



BOSCH

BVMS

en Configuration Manual

Table of contents

1	Using the Help	7
1.1	Finding information	7
1.2	Printing the Help	7
2	Introduction	9
3	System overview	11
3.1	Hardware requirements	11
3.2	Software requirements	11
3.3	License requirements	11
4	Concepts	12
4.1	BVMS design concepts	12
4.1.1	Single Management Server System	12
4.1.2	Unmanaged site	13
4.2	Viewing modes of a panoramic camera	14
4.2.1	360° panoramic camera - floor- or ceiling mounted	15
4.2.2	180° panoramic camera - floor- or ceiling mounted	17
4.2.3	360° panoramic camera - wall mounted	18
4.2.4	180° panoramic camera - wall mounted	19
4.2.5	Cropped view on a panoramic camera	20
4.3	SSH Tunneling	21
5	Getting started	22
5.1	Installing BVMS Viewer	22
5.2	Starting BVMS Viewer Configuration Client	22
5.3	Activating the software licenses	22
5.3.1	Retrieving the computer signature	23
5.3.2	Obtaining the Activation Key	23
5.3.3	Activating the system	24
5.4	Preparing devices	24
5.5	Configuring the language of Configuration Client	24
5.6	Configuring the language of Operator Client	24
5.7	Scanning for devices	25
6	Managing configuration data	26
6.1	Activating the working configuration	26
6.2	Activating a configuration	27
6.3	Exporting configuration data	27
6.4	Importing configuration data	28
7	Global Configuration Client windows	29
7.1	Menu commands	29
7.2	Activation Manager dialog box (System menu)	29
7.3	Activate Configuration dialog box (System menu)	30
7.4	Initial Device Scan dialog box (Hardware menu)	30
7.5	License Investigator dialog box (Tools menu)	31
7.6	License Manager dialog box (Tools menu)	31
7.7	Options dialog box (Settings menu)	31
8	Devices page	33
8.1	Updating device states and capabilities	33
8.2	Adding a device	34
8.3	DiBos page	36
8.3.1	Adding a DiBos System via scan	36

8.3.2	Settings page	37
8.3.3	Cameras page	37
8.3.4	Inputs page	37
8.3.5	Relays page	37
8.4	DVR (Digital Video Recorder) page	37
8.4.1	Adding a DVR device via scan	38
8.4.2	Add DVR dialog box	38
8.4.3	Settings tab	39
8.4.4	Cameras tab	39
8.4.5	Inputs tab	39
8.4.6	Relays tab	39
8.4.7	Configuring the integration of a DVR	39
8.5	Workstation page	40
8.5.1	Adding a workstation manually	40
8.5.2	Settings page	41
8.6	Decoders page	41
8.6.1	Adding an Encoder / Decoder manually	42
8.6.2	Edit Encoder / Edit Decoder dialog box	43
8.6.3	Changing the password of an encoder / decoder (Change password / Enter password)	44
8.6.4	Decoder profile	45
8.6.5	Monitor display	45
8.6.6	Delete decoder logo	46
8.7	Monitor Wall page	46
8.7.1	Adding a Monitor Wall manually	46
8.8	Assign Keyboard page	47
8.9	VRM Devices page	48
8.9.1	Adding VRM Devices via scan	48
8.9.2	Adding a primary or secondary VRM manually	50
8.9.3	Editing a VRM device	51
8.9.4	Encrypting recording for VRM	51
8.9.5	Adding VSG devices via scan	53
8.10	Bosch Encoder / Decoder page	53
8.11	Live Only page	53
8.11.1	Adding live only devices via scan	53
8.11.2	Adding an Encoder / Decoder manually	54
8.11.3	Providing the destination password for a decoder (Authenticate...)	55
8.12	Local Storage page	56
8.13	Unmanaged Site page	56
8.13.1	Adding an unmanaged site manually	57
8.13.2	Importing unmanaged sites	57
8.13.3	Unmanaged Site page	57
8.13.4	Adding an unmanaged network device	58
8.13.5	Configuring the time zone	59
9	Bosch Encoder / Decoder / Camera page	60
9.1	Adding a live only encoder	61
9.2	Adding a local storage encoder	61
9.3	Editing an Encoder	61
9.3.1	Encrypting live video (Edit Encoder)	61
9.3.2	Updating the device capabilities (Edit Encoder)	62

9.3.3	Edit Encoder / Edit Decoder dialog box	63
9.4	Managing the verification of authenticity	64
9.4.1	Configuring the authentication	64
9.4.2	Uploading a certificate	64
9.4.3	Downloading a certificate	65
9.4.4	Installing a certificate on a workstation	65
9.5	Providing the destination password for a decoder (Authenticate...)	65
9.6	Changing the password of an encoder / decoder (Change password / Enter password)	66
9.7	Recovering recordings from a replaced encoder (Associate with recordings of predecessor)	67
9.8	Configuring encoders / decoders	67
9.8.1	Configuring multiple encoders / decoders	67
9.8.2	Recording Management page	69
9.8.3	Recording preferences page	70
9.9	Configuring multicast	70
10	Maps and Structure page	72
11	Configuring the Logical Tree	73
11.1	Configuring the Logical Tree	73
11.2	Adding a device to the Logical Tree	73
11.3	Removing a tree item	73
11.4	Adding a camera sequence	74
11.4.1	Sequence Builder dialog box	74
11.5	Managing pre-configured camera sequences	75
11.5.1	Add Sequence dialog box	76
11.5.2	Add Sequence Step dialog box	76
11.6	Adding a folder	77
11.7	Configuring bypass of devices	77
12	Cameras and Recording page	78
12.1	Cameras page	78
13	Configuring cameras and recording settings	80
13.1	Configuring PTZ port settings	80
13.2	Configuring predefined positions and auxiliary commands	80
13.3	Predefined positions and AUX commands dialog box	82
14	User Groups page	83
14.1	User Group Properties page	84
14.2	User Properties page	85
14.3	Logon Pair Properties page	86
14.4	Camera Permissions page	86
14.5	LDAP Server Settings dialog box	87
14.6	Logical Tree page	89
14.7	Operator Features page	89
14.8	User Interface page	90
14.9	Account policies page	91
15	Configuring users, permissions and Enterprise Access	93
15.1	Creating a group or account	94
15.1.1	Creating a standard user group	94
15.2	Creating a user	94
15.3	Creating a dual authorization group	95
15.4	Adding a logon pair to dual authorization group	95

15.5	Configuring Admin Group	96
15.6	Configuring LDAP settings	97
15.7	Associating an LDAP group	97
15.8	Configuring operating permissions	98
15.9	Configuring device permissions	98
	Glossary	100
	Index	104

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 **Display 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.



Notice!

This symbol indicates a potential risk of property damage or data loss.

1.2 Printing the Help

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

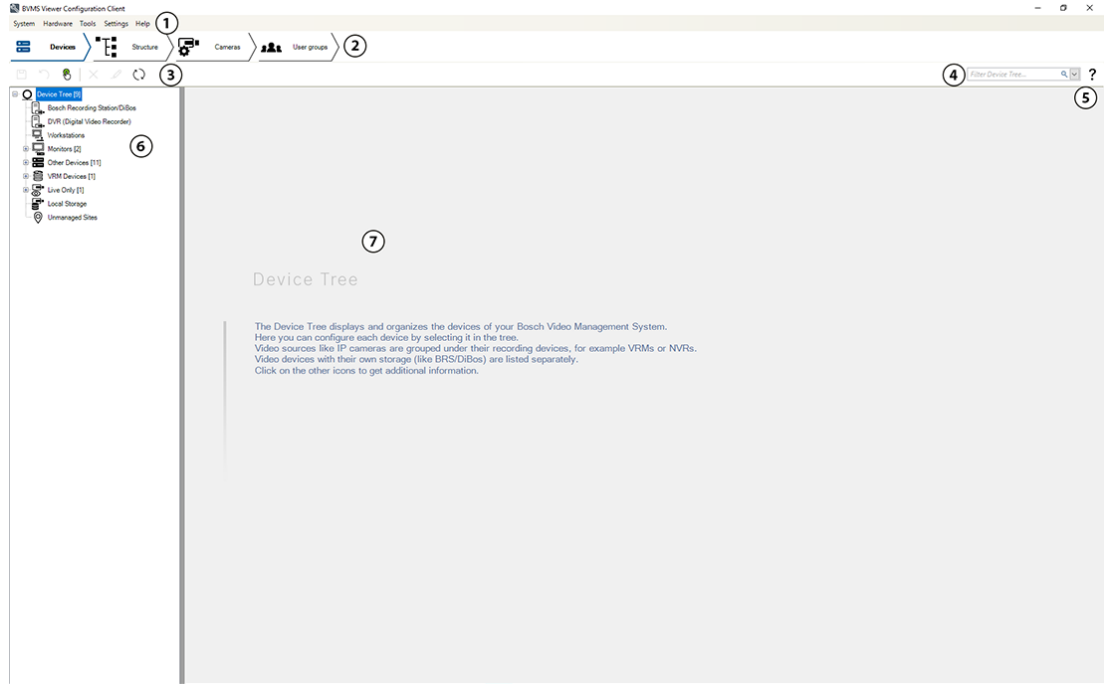
To print a Help topic:

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



Covered by one or more claims of the patents listed at patentlist.hevcadvance.com.





1	Menu bar	Allows you to select a menu command.
2	Pages bar	Allows you to configure all necessary steps from left to right.
3	Tool bar	Displays the available buttons according to the active tab. Hover over an icon to display the tooltip.
4	Search bar	Allows you to search for a specific device and their corresponding parents in the device tree.
5	Help icon	Displays the online help for the BVMS Configuration Client.
6	Selection window	Hierarchical list of all available devices in the system.
7	Configuration window	Allows you to configure the selected device.

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>.

The idea of the BVMS Configuration Client is to start with the configuration of the devices, followed by the configuration of the logical tree and the recordings. The last step is to configure the user groups in the user groups page. After configuring all pages from left to right, everything is configured and the operator can start using the Operator Client.

After configuring each page, save the configuration by clicking  in the tools menu.

To make the changes visible in the BVMS Operator Client , click  .

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



Notice!

BVMS Viewer offers only basic features. Advanced features are included in BVMS Professional. Visit our website www.boschsecurity.com for more information.

This chapter provides background information on selected issues.

