BOSCH

BVMS

en Configuration Manual

Table of contents

1	**Using the Help**	**14**
1.1	Finding information	14
1.2	Printing the Help	14
2	**Introduction**	**16**
3	**System overview**	**18**
3.1	Hardware requirements	19
3.2	Software requirements	19
3.3	License requirements	19
4	**Concepts**	**20**
4.1	Recording settings	20
4.1.1	Basic stream settings (schedule-independent)	20
4.1.2	Stream assignment for Live	20
4.1.3	Scheduled Recording Settings	20
4.2	Config Wizard	23
4.3	BVMS design concepts	23
4.3.1	Single Management Server System	24
4.3.2	Enterprise System	25
4.3.3	Server Lookup	26
4.3.4	Unmanaged site	27
4.4	Remote access	28
4.5	Automated Network Replenishment (ANR)	31
4.6	Dual / failover recording	32
4.7	VRM recording modes	33
4.8	Playback of VRM recording sources	36
4.9	Alarm handling	43
4.10	Adding Video IP devices from Bosch	45
4.11	Region of Interest (ROI)	45
4.12	Intelligent Tracking	46
4.13	Inactivity logoff	46
4.14	Malfunction relay	47
4.15	Text data	48
4.16	Offline Operator Client	48
4.16.1	Working with Offline Mode	49
4.17	Version independent Operator Client	51
4.17.1	Working with Compatibility Mode	51
4.18	ONVIF event mapping	52
4.19	Viewing modes of a panoramic camera	53
4.19.1	360° panoramic camera - floor- or ceiling mounted	53
4.19.2	180° panoramic camera - floor- or ceiling mounted	55
4.19.3	360° panoramic camera - wall mounted	56
4.19.4	180° panoramic camera - wall mounted	57
4.19.5	Cropped view on a panoramic camera	58
4.20	Verification of authenticity	59
4.21	SSH Tunneling	60
4.22	Multipathing	60
5	**Supported hardware**	**61**
5.1	Installing hardware	62
5.2	Installing a KBD Universal XF keyboard	62

5.3	Connecting a Bosch IntuiKey keyboard to BVMS	63
5.3.1	Scenarios for Bosch IntuiKey keyboard connections	63
5.3.2	Connecting a Bosch IntuiKey keyboard to a decoder	64
5.3.3	Updating Bosch IntuiKey keyboard firmware	65
5.4	Connecting Bosch Allegiant Matrix to BVMS	66
5.4.1	Bosch Allegiant Connection Overview	66
5.4.2	Configuring the control channel	68
5.4.3	Bosch Allegiant Satellite System Concept	70
5.5	Allegiant CCL commands supported in BVMS	70
6	**Getting started**	**72**
6.1	Installing the software modules	72
6.2	Using Config Wizard	72
6.3	Starting Configuration Client	82
6.4	Configuring the language of Configuration Client	83
6.5	Configuring the language of Operator Client	83
6.6	Scanning for devices	84
6.7	Accessing the system	84
6.8	Using Server Lookup	84
6.9	Configuring remote access	85
6.9.1	Configuring without Enterprise System	85
6.9.2	Configuring with Enterprise System	85
6.10	Activating the software licenses	86
6.10.1	Downloading Bundle Information file	86
6.10.2	Retrieving the computer signature	86
6.10.3	Obtaining the activation key	87
6.10.4	Activating the system	87
6.11	Maintaining BVMS	88
6.12	Replacing a device	89
6.12.1	Replacing a MS / EMS	89
6.12.2	Replacing a VRM	90
6.12.3	Replacing an encoder or decoder	91
6.12.4	Replacing an Operator Client	93
6.12.5	Final tests	94
6.12.6	Recovering Divar IP 3000/7000	94
6.13	Configuring time synchronization	94
6.14	Configuring the storage media of an encoder	94
7	**Creating an Enterprise System**	**96**
7.1	Configuring the Server List for Enterprise System	96
7.2	Creating an Enterprise User Group	97
7.3	Creating an Enterprise Account	98
8	**Configuring Command Scripts**	**100**
8.1	Managing Command Scripts	100
8.2	Configuring a Command Script to be started automatically	101
8.3	Importing a Command Script	101
8.4	Exporting a Command Script	101
8.5	Configuring a startup Command Script (settings page)	102
9	**Managing configuration data**	**103**
9.1	Activating the working configuration	103
9.2	Activating a configuration	104

9.3	Exporting configuration data	104
9.4	Importing configuration data	105
9.5	Exporting configuration data to OPC	105
9.6	Checking the status of your encoders/decoders	106
9.7	Configuring SNMP monitoring	106
9.8	Creating a report	106
10	**Configuration examples**	**108**
10.1	Adding a Bosch ATM/POS bridge	108
10.2	Adding a Bosch Allegiant input alarm	109
10.3	Adding and configuring 2 Dinion IP cameras with VRM recording	109
11	**Global Configuration Client windows**	**111**
11.1	Configuration window	111
11.2	Menu commands	112
11.3	Activation Manager dialog box (System menu)	114
11.4	Activate Configuration dialog box (System menu)	114
11.5	Initial Device Scan dialog box (Hardware menu)	115
11.6	Protect Devices with Global Default Password dialog box (Hardware menu)	115
11.7	Change device passwords dialog box (Hardware menu)	116
11.8	Update device firmware dialog box (Hardware menu)	116
11.9	Change device IP and network settings dialog box (Hardware menu)	117
11.10	Device Monitor dialog box (Hardware menu)	118
11.11	License Investigator dialog box (Tools menu)	119
11.12	License Manager dialog box (Tools menu)	119
11.13	Reports dialog boxes (Reports menu)	120
11.13.1	Recording Schedules dialog box	120
11.13.2	Scheduled Recording Settings dialog box	120
11.13.3	Task Schedules dialog box	120
11.13.4	Cameras and Recording Parameters dialog box	120
11.13.5	Stream Quality Settings dialog box	120
11.13.6	Event Settings dialog box	120
11.13.7	Compound Event Settings dialog box	120
11.13.8	Alarm Settings dialog box	120
11.13.9	Configured Users dialog box	120
11.13.10	User Groups and Accounts dialog box	121
11.13.11	Device Permissions dialog box	121
11.13.12	Operating Permissions dialog box	121
11.14	Alarm Settings dialog box (Settings menu)	121
11.15	SNMP Settings dialog box (Settings menu)	121
11.16	Options dialog box (Settings menu)	122
11.17	Remote Access Settings dialog box (Settings menu)	123
11.17.1	Port Mapping Table dialog box	124
12	**Devices page**	**125**
12.1	Change device passwords dialog box	125
12.2	Adding a device	126
12.3	Server list / Address Book page	129
12.3.1	Add Server dialog box	130
12.3.2	Configuring Server Lookup	130
12.3.3	Configuring the Server List	130
12.3.4	Exporting the Server List	131

12.3.5	Importing a Server List	131
12.4	NVRs / Failover NVRs / Redundant NVRs page	131
12.5	DiBos page	131
12.5.1	Adding a DiBos System via scan	132
12.5.2	Settings page	132
12.5.3	Cameras page	132
12.5.4	Inputs page	133
12.5.5	Relays page	133
12.5.6	Configuring the integration of a DiBos system	133
12.6	DVR (Digital Video Recorder) page	133
12.6.1	DVR devices	134
12.6.2	Adding a DVR device via scan	135
12.6.3	Add DVR dialog box	135
12.6.4	Settings tab	135
12.6.5	Cameras tab	136
12.6.6	Inputs tab	136
12.6.7	Relays tab	136
12.6.8	Configuring the integration of a DVR	136
12.7	Matrix Switches page	137
12.7.1	Adding a Bosch Allegiant device	137
12.7.2	Configuring a Bosch Allegiant device	137
12.7.3	Outputs page	138
12.7.4	Inputs page	138
12.7.5	Connection page	139
12.7.6	Cameras page	139
12.8	Workstation page	139
12.8.1	Adding a workstation manually	140
12.8.2	Configuring a Bosch IntuiKey keyboard (settings page) (workstation)	140
12.8.3	Enabling Forensic Search on a workstation (settings page)	140
12.8.4	Configuring a startup Command Script (settings page)	141
12.8.5	Settings page	141
12.8.6	Changing the network address of a workstation	143
12.9	Decoders page	143
12.9.1	Adding an Encoder / Decoder manually	143
12.9.2	Edit Encoder / Edit Decoder dialog box	144
12.9.3	Changing the password of an encoder / decoder (Change password / Enter password)	146
12.9.4	Decoder profile	147
12.9.5	Monitor display	147
12.9.6	Configuring a Bosch IntuiKey keyboard (decoder)	148
12.9.7	Configuring a decoder for use with a Bosch IntuiKey keyboard	148
12.9.8	Delete decoder logo	148
12.10	Monitor groups page	149
12.10.1	Adding a monitor group manually	149
12.10.2	Configuring a monitor group	149
12.11	Monitor Wall page	150
12.11.1	Adding a Monitor Wall manually	151
12.12	Communication Devices page	152
12.12.1	Adding an E-mail/SMTP Server	152
12.12.2	Adding a SMS Device	152

12.12.3	SMTP Server page	152
12.12.4	Configuring a communication device	153
12.12.5	Send Test E-mail dialog box	154
12.12.6	GSM Settings / SMSC Settings page	154
12.13	ATM/POS page	155
12.13.1	Adding a Bosch ATM/POS-Bridge manually	155
12.13.2	Bosch ATM/POS-Bridge page	156
12.13.3	Configuring a peripheral device	156
12.13.4	DTP Settings page	157
12.13.5	ATM Settings page	157
12.13.6	Inputs page	157
12.14	Foyer Card Readers	158
12.14.1	Add Foyer Card Reader dialog box	158
12.14.2	Settings for Foyer Card Reader page	158
12.15	Virtual Inputs page	159
12.15.1	Adding Virtual Inputs manually	159
12.16	SNMP page	160
12.16.1	Adding an SNMP manually	160
12.16.2	Configuring an SNMP trap receiver (SNMP trap receiver page)	160
12.16.3	SNMP Trap Logger dialog box	161
12.17	Assign Keyboard page	162
12.18	I/O Modules page	163
12.18.1	Adding an I/O module manually	163
12.18.2	Configuring an I/O module	163
12.18.3	ADAM page	164
12.18.4	Inputs page	164
12.18.5	Relays page	164
12.19	Allegiant CCL Emulation page	165
12.19.1	Adding an Allegiant CCL emulation manually	165
12.19.2	Allegiant CCL commands	165
12.19.3	Configuring an Allegiant CCL emulation	166
12.20	Mobile Video Service page	166
12.20.1	Mobile Video Service	166
12.20.2	Adding a Mobile Video Service manually	167
12.21	Intrusion panels page	167
12.21.1	Adding an Intrusion Panel manually	168
12.21.2	Settings page	168
12.22	Video analytics page	168
12.22.1	Video Analytics Settings page	168
12.22.2	Adding a Video Analytics Device	169
12.22.3	Person Identification settings page	169
12.22.4	Adding a Person Identification device (PID)	170
12.22.5	Restoring access to a PID after a BVMS central server breakdown	171
12.22.6	Adding cameras to a Person Identification device (PID)	171
12.22.7	Configuring camera parameters for Person Identification alarms	172
12.22.8	Configuring person groups	172
12.23	Access control systems page	173
12.23.1	Adding an access control system	173
12.23.2	Editing an access control system	174

12.23.3	Settings page	174
12.24	VRM Devices page	174
12.24.1	Adding VRM Devices via scan	175
12.24.2	Adding a primary or secondary VRM manually	176
12.24.3	Editing a VRM device	177
12.24.4	VRM Settings page	178
12.24.5	SNMP page	178
12.24.6	Accounts page	178
12.24.7	Advanced page	179
12.24.8	Encrypting recording for VRM	179
12.24.9	Changing the password of a VRM device	180
12.24.10	Adding a VRM pool	180
12.24.11	Adding a Failover VRM manually	180
12.24.12	Adding a Mirrored VRM manually	181
12.24.13	Adding Encoders via scan	182
12.24.14	Adding VSG devices via scan	183
12.24.15	Synchronizing BVMS configuration	184
12.25	Pool page	184
12.25.1	Configuring automatic recording mode on a pool	185
12.25.2	Adding an Encoder / Decoder manually	185
12.25.3	Adding an iSCSI device manually	186
12.25.4	Adding a Video Streaming Gateway manually	187
12.25.5	Adding a DSA E-Series iSCSI device manually	188
12.25.6	Adding Encoders via scan	190
12.25.7	Adding VSG devices via scan	191
12.25.8	Configuring dual recording in the Device Tree	191
12.26	Bosch Encoder / Decoder page	192
12.27	iSCSI device page	192
12.27.1	iSCSI storage pool	192
12.27.2	Adding an iSCSI device manually	193
12.27.3	Adding a DSA E-Series iSCSI device manually	194
12.27.4	Configuring an iSCSI device	196
12.27.5	Basic Configuration page	197
12.27.6	Load Balancing dialog box	198
12.27.7	Moving an iSCSI system to another pool (Change pool...)	199
12.27.8	LUNs page	199
12.27.9	Adding a LUN	200
12.27.10	Formatting a LUN	201
12.27.11	iqn-Mapper dialog box	201
12.28	Video Streaming Gateway device page	202
12.28.1	Adding a Video Streaming Gateway manually	202
12.28.2	Editing a Video Streaming Gateway	204
12.28.3	Adding a camera to a VSG	204
12.28.4	Add Bosch Encoder dialog box	205
12.28.5	Add ONVIF Encoder dialog box	206
12.28.6	Add JPEG Camera dialog box	207
12.28.7	Add RTSP Encoder dialog box	208
12.28.8	Moving a VSG to another pool (Change pool)	209
12.28.9	Configuring multicast (multicast tab)	209

12.28.10	Configuring logging (advanced tab)	210
12.29	Live Only page	211
12.29.1	Adding live only devices via scan	211
12.29.2	Adding an Encoder / Decoder manually	211
12.29.3	Providing the destination password for a decoder (Authenticate...)	213
12.30	Local Storage page	213
12.31	Unmanaged Site page	214
12.31.1	Adding an unmanaged site manually	214
12.31.2	Importing unmanaged sites	215
12.31.3	Unmanaged Site page	215
12.31.4	Adding an unmanaged network device	215
12.31.5	Configuring the time zone	216
13	**Bosch Encoder / Decoder / Camera page**	**217**
13.1	Adding an encoder to a VRM pool	218
13.2	Adding a live only encoder	218
13.3	Adding a local storage encoder	219
13.4	Editing an Encoder	219
13.4.1	Encrypting live video (Edit Encoder)	219
13.4.2	Updating the device capabilities (Edit Encoder)	220
13.4.3	Edit Encoder / Edit Decoder dialog box	220
13.5	Managing the verification of authenticity	222
13.5.1	Configuring the authentication	222
13.5.2	Uploading a certificate	222
13.5.3	Downloading a certificate	223
13.5.4	Installing a certificate on a workstation	223
13.6	Providing the destination password for a decoder (Authenticate...)	223
13.7	Changing the password of an encoder / decoder (Change password / Enter password)	224
13.8	Moving an encoder to another pool (Change Pool)	225
13.9	Recovering recordings from a replaced encoder (Associate with recordings of predecessor)	225
13.10	Configuring encoders / decoders	226
13.10.1	Configuring the storage media of an encoder	226
13.10.2	Configuring multiple encoders / decoders	227
13.10.3	Configuring failover recording mode on an encoder	229
13.10.4	Recording Management page	229
13.10.5	Recording preferences page	230
13.11	Configuring multicast	230
14	**ONVIF page**	**232**
14.1	Adding an live only ONVIF device via scan	232
14.2	ONVIF Encoder page	232
14.3	ONVIF Encoder Events page	233
14.3.1	Adding and removing an ONVIF profile	235
14.3.2	Exporting an ONVIF mapping table file	236
14.3.3	Importing an ONVIF mapping table file	236
14.3.4	Configuring an ONVIF mapping table	237
14.4	ONVIF Configuration page	239
14.4.1	Unit Access	239
14.4.2	Date / Time	240
14.4.3	User Management	241

14.4.4	Video Encoder Profile page	242
14.4.5	Audio Encoder Profile	244
14.4.6	Imaging General	244
14.4.7	Backlight Compensation	245
14.4.8	Exposure	245
14.4.9	Focus	246
14.4.10	Wide Dynamic Range	247
14.4.11	White balance	247
14.4.12	Network Access	248
14.4.13	Scopes	250
14.4.14	Relays	251
14.5	ONVIF Event Source page	252
14.6	Assigning an ONVIF profile	253
15	**Maps and Structure page**	**254**
15.1	Resource Manager dialog box	255
15.2	Select Resource dialog box	256
15.3	Sequence Builder dialog box	256
15.4	Add Sequence dialog box	257
15.5	Add Sequence Step dialog box	257
15.6	Add URL dialog box	258
15.7	Select Map for Link dialog box	258
15.8	Malfunction Relay dialog box	258
15.9	Link to External Application dialog box	259
16	**Configuring the Logical Tree**	**260**
16.1	Configuring the Logical Tree	260
16.2	Adding a device to the Logical Tree	260
16.3	Removing a tree item	260
16.4	Managing resource files	261
16.5	Adding a Command Script	262
16.6	Managing pre-configured camera sequences	262
16.7	Adding a camera sequence	264
16.8	Adding a folder	264
16.9	Adding a map	264
16.10	Adding a link to another map	265
16.11	Assigning a map to a folder	265
16.12	Managing devices on a map	266
16.13	Adding a document	266
16.14	Adding a malfunction relay	267
16.15	Configuring bypass of devices	267
17	**Schedules page**	**269**
17.1	Recording Schedules page	269
17.2	Task Schedules page	270
18	**Configuring schedules**	**271**
18.1	Configuring a Recording Schedule	271
18.2	Adding a Task Schedule	272
18.3	Configuring a standard Task Schedule	272
18.4	Configuring a recurring Task Schedule	272
18.5	Removing a Task Schedule	273
18.6	Adding holidays and exception days	273

18.7	Removing holidays and exception days	274
18.8	Renaming a schedule	274
19	**Cameras and Recording page**	**276**
19.1	Cameras page	276
19.2	Scheduled Recording Settings dialog box (only VRM and Local Storage)	279
19.3	Recording settings pages (NVR only)	281
19.4	Copy Recording Settings dialog box (NVR only)	282
19.5	Stream Quality Settings dialog box	283
19.6	PTZ/ROI Settings dialog box	285
20	**Configuring cameras and recording settings**	**287**
20.1	Copying and pasting in tables	287
20.2	Exporting the Camera Table	288
20.3	Configuring stream quality settings	288
20.4	Configuring camera properties	289
20.5	Configuring recording settings (only VRM and Local Storage)	289
20.6	Configuring recording settings (NVR only)	290
20.7	Configuring PTZ port settings	291
20.8	Configuring PTZ camera settings	291
20.9	Configuring the ROI function	292
20.10	Configuring predefined positions for the ROI function	292
20.11	Copying recording settings (NVR only)	293
20.12	Configuring the ANR function	293
20.13	Configuring dual recording in the Camera Table	294
20.14	Managing Video Streaming Gateway	294
20.14.1	Assigning an ONVIF profile	294
21	**Events page**	**295**
21.1	Debounce Settings tab	296
21.2	Settings tab for advanced map display	296
21.3	Settings tab for event configuration	297
21.4	Command Script Editor dialog box	297
21.5	Create Compound Event / Edit Compound Event dialog box	298
21.6	Select Script Language dialog box	298
21.7	Edit Priorities of Event Type dialog box	299
21.8	Select Devices dialog box	299
21.9	Text Data Recording dialog box	299
22	**Alarms page**	**300**
22.1	Alarm Settings dialog box	301
22.2	Select Image Pane Content dialog box	301
22.3	Select Resource dialog box	302
22.4	Alarm Options dialog box	303
23	**Configuring events and alarms**	**307**
23.1	Copying and pasting in tables	308
23.2	Removing a table row	308
23.3	Managing resource files	308
23.4	Configuring an event	308
23.5	Duplicating an event	309
23.6	Logging user events	309
23.7	Configuring user event buttons	310
23.8	Creating a Compound Event	310

23.9	Editing a Compound Event	311
23.10	Configuring an alarm	312
23.11	Configuring settings for all alarms	312
23.12	Configuring the pre- and post-alarm duration for an alarm	313
23.13	Triggering alarm recording with text data	313
23.14	Adding text data to continous recording	314
23.15	Protecting alarm recording	314
23.16	Configuring blinking hotspots	315
23.17	Configuring events and alarms for an access control system	316
24	**User Groups page**	**317**
24.1	User Group Properties page	319
24.2	User Properties page	319
24.3	Logon Pair Properties page	320
24.4	Camera Permissions page	321
24.5	Control Priorities page	322
24.6	Copy User Group Permissions dialog box	323
24.7	Decoder Permissions page	323
24.8	Events and Alarms page	324
24.9	LDAP Server Settings dialog box	324
24.10	Credentials page	326
24.11	Logical Tree page	326
24.12	Operator Features page	327
24.13	Priorities page	330
24.14	User Interface page	330
24.15	Server Access page	331
24.16	Configuration Permissions page	332
24.17	User Group Permissions page	333
24.18	Account policies page	334
25	**Configuring users, permissions and Enterprise Access**	**336**
25.1	Creating a group or account	337
25.1.1	Creating a standard user group	337
25.1.2	Creating an Enterprise User Group	337
25.1.3	Creating an Enterprise Account	338
25.2	Creating a user	339
25.3	Creating a dual authorization group	340
25.4	Adding a logon pair to dual authorization group	340
25.5	Configuring Admin Group	341
25.6	Configuring LDAP settings	342
25.7	Associating an LDAP group	342
25.8	Scheduling user logon permission	343
25.9	Configuring operating permissions	343
25.10	Configuring device permissions	344
25.11	Configuring various priorities	344
25.12	Copying user group permissions	345
26	**Configuring video-based fire alarm detection**	**346**
26.1	Configuring a fire detection camera	346
26.2	Adding an encoder to a VRM pool	347
26.3	Adding Encoders via scan	347
26.4	Adding live only devices via scan	347

26.5	Adding local storage encoders via scan	348
26.6	Configuring a fire event	349
26.7	Configuring a fire alarm	349
27	**Configuring MIC IP 7000 connected to a VIDEOJET 7000 connect**	**350**
28	**Troubleshooting**	**351**
28.1	Configuring the desired language in Windows	353
28.2	Reestablishing the connection to a Bosch IntuiKey keyboard	353
28.3	Reducing the number of Allegiant cameras	353
28.4	Used ports	354
28.5	Enabling logging for ONVIF events	359
	Glossary	**361**
	Index	**370**

1 Using the Help

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.

Concepts, page 20 provides background information on selected issues.

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.

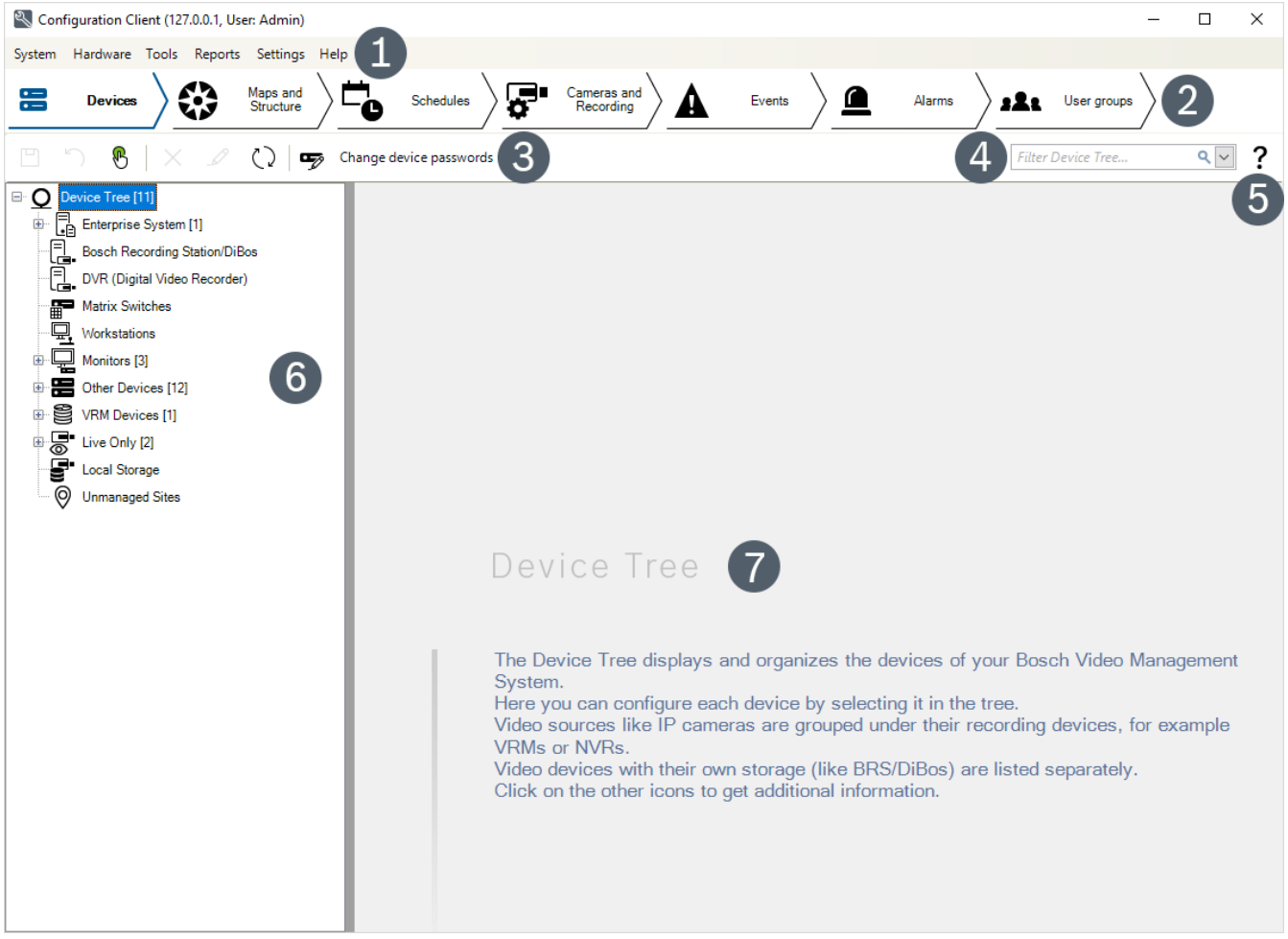
To print a Help topic:

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

Click the link to access the Open Source Software licenses used by BVMS and the Mobile App: http://www.boschsecurity.com/oss/



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.

This manual guides you through the basic steps of the configuration and operation with BVMS. For detailed help and step-by-step instructions read the Configuration Manual and the User Manual or use the Online Help.

BVMS integrates digital video, audio and data across any IP network.

The system consists of the following software modules:

- Management Server
- VRM recording (Video Recording Manager)
- Operator Client
- Configuration Client

To achieve a running system, you must perform the following tasks:
- Install services (Management Server and VRM)
- Install Operator Client and Configuration Client
- Connect to network
- Connect devices to network
- Basic configuration:
  - Add devices (e.g. by device scan)
  - Build logical structure
  - Configure schedules, cameras, events, and alarms
  - Configure user groups

BVMS Archive Player displays exported recordings.

The idea of the BVMS Configuration Client is to start with the configuration of the devices, followed by the configuration of the logical tree. After these two steps, the schedules, recordings, events, and alarms for the devices can be configured on their respective pages. 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

If you plan to install and configure BVMS, participate in a system training on BVMS.
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.

Important components

Component	Description
Management Server (selectable in Setup)	Stream management, alarm management, priority management, Management logbook, user management, device state management. Additional Enterprise System license: Managing Enterprise User Groups and Enterprise Accounts.
Config Wizard	Easy and fast setup of a recording system.
Configuration Client (selectable in Setup)	System configuration and administration for Operator Client.
Operator Client (selectable in Setup)	Live monitoring, storage retrieval and playback, alarm and accessing multiple Management Server computers simultaneously.
Video Recording Manager (selectable in Setup)	Distributing storage capacities on iSCSI devices to the encoders, while handling load balancing between multiple iSCSI devices. Streaming playback video and audio data from iSCSI to Operator Clients.
Mobile Video Service (selectable in Setup)	Provides a transcoding service that transcodes the live and recorded video stream from a camera configured in BVMS to the available network bandwidth. This service enables video clients like an iPhone or a Web client to receive transcoded streams, for example for unreliable network connections with limited bandwidth.
Web Client	You can access live and playback videos via Web browser.
Mobile App	You can use the Mobile App on iPhone or iPad to access live and playback video.
Bosch Video Streaming Gateway (selectable in Setup)	Provides the integration of 3rd party cameras and NVR-like recording, e.g. in low-bandwidth networks.
Cameo SDK (selectable in Setup)	The Cameo SDK is used to embed BVMS live and playback Image panes to your external third-party application. The Image panes follow the BVMS based user permissions. The Cameo SDK provides a subset of the BVMS Operator Client functionalities that enables you to create applications similar to the Operator Client.

Component	Description
Client Enterprise SDK	The Client Enterprise SDK is meant to control and monitor the behaviour of Operator Client of an Enterprise System by external applications. The SDK allows to browse devices that are accessible by the running, connected Operator Client and to control some UI functionalities.
Client SDK / Server SDK	The Server SDK is used to control and monitor the Management Server by scripts and external applications. You can use those interfaces with a valid administrator account. The Client SDK is used to control and monitor the Operator Client by external applications and scripts (part of the related server configuration).

3.1 Hardware requirements

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

3.2 Software requirements

See the data sheet for BVMS.
BVMS must not be installed on a computer where you want to install BVMS Archive Player.

3.3 License requirements

See the data sheet for BVMS for the available licenses.

4 Concepts

This chapter provides background information on selected issues.

4.1 Recording settings

Recording settings in BVMS consist of basic settings (non-scheduled) and scheduled recording settings.
Use the basic settings for the initial configuration of streams.
Use the **Scheduled Recording Settings** for assigning these streams to different use-cases, such as continuous recording, pre-alarm recording, or alarm recording. The recording settings are arranged in the **Scheduled Recording Settings** dialog box accessible on the **Cameras and Recording** page.

4.1.1 Basic stream settings (schedule-independent)

You can configure different codec profiles in the **Cameras and Recording** page of Configuration Client.

Stream 1		Stream 2		Live Video		Recording					Secondary Recording		
Codec	Quality	Codec	Quality	Strea	ROI	Setting	ANR	Max	Storage	Storage	Setting	Storag	Storage Ma
H.264 MP 1080p25/30 fixed	Bit Rate Optimize	H.264 MP 1080p4/5 fixed	Bit Rate Optimized	Stream 2		Continuous, Alarm Recording			1	30	Continuous, Alarm Recording	1	
H.264 MP HD 2640x2640	Bit Rate Optimize	H.264 MP HD 800x800	Balanced	Stream 2		Continuous, Alarm Recording			1	30	Continuous, Alarm Recording	1	
H.264 MP 1080p25/30 fixed	Bit Rate Optimize	Copy from Stream 1	Quality of Stream 1	Stream 2		Continuous, Alarm Recording			1	30	Continuous, Alarm Recording	1	
H.264 MP 720p50/60 fixed	Bit Rate Optimize	Copy from Stream 1	Quality of Stream 1	Stream 2		Continuous, Alarm Recording			1	30	Continuous, Alarm Recording	1	

Codecs and HD resolution

Codecs are part of the basic stream settings. BVMS gives you default settings for all codecs and qualities. You can change these settings.
It depends on the camera device type which codec you can select.

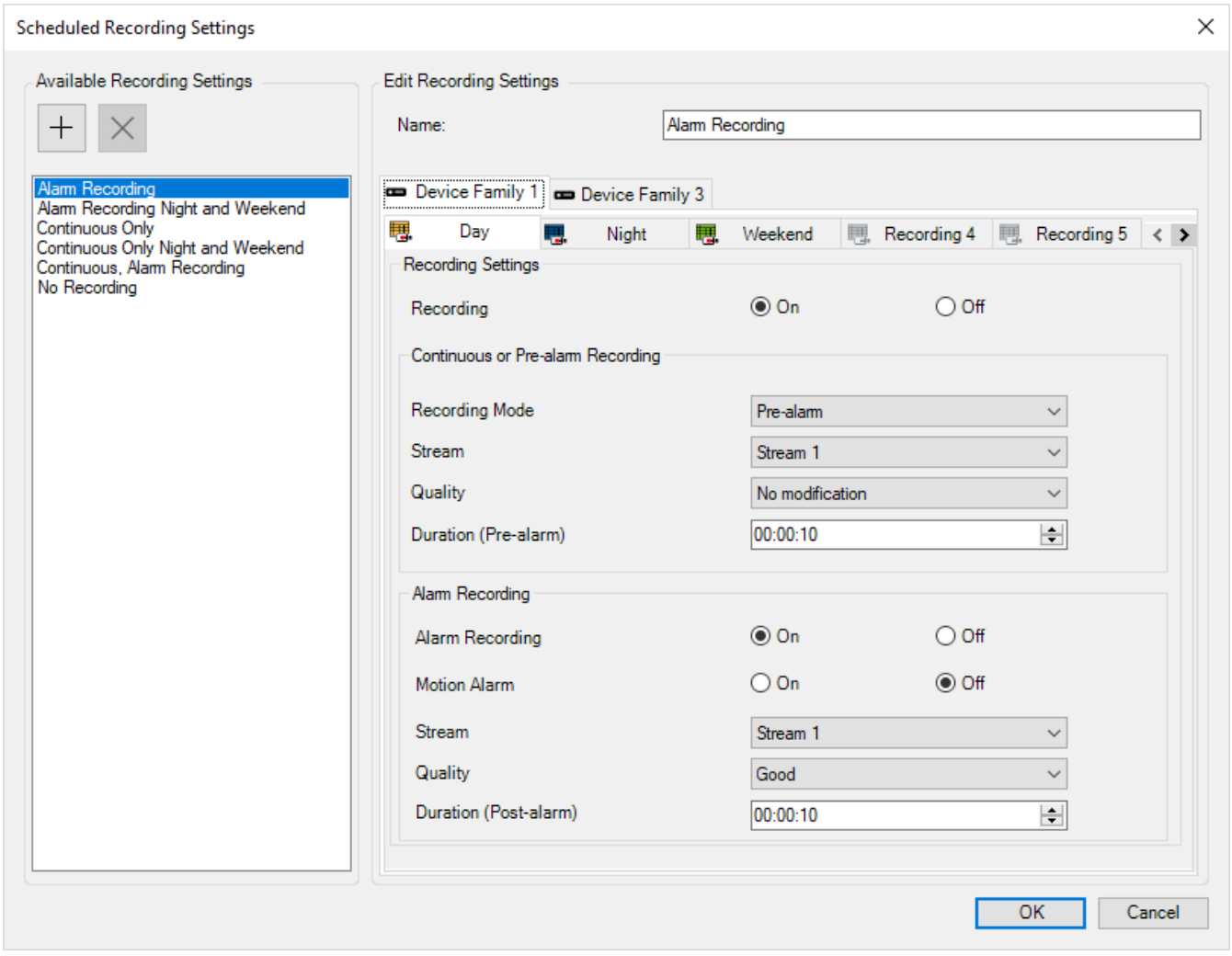
4.1.2 Stream assignment for Live

You can assign either stream 1 or stream 2 for Live. The quality and codec of the basic stream settings are used.

Stream 1		Stream 2		Live Video		Recording					Secondary Recording		
Codec	Quality	Codec	Quality	Strea	ROI	Setting	ANR	Max	Storage	Storage	Setting	Storag	Storage Ma
H.264 MP 1080p25/30 fixed	Bit Rate Optimize	H.264 MP 1080p4/5 fixed	Bit Rate Optimized	Stream 2		Continuous, Alarm Recording			1	30	Continuous, Alarm Recording	1	
H.264 MP HD 2640x2640	Bit Rate Optimize	H.264 MP HD 800x800	Balanced	Stream 2		Continuous, Alarm Recording			1	30	Continuous, Alarm Recording	1	
H.264 MP 1080p25/30 fixed	Bit Rate Optimize	Copy from Stream 1	Quality of Stream 1	Stream 2		Continuous, Alarm Recording			1	30	Continuous, Alarm Recording	1	
H.264 MP 720p50/60 fixed	Bit Rate Optimize	Copy from Stream 1	Quality of Stream 1	Stream 2		Continuous, Alarm Recording			1	30	Continuous, Alarm Recording	1	

4.1.3 Scheduled Recording Settings

To display the **Scheduled Recording Settings** dialog box, click **Edit scheduled recording settings** in the toolbar of the **Cameras and Recording** page.
Cameras are typically grouped by location and/or schedule (e.g. **Alarm Recording Night and Weekend**), and not by technical differences between camera models.
You can map these groups as templates in the **Scheduled Recording Settings** dialog box. You perform all recording configurations in this dialog box.
Continuous, Alarm Recording is the default setting for a camera that is added to BVMS.



