a PTZ camera or send E-mails. For that functionality Bosch Video Management System provides a specific set of commands. Command Scripts are divided into Client Scripts and Server Scripts. Client Scripts are used on client workstations to execute certain tasks that can run on a client workstation. Server Scripts are executed automatically by an event that was triggered in the system. They get arguments provided by the event like date and time. A Command Script can consist of several scriptlets. You can create a Command Script using the following scripting languages: C#, VB.Net. Command Scripts are executed in response to events or alarms automatically according to a schedule (Server Scripts only), manually from the Logical Tree, or manually from icons or on maps.

decoder

Changes a digital stream to an analog stream, e.g., to display digital video on a analog monitor.

Device Tree

Hierarchical list of all the available devices in the system.

dewarping

The use of software to convert a circular image from a fisheye lens with radial distortion to a rectilinear image for normal viewing (dewarping is the correction of distortion).

dual authorization

Security policy that requires two different users to log on to the Operator Client. Both the users must be member of a normal Bosch Video Management System user group. This user group (or these user groups if the users are members of different user groups) must be part of a dual authorization group. A dual authorization group has its own access rights within Bosch Video Management System. This dual authorization group should have more access rights than the normal user group that the user belongs to. Example: User A is member of a user group called Group A. User B is member of Group B. Additionally a dual authorization group is configured with Group A and Group B as members. For the users of Group A, dual authorization is optional, for users of Group B it is mandatory. When user A logs on, a second dialog box for confirming the logon is displayed. In this dialog box, a second user can log on if he is available. If not, user A can continue and start the Operator Client. He then has only the access rights of Group A. When user B logs on, again a second dialog box for logging on is displayed. In this dialog box, a second user must log on. If not, user B cannot start the Operator Client.

DVR

Digital Video Recorder

dwell time

Preset amount of time a camera is displayed in an Image window until the next camera is displayed during a camera sequence.

DWF

Design Web Format. Used to display technical drawings on a computer monitor.

Edge dewarping

Dewarping performed in the camera itself.

Encoder

Changes an analog stream to a digital stream, e.g., to integrate analog cameras in a digital system like Bosch Video Management System. Some encoders can have a local storage like a flash card, a USB hard disk, or they can store their video data on iSCSI devices. IP cameras have an encoder built in.

Enterprise Access

Enterprise Access is a feature of BVMS which consists of one or more Enterprise Accounts. Each Enterprise Account contains device permissions to devices of a particular Management Server.

Enterprise Account

Enterprise Account is an authorization that enables a user of Operator Client to connect to the devices of a Management Server being part of an Enterprise System. In an Enterprise Account, all permissions for the devices of this Management Server are configured. Operator Client can simultaneously connect to all Management Server computers that are part of this Enterprise System. This access is either controlled by the membership to an Enterprise User Group, and is controlled by the device permissions configured in the Enterprise Account for this Management Server.

Enterprise User Group

Enterprise User Group is a user group that is configured on an Enterprise Management Server. Enterprise User Group defines the users that are authorized to access multiple Management Server computers simultaneously. Defines the operating permissions available for these users.

Failover VRM

Software in the BVMS environment. Takes over the task of the assigned Primary VRM or Secondary VRM in case of failure.

Hot spot

Mouse sensitive icon on a map. Hot spots are configured in Configuration Client. Hot spots can be for example cameras, relays, inputs. The operator uses it for localizing and selecting a device in a building. If configured, hot spots can display a blinking background color when a specific state event or alarm occurs.

Image pane

Used for displaying live and recorded video of a single camera, a map, or an HTML file.

IQN

iSCSI Qualified Name. The initiator name in IQN format is used for provisioning addresses for both iSCSI initiators and targets. With IQN mapping you create an initiator group that controls the

access to the LUNs on an iSCSI target and you write the initiator names of each encoder and the VRM into this initiator group. Only the devices whose initiator names are added to an initiator group are permitted to access a LUN. See LUN and see iSCSI.

iSCSI

Internet Small Computer System Interface. Protocol that manages storage via a TCP/IP network. iSCSI enables access to stored data from everywhere in the network. Especially with the advent of Gigabit Ethernet, it has become affordable to attach iSCSI storage servers simply as remote hard disks to a computer network. In iSCSI terminology, the server providing storage resources is called an iSCSI target, while the client connecting to the server and accessing the resources of the server is called iSCSI initiator.

LDAP

Lightweight Directory Access Protocol. Network protocol running over TCP / IP that allows accessing directories. A directory can be for example a list of user groups and their access rights. Bosch Video Management System uses it to get access to the same user groups as MS Windows or another enterprise user management system.

Live Mode

Logbook

Container for logging all events in Bosch Video Management System.

Logical number

Logical numbers are unique IDs assigned to each device in the system for ease of reference. Logical numbers are only unique within a particular device type. Typical use of logical numbers are Command Scripts.

Logical Tree

Tree with a customized structure of all the devices. The Logical Tree is used in the Operator Client to select cameras and other devices. In the Configuration Client, the "Full Logical Tree" is configured (on the Maps and Structure page) and tailored for each user group (on the User Groups page).