4.1 BVMS design concepts

Single Management Server System, page 12

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

Unmanaged site, page 13

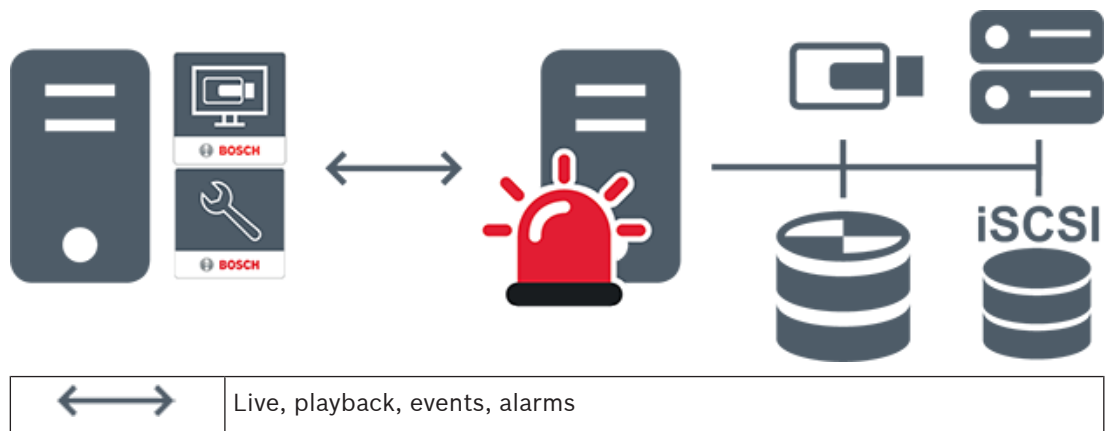
Devices can be grouped to unmanaged sites. Devices under unmanaged sites are not monitored by the Management Server. The Management Server provides a list of unmanaged sites to the Operator Client. The Operator can connect on demand to the site and gets access to live video data and recorded video data.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







4.1.1 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



	Management Server
	Operator Client / Configuration Client
	Cameras
	VRM
	iSCSI
	Other devices

4.1.2

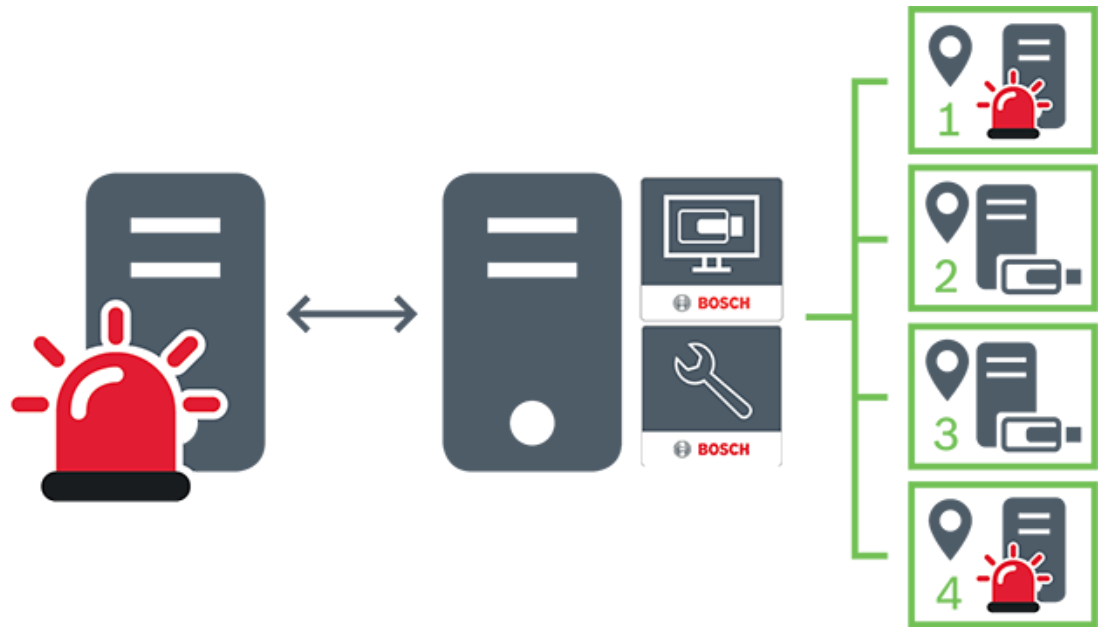
Unmanaged site

- 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 site .

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

- Bosch DIVAR AN 3000 / 5000 analog recorders
- DIVAR hybrid recorders
- DIVAR network 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

Refer to

- *Adding an unmanaged site manually, page 57*

4.2

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.

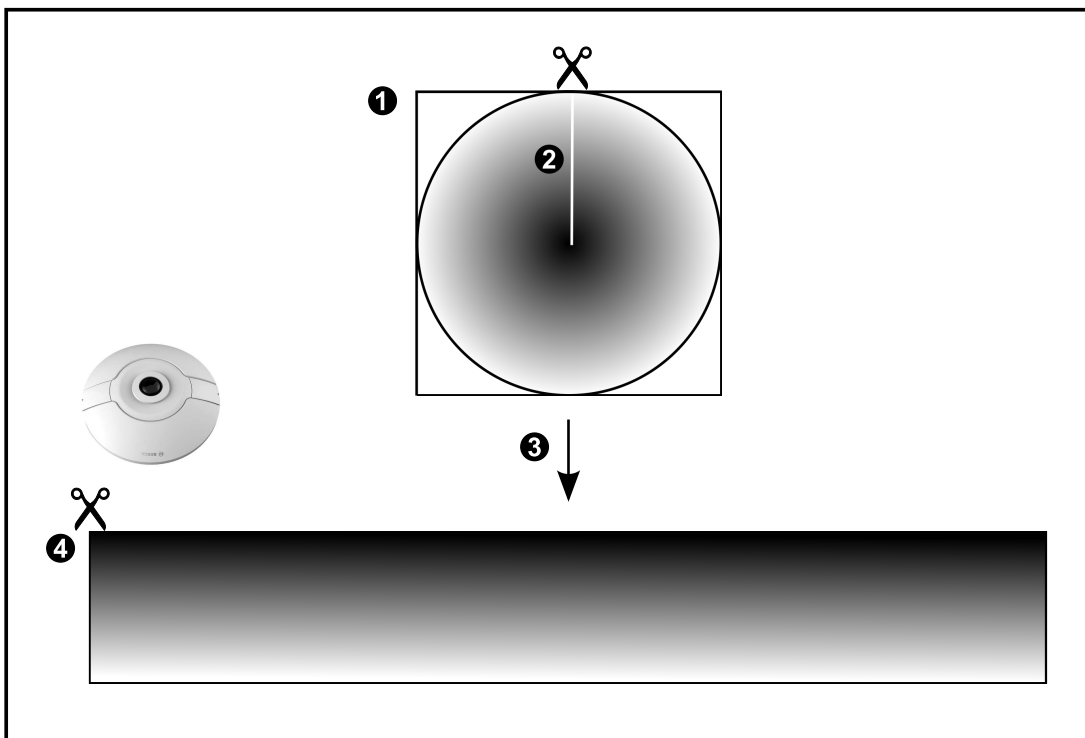
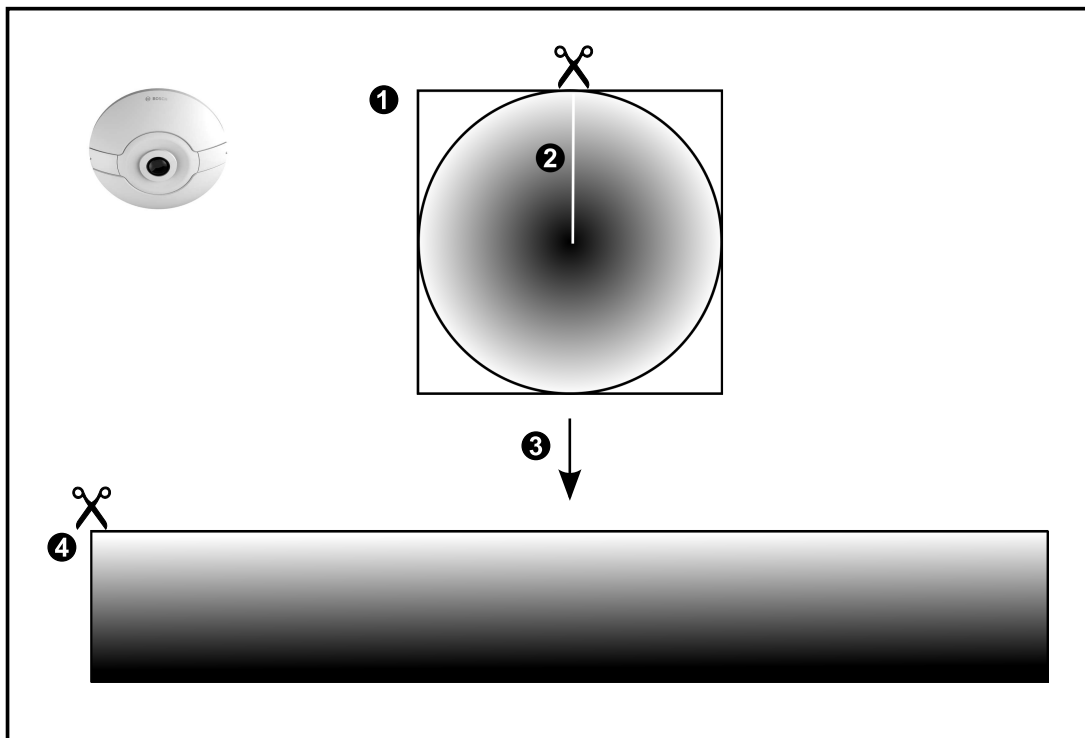
Refer to