Stream 1		Stream 2		Live Video		Recording					Secondary Recording		
Codec	Quality	Codec	Quality	Strea	ROI	Setting	ANR	Max	Storage	Storage	Setting	Storag	Storage Ma
H.264 MP 1080p25/30 fixed	Bit Rate Optimize	H.264 MP 1080p4/5 fixed	Bit Rate Optimized	Stream 2		Continuous, Alarm Recording			1	30	Continuous, Alarm Recording	1	
H.264 MP HD 2640x2640	Bit Rate Optimize	H.264 MP HD 800x800	Balanced	Stream 2		Continuous, Alarm Recording			1	30	Continuous, Alarm Recording	1	
H.264 MP 1080p25/30 fixed	Bit Rate Optimize	Copy from Stream 1	Quality of Stream 1	Stream 2		Continuous, Alarm Recording			1	30	Continuous, Alarm Recording	1	
H.264 MP 720p50/60 fixed	Bit Rate Optimize	Copy from Stream 1	Quality of Stream 1	Stream 2		Continuous, Alarm Recording			1	30	Continuous, Alarm Recording	1	

In the dialog you configure for a device family and a schedule which stream for the selected recording mode is to be used. Usually you should not configure the quality for devices of **Device Family 2** or **Device Family 3** in this dialog box. Select the quality for each camera individually in the Recording Table. The quality settings of the dialog are only active for Secondary Recording, when on the stream no Primary Recording is active. For **Device Family 1** we recommend configuring a quality setting in the dialog, not in the Recording Table.

In the **Scheduled Recording Settings** dialog box, you configure the recording settings of the devices. BVMS displays pre-defined recording settings (templates). You can modify these templates to your needs or you can add templates.

You can configure the recording settings per device family independently per schedule.

Possible recording settings are:

	Device Family 1	**Device Family 2**	**Device Family 3**
Recording Settings			
Recording	**On** / **Off** (setting valid for all device families)		
Continuous or Pre-alarm Recording			

	Device Family 1	Device Family 2	Device Family 3
Recording Mode	**Continuous** **Pre-alarm**	**Continuous** **Pre-alarm**	**Continuous** **Pre-alarm**
Stream	**Stream** 1	**Stream** 1 **Stream** 2	**Stream** 1 **Stream** 2 **I-frame only (from Stream1)**
Quality	**No modification** Pre-defined / user-defined qualities (recommended)	**No modification** (recommended) Pre-defined / user-defined qualities	**No modification** (recommended) Pre-defined / user-defined qualities
Duration (pre-alarm)	10s - 3h For pre-alarm recording of less than 10 seconds the RAM of the camera is used.	10s - 3h For pre-alarm recording of less than 10 seconds the RAM of the camera is used.	10s - 3h For pre-alarm recording of less than 10 seconds the RAM of the camera is used.
Alarm Recording			
Alarm Recording	**On** / **Off** (setting valid for all device families)	**On** / **Off** (setting valid for all device families)	**On** / **Off** (setting valid for all device families)
Motion Alarm	**On** / **Off** (setting valid for all device families)	**On** / **Off** (setting valid for all device families)	**On** / **Off** (setting valid for all device families)
Stream	**Stream** 1	**Stream** 1 **Stream** 2	**Stream** 1 **Stream** 2 **I-frame only (from Stream1)**
Quality	**Good** (recommended) Pre-defined / user-defined qualities	**No modification** (recommended) Pre-defined / user-defined qualities	**No modification** (recommended) Pre-defined / user-defined qualities
Duration (post-alarm)	1s - 3h	1s - 3h	1s - 3h

Enter a descriptive name for your configuration which is then displayed in the **Available Recording Settings** list.

You can select all configured recording settings in the **Recording** - **Setting** column. Assign one recording setting per camera. You can copy and paste one setting to all cameras for fast configuration.

Changing qualities in schedules

You can configure stream qualities per recording schedule. Depending on the used device family, you can modify the quality properties.

Device Family 1	Device Family 2 or Device Family 3
Streams	Alarm Recording
You can change recording qualities (incl. resolution change) for alarm recording.	You can modify the existing stream with the settings of another stream quality. But only the **Image encoding interval** value and the **Target bit rate [Kbps]** value are modified. Other settings like the resolution are not modified.

Device Family 1	Device Family 2 or Device Family 3
Notes	
For the XFM4 platform possible recording gaps can be up to 4 frames, 133/160ms (NTSC/PAL) on alarm recording and schedule change if active recording quality differs.	Possible recording gaps can be up to 12 frames, with 1 IPS up to 12 seconds on schedule change if active recording quality differs from old to new schedule.
Examples	
	Stream 2 is selected for normal recording and configured with **Normal** quality. For an alarm, the **Excellent** quality is selected. When an alarm occurs, all settings of the **Normal** quality are used except the **Image encoding interval** value and the **Target bit rate [Kbps]** value which are modified with the values of **Excellent** .

4.2 Config Wizard

Intended use for Config Wizard is the quick and easy configuration of a smaller system. Config Wizard helps you to achieve a configured system including VRM, iSCSI system, Mobile Video Service, cameras, recording profiles and user groups.
You must add iSCSI systems manually on a standard software installation.
User groups and their permissions are configured automatically. You can add or remove users and set passwords.
Config Wizard can access Management Server only on the local computer.
You can save an activated configuration for backup purposes and import this configuration later. You can change this imported configuration after import.
Config Wizard adds the local VRM automatically both on a standard software installation and on DIVAR IP 3000 and DIVAR IP 7000.
On a DIVAR IP 3000 and on a DIVAR IP 7000 the local iSCSI device is also added automatically if not already available.
On a DIVAR IP 3000 and on a DIVAR IP 7000, a local Mobile Video Service is added automatically if not already available.

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

See also
– *Using Config Wizard, page 72*

4.3 BVMS design concepts

Single Management Server System, page 24
A single BVMS Management Server System provides management, monitoring and control of up to 2000 cameras/encoders.

Enterprise System, page 25
An Enterprise Management Server provides simultaneous access to multiple Management Servers. The Enterprise System allows full access to events and alarms from multiple subsystems.

Server Lookup, page 26
The Server Lookup feature provides a list of available BVMS Management Servers to the BVMS Operator Client. The Operator can select a server out of the list of available server. Connected to the Management Server the Client has full access to the Management Server.

Unmanaged site, page 27
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.

4.3.1 Single Management Server System

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

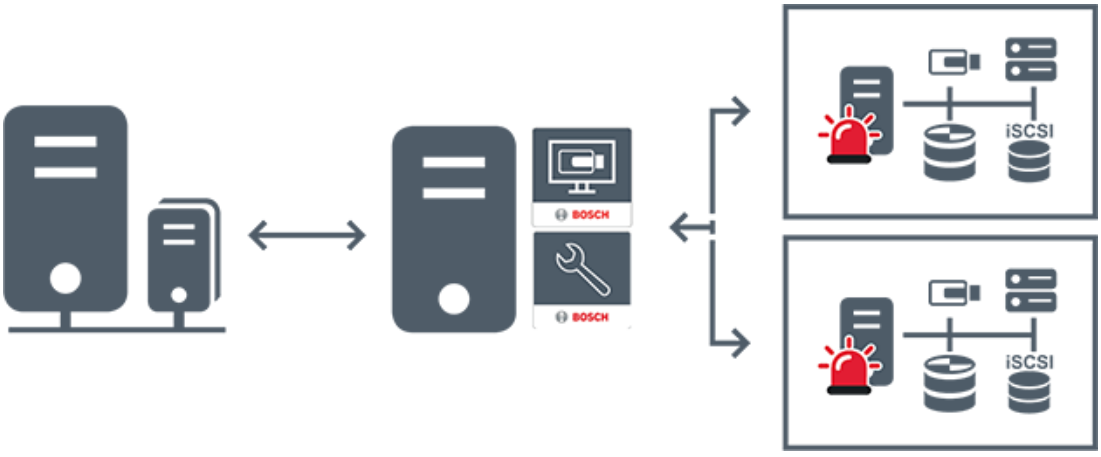
Responsibilities:
- Configuring data
- Event log (logbook)
- User profiles
- User priorities
- Licensing
- Event- and alarm-management

	Live, playback, events, alarms
	Management Server

	Operator Client / Configuration Client
	Cameras
	VRM
	iSCSI
	Other devices

4.3.2 Enterprise System

- The target of a BVMS Enterprise System is to enable a user of an Operator Client to simultaneously access multiple Management Servers (subsystems).
- Clients connected to an Enterprise Server have full access to all cameras and recordings from the subsystems.
- Clients connected to an Enterprise Server have full real time awareness of events and alarms of all subsystems.
- Typical application areas:
  - Metros
  - Airports



	Live, playback, events, alarms
	BVMS Enterprise Management Server

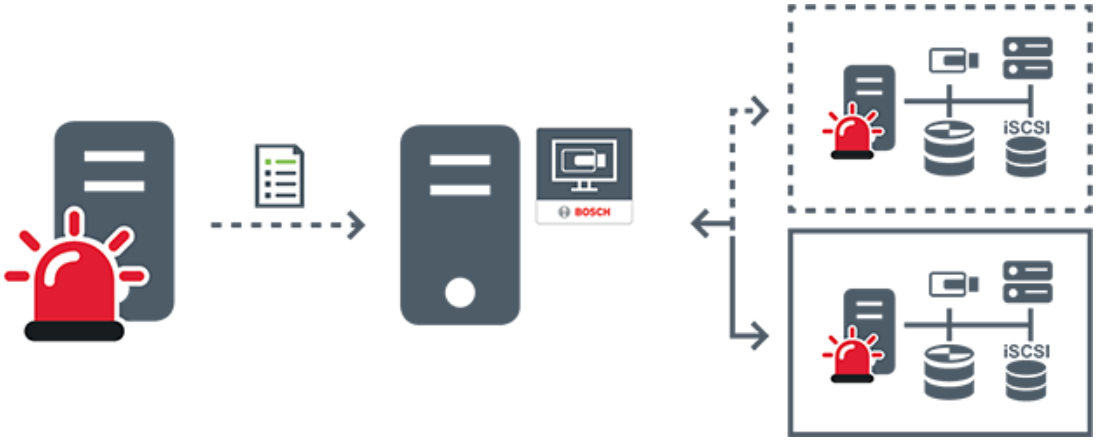
	BVMS Operator Client / Configuration Client
	BVMS Subsystem

See also

- *Creating an Enterprise System, page 96*
- *Configuring the Server List for Enterprise System, page 96*
- *Configuring users, permissions and Enterprise Access, page 336*
- *Accessing the system, page 84*

4.3.3 Server Lookup

- The BVMS Server Lookup feature allows Operators to connect to a BVMS Management Server out of a provided list of servers.
- A single user of Configuration Client or Operator Client can connect to multiple system access points sequentially.
- System access points can be Management Server or Enterprise Management Server.
- Server Lookup uses dedicated Management Server to host the Server List.
- Server Lookup and Management Server or Enterprise Management Server functionally can be run on one machine.
- Server Lookup supports you in locating system access points by their names or descriptions.
- Once connected to the Management Server the Operator Client receives events and alarms from the BVMS Management Server and shows live and playback



	On demand live, playback, events, alarms - connected
	On demand live, playback, events, alarms - not connected
	Management Server

	Server list
	Operator Client
	Connected BVMS from server list
	Not connected BVMS from server list

See also

- *Configuring Server Lookup, page 130*
- *Server list / Address Book page, page 129*
- *Using Server Lookup, page 84*
- *Exporting the Server List, page 131*
- *Importing a Server List, page 131*

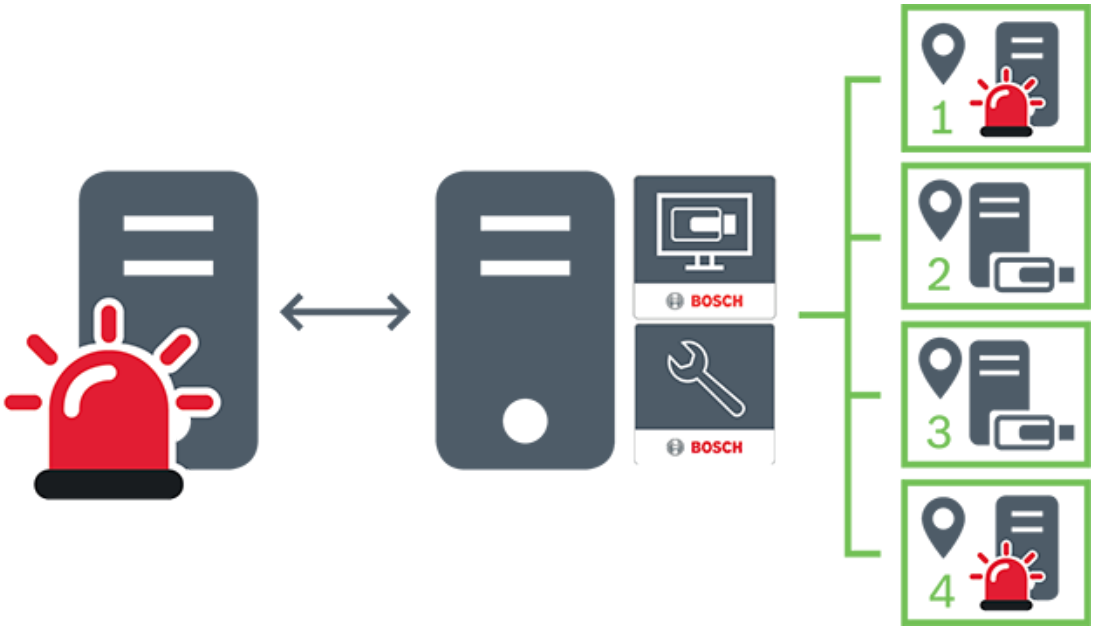
4.3.4 Unmanaged site

- 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 thesite.



	Live, playback, events, alarms
	On demand live and playback video traffic
	Management Server
	Operator Client / Configuration Client
	site
	DVR

See also

– *Adding an unmanaged site manually, page 214*

4.4 Remote access

Notice!

To prevent unauthorized access to video data through the Internet, we strongly recommend that you protect all users and devices in the system with an appropriate password.
Protect all levels of a camera / encoder (service / user / live) with a password.

Related Topics for changing passwords

– *User Properties page, page 319*
– Changing the password of an encoder / decoder

– *Changing the password of a VRM device, page 180*

The target of remote access in BVMS is to connect different private networks to public networks.

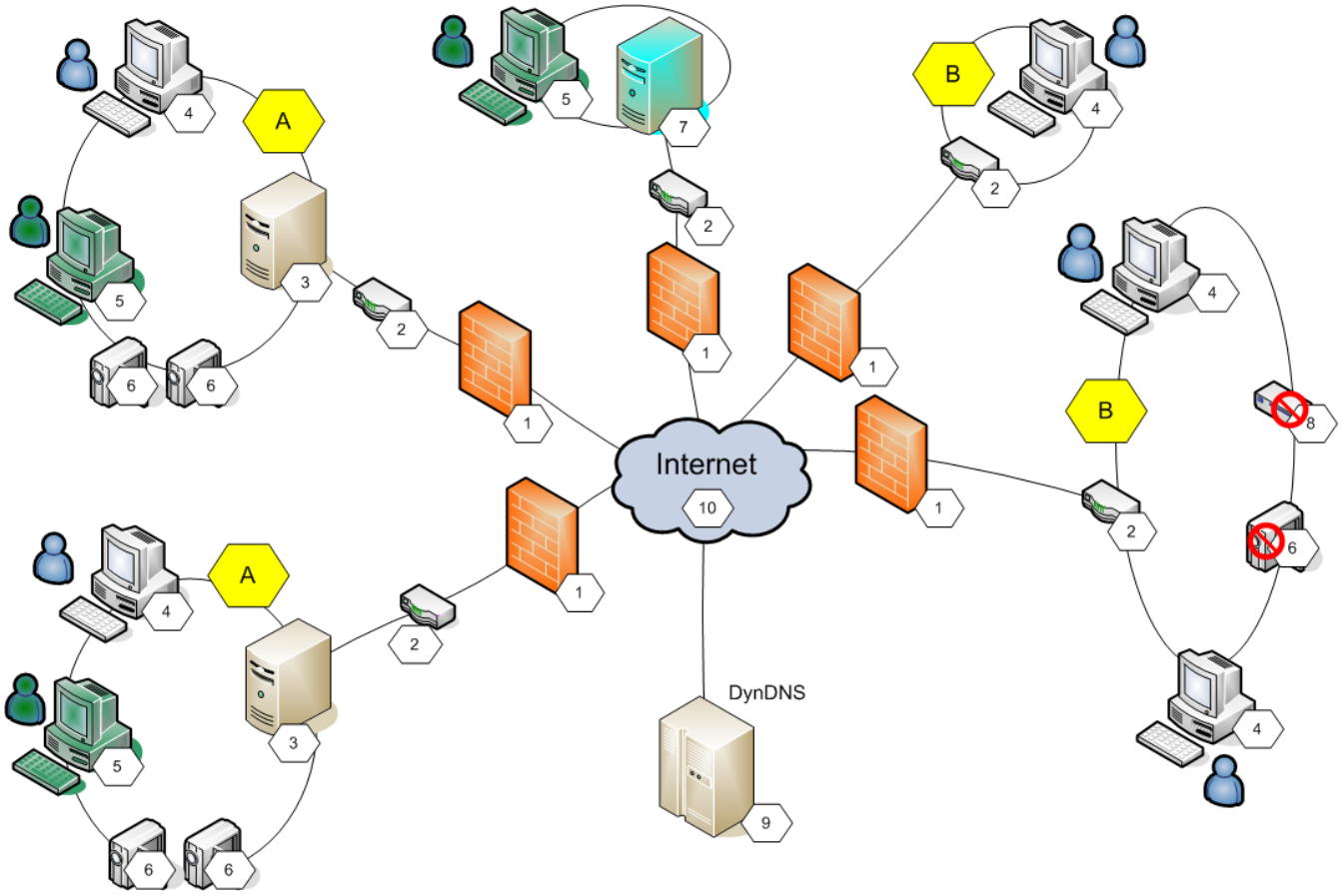
Multiple networks with private (local) network addresses can be accessed simultaneously or sequentially by Operator Client computers via public interfaces (routers). Task of the router is to translate the incoming public network traffic to the corresponding private network address.

The users of Operator Client can access Management Server or Enterprise Management Server and their devices via remote access.

You cannot access the following devices/features via remote access:

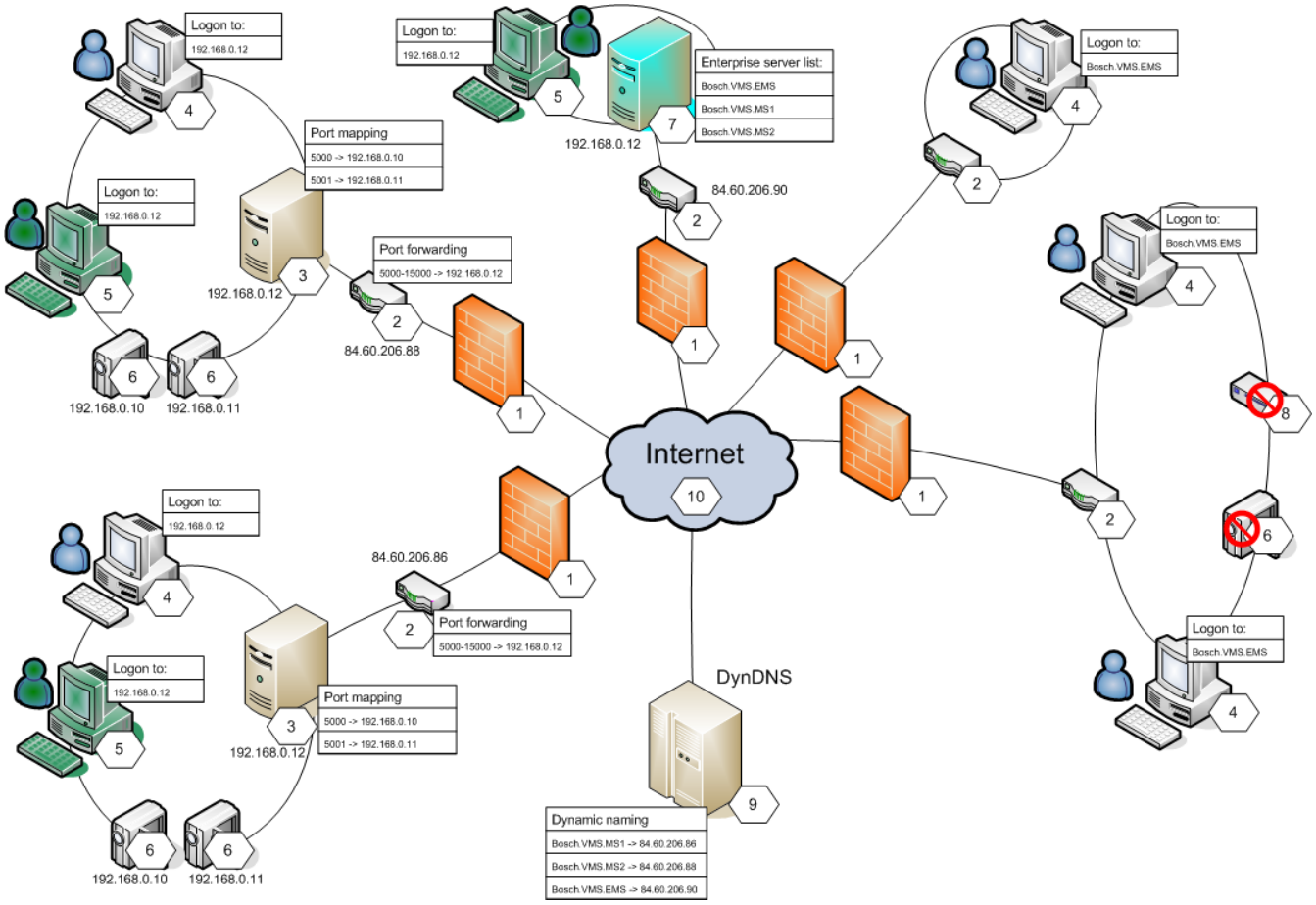
– Playback of local storage
– ONVIF
– DiBos
– Direct iSCSI replay

The following image shows an example of remote access to BVMS devices in a single system:



1	Firewall	**6**	IP camera / encoder
2	Router	**7**	Enterprise Management Server
3	Management Server	**8**	Decoder
4	Operator Client	**9**	DynDNS Server
5	Configuration Client	**10**	World Wide Web
A	Remote network	**B**	Local network

The following image shows an example of remote access from private network with Enterprise System to remote BVMS systems:



1	Firewall	**6**	IP camera / encoder
2	Router Port forwarding	**7**	Enterprise Management Server Enterprise server list
3	Management Server Port mapping	**8**	Decoder
4	Operator Client Logon to	**9**	DynDNS Server Dynamic naming
5	Configuration Client Logon to	**10**	World Wide Web

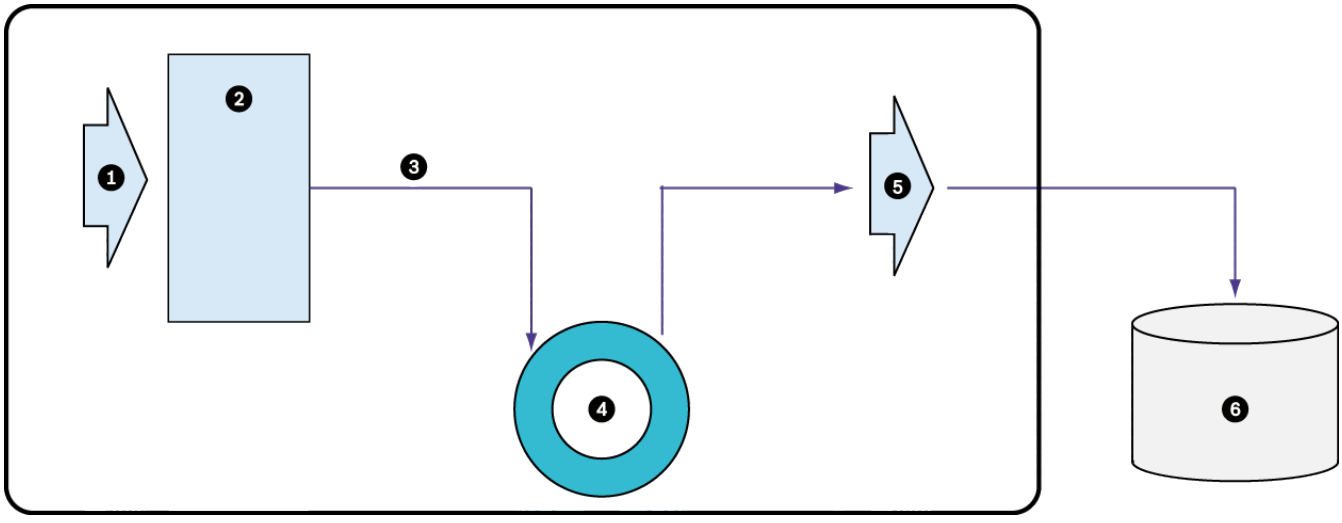
To enable the remote access of an Operator Client to devices in a remote network, each device is assigned a public port number in addition to the public network address of the router. For access, Operator Client uses this public port number together with the public network address. In the private network the incoming traffic for the public port number is forwarded to the private network address and port number of the corresponding device. You configure the port mapping in Configuration Client for use by Operator Client.

Notice!
Additionally the network administrator must configure the port forwarding on the router of the private network. The network administrator must ensure that remote access via these ports is running outside of BVMS environment.

See also
- *Configuring remote access, page 85*
- *Remote Access Settings dialog box (Settings menu), page 123*
- *Port Mapping Table dialog box, page 124*

4.5 Automated Network Replenishment (ANR)

Intended use
When a failure of the network or the central storage occurs, the ANR function ensures that the encoder transmits the locally buffered recording of the missing time period to the central storage after the failure is fixed.
The following graphic shows the transmission of video data after a network or storage failure is fixed.



1	Video	5	IP network
2	Encoder	6	iSCSI target (central storage)
3	Write to buffer immediately		
4	SD card (ring buffer)		

Example: Work around network failure
If the network fails unexpectedly, the ANR function completes the central storage with the locally buffered recording when the network is available again.

Example: Store video data when network is not available
A subway has no network connection to the central storage when located between stations. Only during regular stops the buffered recording can be transmitted to the central storage. Ensure that the time period that is required for transferring the buffered recording, does not exceed the time period of a stop.

Example: ANR for alarm recording
The pre-alarm recording is stored locally. Only in case of an alarm, this pre-alarm recording is transmitted to the central storage. If no alarm occurs, the obsolete pre-alarm recording is not transmitted to the central storage and, hence, does not burden the network.

Limitations

Notice!
You cannot use playback from the local storage media when the passwords for `user` and `live` are set on the encoder. Remove the passwords if required.

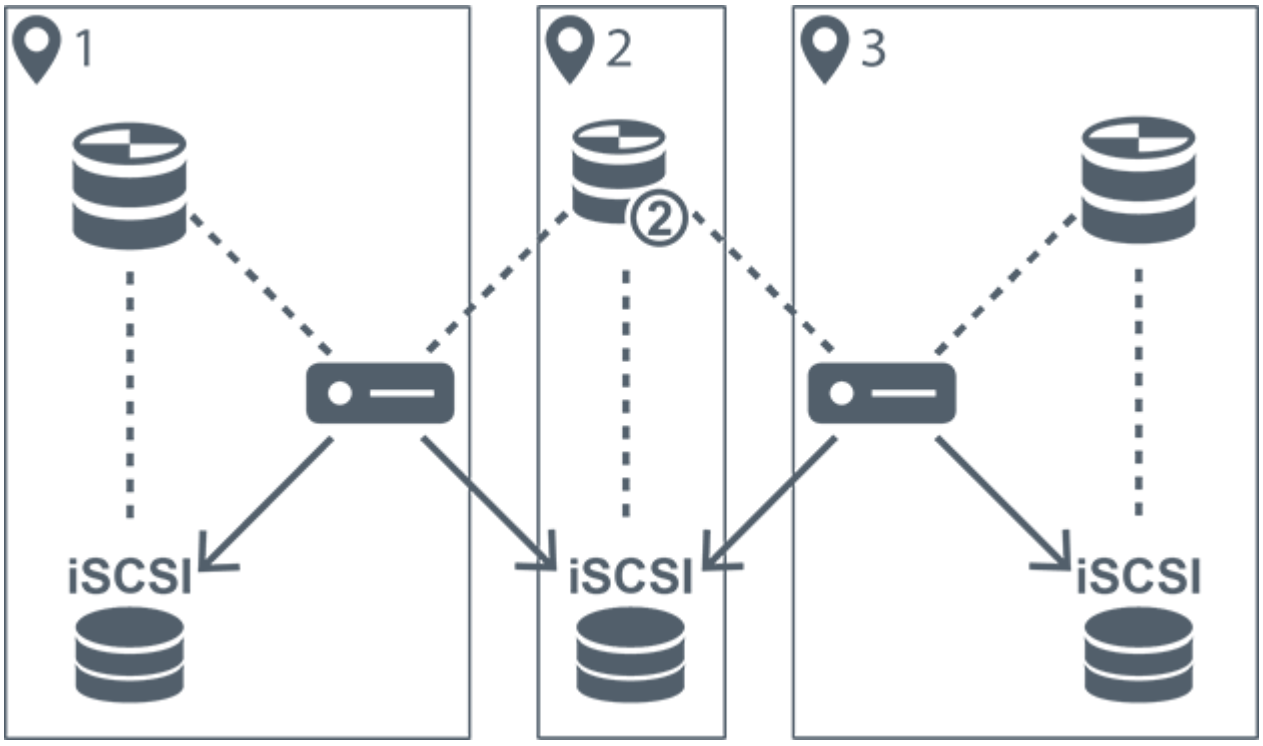
The ANR function only works with VRM recording.
The ANR function does not work with an encoder for which a secure connection for live display is configured.
You must have configured the storage media of an encoder to use the ANR function.
The encoder for which you configure the ANR function, must have firmware version 5.90 or later. Not all encoder types support the ANR function.
You cannot use the ANR function with dual recording.
Your iSCSI storage system must be properly configured.
The following list contains the possible reasons if you cannot configure the ANR function:
- Encoder is not reachable (wrong IP address, network failure, etc.).
- Storage media of the encoder not available or read-only.
- Wrong firmware version.
- Encoder type does not support the ANR function.
- Dual recording is active.

See also
- *Configuring an iSCSI device, page 196*
- *Configuring the storage media of an encoder, page 94*
- *Configuring the ANR function, page 293*

4.6 Dual / failover recording

Intended use
A Primary VRM manages the normal recording of the cameras of your system. You use a Secondary VRM to achieve dual recording of your cameras.
Dual recording allows you to record video data from the same camera to different locations. Dual recording is usually performed with different stream settings and recording modes. As a special case of dual recording you can configure mirrored recording: the same video signal is recorded twice to different locations.
Dual recording is realized by using 2 VRM servers managing multiple iSCSI devices that can be located at different locations.
A Secondary VRM can manage the secondary recording for multiple Primary VRMs.
The user can select between the recordings managed by the Primary VRM and those managed by the Secondary VRM. For a single camera, the user can switch over to the recordings of the Secondary / Primary VRM. The user can also display the recordings of the same camera managed by Primary VRM and Secondary VRM simultaneously.
For dual recording, you must install a Secondary VRM during Setup.
A Failover VRM is used for continuing the recording of a failed Primary VRM or a failed Secondary VRM computer.

The following graphic shows an example of a dual recording scenario:



1	Site 1		Encoder
2	Central site		iSCSI storage device
3	Site 2		Control connection
	Primary VRM		Video stream
	Secondary VRM		

Limitations

You cannot use dual recording together with ANR.

Cameo SDK only supports the playback of primary recording.

See also

- *Configuring dual recording in the Camera Table, page 294*
- *Adding a Mirrored VRM manually, page 181*
- *Adding a Failover VRM manually, page 180*
- *Cameras page, page 276*

4.7 VRM recording modes

This chapter shows graphics to illustrate the possible VRM recording modes.

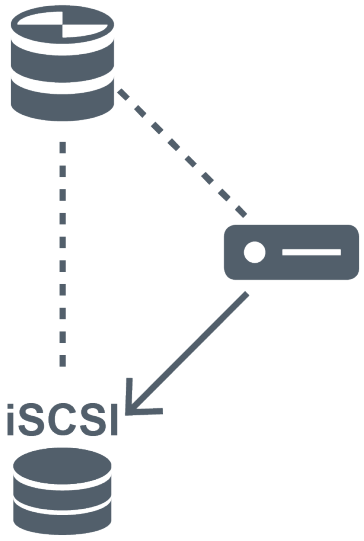
List of possible VRM recording modes:

- Primary VRM recording
- Mirrored VRM recording

– Secondary VRM recording
– Failover VRM recording

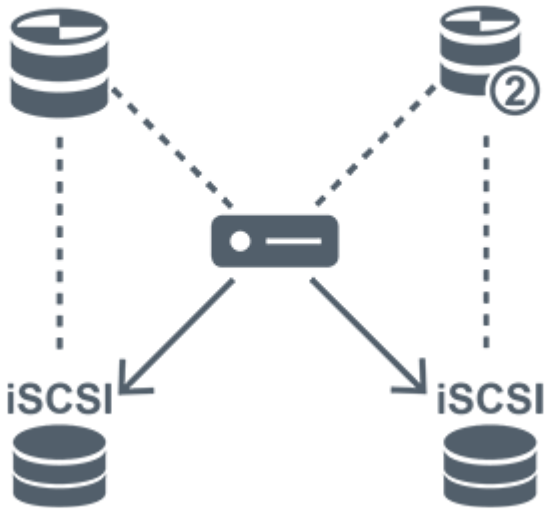
For ANR recording, see chapter *Automated Network Replenishment (ANR), page 31*.

Primary VRM recording



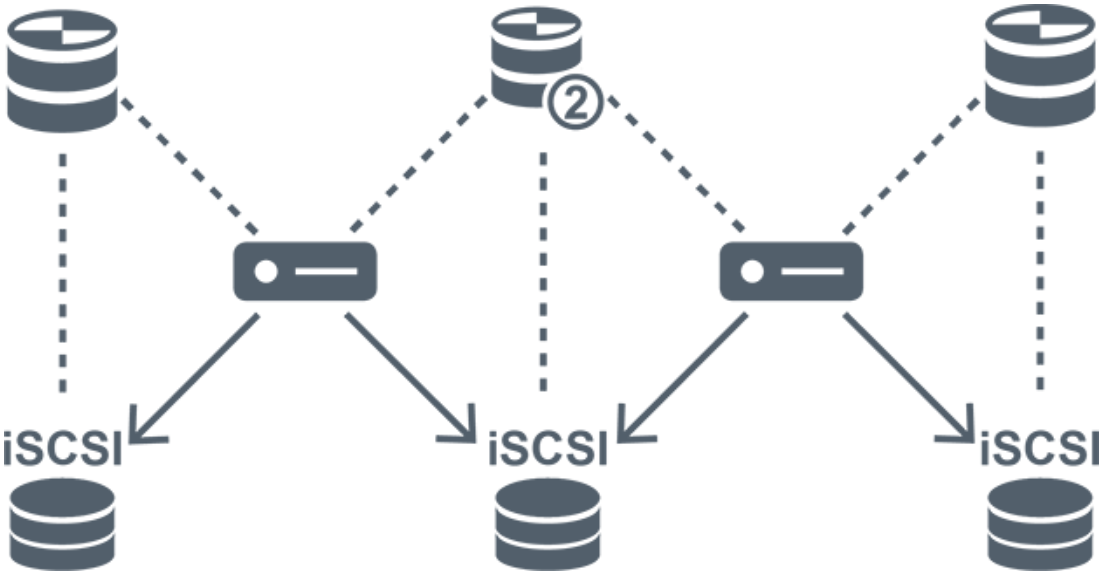
	Primary VRM		Control connection
iSCSI	iSCSI storage device	→	Video stream
	Encoder		

Mirrored VRM recording



	Primary VRM		Secondary VRM
iSCSI	iSCSI storage device		Control connection
	Encoder	→	Video stream

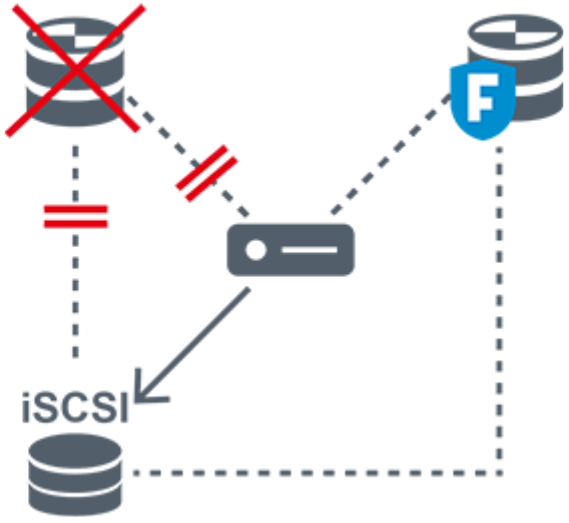
Secondary VRM recording



	Primary VRM		Secondary VRM
iSCSI	iSCSI storage device		Control connection

	Encoder	→	Video stream

Failover VRM recording



	Primary VRM		Primary Failover VRM
iSCSI	iSCSI storage device		Encoder
-------	Control connection	→	Video stream

4.8 Playback of VRM recording sources

The following graphics show Image panes with playback from all possible VRM recording sources. Each graphic displays the storage device, the VRM instance (if available), and a section of an Image pane as example of the playback. If applicable, the recording source is indicated by an appropriate icon on the Image pane bar.