LUN

Logical Unit Number. Used in the iSCSI environment to address an individual disk drive or a virtual partition (volume). The partition is part of a RAID disk array (the iSCSI target).

MOV

File extension of the default video format used by QuickTime Player from Apple.

MSS

Maximum Segment Size. The largest amount of data, specified in bytes, that a computer or communications device can handle in a single, unfragmented piece.

Multicast

Communication between a single transceiver and multiple receivers on a network by distribution of a single data stream on the network to a number of receivers in a defined group. Requirement for multicast operation is a multicast compliant network with implementation of the UDP protocol and the IGMP protocol.

ONVIF

Open Network Video Interface Forum. Global standard for network video products. ONVIF conformant devices are able to exchange live video, audio, metadata, and control information and ensure that they are automatically discovered and connected to network applications such as video management systems.

Panoramic camera

Camera with a 360° or 180° view angle.

Port

1) On computer and telecommunication devices, a port (noun) is generally a specific place for being physically connected to some other device, usually with a socket and plug of some kind. Typically, a personal computer is provided with one or more serial ports and usually one parallel port. 2) In programming, a port (noun) is a "logical connection place" and specifically, using the Internet protocol, TCP/IP, the way a client program specifies a particular server program on a computer in a network. Higher-level applications that use TCP/IP such as the Web protocol, Hypertext Transfer Protocol, have ports with preassigned numbers. These are known as "well-

known ports" that have been assigned by the Internet Assigned Numbers Authority (IANA). Other application processes are given port numbers dynamically for each connection. When a service (server program) initially is started, it is said to bind to its designated port number. As any client program wants to use that server, it also must request to bind to the designated port number. Port numbers are from 0 to 65535. Ports 1 to 1023 are reserved for use by certain privileged services. For the HTTP service, port 80 is defined as a default and it does not have to be specified in the Uniform Resource Locator (URL).

POS

Point of sale.

PTZ camera

Camera with pan, tilt, and zoom function.

RADIUS server

Remote Authentication Dial-In User Service: a client/server protocol for the authentication, authorization and accounting of users with dial-up connections on a computer network. RADIUS is the de-facto standard for central authentication of dial-up connections via Modem, ISDN, VPN, Wireless LAN (see 802.1x) and DSL.

Recording Schedule

Used for scheduling recording and for scheduling some events like starting backup or limiting log on. Recording Schedules cannot have gaps or overlaps. It also determines the video recording quality.

ROI

Region of Interest. Intended use of ROI is to save bandwidth when zooming into a section of the camera image with a fixed HD camera. This section behaves like a PTZ camera.

RTSP

Real Time Streaming Protocol. A network protocol which allows to control the continuous transmission of audio-visual data or software over IP-based networks.

SNMP

Simple Network Management Protocol. IP based protocol that allows to get information from networking devices (GET), to set parameters on network devices (SET) and to be notified about certain events (EVENT).

SNTP

Simple Network Time Protocol is a simplified version of NTP (see NTP). SNTP can be used when the ultimate performance of the full NTP implementation described in RFC 1305 is not needed or justified. SNTP version 4 is described in RFC 2030 (see RFC).

TCP/IP

Transmission Control Protocol / Internet Protocol. Also known as Internet protocol suite. Set of communication protocols used to transmit data over an IP network.

tilt angle

The angle between the horizontal and the camera.

UDP

User Datagram Protocol. A connection less protocol used to exchange data over an IP network. UDP is more efficient than TCP for video transmission because of lower overhead.

unmanaged site

Item of the Device Tree in BVMS that can contain video network devices like Digital Video Recorders. These devices are not managed by the Management Server of your system. The user of Operator Client can connect to the devices of an unmanaged site on demand.

User group

User groups are used to define common user attributes, such as permissions, privileges and PTZ priority. By becoming a member of a group, a user automatically inherits all the attributes of the group.

Video Streaming Gateway (VSG)

Virtual device that allows integrating Bosch cameras, ONVIF cameras, JPEG cameras, RTSP encoders.

VIDOS NVR

VIDOS Network Video Recorder. Software that stores the audio and video data of IP encoders on a RAID 5 disk array or any other storage medium.

VIDOS NVR provides functions for playback and
retrieval of the recorded video. You can integrate
cameras in your Bosch Video Management System
that are connected to a VIDOS NVR computer.

VRM

Video Recording Manager. Software package in
Bosch Video Management System which manages
storing video (MPEG-4 SH++, H.264 and H.265)
with audio data and metadata on iSCSI devices in
the network. VRM maintains a database
containing the recording source information and a
list of associated iSCSI drives. VRM is realized as
a service running on a computer in the Bosch
Video Management System network. VRM does
not store video data itself but distributes storage
capacities on iSCSI devices to the encoders, while
handling load balancing between multiple iSCSI
devices. VRM streams playback from iSCSI to
Operator Clients.

Workstation

In the BVMS environment: A dedicated computer
where Operator Client is installed. This computer
is configured as a workstation in Configuration
Client to enable specific functions.

Index