– *Configuring predefined positions and auxiliary commands, page 80*

4.2.1

360° panoramic camera - floor- or ceiling mounted

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

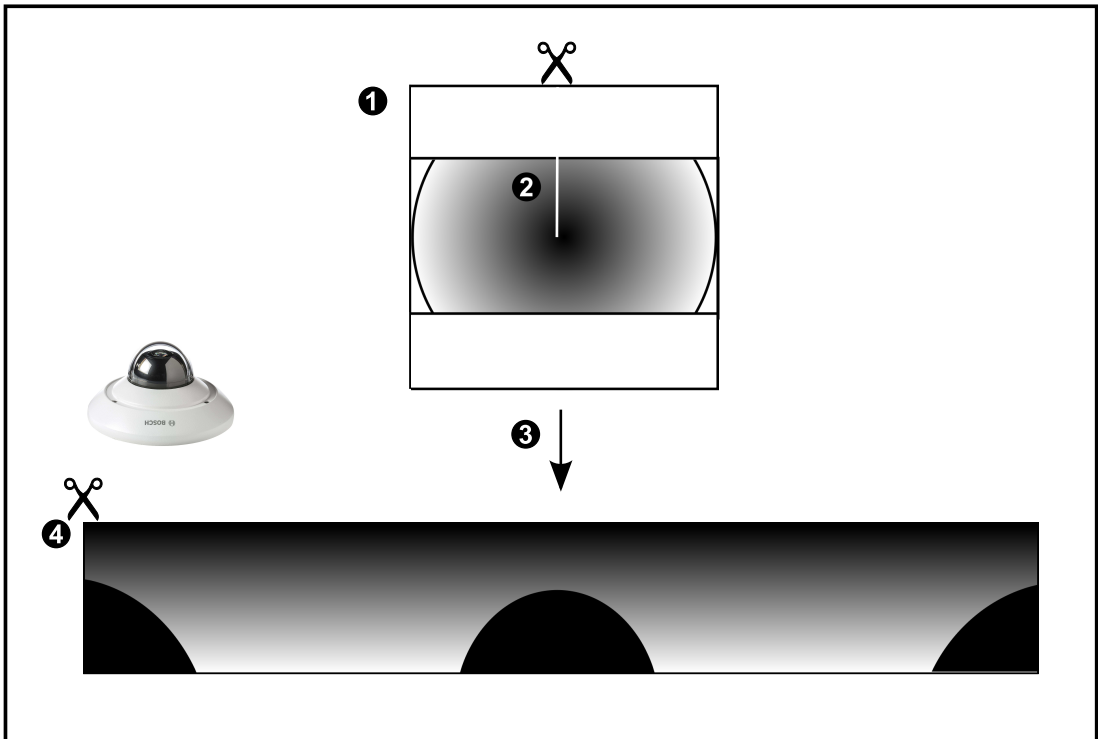
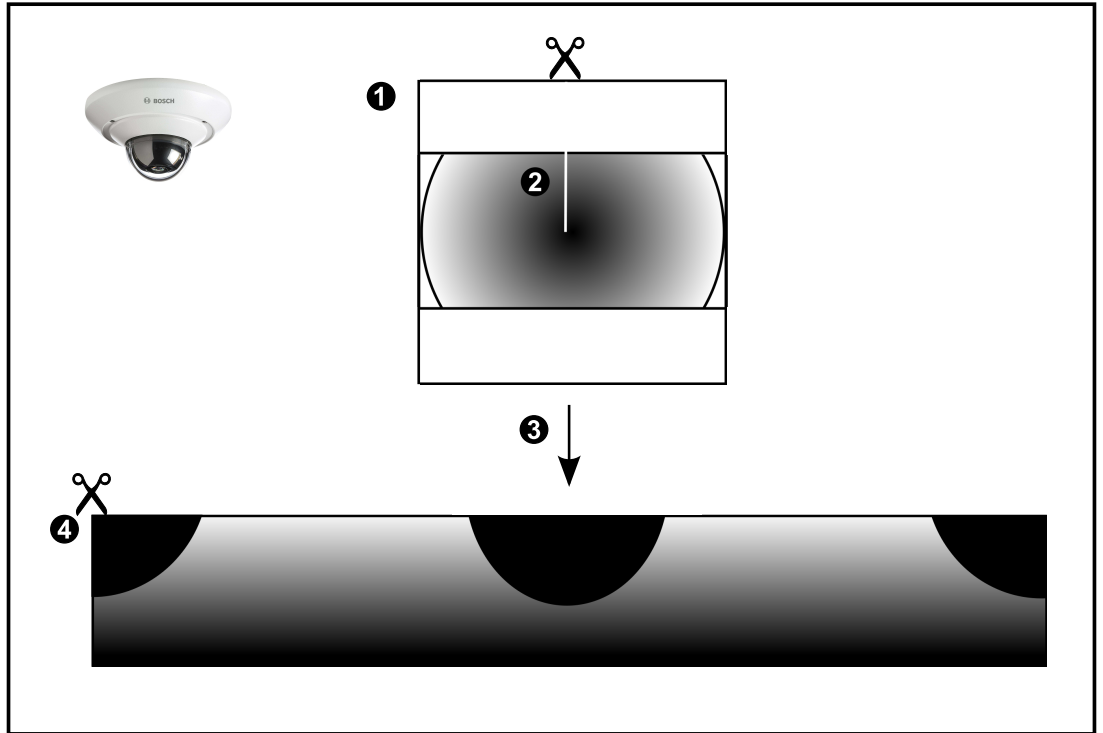


1	Full circle image	3	Dewarping
2	Snipping line (operator can change its position when not zoomed in)	4	Panorama view

4.2.2

180° panoramic camera - floor- or ceiling mounted

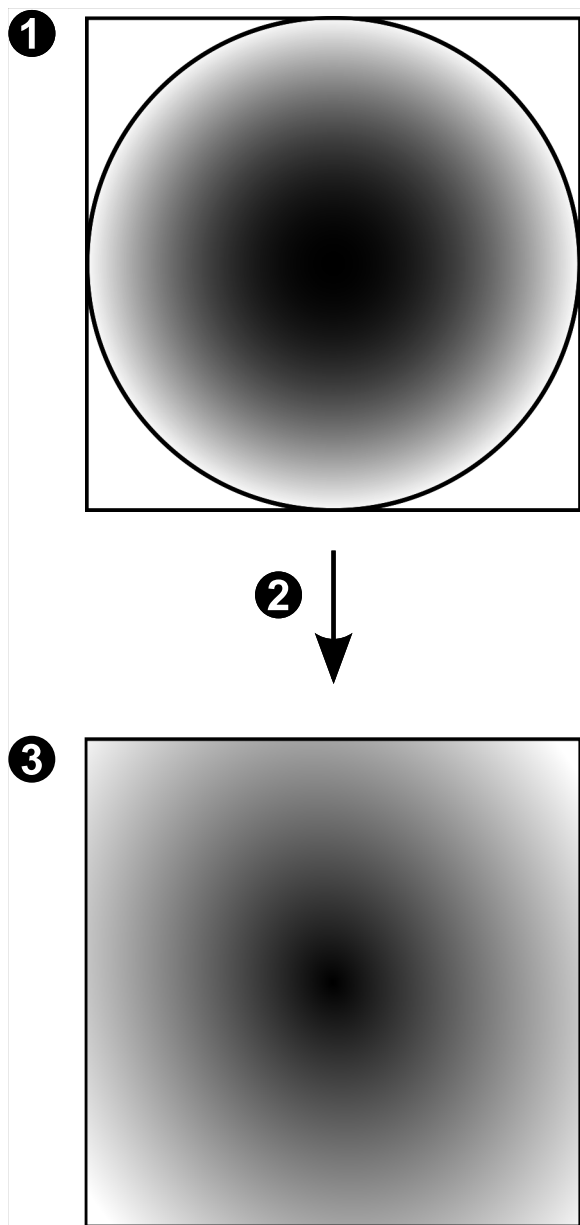
The following figure illustrates the dewarping of a 180° camera which is floor- or ceiling mounted.



1	Full circle image	3	Dewarping
2	Snipping line (operator can change its position when not zoomed in)	4	Panorama view

4.2.3 360° panoramic camera - wall mounted

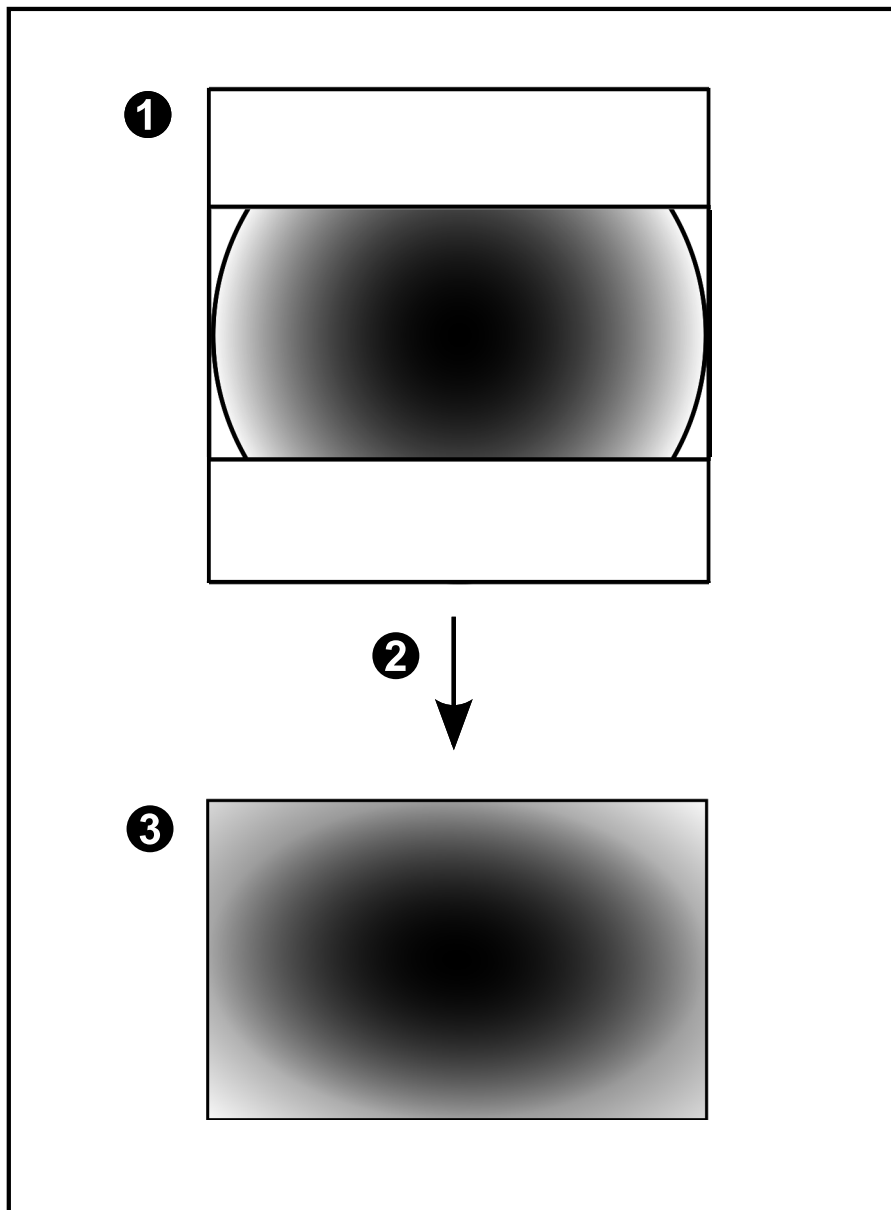
The following figure illustrates the dewarping of a 360° camera which is wall mounted.



1	Full circle image	3	Panorama view
2	Dewarping		

4.2.4 180° panoramic camera - wall mounted

The following figure illustrates the dewarping of a 180° camera which is wall mounted.