- *Playback of single recording, page 36*
- *Playback of dual VRM recording, page 38*
- *Playback of Primary VRM recording with optional Failover VRM, page 39*
- *Playback of Secondary VRM recording with optional Failover VRM, page 41*
- *Automatic Network Replenishment, page 43*

Playback of single recording

This Image pane is displayed when only a Primary VRM is configured. You cannot select another recording source.

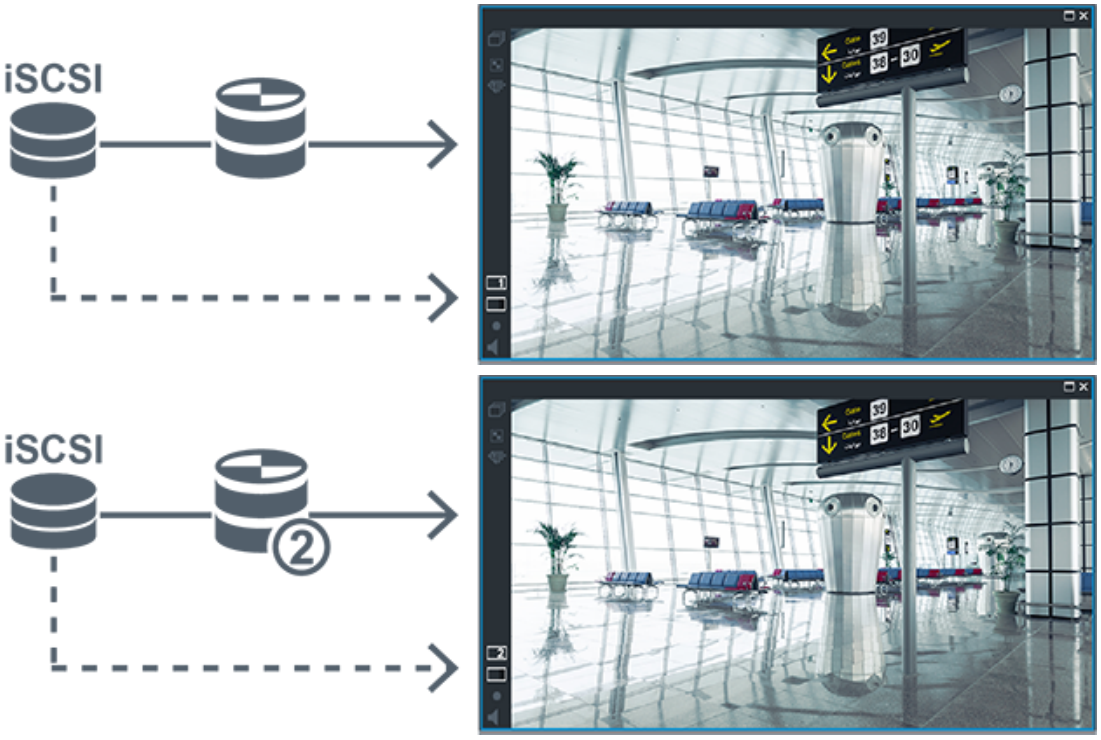
⇢: If configured for this workstation, playback is provided directly by the iSCSI storage device.

iSCSI	iSCSI storage device
	Primary VRM

Playback of dual VRM recording

A Primary VRM and a Secondary VRM are configured. Click the recording source icon to display primary or secondary playback.

If configured for this workstation, playback is provided directly by the iSCSI storage device.



	iSCSI storage device
	Primary VRM
	Secondary VRM

Playback of Primary VRM recording with optional Failover VRM

While the Primary VRM is working, it provides playback. The Failover VRM runs in idle state. If configured for this workstation, playback is provided directly by the iSCSI storage device. If a Secondary VRM or ANR recording is configured, you can switch the recording source.

When the Primary VRM is not connected, the configured Failover VRM provides playback. Close the Image pane and display the camera again in an Image pane:

When the Primary VRM and the optional Primary Failover VRM are both not connected, the encoder provides playback. Close the Image pane and display the camera again in an Image pane:

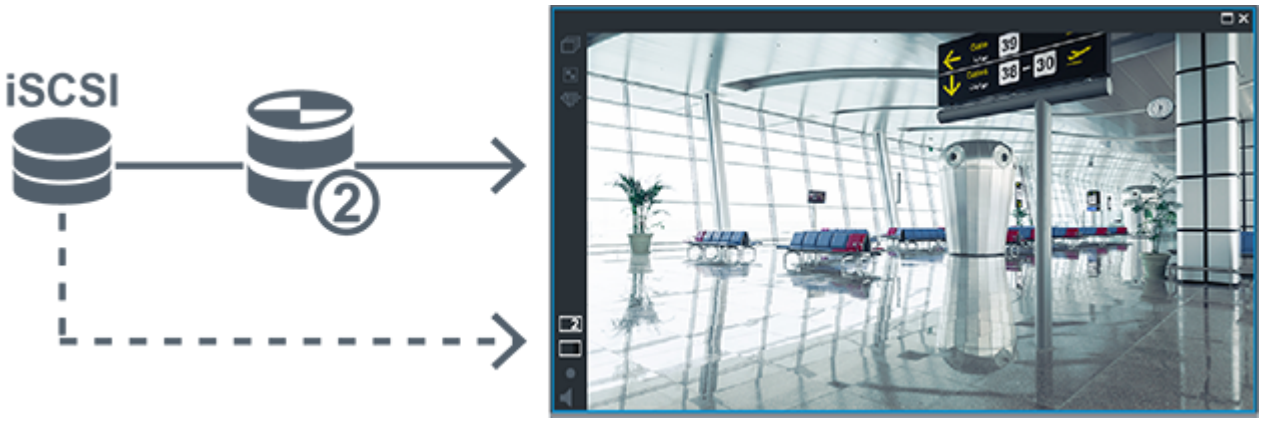
	iSCSI storage device
	Primary VRM

	Primary Failover VRM
	Encoder

Encoder playback can only access a limited recording period.

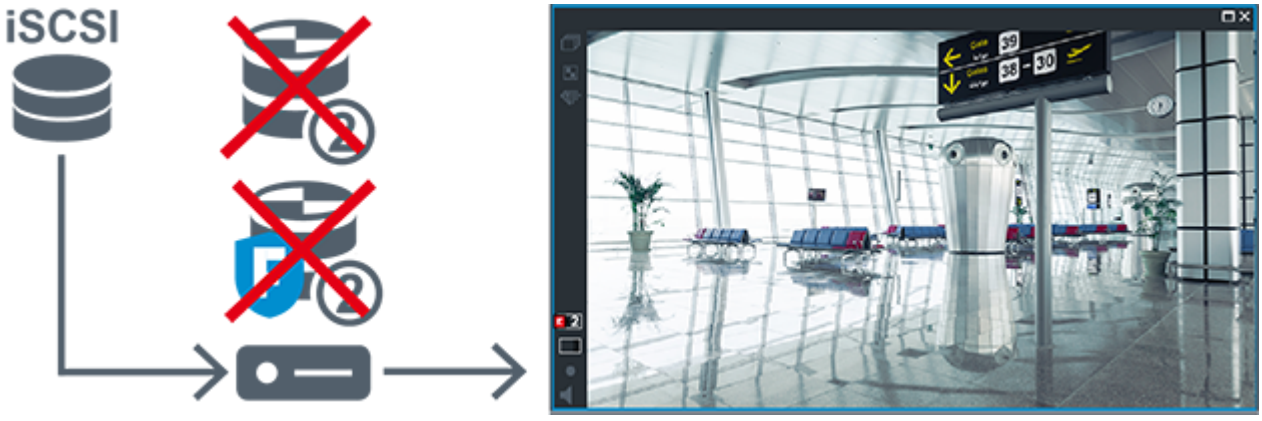
Playback of Secondary VRM recording with optional Failover VRM

While the Secondary VRM is working, it provides playback. The Failover VRM runs in idle state. If configured for this workstation, playback is provided directly by the iSCSI storage device.



When the Secondary VRM is not connected, the configured Failover VRM provides playback. Close the Image pane and display the camera again in an Image pane:

When the Secondary VRM and the optional Secondary Failover VRM are both not connected, the encoder provides playback. Close the Image pane and drag the camera again to an Image pane:



iSCSI	iSCSI storage device
	Primary VRM

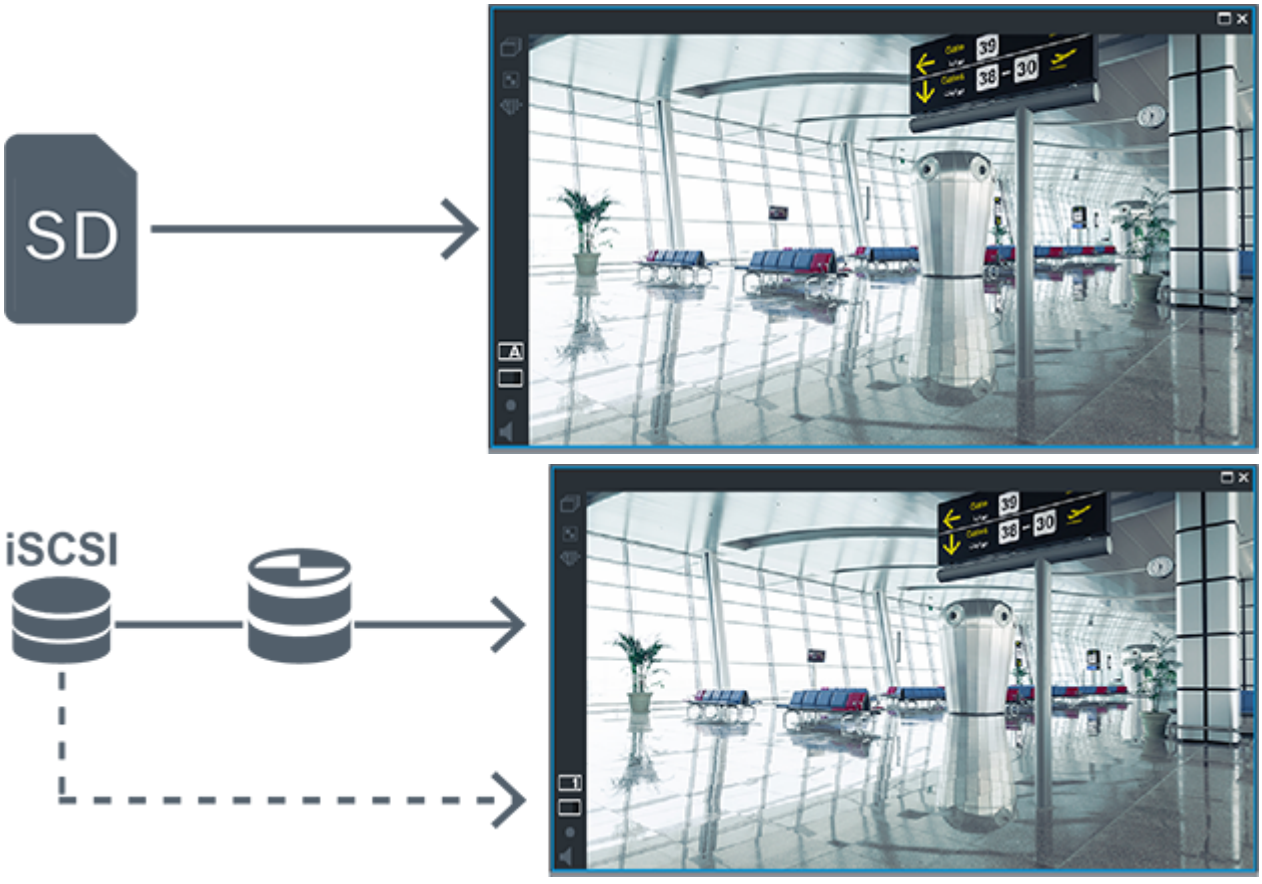
	Secondary Failover VRM
	Encoder

Encoder playback can only access a limited recording period.

Automatic Network Replenishment

ANR is configured. Click the recording source icon to display primary playback (primary failover playback, primary encoder playback) or ANR playback.

If configured for this workstation, playback is provided directly by the iSCSI storage device.



iSCSI	iSCSI storage device
	Primary VRM
SD	SD card

4.9 Alarm handling

Alarms can be individually configured to be handled by one or more user groups. When an alarm occurs, it appears in the Alarm List of all users in the user groups configured to receive that alarm. When any one of these users starts to work on the alarm, it disappears from the Alarm List of all other users.

Alarms are displayed on a workstation’s alarm monitor. This behavior is described in the following paragraphs.

Alarm flow

1. An alarm occurs in the system.
2. Alarm notifications appear in the Alarm Lists of all users configured for this alarm. Alarm video is immediately displayed on configured monitors. If it is an automatically displayed alarm (auto pop-up), the alarm video is also automatically displayed on the

Operator Client workstation’s alarm monitors.
If the alarm is configured as an auto-clear alarm, the alarm is removed from the Alarm List after the auto-clear time (configured in the Configuration Client).
On monitors, any quad views from VIP XDs are temporarily replaced by full-screen displays.

3. One of the users accepts the alarm. The alarm video is then displayed on this user's workstation (if it is not already displayed via auto pop-up). The alarm is removed from all other Alarm Lists and alarm video displays.
4. The user who accepted the alarm invokes a workflow that can include reading an action plan and entering comments. This step is optional - requirements for workflow can be configured by the administrator.
5. Finally, the user clears the alarm. This removes the alarm from his Alarm List and alarm display.
   On a monitor group, the monitors return to the cameras that were displayed before the alarm occurred.

Alarm Image window

1. To display alarm video, the Alarm Image window replaces the Live or Playback Image window on the monitor that has been configured for alarm display.
2. Each alarm gets a row of Image panes. Up to 5 Image panes can be associated with each alarm. These Image panes can display live video, playback video, or maps.
   On a monitor group, each alarm can call up cameras on a row of monitors. The number of cameras in the row is limited by the number of columns in the monitor group. Monitors in the row that are not used for alarm video can be configured to either continue with their current display or to display a blank screen.
3. Higher priority alarms are displayed above lower priority alarms on both monitor rows and the Operator Client workstation display alarm rows.
4. If the Alarm image window is completely full of Alarm image rows and an additional alarm must be displayed, the lowest priority alarms "stack up" in the bottom row of the Alarm image window. You can step through the stacked alarms with the controls at the left side of the alarm row.
   You can step through the alarm stacks on monitor groups with control buttons in the **Monitors** window of the Operator Client workstation display. Monitors in alarm are indicated by red icons with blinking "LEDs".
   The alarm title, time, and date can be optionally be displayed on all monitors, or only the first monitor in the alarm row.
5. For equal priority alarms, the administrator can configure the order behavior:
   - Last-in-First-out (LIFO) mode: in this configuration, new alarms are inserted *above* older alarms of the same priority.
   - First-in-First-out (FIFO) mode; in this configuration, new alarms are inserted *below* older alarms of the same priority.
6. An alarm's Image row can appear in the Alarm Image window in one of two ways:
   - When it is generated (auto pop-up). This occurs when the alarm priority is higher than display priority.
   - When the alarm is accepted. This occurs when the alarm priority is lower than display priority.

Auto pop-up alarms

Alarms can be configured to automatically display (pop up) in the Alarm Image window, based on the alarm priority. Each user group's live and playback displays are also assigned priorities. When alarms are received with priority higher than that of the user's display, the alarm

automatically displays its alarm row in the Alarm Image window. If the Alarm Image window is not currently displayed, it automatically replaces the Live or Playback Image window on the alarm-enabled monitor.
Although auto pop-up alarms are displayed in the Alarm Image window, they are not automatically accepted. They can be displayed on multiple users' displays simultaneously. When a user accepts an auto pop-up alarm, it is removed from all other users Alarm Lists and alarm displays.

Alarm handling in case of shutdown
On a server shutdown all active alarms are preserved. The alarms are restored and reappear in the **Alarm List** window, when the system restarts.
Alarms in the state **Accepted** or **Workflow** are automatically set back to the state **Active** when the system restarts. Comments entered for alarms in the state **Workflow** are preserved.

Notice!
The alarm data is automatically saved every minute, so the maximum data loss is the data accumulated in one minute.

See also
– *Configuring the pre- and post-alarm duration for an alarm, page 313*

4.10 Adding Video IP devices from Bosch

As of BVMS version 4.5.5 and firmware version 5.70 you can add all Video IP devices from Bosch to your system. You use the **<Auto Detect>** selection for adding these devices. An encoder that you add with the **<Auto Detect>** selection, must be available in the network. The device capabilities of the encoder are retrieved and default stream qualities are applied.

Notice:
You cannot add a device with the **<Auto Detect>** selection to an NVR.

Related Topics
– Adding devices
– *Updating the device capabilities (Edit Encoder), page 220*
– *Adding an Encoder / Decoder manually, page 143*
– *Edit Encoder / Edit Decoder dialog box, page 144*

4.11 Region of Interest (ROI)

Intended use
Intended use of ROI is to save network bandwidth when zooming into a section of the camera image with a fixed HD camera. This section behaves like a PTZ camera.

Functional description
The ROI feature is only available for stream 2.
Fixed HD cameras provide ROI streams with SD resolution.
When a TCP connection is used in Live Mode, the encoder adapts the encoding quality to the network bandwidth. The best adapted quality never exceeds the configured quality of the stream.
In addition to that the encoder streams only the area selected by the user (through zooming and panning actions).
The usage of ROI has the following advantages:
– Decreased network bandwidth usage
– Decreased decoding performance required on the client

A user with a higher priority for PTZ control can take over the control of ROI and can change the image section. The recording of stream 2 has the highest priority. This means that a continuous recording of stream 2 makes the control of ROI impossible. If alarm recording of stream 2 is configured, you cannot control ROI when an event occurs that triggers alarm recording.

Limitations

You can use ROI only with fixed HD cameras.
You can use ROI only in Live Mode.
Enable TCP mode for this camera to adapt the network bandwidth. The encoder adapts the encoding quality to the network bandwidth. Whenever a second client is requesting the same stream (for example for recording), the bandwidth adaption is turned off.
Additionally the required performance of the decoding process on the client is decreased.
If stream 2 is configured to **H.264 MP SD ROI** or **H.265 MP SD ROI** on the **Cameras and Recording** page but not yet set on the encoder, the PTZ control does not work. Activate the configuration to set this property on the encoder.

See also

- *Cameras page, page 276*
- *Camera Permissions page, page 321*

4.12 Intelligent Tracking

Intended use

Intended use of Intelligent Tracking is to enable a camera to follow a selected object. You can configure whether the selection of an object is automatically or manually. The camera can be a PTZ camera or a fixed HD camera (only with ROI enabled).
The following 3 modes are available:

- **Off**: Intelligent Tracking is turned off.
- **Auto**: Intelligent Tracking turned on, the largest object is automatically selected for tracking, recommended use: rarely moving objects in the image.
- **Click**: User selects object to be tracked.

After selecting the object to be tracked, a PTZ camera moves to follow the object until this object leaves the visible area of the camera or the operator stops tracking.
A fixed HD camera with the Intelligent Tracking feature enabled defines a surrounding region close to the borders of the selected object and zooms into the image to display only the region. Then the region is moved according to the movement of the object.

Limitations

Intelligent Tracking can only be used for Live operations. You cannot use Intelligent Tracking later in recorded videos.
For a PTZ camera to be used for Intelligent Tracking , we recommend configuring to return to a defined preposition after a longer period of inactivity. Otherwise it can happen that a PTZ camera follows an automatically selected object and after the object having disappeared, the PTZ camera shows an irrelevant image.

4.13 Inactivity logoff

Intended use

Intended use of inactivity logoff is to protect an Operator Client or Configuration Client during the absence of the operator or administrator.
You can configure per user group that Operator Client shall be logged off automatically after a specified time period without activity.

For Configuration Client no user groups are available. The inactivity logoff setting is valid only for the **admin** user.
All operations with keyboard, mouse and CCTV keyboard affect the specified time period for inactivity logoff. Automatic activities of Operator Client do not affect the time period. Automatic activities of Configuration Client like firmware upload or iSCSI setup prevent the inactivity logoff.
You can also configure the inactivity logoff for a BVMS Web Client.
Short before an inactivity logoff, a dialog box reminds the user to actively prevent the inactivity logoff.
The Logbook records an occurred inactivity logoff.

Example
If a workstation is located in a public area, the inactivity logoff minimizes the risk that on an unattended workstation Operator Client is accessed by an unauthorized person.
An administrator group member shall logoff automatically after inactivity but a desk officer (operator group) might just watch video without operating the system and does not want an inactivity logoff.

Limitations
Client SDK activity does not support the inactivity logoff, this means that the activity of Client SDK does not affect the specified time period.

See also
- *Options dialog box (Settings menu), page 122*
- *Operator Features page, page 327*

4.14 Malfunction relay

Intended use
A malfunction relay is intended to switch in case of any severe system error to trigger an external alert (strobe, siren, etc.).
The user must reset the relay manually.
The malfunction relay can be one from the following list:
- BVIP encoder or decoder relay
- ADAM relay
- Intrusion panel output

Example
If something happens that severely affects the system functioning (for example a hard disk failure) or an incident occurs that endangers the security of a site (for example a failing reference image check), the malfunction relay is activated. This can for example trigger an audible alarm or can close doors automatically.

Functional description
You can configure a single relay to act as a malfunction relay. The malfunction relay gets activated automatically when an event from a set of user-defined events is triggered. Activation of a relay means that a command will be sent to the relay to close it. The subsequent “Relay Closed” event is decoupled from the command and will only be generated and received if the relay state is physically changed! For example a relay being closed before, will not send this event.

Apart from being automatically triggered by the set of user-defined events, the malfunction relay is treated like any other relay. Therefore, the user is able to deactivate the malfunction relay in Operator Client. The Web Client also allows deactivating the malfunction relay. Because the regular access permissions apply to the malfunction relay as well, all clients need to consider the permissions of the logged-on user.

See also
- *Adding a malfunction relay, page 267*
- *Malfunction Relay dialog box, page 258*

4.15 Text data

Intended use

The operator can search for text data to find the corresponding recordings. The text data must be stored in the Logbook.
Text data is delivered by systems like foyer card readers, automatic teller machines or virtual inputs. Text data contains textual transaction data like account numbers and bank routing codes.

Functional description

Text data of a device is recorded together with the corresponding video data.

Limitations

For searching recordings with text data, the text data must be configured to be stored in the Logbook.
The encoder for which you configure the recording text data function, must have firmware version 5.92 or later.
The text data of maximum 32 different devices can be recorded synchronously for one camera.
Maximum 3000 bytes of text data can be stored on an encoder per event.
If you see problems with Logbook searches, display of additional data, or CSV exports of Logbook search results, the reason can be that the additional text data contains non-printable characters, for example x00-x1F.

See also
- *Triggering alarm recording with text data, page 313*
- *Text Data Recording dialog box, page 299*

4.16 Offline Operator Client

With the feature of the Offline Operator Client the following use cases are possible:
- Operator Client continues operation for Live, Playback and Export without connection to the Management Server computer.
- If a workstation was connected once to the Management Server computer, it can log on offline any time with any user.

For Offline Mode BVMS must have version 3.0 or later.
If an Operator Client workstation is disconnected from the Management Server computer, it is possible to continue working. Some main functions are still available, for example live and playback video.
As of BVMS V5.5 an Operator Client workstation can work offline with a configuration of BVMS V5.0.5.

Notice!
When a password change on the Management Server occurs during the period when Operator Client is offline, this password change is not propagated to this Operator Client. When Operator Client is online, the user must log on using the new password.
When Operator Client is offline, the user must again use the old password for logon. This is not changed until a new configuration is activated and transferred to the Operator Client workstation.

Notice!
When a camera is called up for display in a monitor group with a workstation connected Bosch Intuikey keyboard, and the workstation is offline, the keyboard does not send an error tone.

4.16.1 Working with Offline Mode

When Operator Client is disconnected from a Management Server, a respective overlay icon is displayed in the Logical Tree on the disconnected Management Server. You can continue working with Operator Client even if the disconnection lasts longer, but some functions are not available.
If the connection to the Management Server is reestablished, a respective overlay icon is displayed.
If a new configuration on a Management Server has been activated, a respective icon is displayed in the Logical Tree on the icon of the affected Management Server and a dialog box is displayed for some seconds. Accept or refuse the new configuration.
If your Operator Client instance is scheduled to log off at a specific point in time, this logoff occurs even when the connection to the Management Server is not reestablished at this point in time.
When a user of Operator Client logs on using Server Lookup in offline state, the Server List of the last successful logon is displayed. Offline state here means that the Operator Client workstation does not have a network connection to the server containing the Server List.

Functions not available during disconnection
When disconnected from Management Server the following functions are not available in Operator Client:

- Alarm List:
  This includes handling alarms. The alarm list is empty and will automatically be filled on reconnection.
- Allegiant:
  The trunk line handling is not available. In earlier versions, Allegiant cameras were automatically closed with a message-box when a trunk line handling was unavailable. With BVMS V3.0 we will show a more user friendly Image pane informing the user about the impossibility to display this camera right now.
- MG:
  It is not possible to drag cameras on the MG control. The control is disabled and will automatically be enabled on reconnection.
- PTZ priorities:
  Without a connection to Management Server , an offline Operator Client can connect a PTZ camera as long as the PTZ camera itself is not locked. The dome priorities will automatically be updated on reconnection.
- Input:
  Input cannot be switched.

- Logbook:
  The Logbook is not available and cannot be opened. An opened Logbook search window is not closed automatically. Existing search results can be used and exported.
- Operator Client SDK:
  Operator Client SDK functions with IServerApi cannot be processed.
  Creating a RemoteClientApi is not possible.
  Some methods that are only available at client API do not work, for example ApplicationManager (try GetUserName()).
- Password change:
  The operator is not able to change his password.
- Relay:
  Relays cannot be switched.
- Server Script:
  The server methods of the IServerApi will be processed but cannot be sent to the Client which are:
  - AlarmManager
  - AnalogMonitorManager
  - CameraManager
  - CompoundEventManager
  - DecoderManager
  - DeviceManager
  - DomeCameraManager
  - EventManager
  - InputManager
  - LicenseManager
  - Logbook
  - MatrixManager
  - RecorderManager
  - RelayManager
  - ScheduleManager
  - SendManager
  - SequenceManager
  - VirtualInputManager
- State overlays:
  No state overlays of cameras, inputs or relays are available.

States of Operator Client

A BVMS Operator Client gives you a visual and textual feedback of its states.
Following Operator Client states are possible:

-
  The Operator Client is connected to the Management Server.
-
  The Operator Client is not connected to the Management Server. One reason can be a physical disconnection from the Management Server to the network.
-

This state can only be displayed after a reestablished connection to the Management Server. All affected functions are back, but the configuration of the Operator Client is outdated due to a newer configuration available in the system. Log on again to update the configuration.

–

This state icon is displayed when the Management Server has an earlier BVMS version than the Operator Client workstation.

Device state overlay

The device states (recording dot, too noisy, too dark, ...) are processed by the Management Server. On disconnection between Client and Server the states cannot be updated in the Client. A new state overlay will give you a visual feedback that all device states are not available at the moment. If the client has an established connection to the server again, the state overlays are updated automatically.

– State unknown

The state overlay of a device in the Logical Tree or on a map when client is disconnected from the Management Server computer.

Reasons for disconnection

Reasons for disconnection between Operator Client and Management Server can be:

- Physical connection is broken.
- Password of logged on user has changed during offline time.
- Management Server has given away floating workstation license to another online Operator Client while the now disconnected Operator Client was offline.
- Operator Client and Management Server have different versions (Management Server earlier than version 5.5).

4.17 Version independent Operator Client

For Compatibility Mode both Operator Client and Management Server must have a version later than 5.5.

A user of Operator Client can successfully log on to a Management Server where a previous software version is running.

If the server provides a newer configuration than available on the Operator Client workstation, this configuration is automatically copied to the Operator Client workstation. The user can decide to download the new configuration.

Operator Client provides a reduced feature set and is connected to this Management Server. The following Management Server related features are available after logon to a Management Server with a previous version:

- User preferences
- Start manual recording
- Display of device states
- Toggling relay states
- Searching the Logbook

  Search for events is not possible.
- Server Lookup
- Remote export

4.17.1 Working with Compatibility Mode

This feature is available in versions later than 5.5.

A BVMS Operator Client gives you a visual and textual feedback of its states.

Following Operator Client states are possible:

-

  The Operator Client is connected to the Management Server.

-

  The Operator Client is not connected to the Management Server. One reason can be a physical disconnection from the Management Server to the network.

-

  This state can only be displayed after a reestablished connection to the Management Server. All affected functions are back, but the configuration of the Operator Client is outdated due to a newer configuration available in the system. Log on again to update the configuration.

-

  This state icon is displayed when the Management Server has an earlier BVMS version than the Operator Client workstation.

4.18 ONVIF event mapping

Intended use

Intended use is the mapping of ONVIF events to BVMS events. ONVIF events can then trigger BVMS alarms and recording.

You can define default event mappings valid only for a specific ONVIF device, for all ONVIF devices of the same manufacturer and model, or for all ONVIF devices of the same manufacturer. Default event mappings are automatically assigned to all affected ONVIF encoders that are added using the BVMS Scan Wizard or are added manually.

When you add an ONVIF encoder to the BVMS configuration without a connection to this ONVIF encoder, no event mappings are assigned. You can update such an ONVIF encoder with event mappings from an ONVIF encoder of the same manufacturer and/or model that you already have added.

You define event mappings specific for each of the following sources:

- ONVIF encoder
- Cameras of this ONVIF encoder
- Relays of this ONVIF encoder
- Inputs of this ONVIF encoder

Example

In an ONVIF camera a motion detection event occurs. This event shall trigger a **Motion Detected** event in BVMS.

To achieve this, you configure for this ONVIF camera:

- ONVIF topic (`MotionDetection`)
- ONVIF data item (`motion`)
- ONVIF data type (`boolean`)
- ONVIF data value (`true`)

Note: It is not sufficient to only configure the **Motion Detected** event. Please configure also the **Motion Stopped** event. You always must configure a pair of events.

Import or export of a Mapping Table

You can export a Mapping Table on a computer where you have created it and import this Mapping table on another computer where the required mapping table is not available.

Troubleshooting

You can create log files for troubleshooting.

See also

- *Configuring an ONVIF mapping table, page 237*
- *Enabling logging for ONVIF events, page 359*
- *ONVIF Encoder Events page, page 233*

4.19 Viewing modes of a panoramic camera

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

The following viewing modes are available:

- Circle view
- Panorama view
- Cropped view

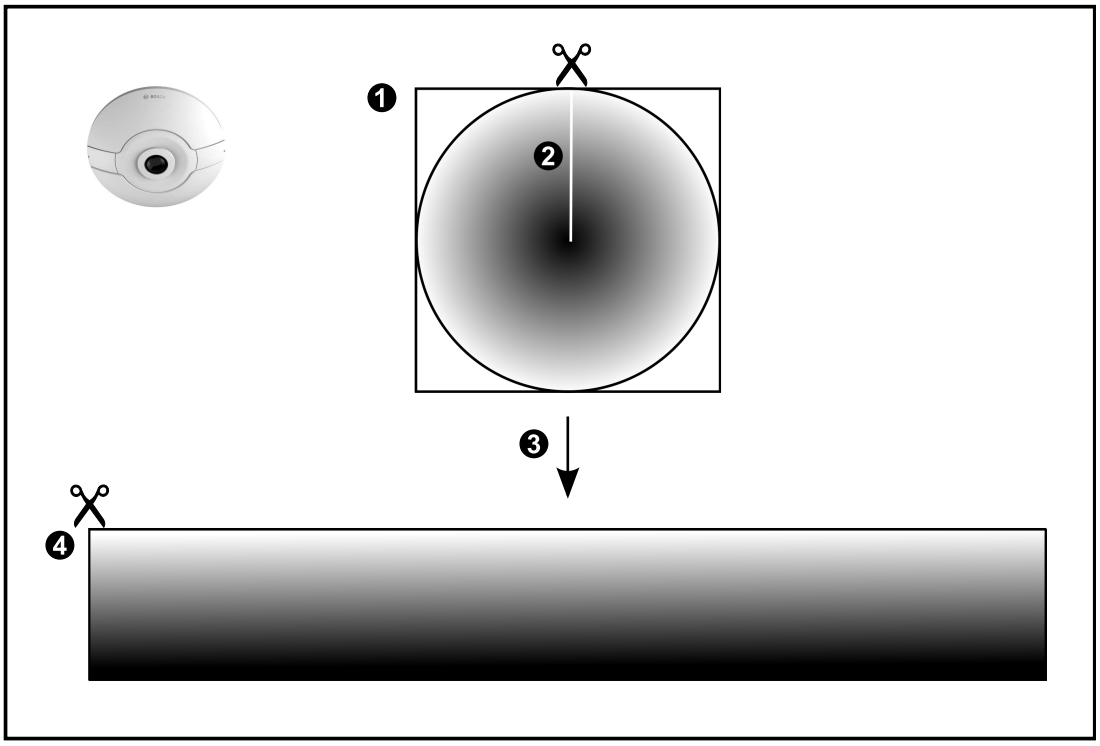
Panorama and cropped view modes are created by the dewarping process in BVMS. Edge dewarping is not used.

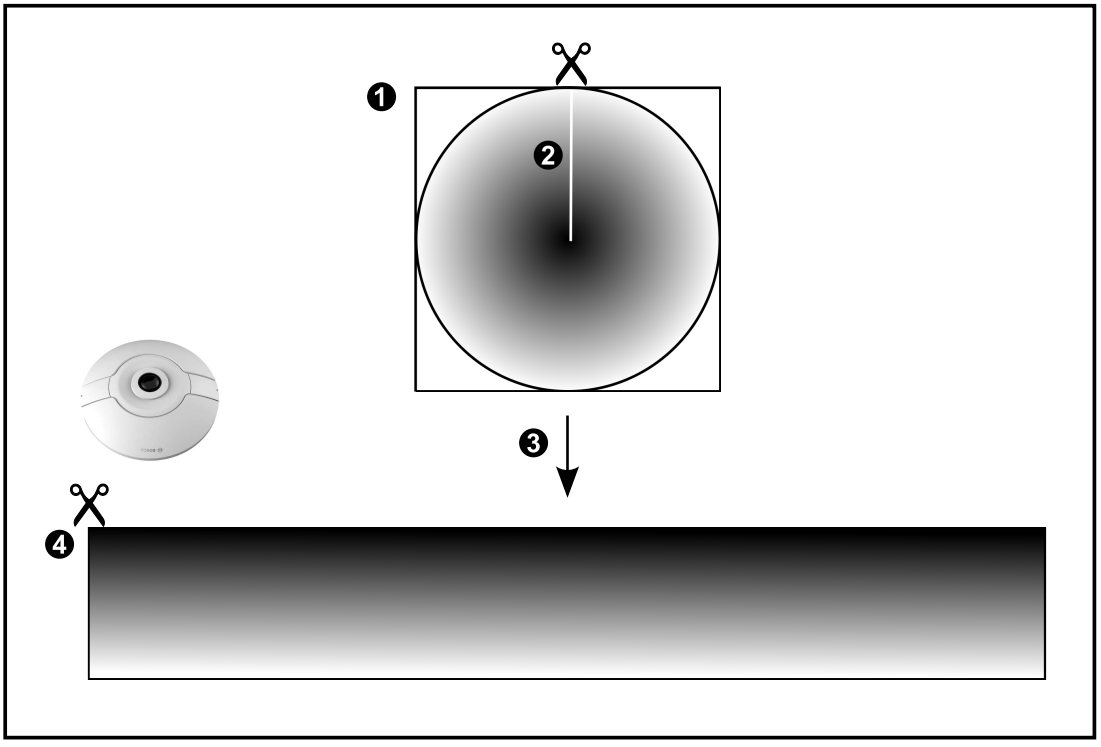
The administrator must configure the mounting position of a panoramic camera in Configuration Client.