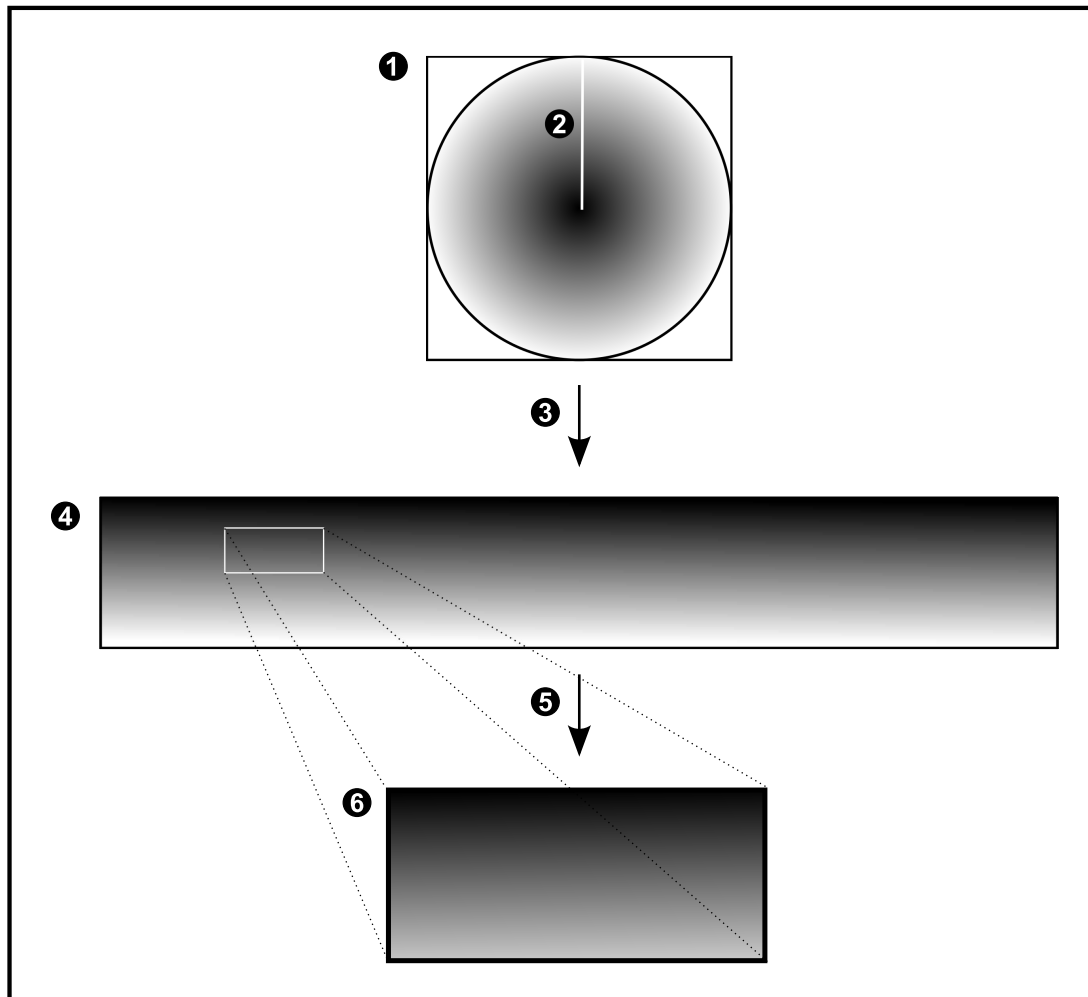


1	Full circle image	3	Panorama view
2	Dewarping		

4.2.5 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

4.3 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.
- (Enterprise) user accounts must have a configured password. (Enterprise) user accounts without a password cannot log on utilizing a SSH connection.
- Local storage cameras do not support 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

Refer to

- *License Manager dialog box (Tools menu), page 31*

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.

- 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:

- Start BVMS Viewer Configuration Client.
- On the **Tools** menu, click **License Manager...**
The **License Manager** dialog box is displayed.
- 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.
- Click **Activate**.
The **License Activation** dialog box is displayed.
- Copy the License Activation Key from the text file where you have saved it and paste it into the **License Activation Key:** field.
- Click **Activate**.
The appropriate software packages are activated.
- 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:


- On the **Settings** menu, click **Options....**
The **Options** dialog box is displayed.
- In the **Language** list, select the desired language.
If you select the **System language** entry, the language of your Windows installation is used.
- 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:

- Click **User groups** > . Click the **User Group Properties** tab. Click the **Operating Permissions** tab.
- In the **Language** list, select the desired language.
- Click  to save the settings.

4. Click  to activate the configuration.
Restart Operator Client.

5.7 Scanning for devices



Main window > **Devices**

You can scan for the following devices to add them with the help of the **BVMS Scan Wizard** dialog box:

- VRM devices
- Live only encoders
- Local storage encoders
- Decoders
- DVR devices
- VIDOS NVRs

If you want to add devices via scan, see the respective device topic in the chapter *Devices* page, page 33.

Refer to

- *Adding VRM Devices via scan, page 48*
- *Adding live only devices via scan, page 53*
- *Adding a device, page 34*

6 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.

6.1 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.
- Note:** Delayed-activation is not executed as long as the user is logged on to the Configuration Client.

Refer to

- *Activate Configuration dialog box (System menu), page 30*

6.2 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.

Refer to

- *Activate Configuration dialog box (System menu), page 30*
- *Activation Manager dialog box (System menu), page 29*

6.3 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.

Refer to

- *Importing configuration data, page 28*

6.4**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.

Refer to

- *Exporting configuration data, page 27*

7 Global Configuration Client windows



Notice!

BVMS Viewer offers only basic features. Advanced features are included in BVMS Professional. Visit our website www.boschsecurity.com for more information.

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

7.1 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.
Exit	Exits the program.

Hardware menu commands

Initial Device Scan...	Displays the Initial Device Scan dialog box.
-------------------------------	---

Tools menu commands

Sequence Builder...	Displays the Sequence Builder dialog box.
License Manager...	Displays the License Manager dialog box.
License Inspector...	Displays the License Inspector dialog box.

Settings menu commands

Options...	Displays the Options dialog box.
-------------------	---

Help menu commands


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

7.2 Activation Manager dialog box (System menu)

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

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

Activation Manager ✕

 Please select the configuration you want to activate. If you activate an older configuration, the system will perform a rollback and the newer configurations will be removed.

Date & Time	User	Description
Working Copy		
● 5/7/2019 4:11:26 AM	TECHDOC-02 : SYSTEM	Added event type data to configuration (BVMS version 10.0.0.701)
5/7/2019 4:10:55 AM	TECHDOC-02 : SYSTEM	Migrated to Version: 10.0.0.701
4/29/2019 9:22:23 AM	TECHDOC-02 : admin	
4/27/2019 4:18:21 AM	TECHDOC-02 : SYSTEM	Migrated to Version: 10.0.0.665
4/26/2019 4:40:24 PM	TECHDOC-02 : admin	
4/25/2019 4:14:54 AM	TECHDOC-02 : SYSTEM	Added event type data to configuration (BVMS version 10.0.0.661)
4/25/2019 4:14:16 AM	TECHDOC-02 : SYSTEM	Migrated to Version: 10.0.0.661
4/23/2019 3:42:19 PM	TECHDOC-02 : admin	
4/19/2019 4:18:47 AM	TECHDOC-02 : SYSTEM	Migrated to Version: 10.0.0.650
4/17/2019 2:32:48 PM	TECHDOC-02 : admin	
⬆ 4/17/2019 2:32:12 PM	TECHDOC-02 : admin	Configuration file created: 'C:\Users\bet1grb\Desktop\BoschVMS.zip'
4/11/2019 4:54:37 PM	TECHDOC-02 : admin	
4/9/2019 4:23:05 PM	TECHDOC-02 : admin	

⬆ Exported configuration

⬇ Imported configuration

● Currently active configuration

⬇ Rollback: This configuration will be removed after activation

Activate
Cancel

Activate

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

Refer to

- *Activating the working configuration, page 26*
- *Activating a configuration, page 27*

7.3 Activate Configuration dialog box (System menu)



Main window >

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

Note: Delayed-activation is not executed as long as the user is logged on to the Configuration Client.

Refer to

- *Activating the working configuration, page 26*

7.4 Initial Device Scan dialog box (Hardware menu)

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.

7.5 License Investigator dialog box (Tools menu)

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.

7.6 License Manager dialog box (Tools menu)

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.

7.7 Options dialog box (Settings menu)

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.

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.

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.

8 Devices page



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.



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.

8.1 Updating device states and capabilities



Main window > **Devices**

For example after a firmware update it can be necessary to synchronize the capabilities of all configured decoders, encoders and VSGs. With this function the capabilities from each device are compared to the capabilities already stored within BVMS. You can update the device capabilities of all devices in the device tree at once.

It is also possible to copy a list of the devices whose capabilities changed into the clipboard. You can then paste the list, for example, into a text editor to examine the changes in detail.

The device list from the clipboard is formatted as CSV and contains the following information:

- Device
- Device type
- IP address


Note: When you have a large system with several 1000 devices configured, the process of refreshing device states and updating device capabilities can take a long time.



Notice!

The capabilities are only retrieved for reachable devices. To see, if a device is not reachable, you have to check the state of the device.

To update the device states and capabilities:

1. Click .

The **Update device capabilities** dialog box is displayed. The state information of all devices is updated and the device capabilities are retrieved.

Only if device capabilities are not up to date, the appropriate devices are displayed in a list and the **Update** button is enabled.
 2. If required, click **Copy device list to clipboard**.
 3. Click **Update**.
 4. Click **OK**.
- ✓ The device capabilities are now updated.

**Notice!**

The state information of all devices will always be updated, even if you cancel the **Update device capabilities** dialog.

8.2**Adding a device**

Main window > **Devices**

You add the following devices to the Device Tree manually, that means you must know the network address of the device to add it:

- Video IP device from Bosch
- Bosch Recording Station/DiBos system
- Analog matrix
 - For adding a Bosch Allegiant device, you need a valid Allegiant configuration file.
- BVMS workstation
 - A workstation must have the Operator Client software installed.
- Communication device
- Bosch ATM/POS Bridge, DTP device
- Virtual input
- Network monitoring device
- Bosch IntuiKey keyboard
- KBD-Universal XF keyboard
- Monitor group
- I/O module
- Allegiant CCL emulation
- Intrusion panel from Bosch
- Server-based analytics device
- Access control systems from Bosch

You can scan for the following devices to add them with the help of the **BVMS Scan Wizard** dialog box:

- VRM devices
- Live only encoders
- Local storage encoders
- Decoders
- DVR devices
- VIDOS NVRs



Notice!

After having added a device, click  to save the settings.



Notice!

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.

BVMS Scan Wizard dialog box

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

Main window >  **Devices** > Right-click  > Click **Scan for Local Storage Encoders** > **BVMS 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**.

User Name

Displays the user name that is configured on the VRM device.
You can type in another user name if required.

Refer to

- *Adding VRM Devices via scan, page 48*
- *Adding a live only encoder, page 61*
- *Adding a local storage encoder, page 61*
- *Scanning for devices, page 25*

8.3**DiBos page**

Main window >  **Devices** >  > 

Displays the property pages of a selected DiBos system.
Allows you to integrate a DiBos system into your system.

**Notice!**


You do not configure the DiBos system itself but only the BVMS related properties.

- ▶ Click a tab to display the corresponding property page.

8.3.1**Adding a DiBos System via scan**

Main window >  **Devices** > Right-click  > **Add BRS/DiBos System** command
Allows you to add a DiBos system to your BVMS.

To add a DiBos system:

1. Right-click .
2. Click **Add BRS/DiBos System**.
The **Add BRS/DiBos System** dialog box is displayed.
3. Enter the appropriate values.
4. Click **Scan**.
The DiBos system is added to your system.
5. In the displayed message box, click **OK** to confirm.

Add DiBos System dialog box**Network address**

Type the DNS name or the IP address of your DiBos system.



User name:

Type the user name for logging on to the DiBos system.

Password:




Type the password for logging on to the DiBos system.

8.3.2 Settings page

Main window >  **Devices** > Expand  >  > **Settings** tab



Displays the network settings of the DiBos system connected to your system. Allows you to change the settings if required.

8.3.3 Cameras page

Main window >  **Devices** > Expand  >  > **Cameras** tab




Displays all cameras available on the DiBos system connected to your system. Allows you to remove cameras.

8.3.4 Inputs page

Main window >  **Devices** > Expand  >  > **Inputs** tab

Displays all inputs available on the DiBos system connected to your system. Allows you to remove items.

8.3.5 Relays page

Main window >  **Devices** > Expand  >  > **Relays** tab

Displays all relays available on the DiBos system connected to your system. Allows you to remove items.

8.4 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.




Notice!


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.


Refer to

- *Configuring the integration of a DVR, page 39*

8.4.1**Adding a DVR device via scan****To add DVR devices via scan:**




1. Right-click  and click **Scan for DVR Devices**.
The **BVMS 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 the Device Tree.

8.4.2**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 **Secure connection** check box is selected by default.

If a secure connection is not possible, a message appears. Click to remove the checkmark.

**Notice!**

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

Refer to

- *Adding a device, page 34*

8.4.3 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.

8.4.4 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.

8.4.5 Inputs tab

Main window > **Devices** >  >  > **Inputs** tab

Displays all inputs of the DVR.

Allows you to remove items.

8.4.6 Relays tab

Main window > **Devices** >  >  > **Relays** tab

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

8.4.7 Configuring the integration of a DVR

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



Notice!

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 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.

Refer to

- Adding a device, page 34
- DVR (Digital Video Recorder) page, page 37

8.5 Workstation page



A workstation must have the Operator Client software installed.

Allows you to configure the following settings for a workstation:

- Add a CCTV keyboard connected to a Bosch Video Management System workstation.

Note: You can not configure a CCTV keyboard for a default workstation. This is only possible for specific configured workstations.


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

Refer to

- Adding a workstation manually, page 40

8.5.1 Adding a workstation manually

To add a BVMS workstation:

1. Right-click 
2. Click **Add Workstation**.
The **Add Workstation** dialog box is displayed.
3. Enter the appropriate value.
4. Click **OK**.

The workstation  is added to your system.

To add a BVMS default workstation:

- ▶ Right-click 
- Click **Add Default Workstation**.

The workstation  is added to your system.



Notice!

You can only add one single default workstation.

If a default workstation is configured, the settings apply for each workstation that is connected to this server and is not configured separately.

If a workstation is configured, the settings for this specific workstation apply and not the default workstation settings.

8.5.2 Settings page



Main window > **Devices** > Expand > **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).

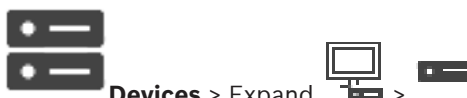
Parity:

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.

8.6 Decoders page



Main window > **Devices** > Expand >

Allows you to add and configure decoders.



Notice!

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

Refer to

- *Scanning for devices, page 25*
- *Bosch Encoder / Decoder / Camera page, page 60*








8.6.1**Adding an Encoder / Decoder manually**

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).

Notice:

If you add a Video IP encoder or decoder from Bosch with the **<Auto Detect>** selection, this device must be available in the network.

To add a Video IP device from Bosch:

- Expand  , expand  , right-click  .
Or
Right-click  .
Or
Right-click  .
- Click **Add Encoder**.
The **Add Encoder** dialog box is displayed.
- Enter the appropriate IP address.
- In the list, select **<Auto Detect>**.
- Click **OK**.
The device is added to the system.
- If the device requires an initial password,  is displayed.
To set an initial password, right-click the device icon and click **Set initial password....**
The **Enter password** dialog box is displayed.
Enter a password for the service user and click **OK**.
The  disappears and you can use the device.

Add Encoder dialog box

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  > Right-click  > Click **Add Decoder** > **Add Encoder** dialog box

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.

8.6.2 Edit Encoder / Edit Decoder dialog box

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 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.

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.

Security

The **Secure connection** check box is selected by default.

If a secure connection is not possible, a message appears. Click to remove the checkmark.

The following decoders support secure connection:

- VID 7000
- VID 8000
- VIP XD HD



Notice!

The connection between a decoder and an encoder is only secure, if both are configured with secure connection.

Device Capabilities

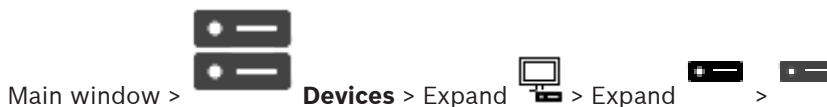
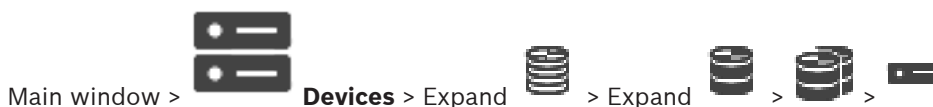
You can sort the displayed device capabilities per category or alphabetically. A message text informs you whether the detected device capabilities match the current device capabilities. Click **OK** to apply the changes of the device capabilities after an upgrade of the device.

Refer to

- *Encrypting live video (Edit Encoder), page 61*
- *Updating the device capabilities (Edit Encoder), page 62*

8.6.3

Changing the password of an encoder / decoder (Change password / Enter password)



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.

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.

Refer to

- *Providing the destination password for a decoder (Authenticate...), page 55*


8.6.4

Decoder profile

Allows you to set the various options for the display of video images on a 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.



Notice!

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.

8.6.5

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.

8.6.6**Delete decoder logo**

Click to delete the logo that has been configured on the Web page of the decoder.

8.7**Monitor Wall page**

Main window >  **Devices** > 

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.

Refer to

– *Sequence Builder dialog box, page 74*




8.7.1**Adding a Monitor Wall manually**

Main window >  **Devices** > Expand  > Right-click  > Click **Add monitor wall**.

Add the required decoder to your BVMS before you add the 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 **OK**.
4. Click  .
5. Click  **Maps and Structure**.
6. Click  **Structure**
7. Drag the monitor wall to the Logical Tree.
8. If required, configure the access to the monitor wall with corresponding user group permissions.

Add monitor wall dialog box

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.

8.8 Assign Keyboard page



Allows you to add a KBD-Universal XF keyboard (connected to a BVMS workstation) or a Bosch IntuiKey keyboard (connected to a BVMS workstation or to a decoder).

To add a CCTV keyboard:

Note: For adding a keyboard you must have added a workstation.

1. Expand  , click  .
The corresponding page is displayed.
2. Click **Add Keyboard**.
A row is added to the table.

3. In the appropriate field of the **Keyboard Type** column, select the desired keyboard type:
 - IntuiKey Keyboard**
 - KBD-Universal XF Keyboard**
4. In the appropriate field of the **Connection** column, select the workstation that is connected with the keyboard.
5. Make the appropriate settings.
The keyboard is added to your system.

Add Keyboard

Click to add a row to the table for configuring a keyboard.

Delete Keyboard

Click to remove the selected row.

Keyboard Type



Displays the type of the keyboard that is connected to your workstation or decoder.

Click a cell to select the required keyboard type.

- **IntuiKey**
Select this type if you have attached an IntuiKey keyboard from Bosch.
- **KBD-Universal XF Keyboard**
Select this type if you have attached a KBD-Universal XF keyboard.

Connection

In a cell, select the device your keyboard is connected to. If you select a workstation, the

keyboard is also added to the  >  page.

Port

In a cell, select the desired COM port.

Baudrate

In a cell, 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.

8.9 VRM Devices page

Refer to

- *Configuring multicast, page 70*

8.9.1 Adding VRM Devices via scan

Main window >  **Devices** > 

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




Notice!



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.

To add VRM devices via scan:

1. Right-click  and click **Scan for VRM Devices**.
The **BVMS 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. In the **Role** list, select the desired role.
It depends on the current type of the VRM device which new role you can select.
5. Click **Next >>**
6. In the **Master VRM** list, select the Master VRM for the selected Mirrored or Failover VRM.
7. Click **Next >>**.
The **Authenticate Devices** dialog box of the wizard is displayed.
8. 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

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

Note: All VRM devices are added with secure connection by default.

To change secure/unsecure connection:

1. Right-click  .
2. Click **Edit VRM Device**.
The **Edit VRM Device** dialog box is displayed.
3. Select the **Secure connection** check box.
The used port changes automatically to the HTTPS port.
Or
deselect the **Secure connection** check box.
The used port changes automatically to the rcpp port.

Refer to

- *Adding a device*, page 34
- *VRM Devices page*, page 48

8.9.2 Adding a primary or secondary VRM manually



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.

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.

You can add a Secondary VRM device manually if you know the IP address and password.



Notice!

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

To add a Secondary VRM device:

1. Make the required settings for your VRM device.
2. In the **Type** list, select the **Secondary** entry.
3. Click **OK**.

The VRM device is added.

You can now configure the Secondary VRM like any Primary VRM.

Add VRM dialog box

Name

Type in a display name for the device.

Network address / port

Type in the IP address of your device.

If the **Secure connection** check box is selected, the port changes automatically to HTTPS port.

You can change the port number, if no default ports are used.

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.

Security

The **Secure connection** check box is selected by default, if HTTPS is supported.

**Notice!**

If you migrate to BVMS version 10.0 and higher, the **Secure connection** check box is not selected by default and the connection is unsecure (rcpp).

To change secure or unsecure connection, use the **Edit VRM Device** command and select or deselect the **Secure connection** check box.

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.

Refer to

- *Editing a VRM device, page 51*

8.9.3**Editing a VRM device**

Main window > **Devices**

Allows you to edit a VRM device.

To change secure/unsecure connection:

1. Right-click .
2. Click **Edit VRM Device**.
The **Edit VRM Device** dialog box is displayed.
3. Select the **Secure connection** check box.
The used port changes automatically to the HTTPS port.
Or
deselect the **Secure connection** check box.
The used port changes automatically to the rcpp port.

**Notice!**

After upgrading to a newer version, we recommend changing to secure connection.

For detailed information about the parameter of the **Edit VRM Device** dialog box, see chapter Adding a primary or secondary VRM manually.

Refer to

- *Adding a primary or secondary VRM manually, page 50*

8.9.4**Encrypting recording for VRM**

Encrypted recording for VRM encoders is not enabled by default.