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

4.19.1 360° panoramic camera - floor- or ceiling mounted

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

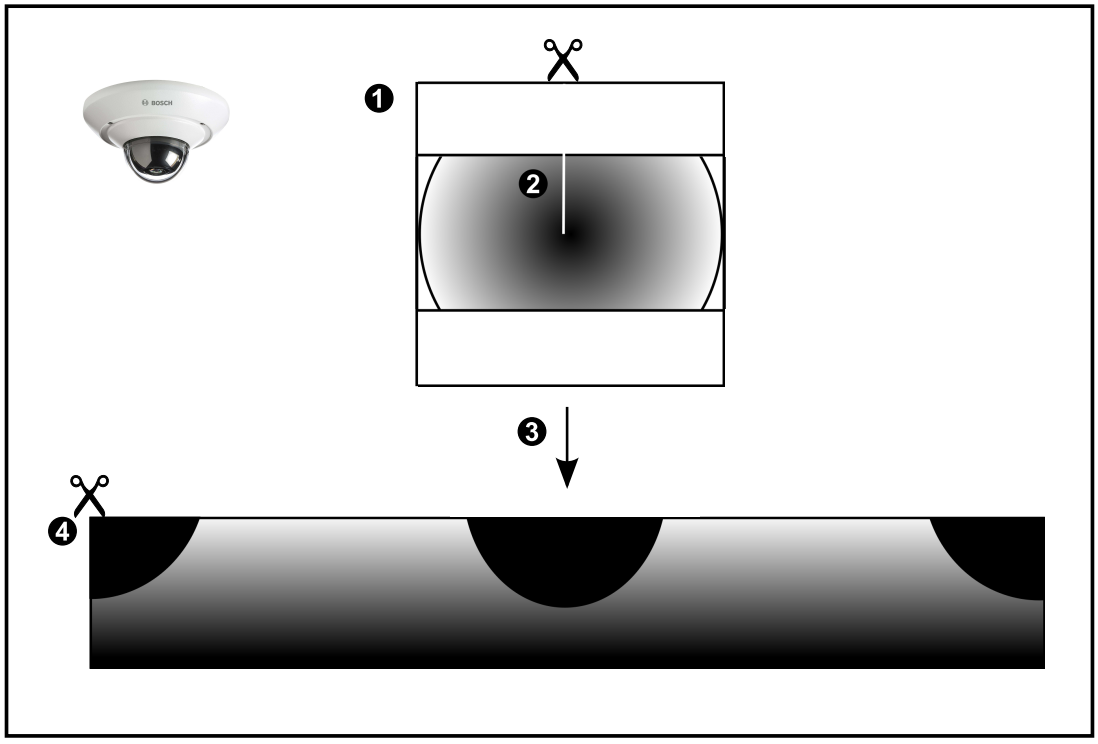


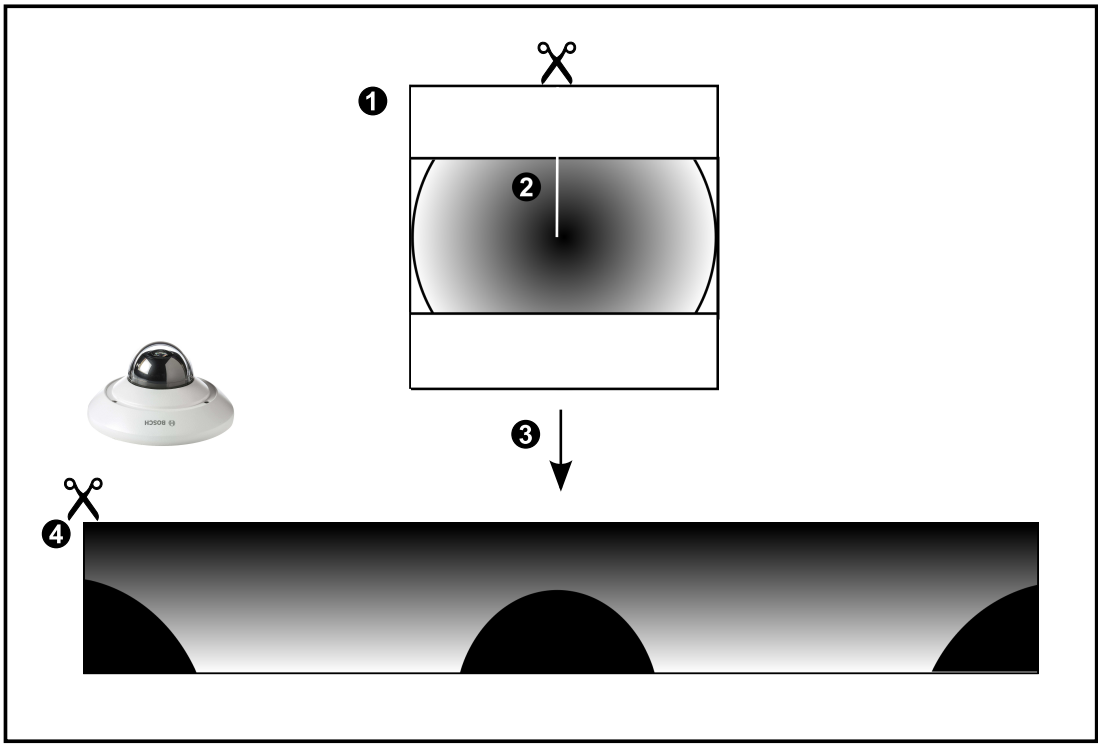


1	Full circle image	3	Dewarping
2	Snipping line (operator can change its position when not zoomed in)	4	Panorama view

4.19.2 180° panoramic camera - floor- or ceiling mounted

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

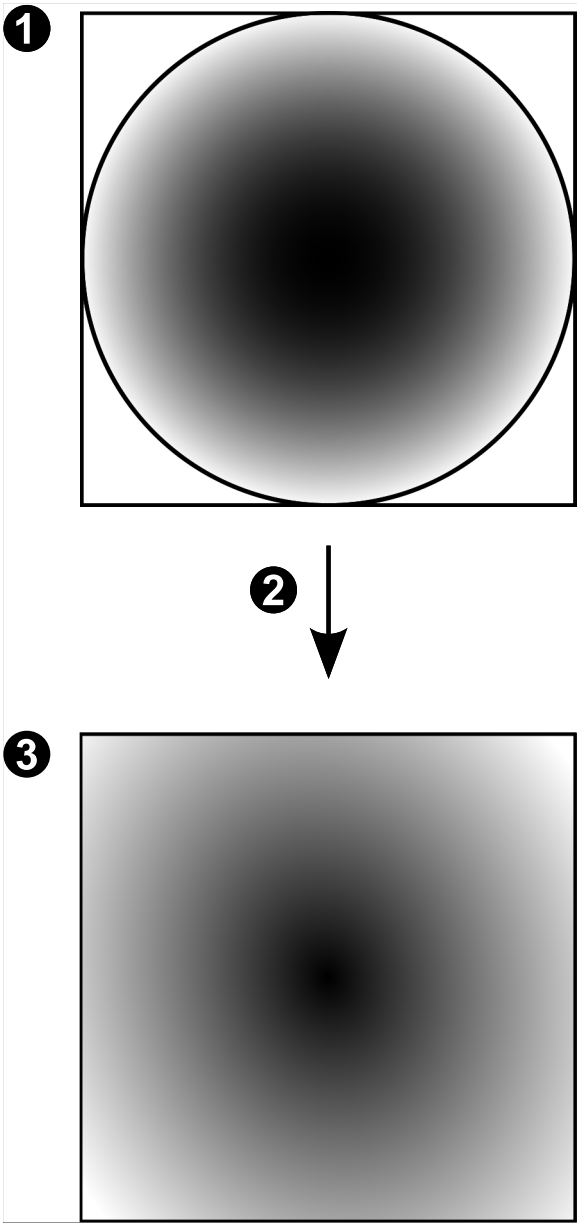




1	Full circle image	3	Dewarping
2	Snipping line (operator can change its position when not zoomed in)	4	Panorama view

4.19.3 360° panoramic camera - wall mounted

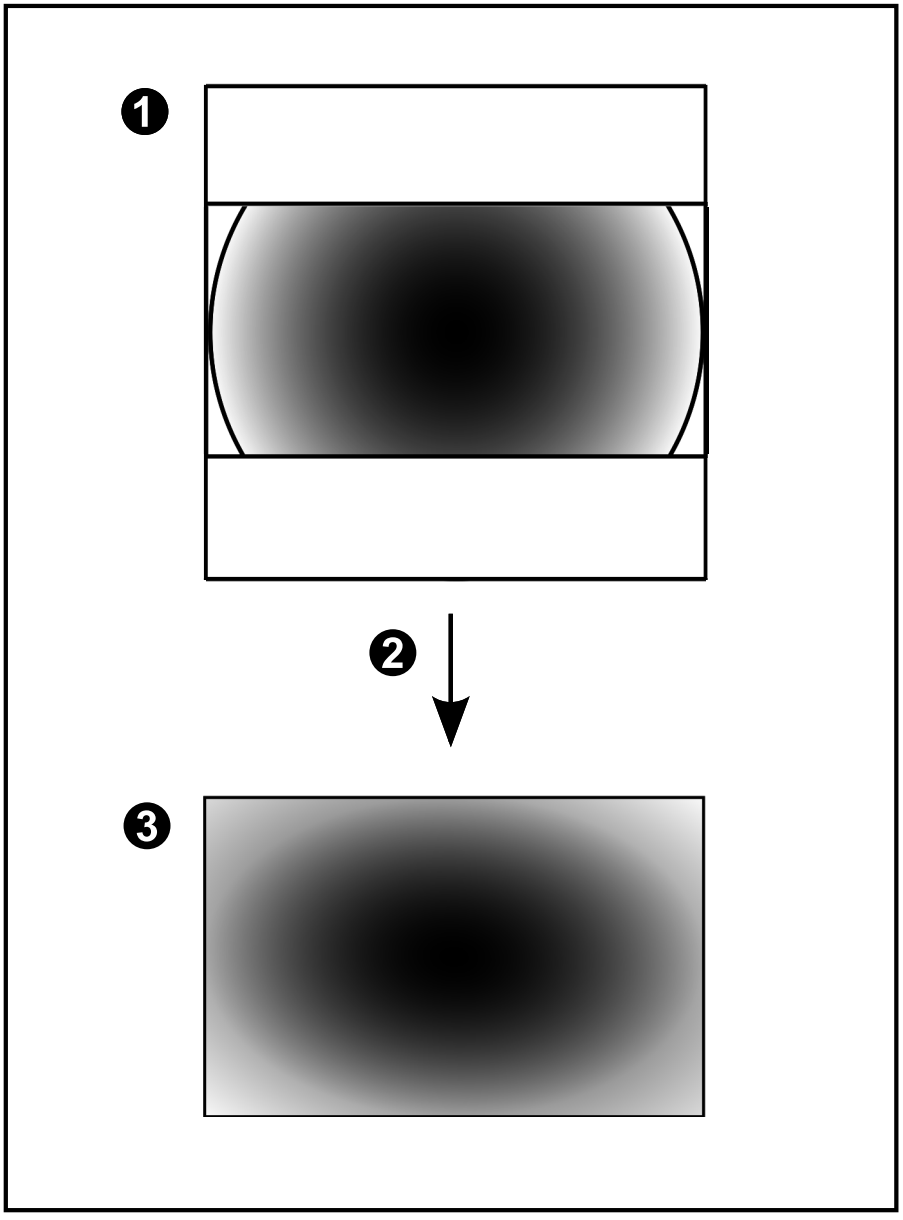
The following figure illustrates the dewarping of a 360° camera which is wall mounted.



1	Full circle image	3	Panorama view
2	Dewarping		

4.19.4 180° panoramic camera - wall mounted

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

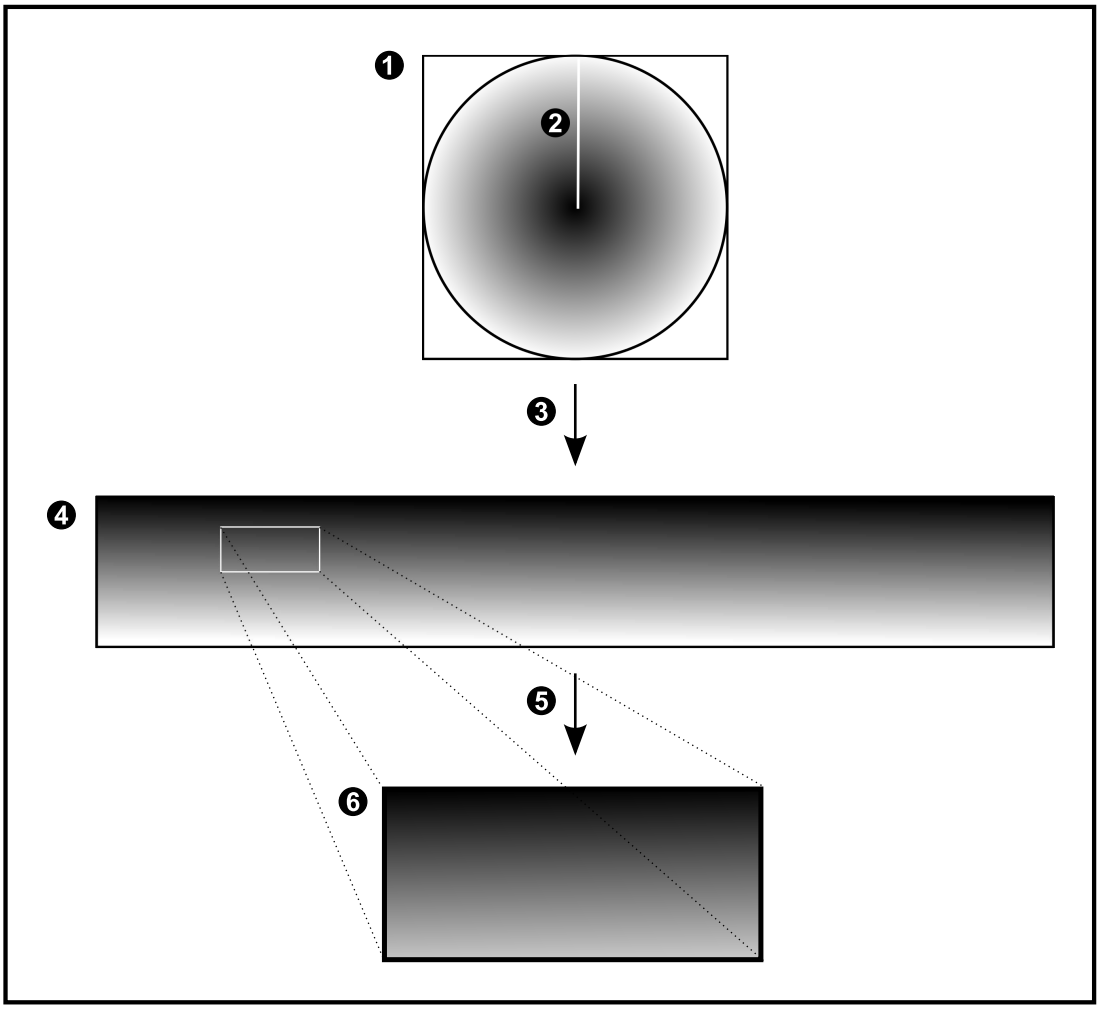


1	Full circle image	3	Panorama view
2	Dewarping		

4.19.5 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

4.20 Verification of authenticity

The user of Operator Client can verify the authenticity of recordings. The authenticity of exports is automatically verified.
The administrator must follow these steps for ensuring an unbroken certificate chain. For large systems (>30 cameras) we recommend the following procedure:
– Let your issuing certificate authority (CA) issue a certificate for each encoder.
– Upload the issued certificate (including private key) in a secure way on each encoder.
– Install the CA certificate on the Operator Client workstations where you want to perform authenticity verification or on other computers where you want to perform exports.

For small systems (<30 cameras) we recommend the following procedure:
– Download the `HTTPS Server` certificate from each encoder.
– Install these certificates on the Operator Client workstations where you want to perform authenticity verification.

Ask the IT support of your company for details.
For activating the secure verification of authenticity, the administrator must perform the following steps:
– Activate the authentication on each desired camera.
– For large systems: Upload and assign the appropriate certificate to each desired camera.
– For small systems: Download a certificate from each encoder. Install the certificates allowing verification on a workstation.

Limitations
Firmware version 6.30 or later is required.
We recommend verifying the authenticity of maximum 4 cameras at the same time.
The user of Operator Client cannot verify the authenticity of live video.
Note: Do not change the certificate when recording is running. If you have to change the certificate, first stop the recording, change the certificate, and start recording again.
For verifying the authenticity of a recording, this recording is replayed in a background process with maximum speed. In networks with low bandwidth the playback can be slow. The verify process can then take as long as the time period selected for verifying. Example: You select a time period of 1 hour. The verifying process can last up to 1 hour.
The user can only verify that a recording is authentic. If the verification process is not successful, this does not necessarily mean that the video has been manipulated. Many other reasons can be responsible for the failure, for example a manual deletion. The user of Operator Client cannot distinct between an intended change of the recording or fraudulent manipulation.
Video authentication deals solely with methods of validating the authenticity of video. Video authentication does not deal with the transmission of video, or data, in any way.
The watermark feature for verifying authenticity in earlier BVMS versions is replaced. The new authenticity verification is automatically available after upgrade to the latest BVMS version. Authenticity checks that were successful in the past, can now not be verified because these recordings do not contain the required extended information.
Verifying authenticity is not supported in the following cases:
– Transcoding
– Local recording
– VSG
– Digital Video Recorder
– Bosch Recording Station
– ANR

See also
- *Configuring the authentication, page 222*
- *Uploading a certificate, page 222*
- *Downloading a certificate, page 223*
- *Installing a certificate on a workstation, page 223*

4.21 SSH Tunneling

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

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

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

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

4.22 Multipathing

BVMS provides multipathing for dual controller systems. Multipath is a fault-tolerance technique that defines more than one physical path between the camera and its iSCSI storage devices through redundant network connections. When using mulitpathing, recording of video data and replaying video data is possible even in case of an iSCSI controller failure.

Prerequisites and restrictions
- Netapp E2800 dual controller iSCSI unit is installed.
- Firmware 6.43 enables devices recording to E2800 to use alternative paths.
- VRM 3.71 to monitor and log devices with multipathing are enabled.
- Two physical iSCSI ports are configured per controller: either 2x2 RJ45 or 2x2 optical.
- Link speed needs to be 10 Gbit/s in order to achieve full performance.
- The Dual-Simplex mode used in E2700 is not supported anymore.

For more details on installation of DSA E2800 Full Duplex see Installation Manual DSA E-Series E2800.

5 Supported hardware

Notice!
Do not connect a device to more than one BVMS! This can lead to recording gaps and other undesired effects.

You can connect the following hardware to BVMS:

- Mobile video clients like iPhone or iPad via DynDNS
- Various IP cameras. encoders and ONVIF cameras (live only or via Video Streaming Gateway)
  Connected via network
- Live only encoders with local storage
  Connected via network
- iSCSI storage devices
  Connected via network
- VIDOS NVR computer
  Connected via network
- Analog cameras
  Connected to encoders, BRS/DiBos devices
- Decoders
  Connected via network
- Monitors
  Connected to a decoder, to a Bosch Allegiant matrix, to a BVMS Client workstation
- BRS/DiBos devices (see the data sheet for BVMS for supported software versions)
  Connected via network
- Bosch Allegiant matrix (Firmware version: 8.75 or greater, MCS version: 2.80 or greater)
  Connected to a COM port of the Management Server or to a remote computer and to an IP encoder on the network.
- KBD-Universal XF keyboard
  Connected to a USB port of a BVMS workstation.
- Bosch IntuiKey keyboard
  Connected to the COM port of a BVMS workstation (Firmware version: 1.82 or greater) or to a hardware decoder (VIP XD).
  If you connect the keyboard to a workstation, the user can control the complete system with the keyboard. If you connect the keyboard to a VIP XD decoder, the user can only control monitors with the keyboard.
- SMS device
  Connected to a COM port of the Management Server
- SMTP E-mail server
  Connected via network
- POS
  Connected via network
- ATM
  Connected via network
- Network monitoring device
  Connected via network
- I/O modules
  Connected via network
  Only ADAM devices are supported.

All devices connected via network are connected to a switch. The computers of the BVMS are also connected to this device.

5.1 Installing hardware

BVMS supports the following hardware components:

- KBD-Universal XF keyboard
- Bosch IntuiKey keyboard
- Bosch Allegiant matrix with cameras and monitor: Connected to a COM port of one of the computers of the network and to IP encoders connected to the network
- Encoders with analog cameras
- Local storage encoders
- IP cameras and IP AutoDomes
- Monitors connected to a decoder (monitor groups for alarm processing are possible)
- DiBos Systems with cameras
- DVR Systems with cameras
- ATM / POS devices
- I/O modules
  Only ADAM devices are supported.

5.2 Installing a KBD Universal XF keyboard

Notice!
Refer to the Instructions Manual delivered with your KBD-Universal XF keyboard available on the online product catalog.

More information
For more information, software downloads, and documentation, visit www.boschsecurity.com and go to the respective product page.
You can connect the following hardware to BVMS:

- Mobile video clients like iPhone or iPad via DynDNS
- Various IP cameras. encoders and ONVIF cameras (live only or via Video Streaming Gateway)
  Connected via network
- Live only encoders with local storage
  Connected via network
- iSCSI storage devices
  Connected via network
- VIDOS NVR computer
  Connected via network
- Analog cameras
  Connected to encoders, BRS/DiBos devices
- Decoders
  Connected via network
- Monitors
  Connected to a decoder, to a Bosch Allegiant matrix, to a BVMS Client workstation
- BRS/DiBos devices (see the data sheet for BVMS for supported software versions)
  Connected via network
- Bosch Allegiant matrix (Firmware version: 8.75 or greater, MCS version: 2.80 or greater)
  Connected to a COM port of the Management Server or to a remote computer and to an IP encoder on the network.

5.3 Connecting a Bosch IntuiKey keyboard to BVMS

This chapter provides background information on configuring a Bosch IntuiKey keyboard.

5.3.1 Scenarios for Bosch IntuiKey keyboard connections

You can connect a Bosch IntuiKey keyboard to the COM port of a BVMS workstation (scenario 1) or to a hardware decoder (e.g. VIP XD, scenario 2).
If you connect the keyboard to a BVMS workstation, you can control the complete system. If you connect the keyboard to a decoder, you can only control the analog monitors of the system.
If you connect the keyboard to an Enterprise Operator Client, you can control the cameras of a specific Management Server by first pressing the server key to type in the number of this server and then type the camera number.

Notice!
For connecting the Bosch IntuiKey keyboard with a BVMS workstation, use the specified Bosch cable.
For connecting the Bosch IntuiKey keyboard with a VIP XD decoder, you need a cable which connects a serial COM port of the keyboard with the serial interface of the decoder. See Connecting a CCTV keyboard to a decoder for connections.

Bosch IntuiKey keyboard connected to a BVMS workstation

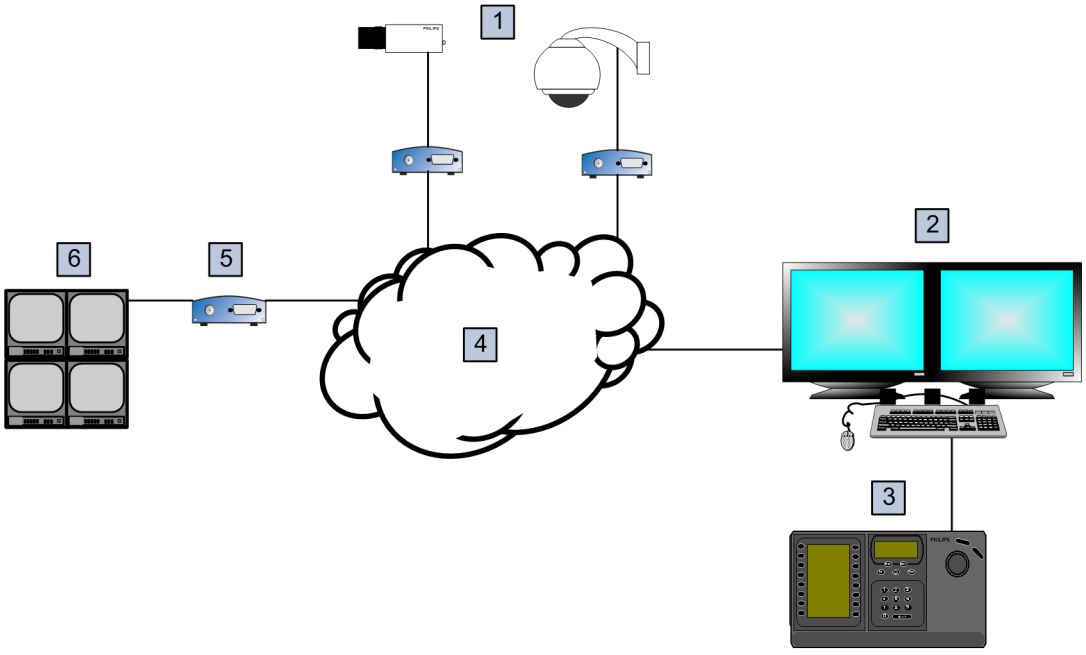


Figure 5.1: Scenario 1: Bosch IntuiKey keyboard connected to a Bosch Video Management System workstation

1	Various cameras connected to network via encoders
2	BVMS workstation
3	Bosch IntuiKey keyboard
4	BVMS network
5	Decoder
6	Monitors

Bosch IntuiKey keyboard connected to a decoder

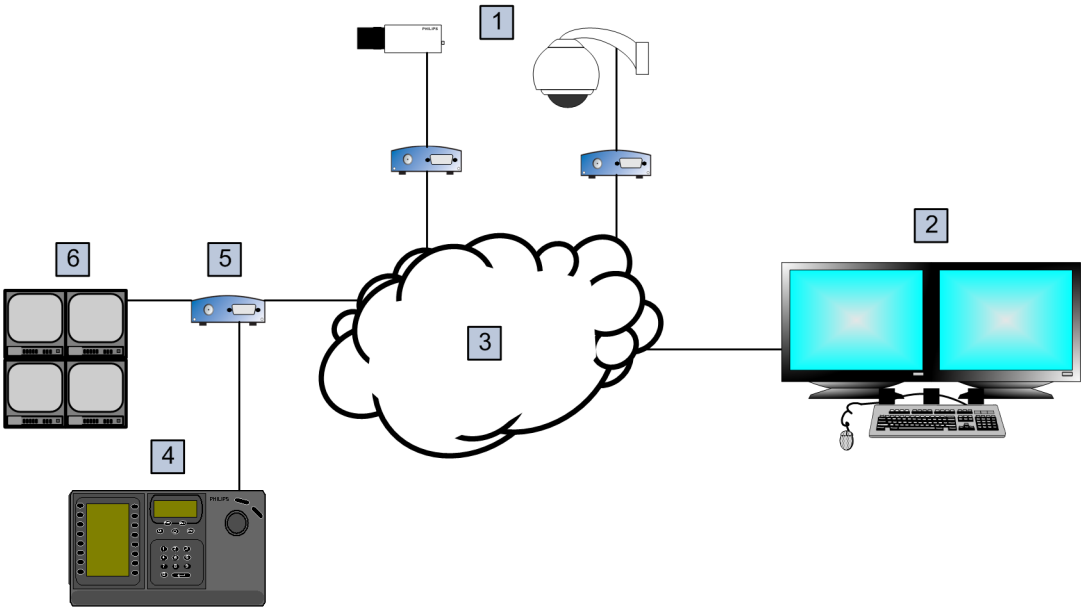


Figure 5.2: Scenario 2: Bosch IntuiKey keyboard connected to a decoder

1	Various cameras connected to network via encoders
2	BVMS workstation
3	BVMS network
4	Bosch IntuiKey keyboard
5	Decoder
6	Monitors

Follow these references to get detailed information on the available windows:

– *Assign Keyboard page, page 162*

Follow these references to get detailed information on the available step-by-step instructions:

– *Configuring a Bosch IntuiKey keyboard (settings page) (workstation), page 140*
– *Configuring a Bosch IntuiKey keyboard (decoder), page 148*
– *Configuring a decoder for use with a Bosch IntuiKey keyboard, page 148*

See also

– *Assign Keyboard page, page 162*

5.3.2 Connecting a Bosch IntuiKey keyboard to a decoder

Configuring the decoder

See *Configuring a decoder for use with a Bosch IntuiKey keyboard, page 148* for details.

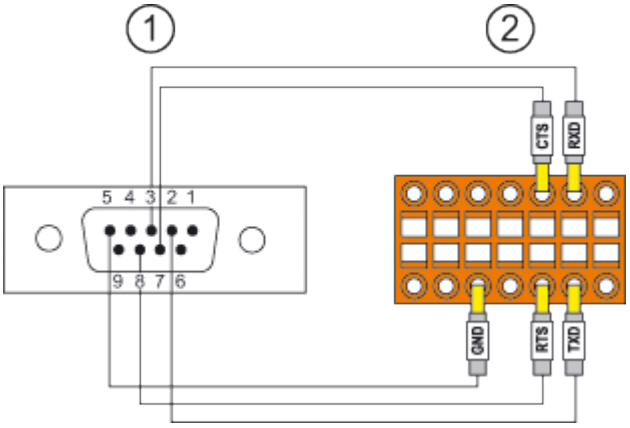
Connections between COM port and VIP XD decoder

The following table lists the connections between an RS232 adapter and a serial interface of a VIP XD decoder:

RS232 adapter	Serial interface of a VIP XD decoder
1	

RS232 adapter	Serial interface of a VIP XD decoder
2	TX
3	RX
4	
5	GND
6	
7	CTS
8	RTS
9	

The following illustration shows the pinout of a standard RS232 adapter (1) and the pinout of the decoder's serial adapter (2):



5.3.3 Updating Bosch IntuiKey keyboard firmware

1. On any PC, install the IntuiKey downloader.
2. Start IntuiKey Firmware Upgrade Utility.
3. Connect the keyboard with a valid serial cable (refer to Bosch Support if such a cable is not available) to this PC.
4. On the keyboard, press Keyboard Control softkey, then Firmware Upgrade.
5. Enter the password: 0 and 1 simultaneously.
   The keyboard is in bootloader mode.
6. On the PC, click Browse to select the firmware file: for example kbd.s20
7. Set the COM port.
8. Click the Download button to download the firmware.
   On the keyboard display, Programming is displayed.
   Do not press the Clr key now. Otherwise the keyboard is not usable after restart (see Notice below).
9. Click Browse to select the language: for example 8900_EN_..82.s20
   On the keyboard display, Programming is displayed.
10. Close IntuiKey Firmware Upgrade Utility.
11. On the keyboard, press Clr key to exit.
    The keyboard restarts. Wait some seconds until the menu for selecting the keyboard language appears.
12. Select the desired language with a softkey.
    The default start display appears.

Notice!
For starting the bootloader mode directly, you can unplug the power supply from the keyboard, press 0 and 1 simultaneously, plug In the power supply again, release 0 and 1.

5.4 Connecting Bosch Allegiant Matrix to BVMS

The BVMSAllegiant Matrix interface provides seamless access to analog matrix cameras in the Operator Client interface. Allegiant cameras appear almost identical to IP cameras. The only difference is a small grid symbol on the camera to indicate that it is a Allegiant camera. You can display cameras using the same tasks as for IP cameras. They are included both in the Logical Tree and the site maps, and users can add them to their Favorites Trees. In-video-window control for Allegiant-connected PTZ cameras is supported, and you can easily display Allegiant cameras on monitors connected to IP decoders.
BVMS provides an interface to the matrix switch via the Allegiant MCS (Master Control Software) application). The MCS, in this case, runs invisibly in the background. This software provides an efficient, event-driven interface to the Allegiant. It provides fast, real-time event response from the Allegiant to BVMS. So, for example, if a defective coax cable results in video loss in the Allegiant, an immediate notification is sent to BVMS. Also, you can program BVMS to respond to Allegiant alarms.

5.4.1 Bosch Allegiant Connection Overview

To achieve a connection between BVMS and an Allegiant matrix switching system, you configure a control channel between the BVMS and the Allegiant matrix.
Two scenarios are possible:

- Local connection
  The Management Server controls the Allegiant matrix.
- Remote connection
  A dedicated Bosch Allegiant PC connected to the network controls the Allegiant matrix.

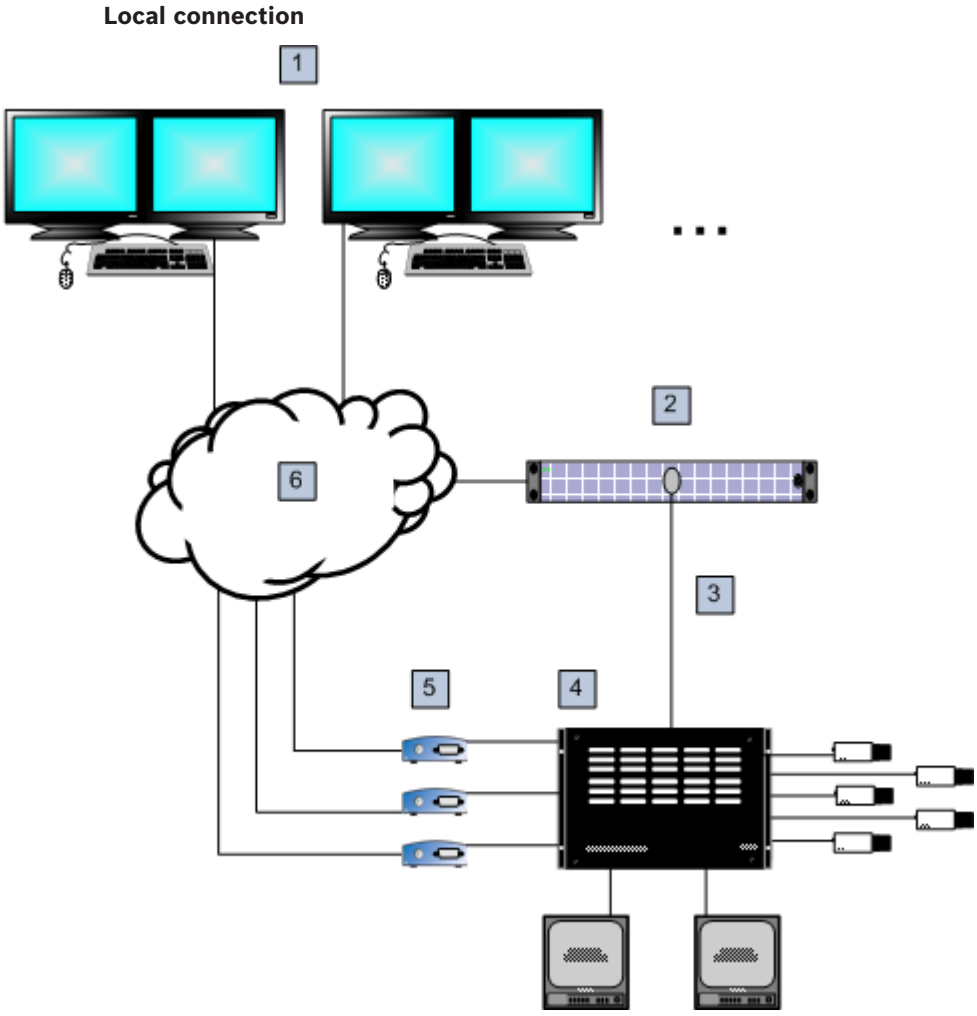


Figure 5.3: Bosch Video Management System local connection to a Bosch Allegiant matrix switch

1	BVMS Client workstations
2	Management Server with Master Control Software
3	RS-232 connection
4	Allegiant matrix
5	encoders
6	Network

Remote connection

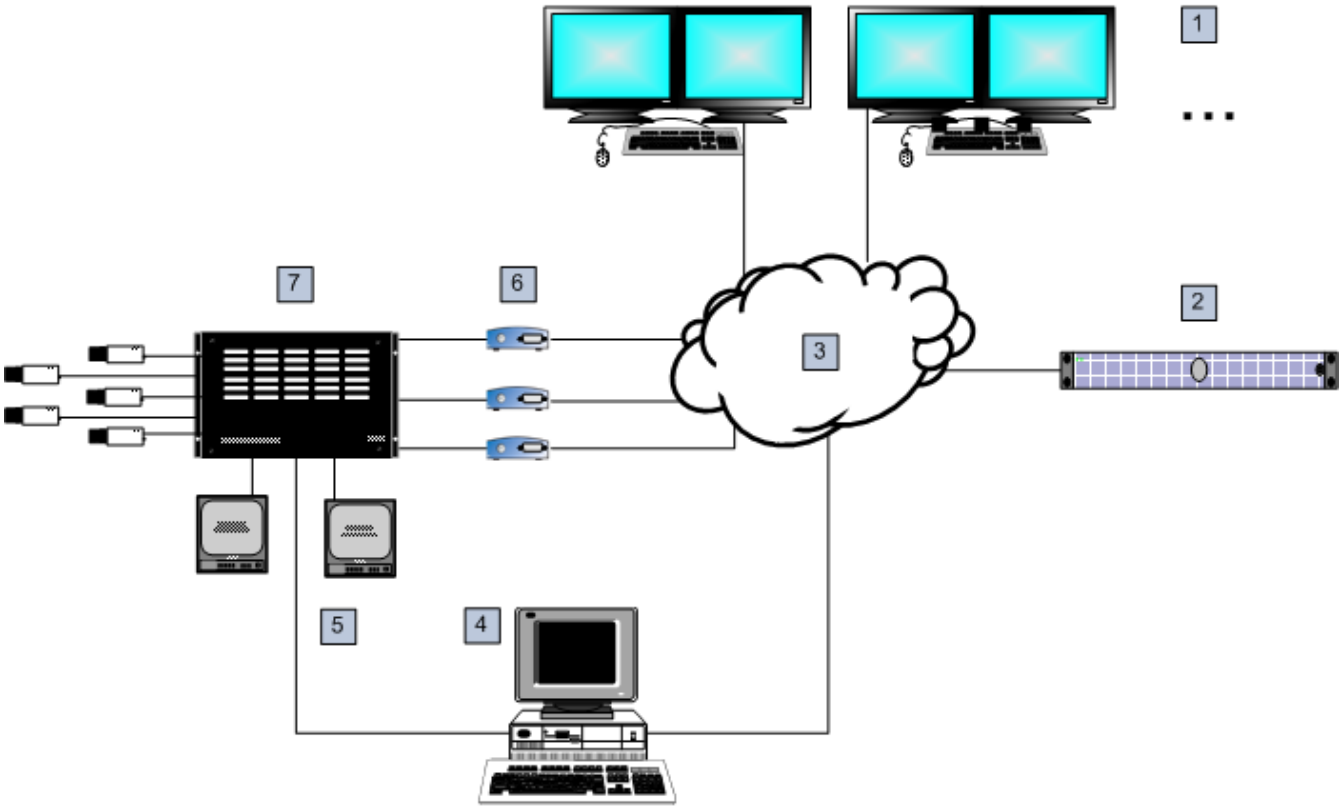


Figure 5.4: Bosch Video Management System remote connection to a Bosch Allegiant matrix switch

1	BVMS Client workstations
2	Management Server with Master Control Software
3	Network
4	Allegiant PC with Master Control Software
5	RS-232 connection
6	encoders
7	Allegiant matrix

5.4.2 Configuring the control channel

Perform the following tasks to configure the control channel:

- Wiring
- Installing the software
- Creating Allegiant configuration file
- Adding the Allegiant matrix to BVMS
- Configuring user names

Wiring

To configure the control channel between BVMS and the Allegiant matrix, connect one PC through an RS-232 serial port to the Allegiant's console port (use the specified Bosch cable for connection). This can be the BVMS Management Server, or any other PC on the network.