You have to enable encrypted recording for the primary and secondary VRM separately.

**Notice!**

You have to create a redundancy key (backup certificate) before you enable encrypted recording for the first time. You only have to create a redundancy key once for each VRM device.

In any case of loss of the regular encryption key, you can decrypt the recordings with the redundancy key.


We recommend to keep a copy of the redundancy key at a secure place (for example in a safe).

To create a redundancy key:

1. Select the appropriate VRM device.
2. Select the **Service** tab.
3. Select the **Recording encryption** tab.
4. Click **Redundancy key**.
5. Choose a certification store location.
6. Type in a password that meets the password complexity requirements, and confirm.
7. Click **Create**.

The redundancy key (backup certificate) is created.

To enable/disable encrypted recording:

1. Select the appropriate VRM device.
2. Select the **Service** tab.
3. Select the **Recording encryption** tab.
4. Select/deselect the **Enable encrypted recording** check box.
5. Click  .

Note: Encryption is only enabled after the next block change. This may take a while. Please check to ensure that the encoders are encrypting.

To check the VRM encoders that are encrypting:

1. Select the appropriate VRM device.
2. Select the **Service** tab.
3. Select the **Recording encryption** tab.

Note: You can also refer to the **Monitoring** tab in the VRM Monitor.


**Notice!**

All VRM encoders, that support encryption, are automatically encrypting recording after encryption is enabled in the VRM.

Encryption can be disabled for a single encoder.


VSG encoders are always encrypting, if encryption is enabled in the VRM.


To enable/disable encrypted recording for a single VRM encoder:


1. Select the appropriate VRM encoder.
2. Select the **Recording** tab.
3. Select the **Recording management** tab.
4. Select/deselect the **Encryption** check box.
5. Click  .

8.9.5 Adding VSG devices via scan

To add VSG devices via scan:

1. Right-click  and click **Scan for Video Streaming Gateways**.
The **BVMS 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 the Device Tree.

8.10 Bosch Encoder / Decoder page

To configure a Bosch Encoder / Decoder, see *Bosch Encoder / Decoder / Camera page, page 60*.

8.11 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.


To add, edit, and configure a live only ONVIF encoder, see ONVIF page.

Refer to

- *Adding a live only encoder, page 61*
- *Scanning for devices, page 25*
- *Bosch Encoder / Decoder / Camera page, page 60*
- *Configuring multicast, page 70*

8.11.1 Adding live only devices via scan

To add Bosch live only devices via scan:

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

- 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.

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

8.11.2 Adding an Encoder / Decoder manually

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).


Notice:

If you add a Video IP encoder or decoder from Bosch with the **<Auto Detect>** selection, this device must be available in the network.

To add a Video IP device from Bosch:

- Expand , expand , right-click .


Or


Right-click .

Or

Right-click .

- Click **Add Encoder**.
The **Add Encoder** dialog box is displayed.
- Enter the appropriate IP address.
- In the list, select **<Auto Detect>**.
- Click **OK**.
The device is added to the system.

- If the device requires an initial password,  is displayed.
To set an initial password, right-click the device icon and click **Set initial password...**
The **Enter password** dialog box is displayed.
Enter a password for the service user and click **OK**.

The  disappears and you can use the device.

Add Encoder dialog box

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  > Right-click  > Click **Add Decoder** > **Add Encoder** dialog box

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.

8.11.3 Providing the destination password for a decoder (Authenticate...)

Main window >  **Devices** > Expand  > Expand  > Right-click  > Click **Authenticate...** > **Enter password** 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:

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


Refer to


- *Changing the password of an encoder / decoder (Change password / Enter password), page 44*


8.12 Local Storage page

Main window >  **Devices** > Expand  > 
 Allows you to add and configure encoders with local storage.

To add local storage encoders via scan:

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

Refer to

- *Configuring multicast, page 70*
- *Adding a local storage encoder, page 61*
- *Bosch Encoder / Decoder / Camera page, page 60*
- *Scanning for devices, page 25*

8.13 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.


Refer to

- *Unmanaged site, page 13*
- *Adding an unmanaged site manually, page 57*
- *Importing unmanaged sites, page 57*
- *Configuring the time zone, page 59*

8.13.1 Adding an unmanaged site manually



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.

Refer to


- *Unmanaged site, page 13*
- *Unmanaged Site page, page 56*

8.13.2 Importing unmanaged sites



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.

8.13.3 Unmanaged Site page

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.

8.13.4**Adding an unmanaged network device**

Main window >  **Devices** >  > 

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.

Add Unmanaged Network Device dialog box

Main window >  **Devices** > Expand  > Right click  > Click **Add Unmanaged Network Device**

Device type:

Select the entry that is applicable for this device.

Available entries:

- **DIVAR AN / DVR**
- **DIVAR IP 3000/7000 / BVMS**
- **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 secure. Video data streaming is not secure.

User name:

Type the valid user name for this network device if available. See *Unmanaged site, page 13* for details.

Password:

Type the valid password if available. See *Unmanaged site, page 13* for details on user credentials.

Refer to

- *Unmanaged site, page 13*

8.13.5**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.

Refer to

- *Unmanaged Site page, page 56*

9 Bosch Encoder / Decoder / Camera page

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

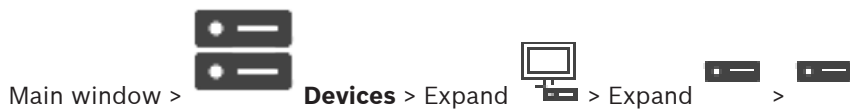
To get detailed information on the encoder, decoder or camera settings, for example Video Content Analysis (VCA) or network settings, refer to the appropriate device manuals.


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

To configure an encoder:






To configure a decoder:





See the Online Help for the  pages for details.

To configure a camera:



- Click  to save the settings.
- Click  to undo the last setting.
- Click  to activate the configuration.

Most of the settings on the encoder / decoder / camera 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.

Refer to

- *Scanning for devices, page 25*

9.1 Adding a live only encoder

To add a live only encoder via scan, see *Adding live only devices via scan, page 53.*

Refer to

- *Adding a device, page 34*
- *Live Only page, page 53*

9.2 Adding a local storage encoder

To add local storage encoders via scan, see *Local Storage page, page 56.*

Refer to

- *Adding a device, page 34*
- *Local Storage page, page 56*

9.3 Editing an Encoder

9.3.1 Encrypting live video (Edit Encoder)



You can activate the secure connection 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, ANR does not work for the affected device.

When activated, encoder replay does not work on encoders with firmware earlier than 6.30. Only encoder with firmware version 7.0 or later support secure UDP. When secure connection is activated in this case, the user of Operator Client can switch a stream to UDP and to UDP multicast.

To activate:




1. Select the check box **Secure connection**.
2. Click **OK**.
Secure connection is enabled for this encoder.




Refer to

- *Configuring multicast, page 70*
- *Edit Encoder / Edit Decoder dialog box, page 63*

9.3.2

Updating the device capabilities (Edit Encoder)

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 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.




Refer to

– *Edit Encoder / Edit Decoder dialog box, page 63*

9.3.3

Edit Encoder / Edit Decoder dialog box


 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 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.

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.

Security

The **Secure connection** check box is selected by default.

If a secure connection is not possible, a message appears. Click to remove the checkmark.

The following decoders support secure connection:

- VID 7000
- VID 8000
- VIP XD HD



Notice!

The connection between a decoder and an encoder is only secure, if both are configured with secure connection.

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.

Refer to

- *Encrypting live video (Edit Encoder), page 61*
- *Updating the device capabilities (Edit Encoder), page 62*





9.4 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.

9.4.1 Configuring the authentication

or

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

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  .


9.4.2 Uploading a certificate

or

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

You can upload a derived certificate to an encoder.

To upload:

1. Click **Service**, and then click **Certificates**.
2. Click **Upload certificate**.
3. Select the appropriate file containing the certificate for this encoder. This file must contain the private key, for example *.pem.
Ensure a secure data transmission.
4. Click **Open**.
5. In the **Usage** list, select **HTTPS server** to assign the uploaded certificate to the **HTTPS server** entry.
6. Click  .

9.4.3 Downloading a certificate

or



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.
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.

9.4.4 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*.

9.5 Providing the destination password for a decoder (Authenticate...)



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.

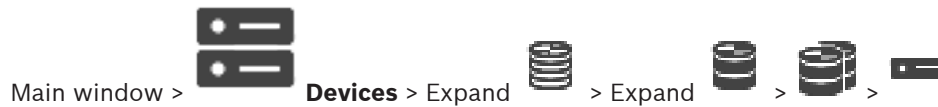
To provide:

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.

Refer to


- *Changing the password of an encoder / decoder (Change password / Enter password), page 66*

9.6 Changing the password of an encoder / decoder (Change password / Enter password)



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.

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.

Refer to

– *Providing the destination password for a decoder (Authenticate...), page 65*

9.7

Recovering recordings from a replaced encoder (Associate with recordings of predecessor)



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.

Associate with recordings of predecessor ... dialog box

Allows you to recover recordings from a replaced encoder. After configuring the settings in the dialog box, the recordings of the replaced encoder are available for the new encoder when selecting the new encoder in the Operator Client .

Network address / port

Type the network address of the device.

User name

Displays the user name used for authenticating at the device.

Password

Type the valid password for authenticating at the device.

Authenticate

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

9.8

Configuring encoders / decoders

9.8.1

Configuring multiple encoders / decoders

Main window

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

- Device passwords
- IP addresses
- Display names
- Subnet mask
- Gateway ID
- Firmware versions



To select multiple devices:

- ▶ Select the required devices by pressing the CTRL- or the SHIFT-key.

To select all available devices:

- ▶ Click the  **Select all** command.

To change the password for multiple devices:

1. On the Main window  **Devices** click the  **Change device passwords** command.
Or
on the **Hardware** menu, click **Change device passwords...**
The **Change device passwords** dialog box is displayed.
2. Select the required devices.
3. Right-click the selected devices.
4. Click **Edit password...** The **Changing passwords** dialog box is displayed.
5. Make the appropriate settings.



Notice!

You can only select the password types that are available for all selected devices.

To configure multiple display names:

1. On the **Hardware** menu, click **Change device IP and network settings...**
The **Change device IP and network settings** dialog box is displayed.
2. Select the required devices.
3. Right-click the selected devices.
4. Click **Set Display Names...**
The **Set Display Names** dialog box is displayed.
5. Make the appropriate settings.

To configure multiple IP addresses:



Notice!

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

1. On the **Hardware** menu, click **Change device IP and network settings....**
The **Change device IP and network settings** dialog box is displayed.
2. Select the required devices.
3. Right-click the selected devices.
4. Click **Set IP addresses....**
The **Set IP Addresses** dialog box is displayed.
5. Make the appropriate settings.

To change subnet mask / gateway ID for multiple devices:

1. Click in the required field of one of the devices you want to change the value.
2. Type the appropriate value.
3. Select all required devices.
4. Right-click the required field of the device you already changed the value.
5. Click the **Copy Cell to** command and the **Selection in Column** command.
Or click the **Complete Column** command, if required.



Notice!

You can also copy complete rows to change IP addresses, display names, subnet masks and gateway IDs for multiple devices.

To update firmware for multiple devices:

1. On the **Hardware** menu, click **Update device firmware... .**
The **Update device firmware** dialog box is displayed.
2. Select the required devices.
3. Click the **Update Firmware** command.
4. Select the file containing the update.
5. Click **OK**.


Operation Result

Displays the appropriate state for the affected devices.

9.8.2

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.

9.8.3**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.

9.9**Configuring multicast**

For each assigned camera you can configure a multicast address with port.

To configure multicast:

1. Select the desired check box to enable multicast.
2. Type a valid multicast address and a port number.
3. If required, configure continuous multicast streaming.





Multicast tab

Main window >  > **Devices** >  > 

or

Main window >  > **Devices** >  > 

or

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

> **Network** tab > **Multicast** tab

Allows you to configure multicast for the assigned cameras.

Enable

Click to enable multicast for this camera.

Multicast Address

Insert a valid multicast address (in the range 224.0.0.0 - 239.255.255.255).

Enter *1.0.0.0*. A unique multicast address is automatically inserted based on the MAC address of the device.

Port

When a firewall is used, enter a port value that is configured as non-blocked port in the firewall.

Streaming

Click to enable continuous multicast streaming to the switch. This means that the multicast connection is not preceded by a RCP+ registration. The encoder streams always all data to the switch. The switch in return (if no IGMP multicast filtering is supported or configured) sends this data to all ports, with the result that the switch will flood.

You need streaming when using a non-Bosch device for receiving a multicast stream.

**Notice!**

Multicast streams are only secure, if the encoder has firmware version 7.0 or later and the **Secure connection** check box is selected.

Refer to

- *Encrypting live video (Edit Encoder), page 61*

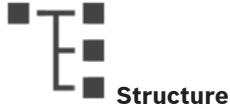
10 Maps and Structure page



Notice!

BVMS Viewer offers only basic features. Advanced features are included in BVMS Professional. Visit our website www.boschsecurity.com for more information.

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



Main window >

Permissions can get lost. If you move a group of devices, these devices lose 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

Resource files can be:

- Camera sequence files

Icons

	Displays a dialog box for adding or editing a camera sequence file.
	Creates a folder in the Logical Tree.

Symbols

	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 .




11 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 lose their permission settings. You must set the permissions in the **User groups** page again.

- Click  to save the settings.
- Click  to undo the last setting.
- Click  to activate the configuration.

Refer to

- *Sequence Builder dialog box, page 74*
- *Add Sequence dialog box, page 76*
- *Add Sequence Step dialog box, page 76*

11.1 Configuring the Logical Tree

Refer to

- *Maps and Structure page, page 72*

11.2 Adding a device to the Logical Tree



Main window > **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.

Refer to

- *Maps and Structure page, page 72*

11.3 Removing a tree item



Main window > **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.

Refer to

- *Maps and Structure page, page 72*

11.4 Adding a camera sequence



Main window > **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.

Refer to

– *Sequence Builder dialog box, page 74*




11.4.1 Sequence Builder dialog box



Main window > **Structure** > 

Allows you to manage camera sequences.

Icons

	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.

Refer to

- *Monitor Wall page, page 46*
- *Managing pre-configured camera sequences, page 75*

11.5

Managing pre-configured camera sequences



Main window > **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.

- Click **OK**.

A new camera sequence  is added.

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


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

- Select the desired camera sequence.
- Click **Add Step**.
The **Add Sequence Step** dialog box is displayed.
- Make the appropriate settings.
- 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:

- Select the desired camera sequence.
- Click . The selected camera sequence is removed.

Refer to

- *Sequence Builder dialog box, page 74*

11.5.1

Add Sequence dialog box

Main window >  **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.

11.5.2

Add Sequence Step dialog box

Main window >  **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.

11.6 Adding a folder



Main window > **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.

Refer to

– *Maps and Structure page, page 72*

11.7 Configuring bypass of devices



Main window > **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 / unbyypass 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 / unbyypass a device on a map:

See Managing devices on a map



Notice!

It is possible to filter bypassed devices in the search text field.

12

Cameras and Recording page

**Notice!**

BVMS Viewer offers only basic features. Advanced features are included in BVMS Professional. Visit our website www.boschsecurity.com for more information.



Main window > **Cameras**

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.

Icons

	Click to display the dialog box for configuring a selected PTZ camera.
--	--



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 .

12.1

Cameras page



Main window > **Cameras** > 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 - 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.



Select a check box to activate PTZ control.

Note:

For port settings refer to COM1.

Port

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

Click a cell to select the appropriate protocol for the PTZ control.

PTZ Address

Type the address number for the PTZ control.

Refer to

- *Configuring predefined positions and auxiliary commands, page 80*
- *Configuring PTZ port settings, page 80*

13 Configuring cameras and recording settings






Notice!

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



Main window > **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  to save the settings.
- Click  to undo the last setting.
- Click  to activate the configuration.

Refer to

- *Cameras page, page 78*
- *Predefined positions and AUX commands dialog box, page 82*

13.1 Configuring PTZ port settings



Main window > **Devices** > **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.

13.2 Configuring predefined positions and auxiliary commands



Main window > **Cameras** >

You can predefine and save camera positions for PTZ, ROI and panoramic cameras. For PTZ cameras you can also define auxiliary commands.

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.

To configure a predefined position:

1. In the **Cameras** table, select the required encoder.

- Only for PTZ cameras: to activate the control of a PTZ camera, select the check box in the





column.

- Click the  button.

The **PTZ Settings** dialog box is displayed.

- You can define the number of predefined positions that you want to use.
- Select the position you want to define.
- In the preview window, use the mouse control to navigate to the position you want to configure.
Scroll to zoom in and out and drag to move the image section.
- If required, type a name for the configured position.

- Click  to save the predefined position.

Note: Click  for each defined position. Otherwise the position is not saved.

- Click **OK**.

To display already configured predefined positions:

- In the **Cameras** table, select the required encoder.

- Click the  button.

The **PTZ Settings** dialog box is displayed.

- Select the appropriate position.

- Click .

The predefined camera position is displayed in the preview window.


Note:

Predefined positions for PTZ and ROI cameras are stored on the camera directly. Predefined positions for panoramic cameras are stored in BVMS.


PTZ cameras move physically to the predefined position. Panoramic and ROI cameras only display an image section of the complete camera view.

To configure auxiliary commands for PTZ cameras:

- In the **Cameras** table, select the required encoder.

- Click the  button.
The **PTZ Settings** dialog box is displayed.

- Select the **Aux Commands** tab.
- Make the appropriate settings.

- Click  to save the predefined commands.

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

Refer to

- *Predefined positions and AUX commands dialog box, page 82*
- *Configuring PTZ port settings, page 80*

13.3 Predefined positions and AUX commands dialog box





Allows you to configure a PTZ, ROI or panoramic camera.

For ROI and panoramic cameras 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.

Icons

	Click to move the camera to the predefined position or to execute the command.
	Click to save 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.

Note: If an ONVIF encoder supports auxiliary commands, the auxiliary commands are provided from the ONVIF encoder directly.

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.

Refer to

- *Configuring PTZ port settings, page 80*
- *Configuring predefined positions and auxiliary commands, page 80*

14 User Groups page



Notice!

BVMS Viewer offers only basic features. Advanced features are included in BVMS Professional. Visit our website www.boschsecurity.com for more information.



Main window > **User groups**

Allows you to configure user groups.

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.

User/user group options

Icon	Description
	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.
	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.

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.



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 .

14.1 User Group Properties page



Main window > > **User groups** > **User Groups** tab > > **Operating Permissions** tab > **User Group Properties** tab

Allows you to configure the following settings for the selected user group:

- Logon schedule
- Association of an LDAP user group

User group properties**Description:**

Type an informative description for the user group.

Language

Select the language of the Operator Client.

LDAP Properties**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.

Change order...

Click to display the **Change LDAP user group order** list. The list shows the LDAP user groups with their associated BVMS user groups and Enterprise User Groups. By drag and drop or using the up and down arrow buttons you can change the order of the groups.



Notice!

A LDAP user can be associated with more than one LDAP user group, which in turn are associated with a particular BVMS user group. The LDAP user gets the permissions of the BVMS user group that is ordered above the other LDAP user groups, that are associated with this LDAP user.

Refer to

- *Configuring LDAP settings, page 97*
- *Associating an LDAP group, page 97*

14.2

User Properties page



Main window > **User groups** > **User Groups** tab

Allows you to configure a new user in a standard user group.

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.

14.3 Logon Pair Properties page

Main window >  **User groups > User Groups tab >  **New dual authorization group > ****

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.

Refer to

- *Adding a logon pair to dual authorization group, page 95*

14.4 Camera Permissions page

Main window >  **User groups > User Groups tab >  > **Device Permissions tab > **Camera Permissions tab******

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.

Text Data

Select a check box to allow displaying metadata.

You can select or clear this check box only when the display of metadata 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.

Reference Image

Select a check box to allow updating the reference image of this camera.

14.5**LDAP Server Settings dialog box**

Main window > **User groups** > **User Groups** 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 HTTP: 389, HTTPS: 636)

Secure connection

Select the check box to activate secure data transmission.

Authentication mechanism

Negotiate selects the appropriate authentication protocol automatically.

Simple transmits the logon credentials unencrypted as clear text.

Anonymous

Use to log on as a guest. Select this option if the LDAP server supports it and you are not able to configure a specific proxy user.

Use following credentials**User name**

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.

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.

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.

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.

Refer to

– *Configuring LDAP settings, page 97*

14.6 Logical Tree page



Main window > **User groups** > **User Groups** tab >  > **Device Permissions** tab > **Logical Tree** tab

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.

Monitor Group


Select the check box to give the users of the selected user group access to this monitor group.

Refer to

- *Configuring device permissions, page 98*

14.7 Operator Features page



Main window > **User groups** > **User Groups** tab >  > **Operating Permissions** tab > **Operator Features** tab

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 to non-native formats

Select the check box to allow exporting video data to non-native 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.

Restrict video

Select the check box to allow restricting video data.

Unrestrict video

Select the check box to allow both restricting and unrestricting video data.

Delete video

Select the check box to allow deleting video data.

Erase text data from logbook entries (for erasing person-related data)

Select the check box to allow erasing text data from logbook entries.

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.

Manual alarm recording

Select the check box to allow manual alarm recording.

Set reference image

Select the check box to allow updating the reference image in the Operator Client.

Set area selection for reference image

Select the check box to allow selecting the area in the camera image for updating the reference image in the Operator Client.

Change password

Select the check box to allow a user of Operator Client to change the password for logging on.