Installing Allegiant Master Control Software

1. Stop the Management Server service if running (**Start** > **Control Panel** > **Services** > Right-click BVMS Management Server > **Stop**)
2. Install the Allegiant Master Control Software on the Management Server and on the Allegiant PC (if present).
3. On an remote Allegiant PC configure it to start the Allegiant Network Host program (ld_alghw.exe) on startup. This starts the necessary Allegiant services to allow other PCs on the network to access the Allegiant. The software runs invisibly. It is not necessary to have a dongle attached to this computer.
   To have the service started on computer startup automatically, copy a link to ld_alghw.exe to the Startup folder of your computer.

Creating a Bosch Allegiant configuration file

1. Using the Allegiant Master Control Software, create a Allegiant configuration file that specifies the computer attached to the Allegiant matrix. For this task, the Master Control dongle is required.
2. On the Transfer menu, click Communication Setup. In the Current Host list, enter the DNS name of the computer connected to the Allegiant matrix, and enter the serial port parameters (COM port number, baud rate, etc.) of the Allegiant-connected serial port. This allows the Master Control Software on the Management Server or PC to go on-line with the Allegiant system. If this is not successful, ensure that either the Master Control Software or the Allegiant Network Host program is running on the computer attached to the Allegiant matrix, and that the network security is configured to allow remote access to this computer.
3. On the Transfer menu, click Upload. Select all tables and click Upload. To save the configuration file, select a directory.
4. Exit the Master Control Software.

Adding the Bosch Allegiant matrix to BVMS

1. Start the BVMS Management Server service, start the Configuration Client, and add the Allegiant device by adding this configuration file (see Adding a device for the step-by-step instruction).
2. Ensure that the Allegiant Master Control Software configuration file used in BVMS matches the current Allegiant configuration.
   BVMS runs the required components of Master Control Software invisibly in the background.

Configuring the user name for logging on the Allegiant services

If the Allegiant matrix is connected to a PC in the network and not to the Management Server, ensure that the Allegiant services on this PC and on the Management Server log on with the same user account. This user must be member of an administrators group.

Further notes in the documentation

Follow these references to get detailed information on the available windows:

– *Matrix Switches page, page 137*

Follow these references to get detailed information on the available step-by-step instructions:

– *Configuring a Bosch Allegiant device, page 137*

See also

– *Matrix Switches page, page 137*

5.4.3 Bosch Allegiant Satellite System Concept

The Allegiant matrix switch allows multiple Allegiant systems to be tied together using the Satellite concept. In this case, multiple Allegiant systems can appear to the BVMS as one large system, providing access to all cameras on all systems.
In an Allegiant Satellite System, monitor outputs of a slave Allegiant are tied to video inputs on the master Allegiant. This connection is called a trunk line. In addition, a control channel is established between the master and the slave. When a camera from a slave Allegiant is requested from the master Allegiant, a command is sent to the slave instructing it to switch the requested camera to a trunk line. At the same time, the master Allegiant switches the trunk input to the requested master Allegiant monitor output. This completes the video connection from the requested slave camera to the desired master monitor.

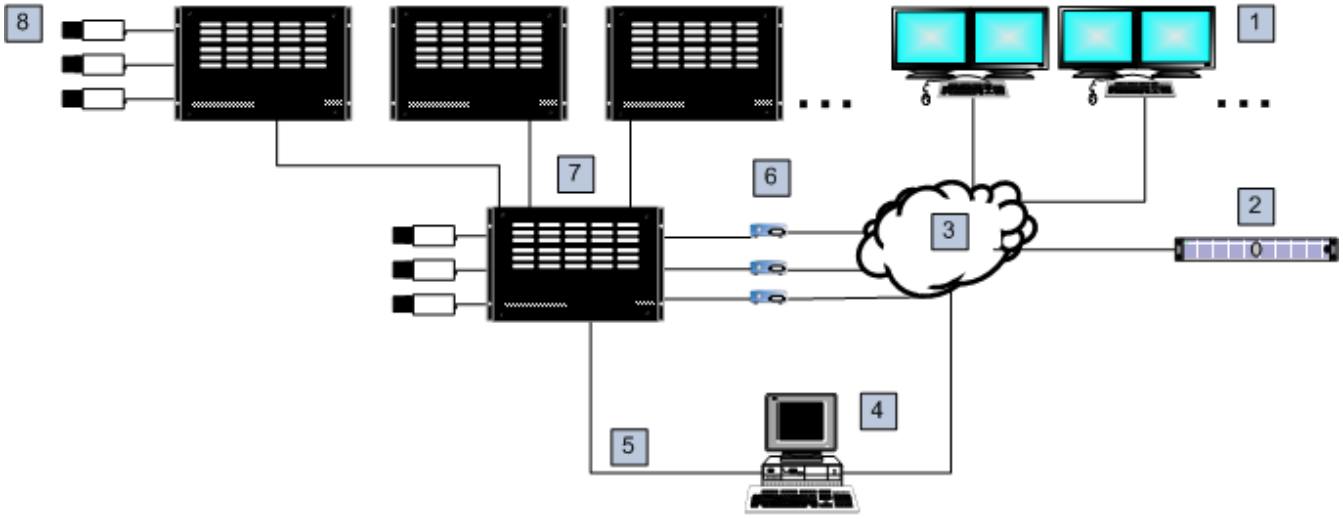


Figure 5.5: Bosch Allegiant system extended with Satellite switches

1	BVMS Client workstations
2	Management Server with Master Control Software
3	Network
4	Allegiant PC with Master Control Software
5	RS-232 connection
6	encoders
7	Allegiant matrix
8	Allegiant Satellite matrix

You can apply the Satellite concept such that an Allegiant can be both a master and a slave. In this way, each Allegiant can view cameras from the others. It is only necessary to connect trunk lines and control lines in both directions, and to properly configure the Allegiant tables. The concept can be further extended, with no practical limit, to multiple Allegiant systems. An Allegiant can have many slaves, and it can be a slave to many masters. You can program the Allegiant tables to allow or disallow user access to camera views as required by site policies.

5.5 Allegiant CCL commands supported in BVMS

To use the CCL commands you need the CCL User Guide. This manual is available in the Online Product Catalog in the document section of each LTC Allegiant Matrix.

Supported command	Description	Remarks
Switching/Sequence		
LCM	Switch Logical Camera to Monitor	LCM, LCM+ and LCM- are equivalent.
LCMP	Switch Logical Camera to Monitor with Pre-position Call	
MON+CAM	Switch Physical Camera to Monitor	
MON-RUN	Run Sequence by Monitor Number	
MON-HOLD	Hold Sequence by Monitor Number	
SEQ-REQ	Sequence Request	
SEQ-ULD	Sequence Unload	
Receiver/Driver		
R/D	Basic Control commands	
REMOTE-ACTION	Simultaneous Pan/Tilt/ Zoom Control commands	
REMOTE-TGL	Toggle Pan/Tilt/Zoom Control commands	
PREPOS-SET	Set Pre-position	
PREPOS	Call Pre-position	
AUX-ON AUX-OFF	Auxiliary Control commands – Auxiliary On – Auxiliary Off	
VARSPEED_PTZ	Variable Speed Control commands	
Alarm		Used to control virtual inputs. For example "+alarm 1" closes virtual input 1, "-alarm 1" opens virtual input 1
+ALARM	Activate an alarm	Opens a virtual input in BVMS.
-ALARM	Deactivate an alarm	Closes a virtual input in BVMS.
System		
TC8x00>HEX	Set Hexadecimal Mode	
TC8x00>DECIMAL	Set Decimal Mode	

6 Getting started

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

6.1 Installing the software modules

Notice!
Do not install DiBos Web client on any BVMS computer.
Install every software module on the computer that is supposed to be used for this module.

To install:

Close Configuration Client before you start the BVMS Setup.

1. Start Setup.exe or start the BVMS Setup on the Welcome screen.
2. In the next dialog box, select the modules to be installed on this computer.
3. Follow the instructions on the screen.

6.2 Using Config Wizard

To start Config Wizard**:**

- Click **Start** > **All Programs** > BVMS > Config Wizard
  The Welcome page is displayed.

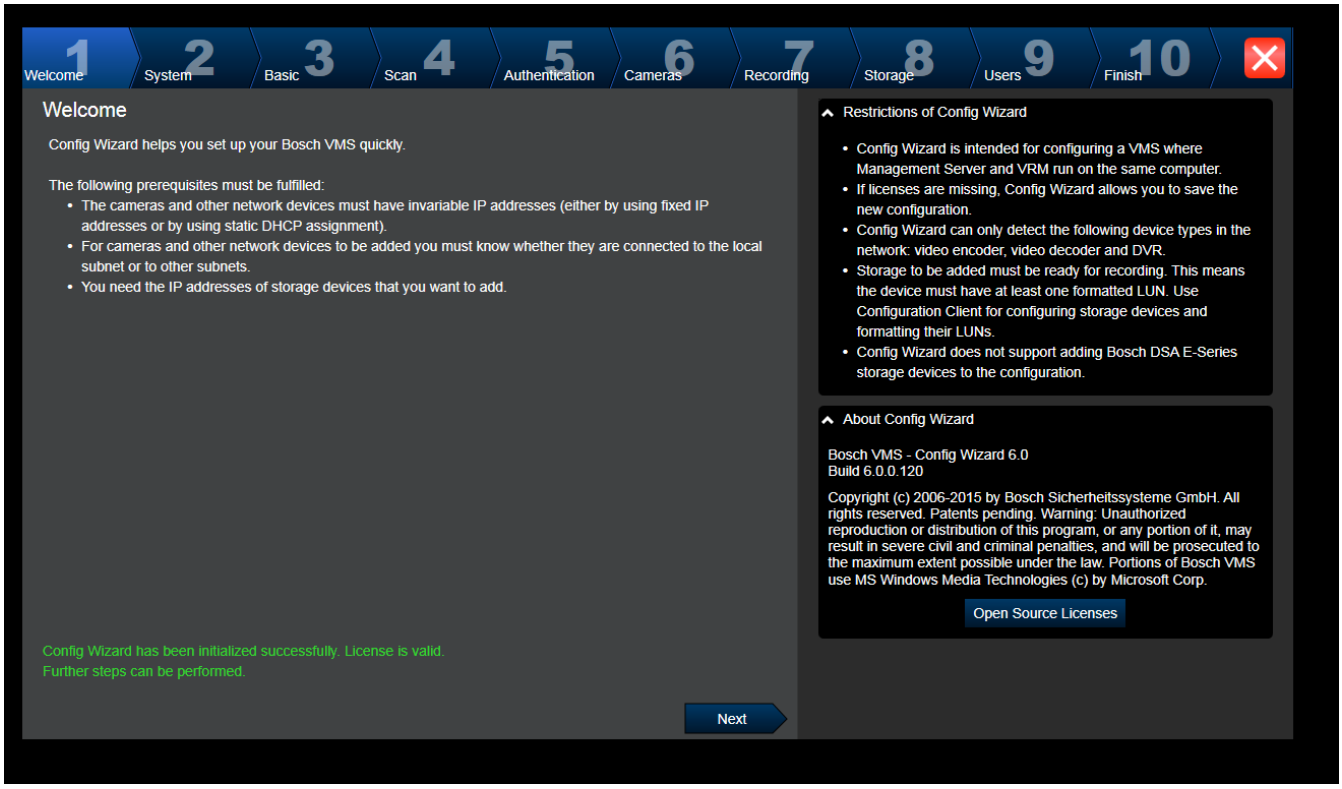
Related Topics

– *Config Wizard, page 23*

Available pages

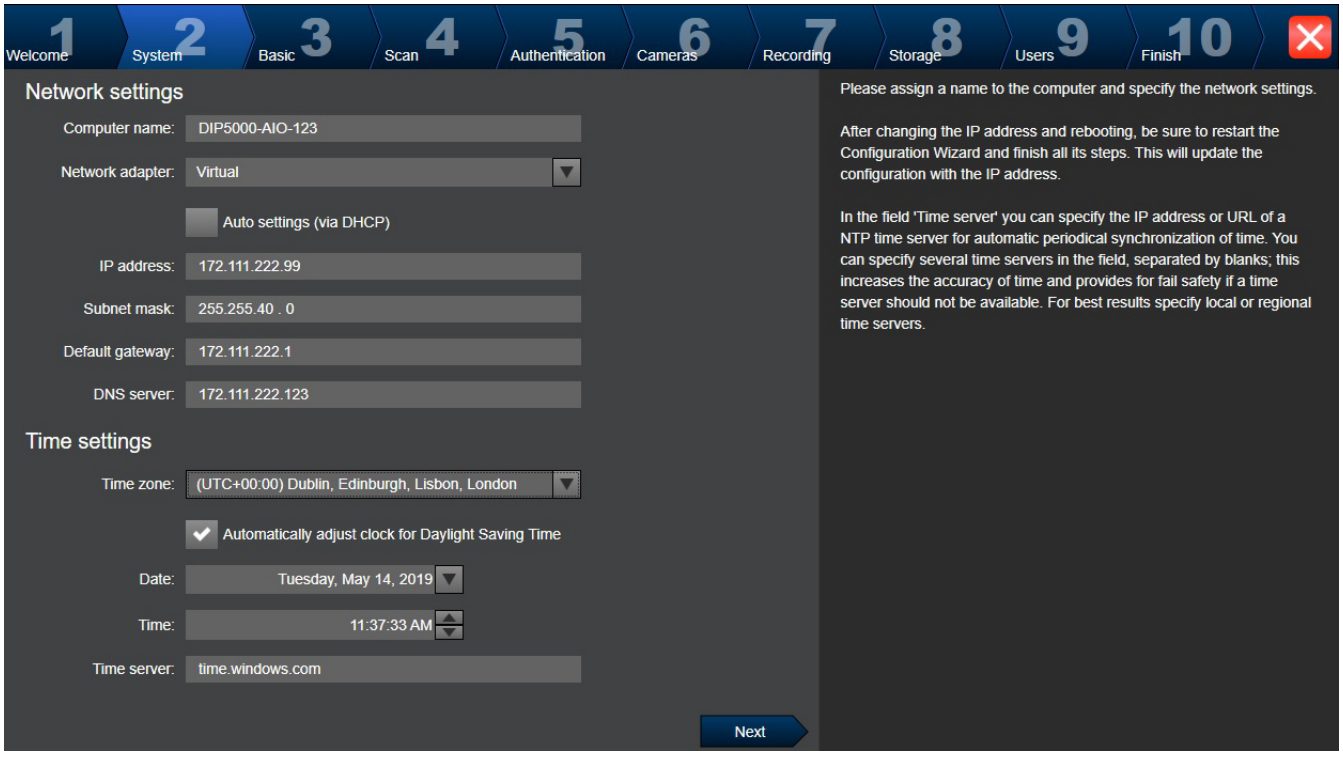
– *Welcome page, page 73*
– *System page, page 74*
– *Basic page, page 75*
– *Scan page, page 76*
– *Authentication page, page 77*
– *Cameras page, page 78*
– *Recording page, page 79*
– *Storage page, page 80*
– *Users page, page 81*
– *Finish page, page 82*

Welcome page



- Click **Next** to continue.

System page

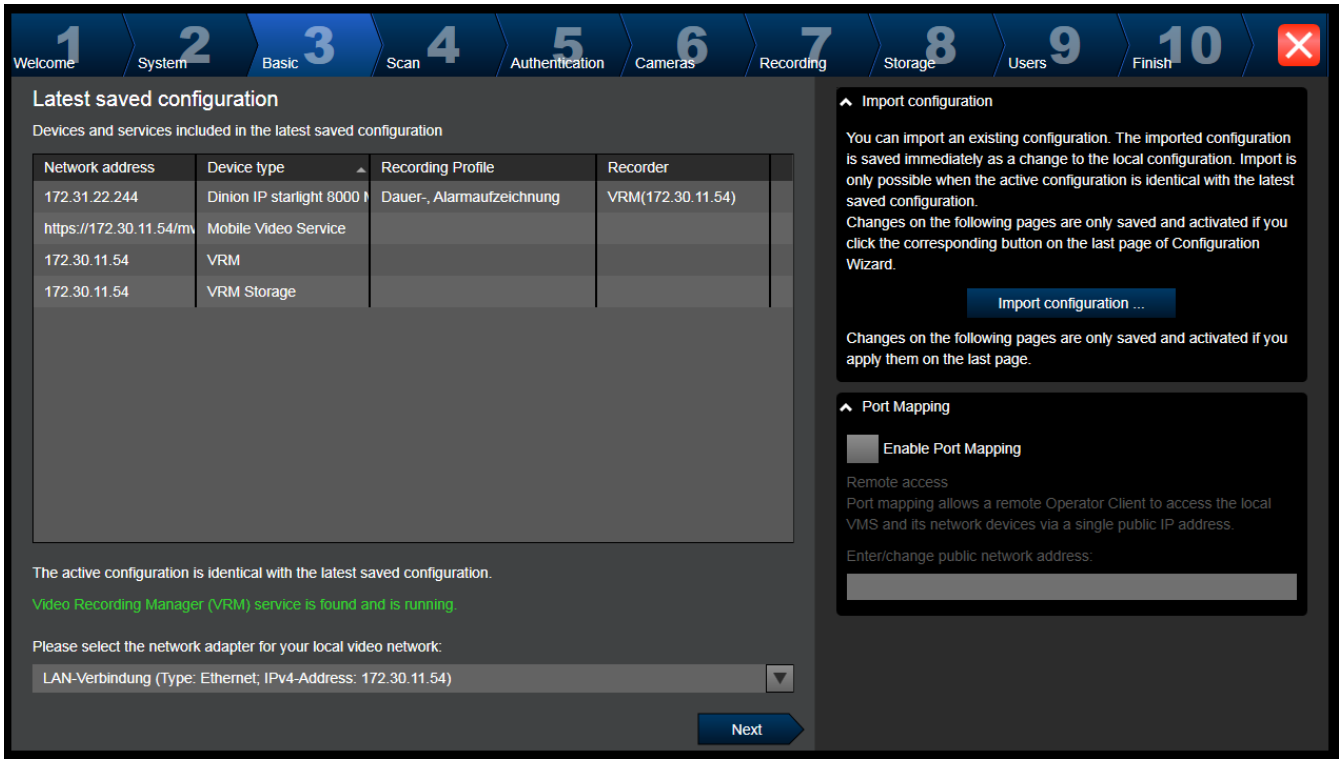


Notice!
Only available on DIVAR IP 3000, DIVAR IP 7000, DIVAR IP all-in-one 5000, DIVAR IP all-in-one 6000 and DIVAR IP all-in-one 7000

You configure the network settings of the operating system.
You configure the time settings of the operating system.

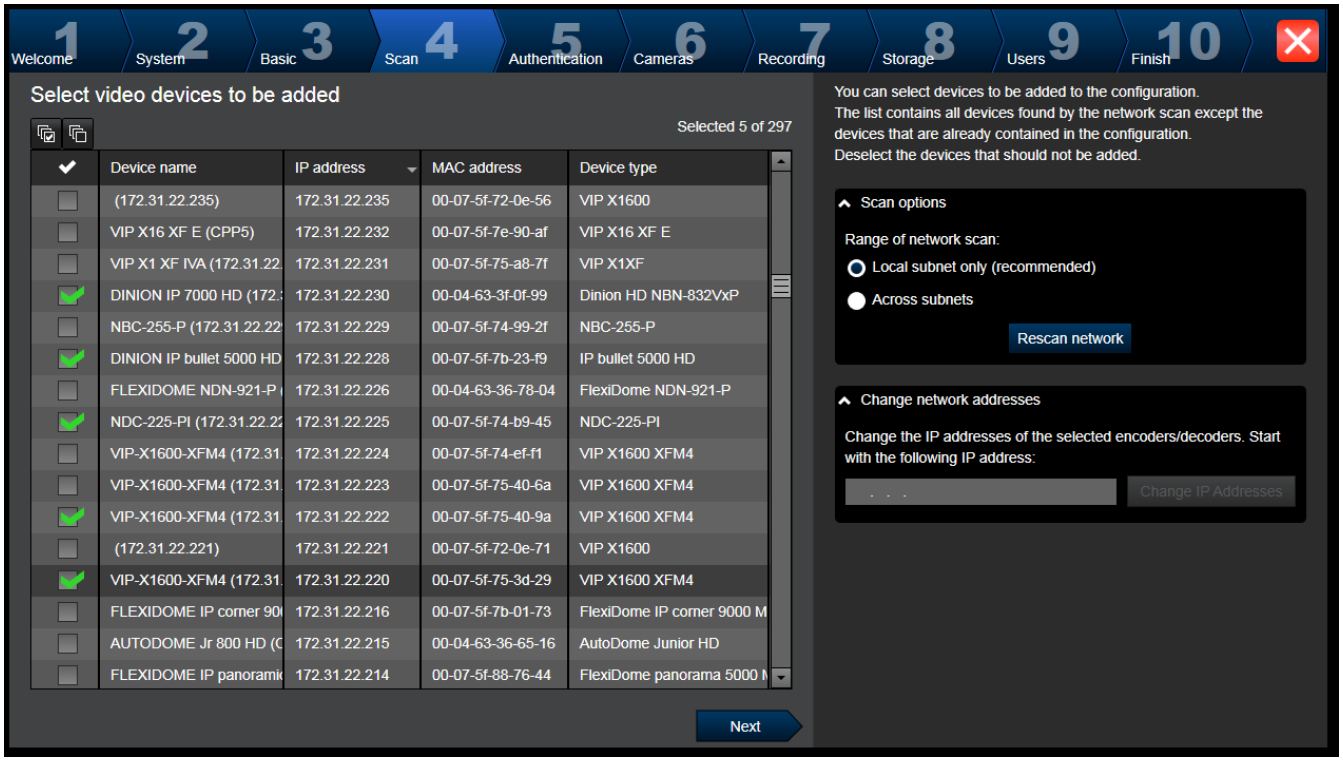
Note:
We highly recommend defining a time server in a video surveillance environment.
As soon as you click **Next**, the settings are activated.

Basic page



This page displays the latest saved configuration. You can import a BVMS file as a change to the existing configuration. This change is saved but not activated when you click **Next**.
You can select the network adapter of your computer that is connected to the video devices (IP cameras, encoders, decoders, iSCSI storage systems) of your system. The IP address of this network adapter is used as IP address of the VRM, the VSG and the local iSCSI storage system.
Click **Port Mapping** to specify the public IP address or DNS name if the system shall be accessed via Internet.

Scan page



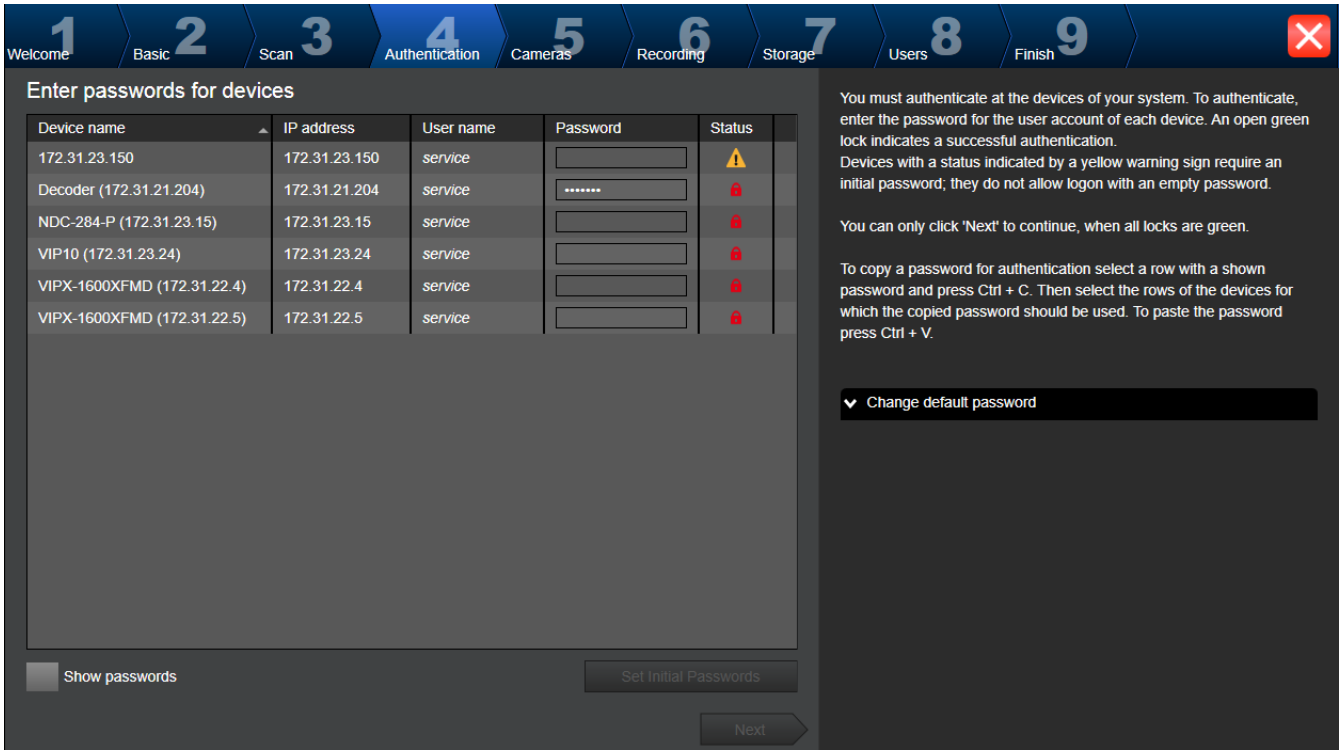
Note:

The scan for devices can take a time. You can cancel the scan. All devices that were already scanned, are displayed in the table.

This page displays all video devices that are not included in the latest saved configuration. Clear the check boxes for the devices that should not be added to the configuration, then click **Next**.

If the selected devices are not located in the same IP range as the DIVAR IP system, the device IP address can be changed by specifying a start address for the device IP range.

Authentication page



This page is used to authenticate at video devices protected by password. For easy authentication with the same password for multiple devices you can use the clipboard (CTRL +C, CTRL+V):

1. Click to activate**Show passwords**.
2. Select a row with a successfully authenticated device (green lock is displayed), press CTRL+C, select multiple rows displaying a red lock and press CTRL+V).

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.

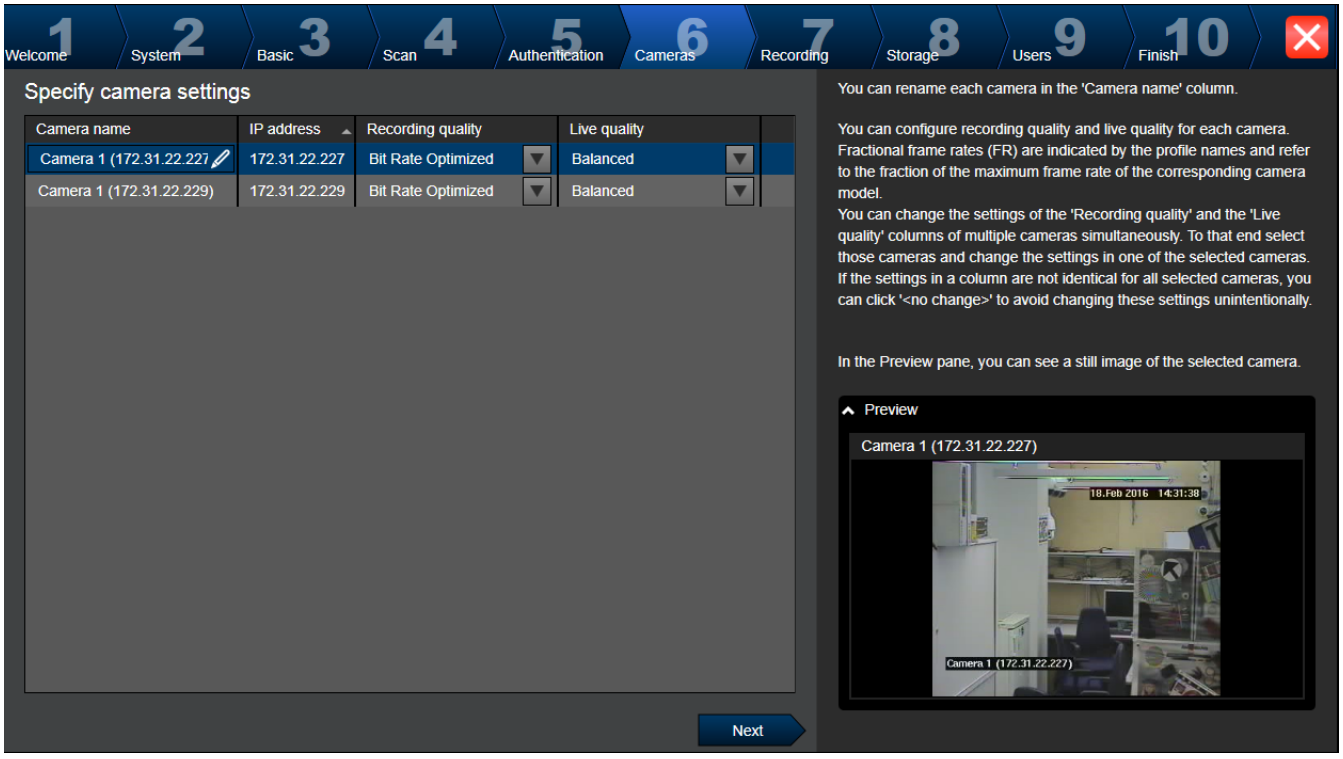
You can provide a global default password for all devices that are currently not protected by a password.

If a device requires an initial password, is displayed.

To set an initial password:

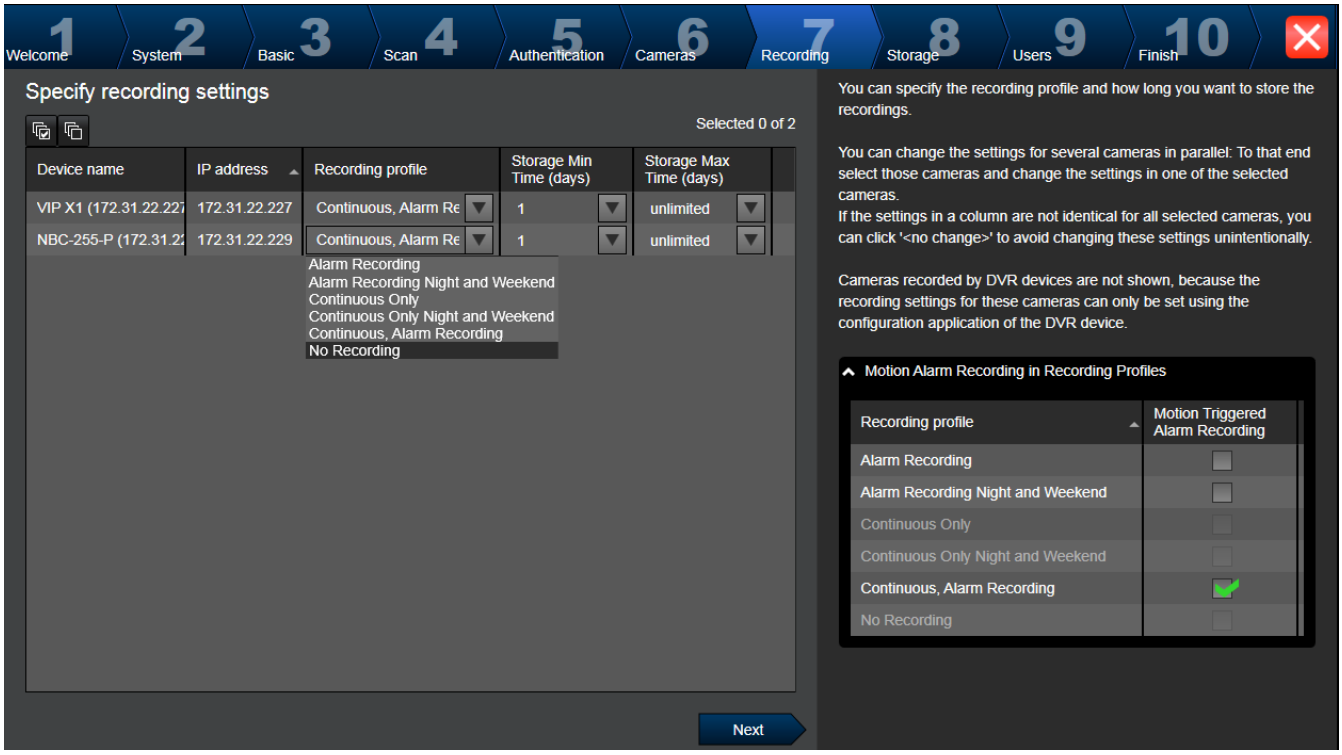
1. Enter the password in the **Password** field.
2. Click **Set Initial Passwords**.
   The initial password is set.
   Note: As long as you have not set the initial password for all devices in the list that require an initial password, you cannot continue.
3. Click **Next** to continue.

Cameras page



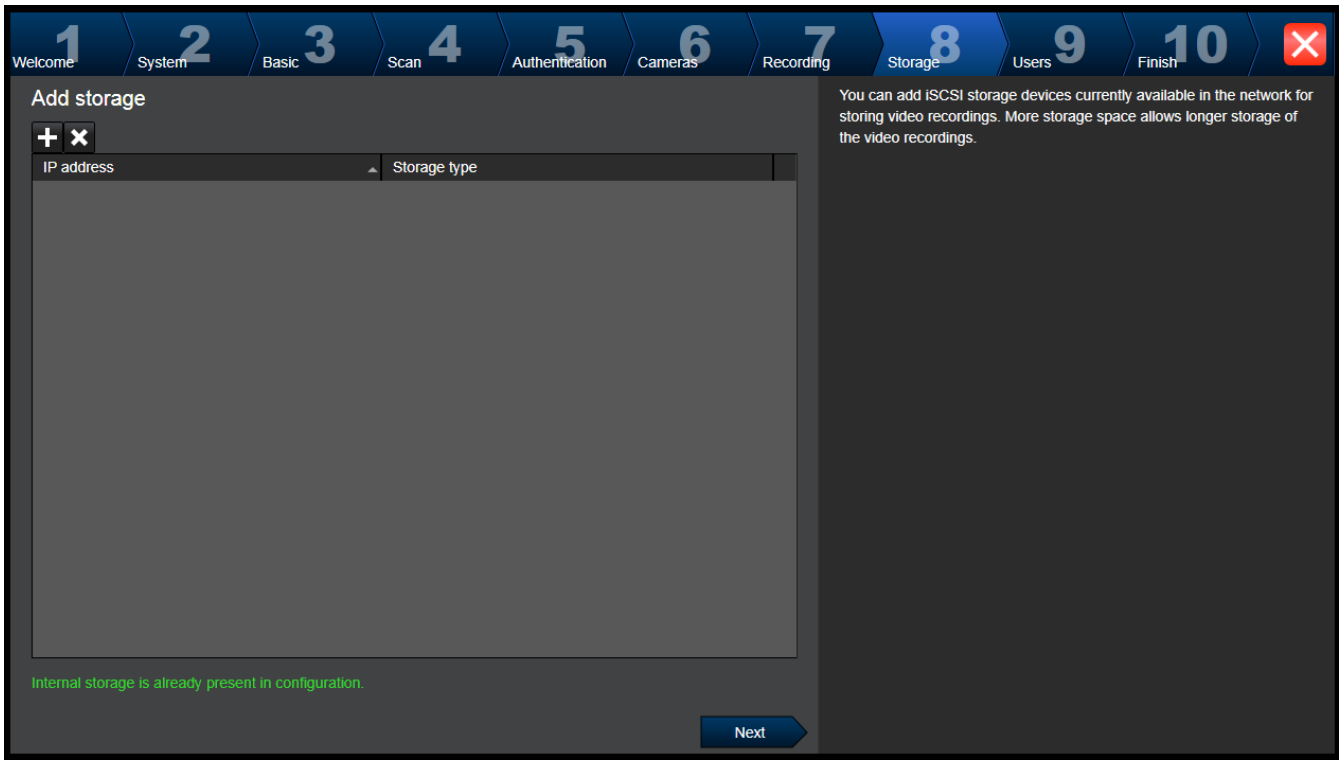
Use this page to manage the cameras of your system.

Recording page



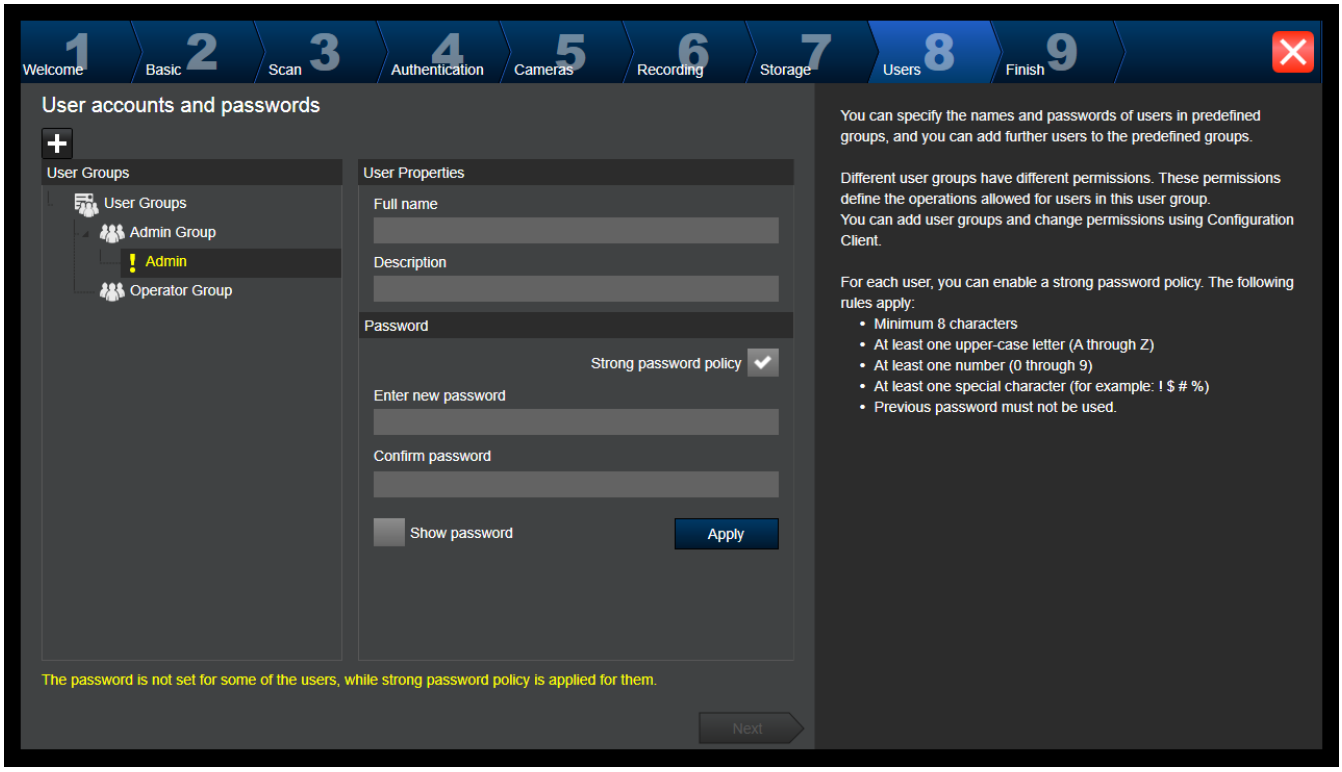
Only those cameras are displayed on this page which were newly added. As soon as you activate this configuration, you cannot change the profile assignment of these cameras.
You can enable motion recording for the recording profiles with both recording and alarm recording enabled. If required, configure recording and alarm recording in Configuration Client (**Scheduled Recording Settings** dialog box).
VCA is activated automatically for each newly added camera.

Storage page



This page allows the addition of further iSCSI storage devices

Users page



On this page you can add new users to the existing user groups.

- ▸ For every new user enter user name and description and set a password.

Strong password policy

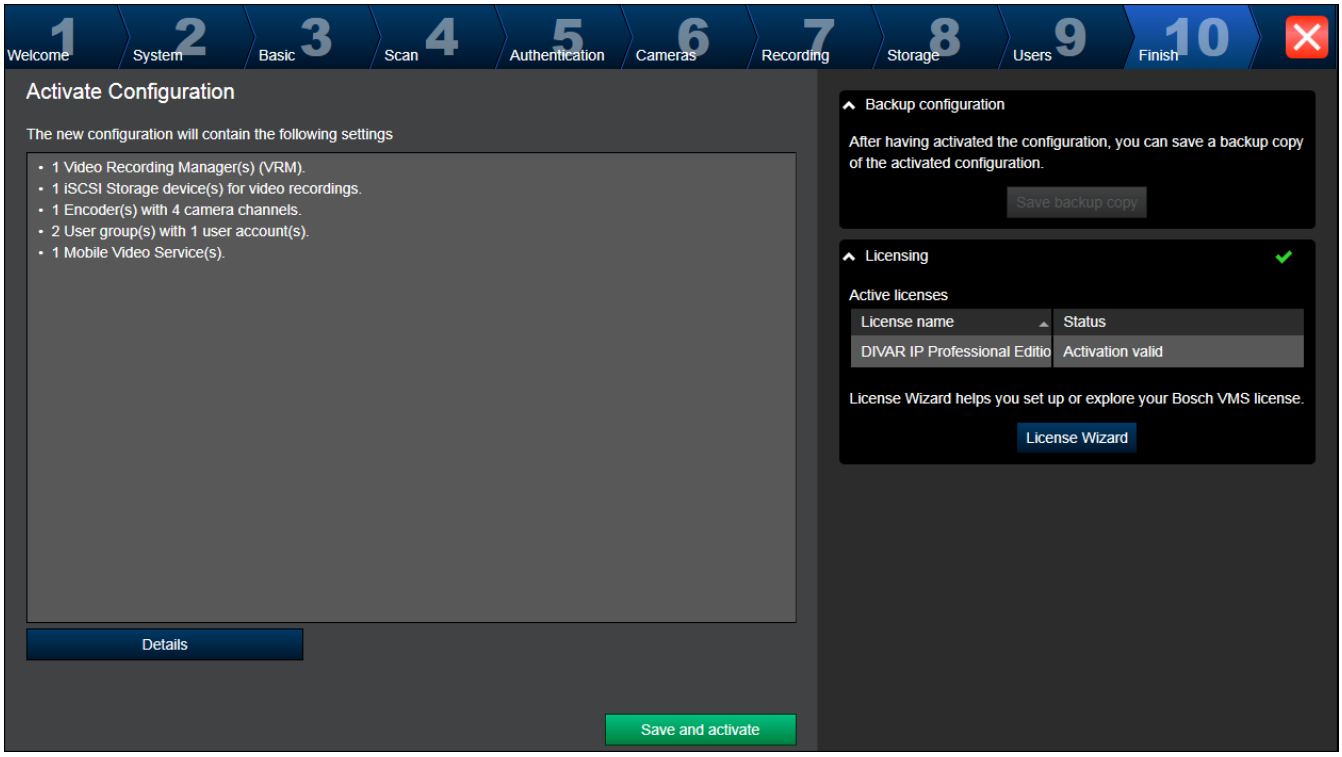
The **Strong password policy** check box is pre-selected for all newly created user groups.
We highly recommend to keep this setting to enhance the protection of your computer against unauthorized access.
The following rules apply:

- – 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: ! $ # %).

- ▸ Click **Apply** to apply the settings, then click **Next** to continue.
  Note: As long as there are users for whom no passwords have been set although the **Strong password policy** was enabled, you cannot continue. To continue, set the missing passwords.

Use Configuration Client to add user groups and to change user group permissions.

Finish page



Before you can activate your configuration you must perform the following tasks:

– Provide a global default password for all devices that are not currently protected by a password.
– Activate your license package if required.

Global default password

If in Configuration Client the option **Enforce password protection on activation** (**Settings** -> **Options**) is disabled, you are not forced to provide a global default password to activate.

Licensing

Expand **Licensing** and click **License Wizard** to check or activate your license package.

After clicking **Save and activate**, the configuration is activated.

After successful activation, the **Finish** page is displayed again. Now you can store a backup of the configuration if desired: Click **Save backup copy**.

After clicking **Save and activate**, the configuration is activated.

After successful activation, the **Finish** page is displayed again. Now you can store a backup of the configuration if desired: Click **Save backup copy**.

6.3 Starting Configuration Client

Notice!

Only admin users can log on to Configuration Client.

The preconfigured default admin user is the user called Admin. Only this user can log on to Configuration Client when you start Configuration Client for the first time.

Once you have started Configuration Client, you can rename the Admin user and change the password.

Note:
You cannot start Configuration Client when another user on another computer in the system has already started Configuration Client.

To start Configuration Client:
1. From the **Start** menu, select **Programs** > BVMS > Configuration Client.
   The dialog box for logging on is displayed.
2. In the **User Name:** field, type your user name.
   When you start the application for the first time, enter Admin as user name, no password required.
3. In the **Password:** field, type your password.
4. Click **OK**.
   The application starts.

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.

See also
- *Strong password policy , page 336*
- *Configuring Admin Group, page 341*

6.4 Configuring the language of Configuration Client

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

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

6.5 Configuring the language of Operator Client

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

To configure the language:
1. Click **User groups** > . Click the **User Group Properties** tab. Click the **Operating Permissions** tab.
2. In the **Language** list, select the desired language.
3. Click to save the settings.
4. Click to activate the configuration.
   Restart Operator Client.

6.6 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
- Encoders
- Live only encoders
- Live only ONVIF encoders
- Local storage encoders
- Decoders
- Video Streaming Gateway (VSG) devices
- DVR devices
- VIDOS NVRs

If you want to add devices via scan, see the respective device topic in the chapter *Devices page, page 125*.

See also

- *Adding VRM Devices via scan, page 175*
- *Adding an live only ONVIF device via scan, page 232*
- *Adding live only devices via scan, page 211*
- *Adding a device, page 126*

6.7 Accessing the system

You access a system performing the following steps:

1. Perform one of the following steps to select the network address of the desired system:
   - Click a preselected list entry.
   - Enter a network address manually.
   - Select a network address using Server Lookup.
2. Log on to the desired system:
   - Single server system
   - Enterprise System

6.8 Using Server Lookup

- The BVMS Server Lookup feature allows Operators to connect to a BVMS Management Server out of a provided list of servers.
- A single user of Configuration Client or Operator Client can connect to multiple system access points sequentially.
- System access points can be Management Server or Enterprise Management Server.
- Server Lookup uses dedicated Management Server to host the Server List.
- Server Lookup and Management Server or Enterprise Management Server functionally can be run on one machine.
- Server Lookup supports you in locating system access points by their names or descriptions.
- Once connected to the Management Server the Operator Client receives events and alarms from the BVMS Management Server and shows live and playback

To access:

1. Start Operator Client or Configuration Client.
   The logon dialog box is displayed.
2. In the **Connection:** list, select **<Address Book...>** for Configuration Client or **<Address Book...>** for Operator Client.
   If private and public IP address has been configured for a server, this is indicated.
   If you select **<Address Book...>** or **<Address Book...>** for the first time, the **Server Lookup** dialog box is displayed.
3. In the **(Enterprise) Management Server Address:** field, type in a valid network address of the desired server.
4. Enter a valid user name and password.
5. If required, click **Remember Settings**.
6. Click **OK**.
   The **Server Lookup** dialog box is displayed.
7. Select the desired server.
8. Click **OK**.
9. If the selected server has both a private and a public network address, a message box is displayed asking whether you are using a computer located in the private network of the selected server.
   The server name is added to the **Connection:** list in the logon dialog box.
10. Select this server in the **Connection:** list and click **OK**.
    If you have selected the **Remember Settings** check box, you can select this server directly when you again want to access this server.

6.9 Configuring remote access

You can configure remote access either for a single system without Enterprise System or for an Enterprise System.

6.9.1 Configuring without Enterprise System

To configure:

1. Configure remote access settings in the **Remote Access Settings** dialog box.
2. Configure the router.

Related Topics

– *Remote Access Settings dialog box (Settings menu), page 123*

6.9.2 Configuring with Enterprise System

To configure:

1. Configure the Server List.
2. Configure Enterprise User Groups and Enterprise Accounts.
3. Configure remote access settings in the **Remote Access Settings** dialog box.
4. Configure the router.

Related Topics

– *Configuring the Server List for Enterprise System, page 96*
– *Creating a group or account, page 337*
– *Remote Access Settings dialog box (Settings menu), page 123*

6.10 Activating the software licenses

When you install BVMS for the first time, you must activate the licenses for the software packages that you have ordered, including the base package and any expansions and/or optional features.

Prerequisites

– Authorization Number that you have received from Bosch
– Computer with internet access
– Account for the Bosch Security Systems Software License Manager

Procedure

To activate the software licenses, you have to perform following steps:

1. *Retrieving the computer signature, page 86*
2. *Obtaining the activation key, page 87*
3. *Activating the system, page 87*

See also

– *License Manager dialog box (Tools menu), page 119*

6.10.1 Downloading Bundle Information file

When you order BVMS software packages, expansions and optional features, you receive from Bosch an Authorization number and usually a XML Bundle file containing all the licenses for the packages, expansions and options you have ordered.
With a Bundle Information file you can ease the process of activating the software licenses.
If you have not received a Bundle Information file from Bosch, you can download it from Bosch Security Systems Software License Manager.

To download the Bundle Information file:

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 Download Bundle File.
   The Download Original Bundle File dialog box is displayed.
4. In the Authorization Number field, enter the authorization number that you have received from Bosch and click Submit.
5. Save the Bundle Information file.

6.10.2 Retrieving the computer signature

To retrieve the computer signature:

1. Start BVMS 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.
   Or
   If you have received a Bundle Information file from Bosch, click **Import Bundle Info** to import it.
   If you have not received a Bundle Information file, download it from Bosch Security Systems Software License Manager, see *Downloading Bundle Information file, page 86*.

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.

6.10.3 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 License Activation.
   The License Activation dialog box is displayed.
4. In the Authorization Number field, enter the authorization number that you have received from Bosch and click .
   The License Activation dialog box is displayed.
5. In the License Activation dialog box, fill in the following fields:
   - Computer Signature : copy the computer signature from the text file where you have saved it and paste it here.
   - Installation Site: enter the installation site information.
   - Comment: if desired, enter a comment (optional).
6. Click Submit.
   The License Activation dialog box is displayed, showing a summary of your license activation and the License Activation Key.
7. Copy the activation key and paste it into a text file or send it via e-mail to a desired e-mail account.

6.10.4 Activating the system

To activate the system:

1. Start BVMS 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.
   Or
   If you have received a Bundle Information file from Bosch, click **Import Bundle Info** to import it.
   If you have not received a Bundle Information file, download it from Bosch Security Systems Software License Manager, see *Downloading Bundle Information file, page 86*.

4. Click **Activate**.
   The **License Activation** dialog box is displayed.
5. Copy the License Activation Key from the text file where you have saved it and paste it into the **License Activation Key:** field.
6. Click **Activate**.
   The appropriate software packages are activated.
7. Click **Close** to close the **License Manager** dialog box.

6.11 Maintaining BVMS

This chapter provides information on how to maintain a just installed or upgraded BVMS.
Perform the following tasks for maintaining the system:

– Export BVMS configuration and user settings. The version history (all versions of the configuration that were activated earlier) is not exported. It is recommended to activate your configuration before exporting.
  – See *To export configuration data:, page 88* for the procedure.

Or

– Perform a backup of the elements.bvms. This is required if you want to restore an (Enterprise) Management Server including the version history. User settings are not included.
  – See *To perform a backup:, page 88* for the procedure.
– Save VRM configuration file (config.xml)
  – See *To save VRM configuration:, page 89* for the procedure.

This exported configuration does not keep the system's history. No rollback is possible.
The entire system configuration including the complete history of system changes is stored in one file:
C:\ProgramData\Bosch\VMS\Elements.bvms.

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.

To perform a backup:

1. Stop the service BVMS **Central Server** on the (Enterprise) Management Server.
2. Copy the file elements.bvms to the desired directory for backup.
3. Start the service BVMS **Central Server** on the (Enterprise) Management Server.

The VRM configuration is stored in a single encrypted file config.xml.
The file can be copied and stored for backup while the VRM service is up and running.
The file is encrypted and contains all VRM relevant data such as:

– User data
– All system devices and their VRM relevant settings

Parts of the VRM configuration are also stored in the BVMS configuration. When you change something within these data, it is written to config.xml after activating the BVMS configuration.
The following settings are not stored in the BVMS configuration:

- **VRM Settings** > **Main Settings**
- **Network** > **SNMP**
- **Service** > **Advanced**
- **Recording preferences**
- **Load Balancing**

When you change something on one of these pages, it is written immediately to the VRM Server and not saved in the BVMS configuration.

To save VRM configuration:

- Copy Config.xml to safe location.
  You can find this file in the following directory for a Primary VRM:
  C:\Program Files (x86)\Bosch\Video Recording Manager\primary\VRM Server
  You can find this file in the following directory for a Secondary VRM:
  C:\Program Files (x86)\Bosch\Video Recording Manager\secondary\VRM Server

6.12 Replacing a device

This chapter provides information on how to repair the system for example when devices fail and must be replaced.

Prerequisite
The maintenance tasks have been performed.

See also
- *Maintaining BVMS, page 88*

6.12.1 Replacing a MS / EMS

There is no difference between Management Server and Enterprise Management Server replacement.
You can either restore the configuration of the old Management Server or Enterprise Management Server or you can import the exported configuration.
When you restore the configuration, the Server ID remains unchanged.
When you import the configuration, the Server ID of the new system is used. You need a new Server ID if you want to create an Enterprise System using an exported configuration that you import in each Management Server as a template. Each Management Server in this Enterprise System must have a unique Server ID.
You can import an exported configuration and the user settings of this configuration. The user settings contain the users that were added in this configuration and their settings in Operator Client like window sizes and favorites.
Note: Importing a configuration does not restore the version history of the old configuration. When you import a configuration, no user settings are imported. You must manually restore the exported user settings.

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.

To restore the exported configuration:
You can only access (copy, delete) this file when the BVMS **Central Server** service is stopped.

1. Stop the service BVMS **Central Server** on the (Enterprise) Management Server.
2. If required, rename the backup file to Elements.bvms.
3. Replace the existing Elements.bvms.
4. Start the service BVMS **Central Server** on the (Enterprise) Management Server.

Note: To reset the system to an empty configuration, stop the service and delete the Elements.bvms.

Further configuration files:

– Elements.bvms.bak (from V.2.2 on): Automatic backup file of the last activation including version history. Later changes of the configuration being not activated, are not included.
– Elements_Backup******.bvms: Configuration from an older version. This file is created after a software update.

To restore the exported user settings:

1. Extract the zip file that was created during the maintenance export.
   The `export.bvms` file and the `UserData` directory are extracted.
2. On the desired (Enterprise) Management Server: Copy the `UserData` directory to `C:\ProgramData\Bosch\VMS\`.

6.12.2 Replacing a VRM

Prerequisites

– Installed OS with correct network settings and the correct version of VRM.

To replace the VRM device from within BVMS:

1. Start BVMS Configuration Client.
2. In the Device Tree, select the VRM device.
3. Perform the settings on the following pages, then save and activate the configuration:

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

– Main window > **Devices** > Expand > Expand > **VRM Settings** > **Main Settings**

– Main window > **Devices** > Expand > Expand > **Network** > **SNMP**

– Main window > **Devices** > Expand > Expand > **Service** > **Advanced**

– Main window > **Devices** > Expand > Expand > > > **Advanced Settings** > **Recording Preferences**

– Main window > **Devices** > Expand > Expand > > > **Load Balancing**

To replace the VRM device without BVMS:

You use the original backup config.xml from the VRM device, containing all configuration settings (no further settings are required).

1. Stop the **Video Recording Manager** service.
2. Copy config.xml to the new server.
3. Start the **Video Recording Manager** service.

To replace an iSCSI device (planned failover):

1. Add the new iSCSI device.
2. Using Configuration Manager, on the iSCSI device to be replaced, configure all LUNs as read-only.

Note: You can remove the old iSCSI device when the old recordings are no longer required.

Notice!
When you configure the new iSCSI device, we recommend to use the same CHAP password as for the old device.
If you use a new CHAP password, make sure to set this new password as a system-wide CHAP password and to assign it to all iSCSI devices and to the VRM.
Otherwise you will not be able to authenticate at the iSCSI and to show direct playback from the iSCSI device.

Related topics
– *System-wide CHAP password , page 178*
– *Global iSCSI connection password (CHAP password): , page 123*

6.12.3 Replacing an encoder or decoder

Notice!
Do not remove a device from the Device Tree if you want to retain its recordings. For replacing this device, exchange the hardware.

Replacing an encoder/decoder of the same type
Prerequisite is a factory default device (IP Address = 192.168.0.1).
1. Disconnect the old device from the network.
2. Do not delete the device from the Device Tree in the BVMS Configuration Client! When deleting the device from VRM, recording is lost.
3. Connect the new device of the same type to the network.

Notice!
The next steps require the above mentioned default IP address. With DHCP assigned IP addresses you cannot perform the initial device scan.

4. Configuration Client: On the **Hardware** menu, click **Initial Device Scan...**.
   The **Initial Device Scan** dialog box is displayed.
5. Click a cell to change the desired address. For changing multiple devices, select the desired rows. You can select multiple devices by pressing the CTRL- or the SHIFT-key. Then right-click the selected rows and click **Set IP Addresses...** or click **Set Subnet Mask...** to change the corresponding values.
   You must enter the correct subnet mask and IP address.
   Subnet mask and IP Address must be identical to the replaced device.
6. Click **OK**.
7. After a few seconds you can access the device setting in the Device Tree.
8. Change all required device settings that are not controlled by BVMS (refer to information below).
9. Save and activate.

Notes:
– The initial device scan only finds devices with default IP addresses (192.168.0.1) or duplicate IP addresses.
– Do not use the VRM or NVR scan to scan defaulted devices since you will not be able to change the IP address afterwards.

Replacing an encoder with DHCP assigned IP address:
Prerequisite is a factory default encoder (DHCP assigned IP).

1. Connect the encoder to the Ethernet port of your computer directly.
2. Write down the network adapter configuration for TCP/IPv4 to restore it later.
3. On the network adapter of your computer, configure the following fixed IP address and subnet mask for your network adapter:
   192.168.0.2
   255.255.255.0
4. Start Internet Explorer.
5. In the **Address** bar, type in 192.168.0.1.
   The Web page of the device is displayed.
6. Click **Settings**, then click **Network**.
7. On the **Network** page, in the **DHCP** list, select **Off**.
8. In the **IP address** field, in the **Subnet mask** field and in the **Gateway address** field, type in the required values valid for your network.
9. Click **Set and Reboot**.
10. Restore the network adapter configuration.

Replacing an encoder/decoder of another device type

– Disconnect the old device from the network.
– Do not delete the device from the Device Tree in the BVMS Configuration Client! When deleting the device from an NVR, recording is lost.
– Connect the new device of the new type to the network.

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

or

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

or

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

or

Main window > **Devices** > Expand > Expand > Right-click > Click **Edit 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.

Replacing a VSG camera

When you replace a VSG camera, ensure that the replaced camera has the same type, the same IP address and the same ONVIF profile as the old camera.
Additionally you must perform the following settings on a new AXIS camera via the Web interface of the VSG camera before replacing the old AXIS camera:

– Set a password for user root
– Configure time synchronization
– Disable link-local address
– Create an ONVIF user
– Disable replay attack protection

Settings controlled by BVMS

Encoders and decoders configured in a BVMS system are controlled by the BVMS Server and thus cannot be shared with other applications.
You can use the BVMS Device Monitor to check which device show a mismatching configuration deviating from the BVMS configuration.
BVMS Configuration Client offers configuration pages for all BVIP devices.
The scale of settings depends on the particular BVIP model (e. g. VIPX 1600 XFM4).
BVMS keeps control of all BVIP settings required for a seamless integration into a BVMS system.
Settings controlled by BVMS:

– Camera name
– Time server settings
– Recording Management (profiles, retention times, schedules)
– Definitions of quality settings
– Passwords

Stored in the BVMS configuration but not changed on the devices:

– IP address (you can change IP addresses with BVMS IP Device Configuration)
– Relay / input names (difference between names in the device and names configured in BVMS is displayed)

System events for mismatching device configuration

– SystemInfo events are generated, once the configuration of a device has been fixed during a periodic check.
– SystemWarning events are generated, once a mismatching configuration has been detected on a device for the first time. Subsequent checks do not raise this event until the configuration has been corrected by an activation or a periodic fix.
– SytemError events are generated, once an error regarding configuration has been detected during activation or periodic checks. Subsequent checks do not raise this event until the configuration has been corrected by an activation or a periodic fix.

6.12.4 Replacing an Operator Client

To replace an Operator Client workstation:

1. Replace the computer.
2. Start the BVMS Setup on the new computer.
3. In the list of components to be installed, select Operator Client.
   If required, select other components that were installed on the replaced computer.
4. Install the software.

6.12.5 Final tests

To check MS / EMS replacement and Operator Client replacement:

1. Activate the configuration.
2. Start Operator Client.
3. Check the Logical Tree in Operator Client.
   It must be identical with Logical Tree in Configuration Client.

To check VRM replacement:

- Start VRM Monitor and check the active recordings.

6.12.6 Recovering Divar IP 3000/7000

Refer to the Installation Manuals of DIVAR IP 3000 or DIVAR IP 7000. In the chapter on recovering the unit you find how to proceed.

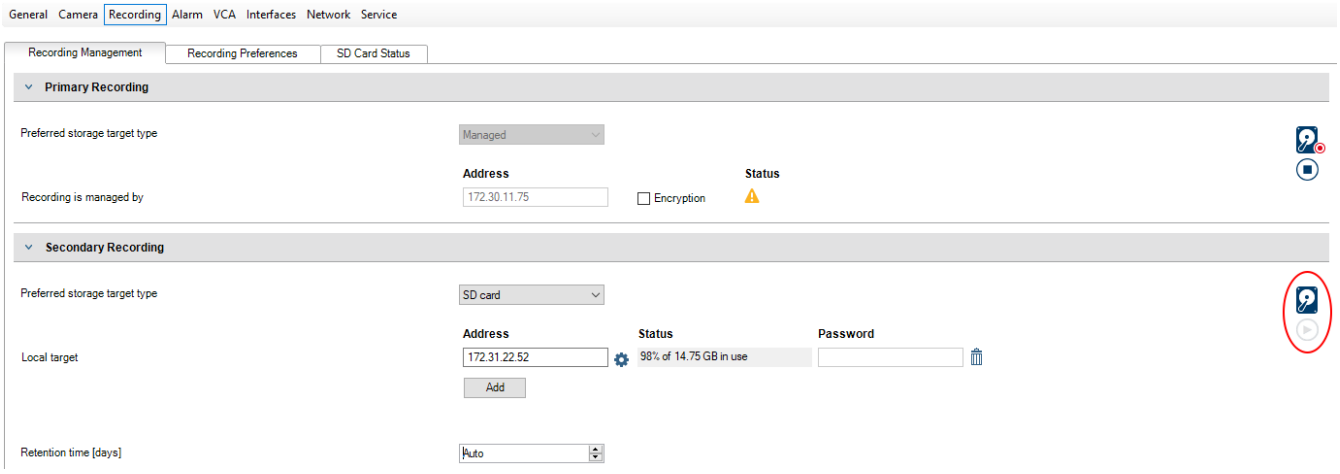
6.13 Configuring time synchronization

Notice!
Ensure that the time of the all computers of BVMS is synchronized with Management Server. Otherwise you can loose recordings.
Configure the time server software on Management Server. On the other computers, configure the IP address of Management Server as time server using standard Windows procedures.

6.14 Configuring the storage media of an encoder

Main window > **Devices** > Expand > Expand > > > **Advanced Settings** > **Recording Management**

Note: Ensure that the desired cameras of this encoder are added to the Logical Tree.
You must configure the storage media of an encoder to use the ANR function.
Note: If you want to configure the storage media of an encoder that has already been added to your system and is recorded via VRM, ensure that secondary recording is stopped:



The ANR function only works on encoders with firmware version 5.90 or later. Not all encoder types support ANR even if the correct firmware version is installed.

To configure the storage media of an encoder:

1. Under **Secondary Recording**, in the **Preferred storage target type** list, select the storage media. Depending on the device type, different media are available.

2. If required, click the ... button to format the storage media.
   After the successful formatting process, the storage media is ready for use with the ANR function.
3. Configure the ANR function for this encoder on the **Cameras and Recording** page.

See also

– *Recording Management page, page 229*
– *Configuring the ANR function, page 293*

7 Creating an Enterprise System

Perform the following tasks to create an Enterprise System on an Enterprise Management Server and on multiple Management Server computers:

1. *Configuring the Server List for Enterprise System, page 96*
2. *Creating an Enterprise User Group, page 97*
3. *Creating an Enterprise Account, page 98*

You need valid licenses for using an Enterprise System.

See also

– *Enterprise System, page 25*

7.1 Configuring the Server List for Enterprise System

Main window > **Devices** > **Enterprise System** > **Server List / Address Book**

You configure multiple Management Server computers in the Server List of an appropriate Management Server.

For simultaneous access you must configure one or more Enterprise User Groups. This changes this Management Server to an Enterprise Management Server.

A user of Operator Client can log on with a user name of an Enterprise User Group to get simultaneous access to the Management Server computers configured in the Server List.

Operating permissions are configured on the Enterprise Management Server in **User groups**, Enterprise User Group tab.

Device permissions are configured on each Management Server in **User groups**, Enterprise Access tab.

– Click to save the settings.

– Click to undo the last setting.

– Click to activate the configuration.

To add servers:

1. Click **Add Server**.
   The **Add Server** dialog box is displayed.
2. Type in a display name for the server and type in the private network address (DNS name or IP address).
3. If required, type in a public network address (DNS name or IP address) for remote access.
4. Click **OK**.
5. Repeat these steps until you have added all desired Management Server computers.

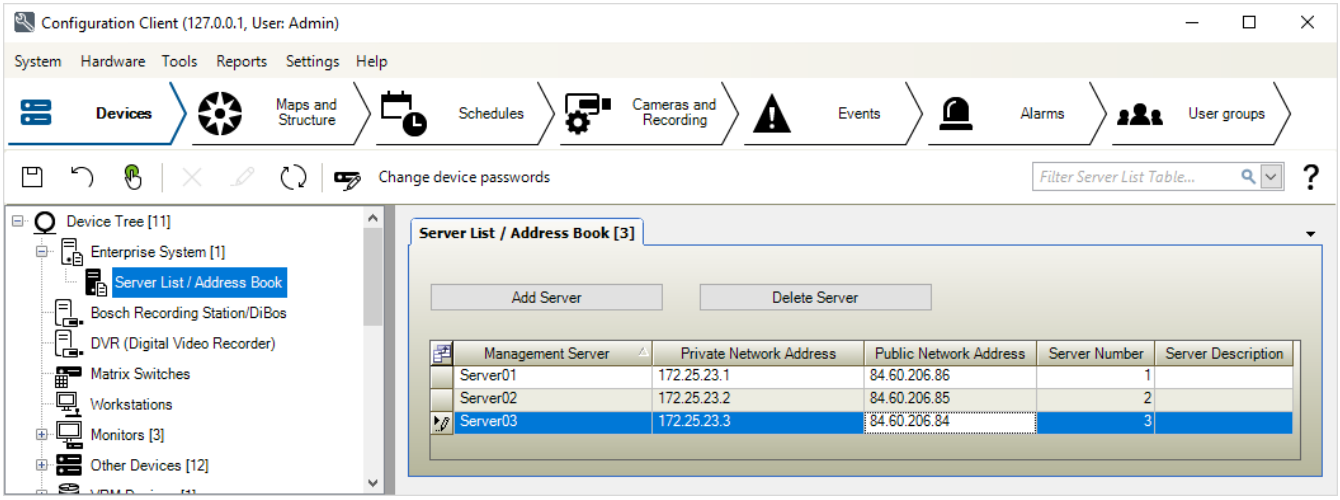
To add colums:

- Right-click on the table header and click **Add column**.
  You can add up to 10 columns.
  To delete a column, right-click the desired column and click **Delete column**.

✓ When you export the Server List, the added columns are also exported.

The Management Server computers for your Enterprise System are configured.

The following screenshot shows an example:



See also

- *Enterprise System, page 25*
- *Server list / Address Book page, page 129*
- *User Groups page, page 317*
- *Using Server Lookup, page 84*

7.2 Creating an Enterprise User Group

Main window > **User groups**

You perform the task of creating an Enterprise User Group for an Enterprise System on the Enterprise Management Server.

You create an Enterprise User Group with users to configure their operating permissions. These operating permissions are available on an Operator Client that is connected to the Enterprise Management Server. An example of an operating permission is the user interface of the alarm monitor.

To create an Enterprise User Group:

1. Click the **Enterprise User Group** tab.
   Note: The **Enterprise User Group** tab is only available if the appropriate license is available and if one or more Management Server computers are configured in **Devices** > **Enterprise System** > **Server List / Address Book**.
2. Click .
   The **New enterprise user group** dialog box is displayed.
3. Type in the name and a description.

4. Click **OK**.
   The Enterprise User Group is added to the corresponding tree.
5. Right-click the new Enterprise group and click **Rename**.
6. Enter the desired name and press ENTER.
7. On the **Operating Permissions** page, configure the operating permissions and server access for the configured Management Server computers as required.

See also
- *User Group Properties page, page 319*
- *Operator Features page, page 327*
- *Priorities page, page 330*
- *User Interface page, page 330*
- *Server Access page, page 331*

7.3 Creating an Enterprise Account

Main window > **User groups**

Notice!
At least one device must be configured in the Device Tree before you can add an Enterprise Account.

You perform the task of creating an Enterprise Account on a Management Server. Repeat this task on each Management Server that is a member of your Enterprise System.
You create an Enterprise Account to configure the device permissions for an Operator Client using an Enterprise System.

To create an Enterprise Account:
1. Click the **Enterprise Access** tab.
2. Click .
   The **New enterprise account** dialog box is displayed.
3. Type in the name and a description.
4. 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.
5. Click **OK**.
   A new Enterprise Account is added to the corresponding tree.
6. Right-click the new Enterprise Account and click **Rename**.
7. Enter the desired name and press ENTER.
8. On the **Device Permissions** page, configure the credentials and the device permissions as required.

See also
- *Strong password policy , page 336*
- *Credentials page, page 326*
- *Logical Tree page, page 326*
- *Events and Alarms page, page 324*
- *Control Priorities page, page 322*

- *Camera Permissions page, page 321*
- *Decoder Permissions page, page 323*

8 Configuring Command Scripts

This chapter describes how to configure Command Scripts. Command Scripts appear at various places of BVMS.

1. Click to save the settings.
2. Click to undo the last setting.
3. Click to activate the configuration.

Notice!
Server Scripts gets activated during restart of Management Server service even if not activated from within Configuration Client.