Operate access doors

Select the check box to allow a user of Operator Client to change the access door state (secure, lock, unlock).

Person management

Select the check box to allow a user of Operator Client to manage persons for person identification alarms.

14.8**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 remaining monitors you can select one of the following entries:
 - **Live video only**
 - **Fullscreen live video**

- **Quad live image**

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**
- **Live video only**

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.

14.9**Account policies page**

Main window >

User groups > **User Groups** 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 93*

**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 number of characters.

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 maximum number of days.

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 number of passwords.

Maximum invalid logon attempts

This setting determines the disabling of an account after a specific number of invalid logon attempts.

Select the check box to enable the setting and enter the maximum number of attempts.

If the **Maximum invalid logon attempts** check box is selected, you can specify the following two settings:

Account lockout duration

This setting determines the number of minutes that a disabled account remains disabled before automatically becoming enabled.

Select the check box to enable the setting and enter the number of minutes.

Reset account lockout counter after

This setting determines the number of minutes that must elapse from the time a user fails to log on before the failed logon attempt counter is reset to zero.

Select the check box to enable the setting and enter the number of minutes.



Notice!

If the maximum number of invalid logon attempts exceeds, the account is disabled.

If the **Account lockout duration** check box is not selected, the account has to be enabled manually.

If the **Account lockout duration** check box is selected, the account automatically becomes enabled after the defined time period.



Notice!

The counter of invalid logon attempts resets to zero:

After a successful login.

Or after the specified duration, if the **Reset account lockout counter after** check box is selected.

Disable offline client

Select the check box to disable logon to an offline client.

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.

From BVMS 10.0.1 on the following **Account policies** settings are selected by default for all user groups:

- **Maximum invalid logon attempts**
- **Account lockout duration**
- **Reset account lockout counter after**

15

Configuring users, permissions and Enterprise Access

**Notice!**

BVMS Viewer offers only basic features. Advanced features are included in BVMS Professional. Visit our website www.boschsecurity.com for more information.






Main window > **User groups**

This chapter provides information on how to configure user groups.

You configure all device permissions and operating permissions per user group and not per user.

The following rules apply:

- A user can only be the member of one 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.
- Click  to save the settings.
- Click  to undo the last setting.
- Click  to activate the configuration.

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.
- Do not use one of the previous passwords.
- Use at least one upper-case letter (A through Z).
- Use at least one number (0 through 9).
- Use at least one special character (for instance: ! \$ # %).

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.

Refer to

- *Account policies page, page 91*
- *User Group Properties page, page 84*
- *User Properties page, page 85*
- *Logon Pair Properties page, page 86*
- *Camera Permissions page, page 86*
- *LDAP Server Settings dialog box, page 87*
- *Logical Tree page, page 89*
- *Operator Features page, page 89*
- *User Interface page, page 90*

15.1 Creating a group or account



Main window > **User groups**

You can create a standard user group.


For adapting the user group permissions to your requirements, create a new user group and change its settings.

15.1.1 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.

Refer to

- *User Group Properties page, page 84*
- *Operator Features page, page 89*
- *User Interface page, page 90*

15.2 Creating a user





Main window > **User groups > User Groups** tab

You create a user as a new member of an existing standard 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.

Refer to

- *User Properties page, page 85*
- *Strong password policy , page 93*
- *User Groups page, page 83*

15.3

Creating a dual authorization group




Main window > **User groups > User Groups** tab

You can create a dual authorization for a standard user group.

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

To create a dual authorization group:

1. Click .
The **New 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.

Refer to

- *Adding a logon pair to dual authorization group, page 95*
- *User Group Properties page, page 84*
- *Operator Features page, page 89*
- *User Interface page, page 90*


15.4

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


Refer to


- *Creating a dual authorization group, page 95*
- *Logon Pair Properties page, page 86*

15.5**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 **Add 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.

Refer to

- *User Groups page, page 83*
- *User Properties page, page 85*
- *Strong password policy, page 93*

15.6 Configuring LDAP settings



Main window >
tab

User groups > User Groups tab >



> Operating Permissions



Notice!

Type the search paths accurately. Wrong paths can make the search on an LDAP server very slow.



Notice!

A LDAP user can be associated with more than one LDAP user group, which in turn are associated with a particular BVMS user group. The LDAP user gets the permissions of the BVMS user group that is ordered above the other LDAP user groups, that are associated with this LDAP user.

You configure LDAP groups in standard 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, follow the link to the appropriate application window below.

Refer to

- *LDAP Server Settings dialog box, page 87*
- *User Group Properties page, page 84*

15.7 Associating an LDAP group



Main window >
tab

User groups > User Groups tab >



> Operating Permissions

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.

**Notice!**

If an LDAP group is associated with a BVMS user group, users of this LDAP group can start the Operator Client using Single Sign-on.

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.

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

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

Refer to

- *LDAP Server Settings dialog box, page 87*
- *User Group Properties page, page 84*

15.8**Configuring operating permissions**

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

- 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.

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

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

Refer to

- *User Group Properties page, page 84*
- *Operator Features page, page 89*
- *User Interface page, page 90*

15.9**Configuring device permissions**

Main window > **User groups** > **User Groups** tab > **Device Permissions** tab

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

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.

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

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

Refer to

- *Logical Tree page, page 89*
- *Camera Permissions page, page 86*

Glossary

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.

Allegiant

Bosch family of analog matrix switching systems.

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: $(\text{network bandwidth} \times \text{estimated network downtime} + \text{safety margin}) \times (1 + 1/\text{backup speed})$. The resulting recording capacity is required because the continuous recording must continue during the copy process.

ATM

Automatic Teller Machine

Bosch ATM/POS Bridge

Receives string via serial cable / COM interface and forwards these strings via Ethernet cable (TCP/IP). The strings are usually POS data or transactions from ATMs.

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.

decoder

Changes a digital stream to an analog stream.

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).

DNS

Domain Name System. A DNS server converts a URL (www.myDevice.com, for example) into an IP address on networks that use the TCP/IP protocol.

DTP

A DTP device (Data Transform Processor) transforms serial data of ATM devices to a defined data format and sends these data via Ethernet to BVMS. You must ensure that a transformation filter is set on the DTP device. This task is performed with a separate software from the manufacturer of the DTP device.

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.

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 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.

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

Feature of Operator Client. Used for live view of video.

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).

monitor group

A set of monitors connected to decoders. The 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 monitor group are logically configured into rows and columns and can be set to different layouts, e. g. full-screen or quad view.

Network monitoring

Measurement of network related values and evaluation of these values against configurable thresholds.

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.

Reference image

A reference image is 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 allows you to detect tampering that would otherwise not be detected, for example if the camera is turned.

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.

Secondary VRM

Software in the BVMS environment. Ensures that the recording performed by one or multiple Primary VRMs is additionally and simultaneously performed to another iSCSI target. The recording settings can deviate from the settings of the Primary VRM.

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.

Text data

Data of a POS or ATM like date and time or bank account number stored with the corresponding video data to provide additional information for evaluation.

UDP

User Datagram Protocol. A connectionless 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.

Virtual input

Used for forwarding events from third-party systems to Bosch Video Management System.

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

A		
accessing the Help	7	
activate	26	
previous configuration	27	
activation		
configuration	26	
delayed	26, 30	
add BVIP decoder	42, 54	
add BVIP encoder	42, 43, 54, 63	
add unmanaged site	56, 57, 59	
add VRM	49	
Allegiant		
CCL emulation	34	
PTZ camera	79	
Allegiant matrix	34	
analog monitor group	34	
ASF	89	
aspect ratio 16/9	90	
ATM POS device	34	
automatic logoff	31	
automatic relogin	26	
automatic restart	26	
B		
Bosch IntuiKey keyboard	34, 40, 47	
Bosch Video Management System		
Online Help	7	
BVIP decoder	62	
add	42, 54	
BVIP device		
password	44, 61, 66	
Web page	61	
BVIP encoder	62	
add	42, 54	
BVIP encoder:add	43, 63	
C		
camera round	72, 75, 76	
camera sequence	72, 75, 76	
CCTV keyboard	47	
change IP address	67	
change network address	67	
change password	44, 61, 66, 85	
Command Script	72	
Commercial Type Number	31	
configuration data		
export	27	
D		
data sheet	11	
DCZ keyboard	47	
decoder:destination password	55, 65	
default IP address	30	
default password	26	
delayed activation	26, 30	
delete user	85	
destination password	55, 65	
device capabilities		
update	62	
Device Tree	33, 51, 72	
Devices pane	72	
devices without password protection	26	
DiBos device	34	
digital keyboard	47	
digital video recorder	34	
dome camera	80, 82	
dual authorization	86	
duplicate IP addresses	30	
E		
E-mail device	34	
empty password	26	
Encoder		
Web page	61	
encoding on NVRs	33, 51	
export		
ASF	89	
configuration data	27	
F		
filtering	33, 72, 78, 84	
finding		
devices	33, 72, 78, 84	
information in the Help	7	
Forensic Search	40	
G		
global default password	26	
H		
HD cameras	90	
help	7	
hotspots	72	
HTML files	72	
I		
I/O modules	34	
inactivity	31	
IntuiKey keyboard	47	
IP address		
change	67	
duplicates	30	

K			
KBD Universal XF keyboard		34, 40	
L			
language			
Configuration Client		31	
Operator Client		84	
LDAP group		97	
LDAP user		84	
LDAP user groups		84, 97	
Logical Tree		73	
M			
Management Server		11	
maps		72	
menu commands		29	
multi monitor mode		90	
multi-select		73	
N			
network address			
change		67	
network monitoring device		34	
new DiBos devices		38, 39	
no password		26	
NVR		11	
O			
offline		85	
online application Help		7	
Operator Client		73	
P			
panoramic camera			
viewing modes		14	
password		44, 61, 66	
password change		44, 61, 66, 85	
password missing		26	
peripheral device		34	
permissions		72, 73	
previous configuration		27	
Primary VRM		50	
printing the Help		7	
PTZ camera		80, 82	
Allegiant		79	
R			
Recording preferences		70	
Recording Table		78	
Region of Interest		87	
Release Notes		11	
remove prepositions		80	
remove user		85	
ROI		87	
S			
scan			
across subnets		31	
encoders		35	
in subnets		31	
live only encoders		35	
local storage encoders		35	
scan for conflicting IP addresses		30	
Secondary VRM		50	
sequence		76	
Server Network		56, 57, 58, 59	
SMS device		34	
system requirements		11	
T			
time zone		57, 58	
U			
update			
device capabilities		62	
user			
delete		85	
remove		85	
user groups		84	
V			
verify authenticity		64	
Video Streaming Gateway		34	
viewing modes of panoramic camera		14	
virtual input		34	
VRM			
add		49	
Primary		50	
Secondary		50	



Bosch Security Systems B.V.

Torenallee 49
5617 BA Eindhoven
Netherlands

www.boschsecurity.com

© Bosch Security Systems B.V., 2020