8.1 Managing Command Scripts

Main window

You can create a Command Script using the following scripting languages:

– C#
– VB.Net

You cannot change the scripting language of an existing Command Script.

You can create a Client Script or a Server Script.

You can add scriptlets to every script.

To get help on entering code, click in the **Command Script Editor** dialog box. The Bosch Script API help is displayed.

To add a server scriptlet:

1. On the **Tools** menu, click the **Command Script Editor...** command.
   The **Select Script Language** dialog box is displayed if no Command Script was created yet.
2. In the **Script Language:** list, select the required entry.
   The **Command Script Editor** dialog box is displayed.
3. In the left pane of the **Command Script Editor** dialog box, right-click ServerScript and click **New Scriptlet**.
   A new scriptlet is added.
4. Enter your code.

To add a client scriptlet

1. On the **Tools** menu, click the **Command Script Editor...** command.
   The **Select Script Language** dialog box is displayed if no Command Script was created yet.
2. In the **Script Language:** list, select the required entry.
   The **Command Script Editor** dialog box is displayed.
3. In the left pane of the **Command Script Editor** dialog box, right-click ClientScript and click **New Scriptlet**.
   A new scriptlet is added.
4. Enter your code.

To delete a scriptlet:

1. Open the **Command Script Editor** dialog box.
2. Click the **Server Script** tab or the **Client Script** tab as required.

3. In the Event Tree, right-click the required event and click .
   The scriptlet is removed.

To exit the Command Script Editor dialog box:

- Click .

See also

– *Command Script Editor dialog box, page 297*

8.2 Configuring a Command Script to be started automatically

Main window > **Alarms** > or > **Alarm Options** column > ...

You configure a Client Command Script to be started in the following cases:

– Workstation starts up.
– User accepts an alarm.

To configure a Command Script at workstation startup:

See Configuring a startup Command Script.

To configure a Command Script after user has accepted an alarm:

1. Click the **Workflow** tab.
2. In the **Execute the following Client Script when alarm is accepted:** list, select the desired Client Script.
   This script is started as soon as a user accepts the selected alarm.

See also

– *Alarm Options dialog box, page 303*

8.3 Importing a Command Script

Main window

You can import Command Scripts that have been developed on another computer. The file must be written in the same scripting language that you used on your system.

To import a Command Script:

1. On the **Tools** menu, click the **Command Script Editor...** command.
   The **Command Script Editor** dialog box is displayed.
2. Click .
   The dialog box for opening a file is displayed.
3. Select the required script file and click **OK**.

See also

– *Command Script Editor dialog box, page 297*

8.4 Exporting a Command Script

Main window

You can export Command Scripts that have been developed on another computer.

To export a Command Script:

1. On the **Tools** menu, click the **Command Script Editor...** command.
   The **Command Script Editor** dialog box is displayed.

2. Click .
   The dialog box for saving a file is displayed.
3. Type the required script file name and click **OK**.

See also

– *Command Script Editor dialog box, page 297*

8.5 Configuring a startup Command Script (settings page)

Main window > **Devices** > Expand > > **Settings** page

You configure a Command Script to be started when the Operator Client on the selected workstation is started.

You must create a corresponding Command Script.

For creating a Command Script, see *Managing Command Scripts, page 100*.

To configure a startup script:

- In the **Startup script:** list, select the required Command Script.

See also

– *Workstation page, page 139*

9 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.

9.1 Activating the working configuration

Main window

You activate the currently working configuration. The Operator Client uses the activated configuration after the next start if the user accepted it. If the activation is enforced, all open instances of the Operator Client in the network exit and start again. The user of each Operator Client instance usually does not have to log on again.
You can configure a delayed activation time. If you configure a delayed activation time, the working configuration is not activated at once but at the time configured. If you configure another activation time later (delayed or not does not matter), this time is active now. The first configured activation time is removed.
When you exit the Configuration Client the system reminds you to activate the current working copy of the configuration.
You cannot activate a configuration that contains a device without password protection.

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

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

To activate the currently working configuration:

1. Click .
   The **Activate Configuration** dialog box is displayed.
   If your configuration contains devices that are not protected by a password, you cannot activate. In this case the **Protect Devices with Default Password...** dialog box is displayed.
   Follow the instructions in this dialog box and click **Apply**.
   The **Activate Configuration** dialog box is displayed again.

2. If appropriate, enter a delayed activation time. By default, the present point in time is configured as activation time. If you do not change the delayed activation time, the activation is performed immediately.
   If appropriate, click to check **Force activation for all Operator Clients**.
3. Type a description and click **OK**.
   The current configuration is activated.
   Each Operator Client workstation is instantly restarted, if connected to the network and the activation is enforced. If a workstation is not connected, it is restarted as soon it is connected again.
   If you configured a delayed activation time, the configuration will be activated later.

See also
- *Protect Devices with Global Default Password dialog box (Hardware menu), page 115*
- *Activate Configuration dialog box (System menu), page 114*

9.2 Activating a configuration

Main window
You can activate a previous version of the configuration that you have saved earlier.
To activate a configuration:
1. On the **System** menu, click **Activation Manager...**.
   The **Activation Manager** dialog box is displayed.
2. In the list, select the configuration you want to activate.
3. Click **Activate**.
   A message box is displayed.
4. Click **OK**.
   The **Activate Configuration** dialog box is displayed.
5. If appropriate, click to check **Force activation for all Operator Clients**. Each Operator Client workstation is automatically restarted to activate the new configuration. The user cannot refuse the new configuration.
   If **Force activation for all Operator Clients** is not checked, on each Operator Client workstation a dialog box appears for some seconds. The user can refuse or accept the new configuration. The dialog box is closed after a few seconds without user interaction. In this case the new configuration is not accepted.

See also
- *Activate Configuration dialog box (System menu), page 114*
- *Activation Manager dialog box (System menu), page 114*

9.3 Exporting configuration data

Main window
You can export the device configuration data of BVMS in a .zip file. This .zip file contains the database file (`Export.bvms`) and the user data (`.dat` file).
You can use these files for restoring a system configuration that has been exported before on the same (Enterprise) Management Server or for importing it on another (Enterprise) Management Server. The user data file cannot be imported but you can use it to manually restore the user configuration.

To export configuration data:

1. On the **System** menu, click **Export Configuration...**
   The **Export Configuration File** dialog box is displayed.

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

See also

– *Importing configuration data, page 105*

9.4 Importing configuration data

Main window

The following use cases are covered:

– Importing a configuration that has been exported (backup has been performed) before on the same server
– Importing a configuration template that has been prepared and exported on another server
– Importing the configuration of an earlier BVMS version.

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

For importing the configuration data you need the appropriate password.

You cannot import user data.

To import the configuration:

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

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

See also

– *Exporting configuration data, page 104*

9.5 Exporting configuration data to OPC

Main window

You can export the device configuration data of BVMS in an XML file to import it in an OPC Server application. The file must be stored in the bin directory of your BVMS installation.

For configuring a BVMS - BIS connection the BVMS - BIS Interface Configuration Manual is available.

Notice!
Install OPC server and BVMS Management Server on different computers.
If both the servers run on the same computer, the performance of the systems is reduced.
Additionally serious software crashes can appear.

To export configuration data:

1. On the **System** menu, click **Export Device Information for OPC...**.
   The **Export Device Information File** dialog box is displayed.
2. Enter a file name and click **Save**.
   The file is saved.
   You can import this file in your OPC server application.

9.6 Checking the status of your encoders/decoders

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

See also

– *Device Monitor dialog box (Hardware menu), page 118*

9.7 Configuring SNMP monitoring

Main window

To configure:

1. On the **Settings** menu, click **SNMP Settings...**.
   The **SNMP Settings** dialog box is displayed.
2. Make the required settings and click **OK**.

To disable SNMP GetRequest:

- In the **SNMP GET port** field, delete the content of the field.
  BVMS no longer listens to SNMP GetRequest.

See also

– *SNMP Settings dialog box (Settings menu), page 121*

9.8 Creating a report

Main window
You can create reports where information on the current configuration is collected.

To create a report:

1. On the **Reports** menu, click the desired command.
   The corresponding dialog box is displayed.
2. Click **CSV Export**.
3. Enter path and filename for the new report.
4. Open the CSV file in Microsoft Excel or another spreadsheet application to check the content.

See also

– *Recording Schedules dialog box, page 120*
– *Task Schedules dialog box, page 120*
– *Cameras and Recording Parameters dialog box, page 120*
– *Stream Quality Settings dialog box, page 120*
– *Event Settings dialog box, page 120*

- *Compound Event Settings dialog box, page 120*
- *Alarm Settings dialog box, page 120*
- *Configured Users dialog box, page 120*
- *User Groups and Accounts dialog box, page 121*
- *Operating Permissions dialog box, page 121*

10 Configuration examples

This chapter contains examples on how to configure selected devices in BVMS.

10.1 Adding a Bosch ATM/POS bridge

This example describes how to set up a Bosch ATM/POS bridge.

Configuring the ATM/POS bridge

1. Ensure that the device is powered.
2. To configure the IP address and subnet mask of the device connect it to a COM port of your computer with a RS232 cable (use the specified Bosch cable for connection). See the Installation Manual of the Bosch ATM/POS bridge for details.
3. On this computer, start a Hyper terminal session (usually: **Start** > **Programs** > **Accessories** > **Communications** > **Hyper Terminal**).
4. Type a name for the session and click **OK**.
5. Select the COM port number and click **OK**.
6. Enter the following COM port settings:
   - 9600 bits/s
   - 8 data bits
   - no parity
   - 1 stop bit
   - hardware flow control

   Click **OK**.
7. Press F1 for displaying the system options menu of the device.
8. Enter 1 to set the IP address and the subnet mask as required.
9. Leave the default settings for the ports:
   - port1: **4201**
   - port2: **4200**

Adding the ATM/POS bridge to BVMS

1. Connect the device to your BVMS network.
2. Start Configuration Client.
3. Click **Devices**, expand the Logical Tree, expand , right-click , click **Add Bosch ATM/POS-Bridge**.

   The **Add Bosch ATM/POS-Bridge** dialog box is displayed.
4. Type a name as desired and type the settings that you configured earlier.
5. Click the **Inputs** tab and select the required inputs.
6. Click to save the settings.
7. Click **Events**.
8. Expand , expand **POS Bridge Input**, click **Data Input**.
9. In the **Trigger Alarm** list, select **Always** to ensure that this event always triggers an alarm. If you want the event trigger an alarm only during a certain time span, select a schedule.
10. Click to save the settings.

11. Click **Alarms**.
12. Configure the desired alarm settings for this event.
13. Click to save the settings and click to activate the configuration.
14. Perform a test to ensure that the alarm is working as desired.

10.2 Adding a Bosch Allegiant input alarm

After a Bosch Allegiant device is added to BVMS, you add Allegiant alarm inputs.

1. On the Device Tree, click the Allegiant device entry.
2. Click the **Inputs** tab and click **Add Input**.
3. Add the desired input alarms.
4. Click **Events**.
5. In the Event Tree, expand **Allegiant Devices**, expand **Allegiant Input**, and click **Input Closed** or **Input Opened** (depends on your application).
6. In the **Trigger Alarm** list, select **Always** to ensure that an event always triggers an alarm. If you want the event trigger an alarm only during a certain time span, select a schedule.
7. Click to save the settings and click to activate the configuration.
8. Perform a test to ensure that the alarm is working as desired.

10.3 Adding and configuring 2 Dinion IP cameras with VRM recording

This section describes how to add 2 Dinion IP cameras for VRM recording, how to configure different recording settings and how to configure Forensic Search for these cameras.

Prerequisite:

VRM and iSCSI devices are properly configured.

This means:

– The VRM is added to the Device Tree.
– An iSCSI device with configured target and LUN is assigned to this VRM.

To add the IP cameras to an existing VRM:

Main window > **Devices** > Expand

1. Right-click and click **Add Encoder**.
   The **Add Encoder** dialog box is displayed.
2. Type the IP address of the IP camera and select the encoder type (Dinion IP).
   Click **OK**.
   Repeat this step for the other IP camera.

To add the IP cameras to the Logical Tree:

Main window > **Maps and Structure**

- Drag the cameras to the Logical Tree.

To change camera properties:

Main window > **Cameras and Recording** > > tab

1. In the **Live Video** column, configure the quality of live display. For these devices, you can only set the live quality per camera, not schedule dependent.
2. Make the appropriate settings in the other columns.

To configure recording settings for the cameras:

1. Click a schedule tab, for example .
2. In the column, click a cell and select the appropriate stream quality.
3. Under **Continuous or Pre-alarm Recording**, in the **Select** column, select the desired recording mode.
   If you click **Pre-alarm**: Click a cell in the **Duration** column to select the alarm recording time before the alarm in seconds.
4. Under **Alarm Recording**, in the **Duration** column, click a cell and type the desired recording time.
5. Repeat the previous steps to configure the recording settings for the other camera.

To enable Forensic Search on a workstation:

Main window > **Devices** > Expand

1. Click the icon of your workstation.
2. Click the **Settings** tab.
3. Click to select the **Enable Forensic Search** check box.

11 Global Configuration Client windows

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

11.1 Configuration window

Main window

Allows you to configure your system. The buttons in the toolbar represent the various pages which you must configure to get a running system. Their sequence represents the recommended workflow of configuration.

- Click a tree item to display the available property pages.

Devices	Click to display the **Devices** page with all devices connected to the system.
Maps and Structure	Click to display the **Maps and Structure** page with Logical Tree, Device Tree, and maps.
Schedules	Click to display the **Recording Schedules** and **Task Schedules** page.
Cameras and Recording	Click to display the **Cameras and Recording** page with the Camera Table and the recording settings of all cameras.
Events	Click to display the **Events** page.
Alarms	Click to display the **Alarms** page.
User groups	Click to display the **User groups** page with all users.
	Click to save the changed settings of the current window.
	Click to restore the saved settings of the current window.
	Click to display the **Activate Configuration** dialog box.

	Click to delete the selected item. (Not available on every page).
	Click to rename the selected item. (Not available on every page).
	Click to display help information on the current window.
	Click to refresh the state information for all devices (not available on every page). You can refresh the state of a single device: Right-click the device and click **Refresh state**. **Note:** When you have a large system with several 1000 devices configured, the process of refreshing states can take a long time.

11.2 Menu commands

System menu commands

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

Hardware menu commands

Initial Device Scan...	Displays the **Initial Device Scan** dialog box.
Protect Devices with Default Password...	Displays the **Protect Devices with Global Default Password** dialog box.
Change device passwords...	Displays the **Change device passwords** dialog box.
Update device firmware...	Displays the **Update device firmware** dialog box.
Change device IP and network settings...	Displays the **Change device IP and network settings** dialog box.
Device Monitor...	Displays the **Device Monitor** dialog box.

Tools menu commands

Command Script Editor...	Displays the **Command Script Editor** dialog box
Resource Manager...	Displays the **Resource Manager** dialog box.

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

Reports menu commands

Recording Schedules...	Displays the **Recording Schedules** report dialog box.
Scheduled Recording Settings...	Displays the **Scheduled Recording Settings** report dialog box.
Task Schedules...	Displays the **Task Schedules** report dialog box.
Cameras and Recording Parameters...	Displays the **Cameras and Recording Parameters** report dialog box.
Stream Quality Settings...	Displays the **Stream Quality Settings** report dialog box.
Event Settings...	Displays the **Event Settings** report dialog box.
Compound Event Settings...	Displays the **Compound Event Settings** report dialog box.
Alarm Settings...	Displays the **Alarm Settings** report dialog box.
Configured Users...	Displays the **Configured Users** report dialog box.
User Groups and Accounts...	Displays the **User Groups And Accounts** report dialog box.
Device Permissions...	Displays the **Device Permissions** report dialog box.
Operating Permissions...	Displays the **Operating Permissions** report dialog box.
Configuration Permissions...	Displays the **Configuration Permissions** report dialog box.
User Group Permissions...	Displays the **User Group Permissions** report dialog box.
Security Settings...	Displays the **Security Settings** report dialog box.
Bypassed devices...	Displays the **Bypassed devices** report dialog box.

Settings menu commands

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

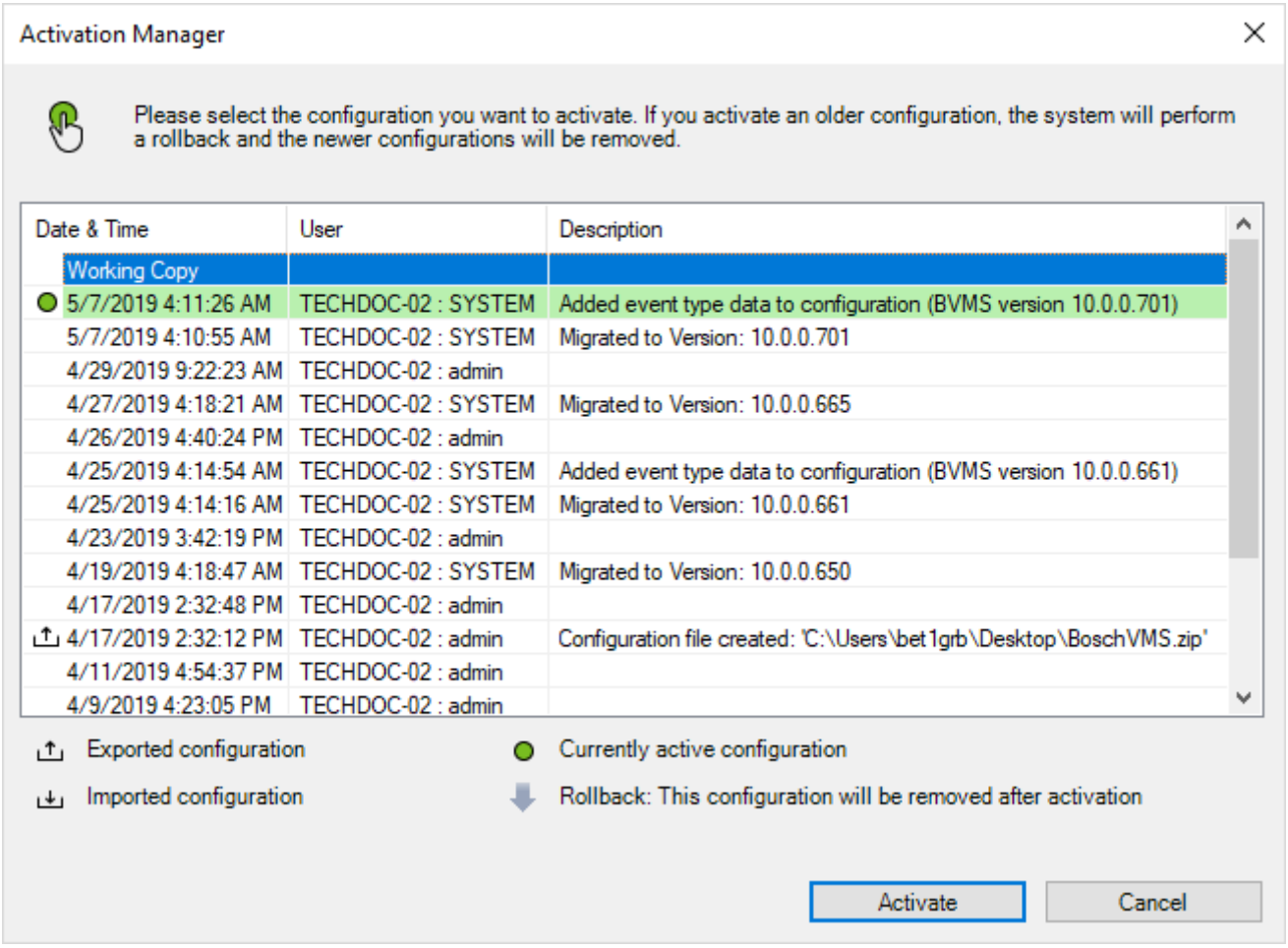
Help menu commands

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

11.3 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.



Activate

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

See also

- *Activating the working configuration, page 103*
- *Activating a configuration, page 104*

11.4 Activate Configuration dialog box (System menu)

Main window >

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

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

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

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

See also
– *Activating the working configuration, page 103*

11.5 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.

11.6 Protect Devices with Global Default Password dialog box (Hardware menu)

Main window > **Hardware** menu > **Protect Devices with Default Password...** command
or

Main window >

This dialog box appears, if an activation is pending and if your configuration contains devices that are not protected by a password. It allows you to enter a global default password that is applied on all affected devices.

Refresh States
Click to rescan the network for devices that are not protected by a password.

Global default password
Type in a password that is used for all currently not protected devices.

Show passwords
Click to enable that all passwords in this dialog are visible.

Enforce password protection on activation
Click to select this checkbox. If enabled, you must apply a global default password for devices that are not protected by a password.

Apply
Click to apply the global default password.
The **Changing Passwords** dialog box is displayed. The changes of passwords are listed.
Click **OK** to close.
If you started with activating your configuration, the **Activation Manager** dialog box is displayed.

See also

– *Activating the working configuration, page 103*

11.7 Change device passwords dialog box (Hardware menu)

See *Change device passwords dialog box, page 125* for details.

To change the settings for multiple devices:

See *Configuring multiple encoders / decoders, page 227*.

11.8 Update device firmware dialog box (Hardware menu)

Main window > **Hardware** menu > **Update device firmware...** command > **Update device firmware** dialog box

Click to refresh the state information for all devices. You can refresh the state of a single device: Right-click the device and click **Refresh state**.

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

Click to select all available devices at once.

Click to update the firmware version.

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 .

To update the firmware version:

1. Select the required device.
2. Click **Update Firmware**.
   A Configuration Client information window is displayed.
3. Click **OK**.
   The file explorer opens.
4. Select the file containing the update.
5. Click **Open**.
   The **Firmware Upload Status** window opens.
6. Click **Start** to start the upload.
7. Click **Close**.
   The firmware is updated.

To change the settings for multiple devices:
See *Configuring multiple encoders / decoders, page 227*.

11.9 Change device IP and network settings dialog box (Hardware menu)

Main window > **Hardware** menu > **Change device IP and network settings...** command> **Change device IP and network settings** dialog box

Click to refresh the state information for all devices. You can refresh the state of a single device: Right-click the device and click **Refresh state**.
Note: When you have a large system with several 1000 devices configured, the process of refreshing states can take a long time.

Click to select all available devices at once.

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 .

The table allows you to set the following properties of the available IP devices:
- Display name
- IP address
- Subnet mask
- Gateway IP

Notice!
Instead of using the commands, you can type the appropriate settings in the required field.

To set the display name for IP devices:
1. Select the required device.
2. Right-click the selected device and click **Set Display Names...** The **Set Display Names** dialog box is displayed.
3. In the **Start with:** field, type the first string.
4. Click **Calculate**. In the **End with:** field, the last string of the range for the selected device is displayed.
5. Click **OK**.

6. In the **Change device IP and network settings** dialog box, click **Apply**.
   The calculated name is updated in the selected device.

Set display names dialog box

Start with:
Type the first name.

End with:
Displays the last name for the selected devices after having clicked **Calculate**.

Calculate
Click to calculate the range of display names for the selected devices.

To set the IP address for IP devices:
1. Select the required device.
2. Right-click the selected device and click **Set IP Addresses...**. The **Set IP Addresses** dialog box is displayed.
3. In the **Start with:** field, type the first IP address.
4. Click **Calculate**. In the **End with:** field, the last IP address of the range for the selected device is displayed.
5. Click **OK**.
6. In the **Change device IP and network settings** dialog box, click **Apply**.
   The new IP address is updated in the selected device.

Set IP addresses dialog box

Start with:
Type the first IP address..

End with:
Displays the last IP address for the selected devices after having clicked **Calculate**.

Calculate
Click to calculate the range of IP addresses for the selected devices.

To set subnet mask / gateway ID for IP devices:
1. Click in the required field.
2. Type the appropriate value.
3. Click **Apply**.
   The new value is updated in the selected device.

Apply
Click to configure the devices with the entered values without closing the dialog box.

To change the settings for multiple devices:
See *Configuring multiple encoders / decoders, page 227*.

11.10 Device Monitor dialog box (Hardware menu)

Main window > **Hardware** menu > **Device Monitor...** command > **Device Monitor** dialog box
Allows you to check the status of the encoders/decoders in your Device Tree that are active in your BVMS.

Display Name
Device name that was configured in BVMS.

Network Address
IP address of the device.

State
The following states can be displayed:
– **Configured**: Configuration of this device is activated.
– **Configuration mismatch**: Configuration of this device is not activated.
– **Unknown**: Status could not be determined.
– **Not Connected**: Not connected.

Last Check
Date and time when the dialog was started and the check was performed. As long as the dialog box is displayed, the devices are not checked again.

See also
– *Checking the status of your encoders/decoders, page 106*

11.11 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.

11.12 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.

See also
– *Activating the software licenses, page 86*

11.13 Reports dialog boxes (Reports menu)

This chapter covers all dialog boxes which are available for configuration reports.

See also

– *Creating a report, page 106*

11.13.1 Recording Schedules dialog box

Main window > **Reports** menu > **Recording Schedules...** command

Lists the configured recording schedules.

▸ Click **CSV Export** to save all information of this dialog box in a CSV file.

11.13.2 Scheduled Recording Settings dialog box

Main window > **Reports** menu > **Scheduled Recording Settings...** command

Lists the configured scheduled recording settings.

▸ Click **CSV Export** to save all information of this dialog box in a CSV file.

11.13.3 Task Schedules dialog box

Main window > **Reports** menu > **Task Schedules...** command

Lists the configured task schedules.

▸ Click **CSV Export** to save all information of this dialog box in a CSV file.

11.13.4 Cameras and Recording Parameters dialog box

Main window > **Reports** menu > **Cameras and Recording Parameters...** command

Lists the recording parameters that are configured in the Camera Table and the Recording Table.

▸ Click **CSV Export** to save all information of this dialog box in a CSV file.

11.13.5 Stream Quality Settings dialog box

Main window > **Reports** menu > **Stream Quality Settings...** command

Lists the configured stream quality settings of all cameras.

▸ Click **CSV Export** to save all information of this dialog box in a CSV file.

11.13.6 Event Settings dialog box

Main window > **Reports** menu > **Event Settings...** command

Lists the events for which a schedule for triggering an alarm is configured.

▸ Click **CSV Export** to save all information of this dialog box in a CSV file.

11.13.7 Compound Event Settings dialog box

Main window > **Reports** menu > **Compound Event Settings...** command

Lists the all compound events.

▸ Click **CSV Export** to save all information of this dialog box in a CSV file.

11.13.8 Alarm Settings dialog box

Main window > **Reports** menu > **Alarm Settings...** command

Lists all alarm settings of the configured alarms, including the settings in the **Alarm Options** dialog box.

▸ Click **CSV Export** to save all information of this dialog box in a CSV file.

11.13.9 Configured Users dialog box

Main window > **Reports** menu > **Configured Users...** command

Lists the users who are permitted to log on to the system.

- Click **CSV Export** to save all information of this dialog box in a CSV file.

11.13.10 User Groups and Accounts dialog box

Main window > **Reports** menu > **User Groups and Accounts...** command

Lists the configured user groups and dual authorization groups.

- Click **CSV Export** to save all information of this dialog box in a CSV file.

11.13.11 Device Permissions dialog box

Main window > **Reports** menu > **Device Permissions...** command

Lists the permissions for using the configured devices for each user group.

- Click **CSV Export** to save all information of this dialog box in a CSV file.

11.13.12 Operating Permissions dialog box

Main window > **Reports** menu > **Operating Permissions...** command

Lists the permissions for using Operator Client for each user group.

- Click **CSV Export** to save all information of this dialog box in a CSV file.

11.14 Alarm Settings dialog box (Settings menu)

See *Alarm Settings dialog box, page 301* for details.

11.15 SNMP Settings dialog box (Settings menu)

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

Allows you to configure SNMP monitoring on your Management Server computer. You specify for which event an SNMP trap is sent, some additional information on your system, and the IP addresses of the computers which are planned to receive SNMP traps from BVMS.

The server sends SNMP traps when events occur. You can receive these traps with the SNMP receiver in Configuration Client using the **SNMP Trap Logger** tool. You can also use another software that can receive SNMP traps.

The SNMP agent in BVMS supports SNMP GetRequest. When an SNMP manager software (for example iReasoning MIB Browser) sends an SNMP GetRequest to the BVMS Management Server then the Management Server sends a corresponding response message.

The MIB file is located in the following file:

```
<installation_directory>\Bosch\VMS\bin\BVMS.mib
```

Only SNMPv1 and v2 are supported.

Note: SNMPv1 and SNMPv2 are not completely compatible. Hence we recommend not using SNMPv1 and SNMPv2 together.

SNMP GET port

Type in the port number for SNMP GetRequest. This is the port where the SNMP agent of the BVMS Management Server listens for SNMP GetRequest.

Note: BVMS does not use the standard port number 161 for SNMP GetRequest, because this port is possibly used by the SNMP agent of the computer where the BVMS Management Server is installed on.

The default value is `12544`.

System contact

Type in contact data for your BVMS. You can retrieve this information with an SNMP GetRequest using the OID .1.3.6.1.2.1.1.4.

System description
Type in a description of your BVMS. You can retrieve this information with an SNMP GetRequest using the OID .1.3.6.1.2.1.1.5.

System location
Type in the location of your BVMS. This string should specify the physical location of the server computer, for example building, room number, rack-number, etc.
You can retrieve this information with an SNMP GetRequest using the OID .1.3.6.1.2.1.1.6.

Trap Receivers
Type the IP address of the computer where BVMS is supposed to send SNMP traps to.

Trap Filter
Click to select the events in the Event Tree to filter the SNMP traps that are sent.

See also
– *Configuring SNMP monitoring, page 106*

11.16 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.

Monitor Group (MG) Settings
Allows you to configure that the users can control all monitor groups with each BVMS client computer. It is then not required to configure this computer as a workstation in the Device Tree.
This setting is enabled after activating the configuration.

Decoders automatically select the stream when connecting to camera
Allows you to configure that all decoders in your system use a compatible stream and not necessarily the Live stream.
This setting is enabled after activating the configuration.

Logbook Configuration
Allows you to configure the connection string for the Logbook database.

Notice!
Change this string only when you want to configure a remote SQL server for the Logbook and only when you are familiar with SQL server technology.

Allows you to define a maximum retention time of the entries within the logbook. After this defined retention time the entries are automatically deleted.
This setting is enabled after activating the configuration.

Advanced State Display
Disable hot spot coloring in maps
Allows you to configure disabling blinking hotspots in maps.

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

Enable advanced alarm display (hotspot coloring in maps depending on alarm)
Allows you to configure for all alarms that the hotspots of the devices belonging to this alarm, are displayed with a background color and blink when the configured alarm occurs.
The configuration of the advanced state display is possible after you saved the configuration.
The hotspots are displayed on a map in Operator Client after you have activated the configuration.

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.
This setting is enabled after activating the configuration.

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

Global iSCSI connection password (CHAP password):
Type the iSCSI CHAP password which is necessary to authenticate at the iSCSI storage device and to enable a direct playback from the iSCSI.
Note: The iSCSI CHAP password and the system-wide CHAP password must be identical.
See *System-wide CHAP password , page 178*

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

See also
– *System-wide CHAP password , page 178*

11.17 Remote Access Settings dialog box (Settings menu)

Main window > **Settings** menu > **Remote Access Settings...** command
Allows you to configure the port mapping for remote access.
You add one or more port ranges. BVMS automatically assigns each private IP address of a configured device to a different public port number of one these ranges.
In the router that connects your private network with the public network, you configure the same port mapping. The router then forwards each packet with public port number from the public network to the private IP address and port number. Private IP address and port number have been configured in the port mapping table for this public port number.

Notice!
Additionally in the router you must manually configure the port forwarding according to the settings in the port mapping table.

Enable Port Mapping
Click to enable / disable port mapping.

Add
Click to add a port range in the **Port Ranges** list.

Edit
Click to change a selected entry in the **Port Ranges** list.

Remove
Click to remove a selected entry in the **Port Ranges** list.

Private IP address (for access within the LAN)
Select the private IP address of your Management Server local network adapter.

Public network address (IP address or DNS name, for access from external, e.g. via Internet)
Type in the public network address of this private network. The remote Operator Client logs on with this public network address to get access to the devices of this Management Server.

Show Port Mapping...
Click to display the **Port Mapping Table** dialog box.

See also
– *Remote access, page 28*

11.17.1 Port Mapping Table dialog box

Main window > **Settings** menu > **Remote Access Settings...** command > **Show Port Mapping...** button > **Port Mapping Table** dialog box
Displays the port mapping for the IP addresses of the configured devices in your BVMS.
You can copy the table into the clipboard and you can add entries that are not managed by BVMS.

Copy to Clipboard
Click to copy the mapping table to the clipboard. This helps you in creating a configuration script for a port mapping in a router (for example a RRAS service).

Protocol
Displays the used network protocol for this device.
You can change the value manually.

Private Port
Displays the private port number used in the private network for this device.
You can change the value manually.

Public Port
Displays the public port number used by Operator Client from public networks to access this device.
You can change the value manually.

Fixed
Click to check to fix the manually assigned port number.
Click to uncheck to enable the automatic assignment of a port number.

12 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.

12.1 Change device passwords dialog box

Main window > **Devices** > **Change device passwords** > **Change device passwords** dialog box
or
Main window > **Hardware** menu > **Change device passwords...** command > **Change device passwords** dialog box

Click to refresh the state information for all devices. You can refresh the state of a single device: Right-click the device and click **Refresh state**.
Note: When you have a large system with several 1000 devices configured, the process of refreshing states can take a long time.

Click to select all available devices at once.

Show passwords
Select the check box when you want the configured passwords being displayed in readable form.

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 .

Note: Only if the **Show passwords** check box is selected, it is possible to also search for passwords.

The table allows you to set the following properties of the available IP devices:

- Service password
- User password
- Live password
- Destination password

To change the password for IP devices:

1. Select the required device.
2. Right-click the selected device and click **Edit password...**.
   The **Changing passwords** dialog box is displayed.
3. Select the required password type.
4. Type in the new password.
5. Click **OK**.
   The new password is updated in the selected device.

To change the settings for multiple devices:

See *Configuring multiple encoders / decoders, page 227*.

12.2 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
- Encoders
- Live only encoders
- Live only ONVIF encoders
- Local storage encoders
- Decoders
- Video Streaming Gateway (VSG) devices
- 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** > Expand > Right-click > Click **Scan for Encoders** > **BVMS Scan Wizard** dialog box

Main window > **Devices** > Expand > Right-click > Click **Scan for Video Streaming Gateways** > **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

Main window > **Devices** > Expand > Expand > Right-click > Click **Scan for decoders** > **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**.

Role

In the list, select the desired entry.

The following table lists which roles each VRM type can have:

Role / Type	Primary VRM	Secondary VRM
Primary (Normal)	X	
Secondary (Normal)		X
Primary Failover	X	
Secondary Failover		X
Mirrored		X

To a Primary VRM you can add a VRM device with the following roles:

– Failover VRM

– Mirrored VRM

To a Secondary VRM you can add VRM devices with the following role:

– Failover VRM

Master VRM

In the list, select the desired entry.

User Name

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

See also

– *Adding VRM Devices via scan, page 175*
– *Adding an encoder to a VRM pool, page 218*
– *Adding a live only encoder, page 218*
– *Adding a local storage encoder, page 219*
– *Scanning for devices, page 84*

12.3 Server list / Address Book page

Main window > **Devices** > **Enterprise System** > **Server List / Address Book**

You can add multiple Management Server computers for simultaneous access in BVMS Enterprise System. You can also add multiple Management Server computers for sequential access for Server Lookup.

You can add additional columns in the Server List. This lets you add further information that the user can search for when using Server Lookup. The added columns are also visible on the **Server Access** page (Main window > **User groups** > **Enterprise User Group** tab > > **Server Access** tab).

Add Server

Click to display the **Add Server** dialog box.

Delete Server

Click to remove the Management Server entries.

Management Server

Displays the names of all added Management Server computers. You can change each entry.

Private Network Address

Displays the private network addresses of all added Management Server computers. You can change each entry.

Public Network Address

Displays the public network addresses of all added Management Server computers. You can change each entry. You need the public network address for accessing this Management Server computer via remote access.

Server Number

Displays the logical numbers of all added Management Server computers. You can change each entry.

Server Description
Type in a description for this Management Server. You need this description to find it in the list of all available servers when you want to access the Management Server exclusively, for example to clarify an alarm coming from another management system.

Click to get a step-by-step instruction:
- *Configuring the Server List for Enterprise System, page 96*
- *Configuring Server Lookup, page 130*
- *Exporting the Server List, page 131*
- *Importing a Server List, page 131*

12.3.1 Add Server dialog box

Main window > **Devices** > **Enterprise System** > **Server List / Address Book**

Server name
Type in the display name of the Management Server.

Private network address
Type in the private IP address or DNS name of the Management Server.

Public network address
Type in the public network address or DNS name used for routed access.

Server description
Type in a description for the Management Server.

12.3.2 Configuring Server Lookup

For Server Lookup, the user of Operator Client or Configuration Client logs on with a user name of a normal user group, not as a user of an Enterprise User Group.

See also
- *Server Lookup, page 26*
- *Server list / Address Book page, page 129*
- *Using Server Lookup, page 84*

12.3.3 Configuring the Server List

Main window > **Devices** > **Enterprise System** > **Server List / Address Book**

To add servers:
1. Click **Add Server**.
   The **Add Server** dialog box is displayed.
2. Type in a display name for the server and type in the private network address (DNS name or IP address).
3. If required, type in a public network address (DNS name or IP address) for remote access.
4. Click **OK**.
5. Repeat these steps until you have added all desired Management Server computers.

To add colums:
- Right-click on the table header and click **Add column**.
  You can add up to 10 columns.
  To delete a column, right-click the desired column and click **Delete column**.

✓ When you export the Server List, the added columns are also exported.

See also
– *Configuring the Server List for Enterprise System, page 96*

12.3.4 Exporting the Server List

Main window > **Devices** > **Enterprise System** > **Server List / Address Book**
You can export the Server List with all configured properties for editing and later import.
When you edit the exported csv file in an external editor, note the limitations described in the Server List chapter.

To export:
1. Right-click on the table header and click **Export Server List...**.
2. Type in a name for the export file and click **Save**.
✓ All columns of the Server List are exported as a csv file.

Related Topics
– *Server Lookup, page 26*
– Server List
– *Server list / Address Book page, page 129*

12.3.5 Importing a Server List

Main window > **Devices** > **Enterprise System** > **Server List / Address Book**
When you have edited the exported csv file in an external editor, note the limitations described in the Server List chapter.

To import:
1. Right-click on the table header and click **Import Server List...**.
2. Click the desired file and click **Open**.

Related Topics
– *Server Lookup, page 26*
– Server List
– *Server list / Address Book page, page 129*

12.4 NVRs / Failover NVRs / Redundant NVRs page

As of BVMS 5.0, NVRs, Failover NVRs, and Redundant NVRs are not supported any longer.

12.5 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.

See also

– *Configuring the integration of a DiBos system, page 133*

12.5.1 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.

12.5.2 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.

See also

– *Configuring the integration of a DiBos system, page 133*

12.5.3 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.

See also

– *Configuring the integration of a DiBos system, page 133*

12.5.4 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.

See also

– *Configuring the integration of a DiBos system, page 133*

12.5.5 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.

See also

– *Configuring the integration of a DiBos system, page 133*

12.5.6 Configuring the integration of a DiBos system

Main window > **Devices** > Expand >

Notice!

You do not configure the DiBos system itself but only the integration into BVMS.

To scan for new DiBos devices:

- Right-click and click **Rescan BRS/DiBos System**.
  The DiBos system is scanned for new devices and they are added.

To remove an item:

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

To rename a DiBos device:

1. Right-click a DiBos device and click **Rename**.
2. Type the new name for the item.

12.6 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.

See also
- *DVR devices, page 134*
- *Configuring the integration of a DVR, page 136*

12.6.1 DVR devices

This chapter gives background information on the DVR devices that you can integrate in BVMS.
Some DVR models (e.g. DHR-700) support recording from encoders / IP cameras. Other DVR models support only analog cameras.
An encoder / IP camera should not be integrated into the configuration of two video systems (DVRs or video management systems).
If encoders / IP cameras are connected to a DVR which is already integrated in BVMS, these encoders / IP cameras are not detected by the BVMS network device scan. This holds true for the network scan started from within Configuration Client or started from within Config Wizard.
If a DVR with connected encoders / IP cameras is integrated in BVMS and these encoders / IP cameras are already added to BVMS, a warning is displayed. Remove these encoders / IP cameras from the DVR or from BVMS.
Config Wizard does not add DVR devices with conflicting IP cameras to the configuration.
DVR devices support a limited number of simultaneous connections. This number defines the maximum number of Operator Client users that can simultaneously display videos from this DVR without black Image panes being displayed.

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!
DIVAR AN 3000/5000: When you delete video data from the DVR, please note that you always delete at least the full hour of video data. For example if you select a time period from 6:50 to 7:05, you will effectively delete the video data from 6:00 through 8:00.

Bosch 700 Series Hybrid and Network HD Recorders: Deletion always starts with the beginning of the recordings of all cameras that are displayed in Operator Client, and ends with the point in time that you enter.

See also
- *DVR (Digital Video Recorder) page, page 133*
- *Configuring the integration of a DVR, page 136*

12.6.2 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.

12.6.3 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.

See also
– *Adding a device, page 126*

12.6.4 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.

12.6.5 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.

12.6.6 Inputs tab

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

12.6.7 Relays tab

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

12.6.8 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.

See also
- *Adding a device, page 126*
- *DVR (Digital Video Recorder) page, page 133*

12.7 Matrix Switches page

Main window > **Devices** > >

Displays the property pages of the Bosch Allegiant device.

You do not configure the Bosch Allegiant device itself but only the BVMS related properties.

For connecting an Allegiant device with BVMS, see the **Concepts** chapter in this Online Help. This chapter provides background information on selected issues.

You can additionally configure control priorities for Allegiant trunk lines.

- Click a tab to display the corresponding property page.

See also

- *Configuring a Bosch Allegiant device, page 137*
- *Connecting Bosch Allegiant Matrix to BVMS, page 66*

12.7.1 Adding a Bosch Allegiant device

To add a Bosch Allegiant device:

1. Right-click and click **Add Allegiant**.
   The **Open** dialog box is displayed.
2. Select the appropriate Allegiant configuration file and click **OK**.
   The Bosch Allegiant device is added to your system.

Note: You can add only one Bosch Allegiant matrix.

12.7.2 Configuring a Bosch Allegiant device

Main window > **Devices** > Expand >

You do not configure the Bosch Allegiant device itself but only the BVMS related properties.

To assign an output to an encoder:

1. Click the **Outputs** tab.
2. In the **Usage** column, click **Digital Trunk** in the desired cells.
3. In the **Encoder** column, select the desired encoder.

Adding an input to a Bosch Allegiant device:

1. Click the **Inputs** tab.
2. Click **Add Inputs**. A new row is added to table.
3. Type the required settings in the cells.

Deleting an input:

1. Click the **Inputs** tab.
2. Click the required table row.
3. Click **Delete Input**. The row is deleted from the table.

See also

- *Connecting a Bosch IntuiKey keyboard to BVMS, page 63*
- *Connection page, page 139*
- *Cameras page, page 139*
- *Outputs page, page 138*
- *Inputs page, page 138*

12.7.3 Outputs page

Main window > **Devices** > Expand > > **Outputs** tab

Allows you to configure the usage of a Bosch Allegiant device output and to assign an encoder to an output.

To store the video data of a Bosch Allegiant device output in BVMS, you must assign an encoder to the output. This encoder must be connected to the output.

No.

Displays the number of the output.

Allegiant Logical No.

Displays the logical number of the output within Allegiant.

BVMS Logical No.

Allows you to change the logical number of the output within BVMS. If you enter an already used number, a message is displayed.

Name

Displays the name of the output.

Usage

Allows you to change the usage of the output.

If you select **Digital Trunk**, you can assign an encoder to this output in the **Encoder** field. The Allegiant output becomes network-compatible.

If you select **Allegiant Monitor**, in Operator Client the user can assign the camera signal to a hardware monitor. PTZ control is possible if the camera is configured as PTZ camera. In Operator Client, the user cannot drag this camera on an Image pane.

If you select **Unused**, the user cannot assign a monitor to an Allegiant camera.

Encoder

Allows you to assign an output to an encoder. You can only select an encoder when you have checked **Digital Trunk**. The encoder is locked for the Logical Tree. If you assign an encoder that is already in the Logical Tree, it is removed from there. In the Operator Client, the user can drag the camera to an Image pane.

See also

– *Configuring a Bosch Allegiant device, page 137*

12.7.4 Inputs page

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

Allows you to add inputs to a Bosch Allegiant device.

Add Input

Click to add a new row in the table for specifying a new input.

Delete Input

Click to remove a row from the table.

Input No.

Type the required number of the input. If you enter an already used number, a message is displayed.

Input Name
Type the required name of the input.

See also
– *Configuring a Bosch Allegiant device, page 137*

12.7.5 Connection page

Main window > **Devices** > Expand > > **Connection** tab
Displays the name of the Bosch Allegiant configuration file.
BVMS can read out a configuration file in structured storage format with the names and configuration information of all cameras connected to the Bosch Allegiant device.

Update Configuration
Click to select an updated Bosch Allegiant configuration file.

See also
– *Configuring a Bosch Allegiant device, page 137*

12.7.6 Cameras page

Main window > **Devices** > Expand > > **Cameras** tab
Displays a camera table of the cameras that are connected to the Bosch Allegiant device.

No.
Displays the consecutive number of the camera.

Allegiant Logical No.
Displays the logical number of the camera.

Camera Name
Displays the name of the camera.

See also
– *Configuring a Bosch Allegiant device, page 137*

12.8 Workstation page

Main window > **Devices** > Expand >
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.
– Assign a Command Script that is executed on startup of the workstation.
– Select the default stream for live display.
– Enable Forensic Search.
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 .

See also

- *Adding a workstation manually, page 140*
- *Configuring a startup Command Script (settings page), page 141*

12.8.1 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.

12.8.2 Configuring a Bosch IntuiKey keyboard (settings page) (workstation)

Main window > **Devices**> Expand >

To configure a Bosch IntuiKey keyboard connected to a workstation:

1. Click the **Settings** tab.
2. In the **Keyboard Settings** field, make the required settings.

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

See also

- *Workstation page, page 139*

12.8.3 Enabling Forensic Search on a workstation (settings page)

Main window > **Devices** > Expand > > **Settings** page

You must enable Forensic Search on a workstation.

Note:
Enable video content analysis on each encoder. Use the VCA page of the encoder in the Device Tree.

To enable Forensic Search:

- Click to select the **Enable Forensic Search** check box.

12.8.4 Configuring a startup Command Script (settings page)

Main window > **Devices** > Expand > > **Settings** page

You configure a Command Script to be started when the Operator Client on the selected workstation is started.

You must create a corresponding Command Script.

For creating a Command Script, see *Managing Command Scripts, page 100*.

To configure a startup script:

- In the **Startup script:** list, select the required Command Script.

See also

– *Workstation page, page 139*

12.8.5 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.

Network address:
Type the DNS name or the IP address of your workstation.

Startup script:
Select the desired script that you want to be started when the workstation's Operator Client is started. You create or import such a script on the **Events** page.

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

Override settings from "Cameras and Recording" page
Select the check box to enable selecting the desired stream for live view.
Note: For DVR devices which offer more than 1 stream (for example DIVAR AN 3000/5000), the Live stream setting from this DVR is also changed here. Live stream settings for DVR devices are not available on the **Cameras and Recording** page.

Live Stream
Select the desired stream for live view.

When you select **Image pane size optimized**, the resolution of each displayed camera is automatically adjusted to the size of the Image pane depending on the resolution of the used monitor. This is useful for displaying multiple cameras with a large resolution, for example 4K ultra HD cameras. Only cameras with streams whose resolution can be configured independently, can adjust the resolution to the Image pane. The user of Operator Client can change the stream selection for each camera individually.

Use transcoded stream instead, if available
Select the check box to enable the usage of a transcoded stream if available. This transcoded stream is used instead of the selected stream for live view.
For a transcoded stream being available in BVMS, either MVS must be installed or your VRM computer offers a built-in hardware transcoder.
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.

Enable Forensic Search
Click to enable Forensic Search for this workstation.

Use direct playback from storage
Select the check box to send the video stream directly from the storage device to this workstation. Now the stream is not sent via VRM. The workstation still needs connection to the VRM to ensure correct playback.
Note: You can only use the direct playback from the iSCSI storage device if you have set the global iSCSI CHAP password.
See *Global iSCSI connection password (CHAP password): , page 123*

Retrieve live video from Video Streaming Gateway instead of camera
Displays the list of Video Streaming Gateway devices. Select the desired entries to enable the transmission of video data via low bandwidth segments between the video source and this workstation.

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.

See also
- *Configuring a startup Command Script (settings page), page 141*
- *Enabling Forensic Search on a workstation (settings page), page 140*
- *Global iSCSI connection password (CHAP password): , page 123*

12.8.6 Changing the network address of a workstation

Main window > **Devices** > Expand

To change the IP address:

1. Right-click and click **Change Network Address**.
   The **Change Network Address** dialog box is displayed.
2. Change the entry in the field according to your requirements.

12.9 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.

See also
- *Scanning for devices, page 84*
- *Bosch Encoder / Decoder / Camera page, page 217*

12.9.1 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:

1. Expand , expand , right-click .
   Or
   Right-click .
   Or
   Right-click .
2. Click **Add Encoder**.
   The **Add Encoder** dialog box is displayed.
3. Enter the appropriate IP address.
4. In the list, select **<Auto Detect>.**

5. Click **OK**.
   The device is added to the system.
6. 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** > Expand > Expand > Right-click > Click **Add Encoder** > **Add Encoder** dialog box
or

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

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

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

12.9.2 Edit Encoder / Edit Decoder dialog box

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

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

or

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

or

Main window > **Devices** > Expand > Expand > Right-click > Click **Edit 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.

See also
- *Encrypting live video (Edit Encoder), page 219*
- *Updating the device capabilities (Edit Encoder), page 220*

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

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

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.

See also
– *Providing the destination password for a decoder (Authenticate...), page 213*

12.9.4 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.

12.9.5 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.

12.9.6 Configuring a Bosch IntuiKey keyboard (decoder)

Main window > **Devices**> Expand >

Notice!
You cannot connect a KBD-Universal XF keyboard to a decoder.

To configure a Bosch IntuiKey keyboard connected to a decoder:

1. In the **Connection** column, click a cell, and select the appropriate decoder.
   You can also select a workstation, if the Bosch IntuiKey keyboard is connected to it.
   A workstation must be configured on the page.
2. In the **Connection Settings** field, make the required settings.

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

See also

- *Assign Keyboard page, page 162*
- *Scenarios for Bosch IntuiKey keyboard connections, page 63*
- *Connecting a Bosch IntuiKey keyboard to a decoder, page 64*

12.9.7 Configuring a decoder for use with a Bosch IntuiKey keyboard

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

Perform the following steps to configure a VIP XD decoder that is connected to a Bosch IntuiKey keyboard.

To configure a decoder:

1. Click the appropriate decoder which is used for connecting a Bosch IntuiKey keyboard.
2. Click the **Periphery** tab.
3. Ensure that the following settings are applied:
   - Serial port function: **Transparent**
   - Baud rate: **19200**
   - Stop bits: **1**
   - Parity check: **None**
   - Interface mode: **RS232**
   - Half-duplex mode: **Off**

See also

- *Scenarios for Bosch IntuiKey keyboard connections, page 63*
- *Connecting a Bosch IntuiKey keyboard to a decoder, page 64*
- *Updating Bosch IntuiKey keyboard firmware, page 65*

12.9.8 Delete decoder logo

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

12.10 Monitor groups page

Main window > **Devices** > Expand >
Allows you to add and configure monitor groups. You assign a monitor group to a BVMS workstation in .

Notice!
You cannot control a monitor group from within Operator Client when the connection to the Management Server is lost.

See also
- *Adding a monitor group manually, page 149*
- *Configuring a monitor group, page 149*

12.10.1 Adding a monitor group manually

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

1. Click **Add monitor group**.
   The **Add monitor group** dialog box is displayed. Type in the name for your new monitor group.
2. Click OK.
   The monitor group is added to your system.
3. Click **Maps and Structure**.
4. Drag the monitor group to the Logical Tree.

12.10.2 Configuring a monitor group

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

Notice!
You cannot control a monitor group from within Operator Client when the connection to the Management Server is lost.

You configure the monitors in a monitor group logically in rows and columns. This arrangement does not have to meet the physical arrangement of the monitors.

To configure a monitor group:
1. Drag the appropriate monitors from the **Unassigned monitors** tab to the monitor groups field.

2. In the **Layout** tab, select the appropriate layout.
3. Drag any available camera from the **Cameras** tab to a monitor pane on the left.
   The logical number of the camera is displayed as a black number on the monitor pane and the color of this pane changes.
4. Change the logical numbers of the image panes as required. If you enter an already used number, a message box is displayed.
5. In the **Options** tab, you can select, if the camera name and number are visible in the monitor pane. You can also select the position of this information.

Monitor image
The black bold number, if present, displays the logical number of the initial camera. The black light number displays the logical number of the monitor.
To un-assign a camera, right-click the monitor pane and click **Clear monitor** or drag the camera outside the image pane.

See also
– *Adding a monitor group manually, page 149*

12.11 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.

See also

– *Sequence Builder dialog box, page 256*

12.11.1 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.

12.12 Communication Devices page

Main window > **Devices** > Expand >

Allows you to add or configure a communication device.

You can configure the following communication devices:

– E-mail
– SMS (GSM or SMSC dial-up provider)

See also

– *Configuring a communication device, page 153*

12.12.1 Adding an E-mail/SMTP Server

To add a communication device:

1. Expand , right-click and click **Add E-mail/SMTP Device**
   The **Add E-mail/SMTP Device** dialog box is displayed.
2. Enter the appropriate settings.
3. Click **OK**.
   The communication device is added to your system.

Add E-mail/SMTP Device dialog box

Name:

Type the display name of the e-mail server.

12.12.2 Adding a SMS Device

To add a communication device:

1. Expand , right-click and click **Add SMS Device**.
   The **Add SMS Device** dialog box is displayed.
2. Enter the appropriate settings.
3. Click **OK**.
   The communication device is added to your system.

Add SMS Device dialog box

Name:

Type the name of the SMS server that is used for being displayed.

GSM modem

Click to add a GSM modem.

SMSC dial up

Click to add a Hayes compatible modem which can connect to an SMSC provider.

12.12.3 SMTP Server page

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

Allows you to configure the e-mail settings of your system. On the **Events** page, you can assign an event to an e-mail. When this event occurs, the systems sends an e-mail. You cannot receive e-mails in BVMS.

SMTP server name
Type the name of the e-mail server. You get the information about the required entry from your provider. Usually this is the IP address or DNS name of your e-mail server.

Sender address
Type the email the email address which is used as the sender address when the system sends an email, for example in case of an alarm.

SSL/TLS
Select the check box to enable the usage of a secure SSL/TLS connection. In this case the network port switches automatically to 587.

Port
Type the required network port number for outgoing mails. You get the information about the required entry from your provider.
Port 25 is selected automatically when you disable the **SSL/TLS** setting.
You can select another port if required.

Connection time-out [s]
Type the number of seconds of inactivity until the connection is disconnected.

Authentification
Select a check box for the required authentication method. You get the information about the required entry from your provider.

User name
Type the user name for authenticating at the e-mail server. You get the information about the required entry from your provider.

Password:
Type the password for authenticating at the e-mail server. You get the information about the required entry from your provider.

Send Test E-mail
Click to display the **Send Test E-mail** dialog box.

See also
– *Configuring a communication device, page 153*

12.12.4 Configuring a communication device

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

To configure a communication device:

1. Click the required device: or .
2. Make the appropriate settings.

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

See also
– *Adding an E-mail/SMTP Server, page 152*
– *Adding a SMS Device, page 152*
– *SMTP Server page, page 152*
– *GSM Settings / SMSC Settings page, page 154*

12.12.5 Send Test E-mail dialog box

Main window > **Devices** > Expand > Expand > > **Send Test E-mail** button

Allows you to send a test e-mail.

From:

Type the e-mail address of the sender.

To

Type the e-mail address of the recipient.

Subject

Type the subject of the e-mail.

Message

Type the message.

Send Test E-mail

Click to send the e-Mail.

See also

– *Configuring a communication device, page 153*

12.12.6 GSM Settings / SMSC Settings page

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

Allows you to configure the SMS settings of your BVMS. On the **Events** page, you can assign an event to a short message. When this event occurs, the system sends a short message. If the number of entered characters exceeds the highest permitted number (usually 160), an SMS is divided into multiple parts.

Device:

Select the required COM port where the external modem is connected to. If your computer has an internal modem, select the corresponding entry.

Speed

Select the required transfer rate.

PIN (for GSM device only)

Type the personal identification number for authenticating at the device.

Data format (for SMSC device only)

Select the required data format. You get the information about the required entry from your provider.

Unicode (for GSM device only)

Select the check box to enable unicode characters. This reduces the highest number of permitted characters to 80.

Dial string (for SMSC device only)

Type the number to connect to the SMSC dial-up provider. You get this number from your provider.

Password: (for SMSC device only)
Type the password that the device needs to connect to the SMSC dial-up provider if required. You get the information about the required entry from your provider.

Protocol (for SMSC device only)
Select the required protocol that the device uses to connect to the SMSC dial-up provider. You get the information about the required entry from your provider.

Recipient
Type the mobile phone number of the recipient of the short messages. Include the country prefix without + sign (e.g. +49170123456).

Message (max. 160 chars)
Type the text for the short message.

SMS Test Message
Click to send a test short message.

See also
- *Configuring a communication device, page 153*

12.13 ATM/POS page

Main window > **Devices** > Expand >
Allows you to add and configure peripheral devices, for example, a Bosch ATM/POS Bridge. If you want to add multiple bridges at one server, you must use different ports.

See also
- *Adding a Bosch ATM/POS bridge, page 108*
- *Configuring a peripheral device, page 156*

12.13.1 Adding a Bosch ATM/POS-Bridge manually

Main window > **Devices** > Expand > Right-click > **Add Bosch ATM/POS-Bridge** .
Allows you to add a Bosch ATM/POS Bridge.

To add a peripheral device:

1. Expand , right-click and click **Add Bosch ATM/POS-Bridge**.
   The **Add Bosch ATM/POS-Bridge** dialog box is displayed.
2. Enter the appropriate settings.
3. Click **OK**.
   The peripheral device is added to your system.

Add Bosch ATM/POS-Bridge dialog box

Name:
Type an appropriate name for the device.

IP address:
Type the IP address of the device.

Port 1:
Type the appropriate port number used as the listening port of the ATM/POS Bridge.

Port 2:
Type the appropriate port number used as the listening port of the BVMS Management Server.

Notice!
When you add multiple ATM/POS Bridges to your system, ensure that the numbers for port 2 of each device deviate. Using the same number for port 2 multiple times can lead to ATM/POS data loss.

See also
– *Adding a Bosch ATM/POS bridge, page 108*

12.13.2 Bosch ATM/POS-Bridge page

Main window > **Devices** > Expand > Expand > > **Bosch ATM/POS-Bridge** tab
Allows you to configure a Bosch ATM/POS Bridge.

IP address:
Type in the IP address of the device.

Port 1:
Type the appropriate port number used as the listening port of the ATM/POS Bridge.

Port 2:
Type the appropriate port number used as the listening port of the BVMS Management Server.

Notice!
When you add multiple ATM/POS Bridges to your system, ensure that the numbers for port 2 of each device deviate. Using the same number for port 2 multiple times can lead to ATM/POS data loss.

See also
– *Configuring a peripheral device, page 156*
– *Adding a Bosch ATM/POS bridge, page 108*

12.13.3 Configuring a peripheral device

Main window > **Devices** > Expand > Expand > **Bosch ATM/POS-Bridge**
or
Main window > **Devices** > Expand > Expand > **DTP Device** >

To configure a peripheral device:
▸ Change the required settings.
For detailed information on the various fields, follow the link to the appropriate application window below.

See also
- *ATM Settings page, page 157*
- *Bosch ATM/POS-Bridge page, page 156*
- *DTP Settings page, page 157*

12.13.4 DTP Settings page

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

Allows you to configure a DTP device with maximum 4 ATM devices connected to this DTP device.

Serial port
In the list, select the appropriate port.

See also
- *ATM Settings page, page 157*
- *Configuring a peripheral device, page 156*

12.13.5 ATM Settings page

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

Allows you to configure an ATM device that is connected to a DTP.

Input number of the DTP device
Select the desired input number. If the number is already used by another ATM device, you can swap the input numbers.

Connection timeout [hours]
Enter the desired number of hours. When during this time period the ATM device did not send any transaction data, BVMS assumes that the connection is disconnected. A corresponding event is triggered. The **Not Authenticated** event is available for an ATM device but not relevant.
Entering **0** means that no connection check is performed.

Data Inputs
Click to enable the desired inputs and type in a desired name for the inputs.

See also
- *Configuring a peripheral device, page 156*

12.13.6 Inputs page

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

Allows you to configure the inputs of a Bosch ATM/POS Bridge.

See also
- *Configuring a peripheral device, page 156*
- *Adding a Bosch ATM/POS bridge, page 108*

12.14 Foyer Card Readers

Main window > **Devices** > Expand > > **Global Settings for Foyer Card Readers** tab

You can configure the settings that are valid for all foyer card readers in your system.

Serial port

Select the serial port to which the foyer card reader is connected.

Locked Out

Allows you to add bank routing codes for locking out. This means that cards with the lock characteristics entered here do not have access authorization. Access is denied by the foyer card reader. The default mode of electric door lock release of the foyer card reader must be set to: **Automatic**

The list may contain entries with wildcards:

?: Indicates any or no character at this position.

*: Indicates a sequence (one or more characters) of any or no characters (exception: * on its own means that all bank sort codes are locked out).

Ignore country code on EC cards

Click to enable that BVMS does not analyze card data that is used to identify in which country the card was issued. Access is possible for cards with a different country code.

12.14.1 Add Foyer Card Reader dialog box

Main window > **Devices** > Expand > Right-click > **Add Foyer Card Reader** command

You can add a foyer card reader.

Name

Type in a name for the device.

Device identifier

Select a unique number for the device. If no numbers are available, the maximum number of foyer card readers have already been added to the system.

12.14.2 Settings for Foyer Card Reader page

Main window > **Devices** > Expand > > > **Settings for Foyer Card Reader** tab

You can configure a foyer card reader.

Device identifier

Displays the unique number of the device.

Enable skimming protection

Click to enable that BVMS triggers an event when an attached skimming device detects skimming. This is not supported by all types of foyer card readers.

Default mode of electric door lock release

Open: The door is open and everybody can access without a card.

Closed: The door is closed, no matter what card is inserted.

Automatic: The door only opens when a card with access authorization is inserted in the reader.

Enable schedule-based control
Click to enable that you can assign a schedule to the selected release mode of the door lock. When a schedule becomes active, BVMS switches the foyer card reader to the corresponding release mode.
If the selected schedules overlap, the effective door release mode is determined by the following priority of modes: 1. **Open** 2. **Closed** 3. **Automatic**

12.15 Virtual Inputs page

Main window > **Devices** > Expand >
Displays the virtual inputs configured in your system.
Allows you to add new virtual inputs and to delete existing ones.

Add Inputs
Click to display a dialog box for adding new virtual inputs.

Delete Inputs
Click to delete a selected virtual input.

Number
Displays the number of the virtual input.

Name
Click a cell to modify the name of the virtual input.

12.15.1 Adding Virtual Inputs manually

Main window > **Devices** > Expand > **Add Inputs** button
Allows you to add new virtual inputs.

To add a virtual input:

1. Expand , click .
   The corresponding page is displayed.
2. Click **Add Inputs**.
   A row is added to the table.
3. Make the appropriate settings.
4. Click **Add**.
   The virtual input is added to your system.

Add Inputs dialog box

Start:
Select the first number of the new virtual inputs.

End:
Select the last number of the new virtual inputs.

Name:
Type in the name of each new virtual input. A consecutive number is appended.

Add
Click to add new virtual inputs.

12.16 SNMP page

Main window > **Devices** > Expand >

Allows you to add or configure an SNMP measurement for maintaining the network quality.

See also

– *Configuring an SNMP trap receiver (SNMP trap receiver page), page 160*

12.16.1 Adding an SNMP manually

Main window > **Devices** > Expand > Right-click > **Add SNMP** command

Allows you to add a network monitoring system to your BVMS.

To add a network monitoring device:

1. Expand , right-click and click **Add SNMP**.
   The **Add SNMP** dialog box is displayed.
2. Type a name for the SNMP device.
   The network monitoring device is added to your system.

Add SNMPdialog box

Name:

Type a name for the network monitoring device.

See also

– *Configuring an SNMP trap receiver (SNMP trap receiver page), page 160*

12.16.2 Configuring an SNMP trap receiver (SNMP trap receiver page)

Main window > **Devices**> Expand

To configure the SNMP trap receiver:

1. Click to display the **SNMP Trap Receiver** page.
2. Make the required settings.

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

SNMP Trap Receiver page.

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

Allows you to select devices for monitoring and to select SNMP trap OIDs that trigger an event for the selected device when they are received.

Notice!
You must enter the IP address of the Bosch Video Management System Management Server as the trap receiver in your devices that you want to monitor.

SNMP Trap Sending Devices:
Allows you to enter a range of IP addresses of the monitored network devices. To monitor a single device enter the corresponding IP address in the **Range From** cell.
Be careful when changing these addresses. Entering a wrong address stops network monitoring of this device.

SNMP Trap Filter Rules:
Allows you to enter OIDs and corresponding values. You can use wildcards as * and ? to enhance the filter range. If you enter OIDs and values in more than one row, these filter rules must match simultaneously to trigger an event. In both columns, you can enter a regular expression in {}. If there are characters outside the brackets, the regular expression is not evaluated.

Show Trap Logger Tool
Click to display the **SNMP Trap Logger** dialog box for tracing SNMP trap OIDs.

12.16.3 SNMP Trap Logger dialog box

Main window > **Devices** > Expand > Expand > Select a generic SNMP Trap Receiver > Click **Show Trap Logger Tool**
Allows you to trace SNMPtrapOIDs. You can receive traps from all devices in your network or only from selected ones. You can filter the traps to be received and you can add OIDs and values of selected traps to the **SNMP Trap Filter Rules:** table.

Start/Pause
Click to start or stop a tracing process.

Only Traps From Sender
Enter the IP address or DNS name of a device. Only traps from this device are traced.

Only Traps Containing
Enter a string a trap can contain. You can use * and ? as wildcards. Strings in {} are treated as regular expressions. Only traps containing such a string are traced.

Received Traps
Displays the traps that are received by a tracing process.

Click to remove all entries in the **Received Traps** field.

Trap Details
Displays the trap details. You can copy the OID and the Value entry to the **SNMP Trap Filter Rules:** table.

See also
– *Configuring an SNMP trap receiver (SNMP trap receiver page), page 160*

12.17 Assign Keyboard page

Main window > **Devices** > Expand >

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.

See also
- *Configuring a decoder for use with a Bosch IntuiKey keyboard, page 148*
- *Configuring a Bosch IntuiKey keyboard (settings page) (workstation), page 140*
- *Configuring a Bosch IntuiKey keyboard (decoder), page 148*

12.18 I/O Modules page

Main window > **Devices** > Expand >
Allows you to add or configure an I/O module.
Currently only ADAM devices are supported.

See also
- *Configuring an I/O module, page 163*

12.18.1 Adding an I/O module manually

To add an I/O module:

1. Expand , right-click and click **Add New ADAM Device**.
   The **Add ADAM** dialog box is displayed.
2. Type the IP address of the device.
3. Select the device type.
   The corresponding page is displayed.
4. Click the **ADAM** tab to change the display names of the inputs if required.
5. Click the **Name** tab to change the display names of the Relays if required.

Notice!
You can also perform a scan for ADAM devices (**Scan for ADAM Devices**). The IP addresses of the devices are detected. If available the device type is preselected. You must confirm this selection.

12.18.2 Configuring an I/O module

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

To configure an I/O module:

Notice!
Avoid changing the device type.
When you reduce the number of inputs or relays, all configuration data for the removed inputs or relays are deleted.

1. Click the **ADAM** tab.
2. In the **Adam type:** list, select the appropriate device type.

3. Click the **Inputs** tab.
4. In the **Name** column, change the display name of an input if required.
5. Click the **Relays** tab.
6. In the **Relays** column, change the name of a relay if required.

To change an IP address:

1. In the device tree, right-click an ADAM device.
2. Select **Change network address**.
3. Type the new IP address and click **Ok**.
4. Activate the configuration.

✓ The new IP address is used to access the device.

See also

– *I/O Modules page, page 163*

12.18.3 ADAM page

Main window > **Devices** > Expand > > > **ADAM** tab

Displays information on the selected ADAM device.

Allows you to change the display name of an ADAM device.

Adam type:

Select the appropriate device type.

Inputs total:

Displays the total number of inputs available with this device type.

Relays/Outputs total:

Displays the total number of relays available with this device type.

12.18.4 Inputs page

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

Allows you to change the display names of the inputs of the selected ADAM device.

Number

Displays the logical number of the input.

Name

Click a cell to change the display name of an input.

12.18.5 Relays page

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

Allows you to change the display names of the relays of the selected ADAM device.

Number

Click a cell to change the logical number of a relay.

Name

Type the display name of the relay.

12.19 Allegiant CCL Emulation page

Main window > **Devices** > Expand >
Allows you to activate the Allegiant CCL emulation.
Allegiant CCL commands supported in BVMS, page 70 lists the CCL commands supported in Bosch Video Management System.

Note:
Do not configure the Allegiant CCL emulation and an Allegiant device to the same COM port. If for both devices the same COM port is configured, the Allegiant device wins. The access of the Allegiant CCL emulation device fails with an appropriate message.
To solve this, the Management Server must have two different COM ports or connect the Allegiant device to another computer.

Enable Allegiant CCL Emulation
Select the check box to enable the emulation.

Baud rate
Select the value for the transmission rate in bit/s.

Stop bits
Select the number of stop bits per character.

Parity check
Select the type of parity check.

Handshake
Select the desired method for flow control.

Model
Select the Allegiant model that you want to emulate.

See also
– *Configuring an Allegiant CCL emulation, page 166*

12.19.1 Adding an Allegiant CCL emulation manually

To add an Allegiant CCL emulation:

1. Expand , click .
   The **Allegiant CCL Emulation** tab is displayed.
2. Click to check **Enable Allegiant CCL Emulation**.
3. Make the required settings.
   The Allegiant CCL emulation service is started on the Management Server.

12.19.2 Allegiant CCL commands

You use CCL commands for switching IP cameras or encoders to IP decoders both configured in BVMS. You cannot use CCL commands to directly control analog cameras or the Allegiant matrix itself.
The Allegiant CCL emulation starts an internal BVMS service that translates CCL commands of the Matrix Switch into BVMS. You configure a COM port of the Management Server to listen to these CCL commands. The CCL emulation helps to exchange existing Allegiant devices with

Bosch Video Management System or to use Bosch Video Management System with applications that support the Allegiant CCL commands. Old Allegiant hardware configured in BVMS cannot be controlled with these commands.

12.19.3 Configuring an Allegiant CCL emulation

Main window > **Devices**> Expand >

To use the CCL commands you need the CCL User Guide. This manual is available in the Online Product Catalog in the document section of each LTC Allegiant Matrix.
The *Allegiant CCL commands supported in BVMS, page 70* section lists the CCL commands supported in Bosch Video Management System.

To configure an Allegiant CCL emulation:

1. Click **Enable Allegiant CCL Emulation**.
2. Configure the communication settings as required.

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

See also

– *Allegiant CCL Emulation page, page 165*

12.20 Mobile Video Service page

Main window > **Devices** >

Allows you to add one or more transcoding service entries to your BVMS. This transcoding service adapts the video stream from a camera configured in BVMS to the available network bandwidth. This enables mobile video clients like an iPhone, iPad or Web Client to receive live or playback video data via unreliable network connections with limited bandwidth.

See also

– *Adding a Mobile Video Service manually, page 167*

12.20.1 Mobile Video Service

Mobile Video Service is transcoding video streams from the source to the available bandwidth of connected clients. The interfaces of the Mobile Video Service are designed to support clients on multiple platforms, for example Mobile devices (IOS; iPad, iPhone) and Windows Internet Explorer HTML client.
Mobile Video Service is based on Microsoft Internet Information Service.
One mobile service may serve several clients synchronously.
For limits refer to data sheet and the Technical Note Mobile Video Service available in the Online Product Catalog for BVMS.

Internet Information Service

Configure the settings for Internet Information Service on the computer where you plan to install MVS for BVMS.

Installation notes

You cannot add Mobile Video Service (MVS) in Configuration Client when the time between the Configuration Client computer and the Mobile Video Service computer is not synchronized. Please ensure that the time is synchronized between the affected computers.

Install and configure Internet Information Service (IIS) before you install Mobile Video Service. If IIS is not installed, BVMS Setup to install Mobile Video Service aborts.
You select the Mobile Video Service component for installation during BVMS Setup.
You cannot install VRM and Mobile Video Service on the same computer.
We recommend that you do not install Mobile Video Service on the same computer where you install Management Server.
With Mobile App you can perform the following tasks:

- Displaying video
  - Live
  - Playback
- Sending live video
- Recording and sending recorded video
- Alarm recording
- Monitoring network and server

Related Topics

- Adding a Mobile Video Service
- *Mobile Video Service page, page 166*

12.20.2 Adding a Mobile Video Service manually

Main window > **Devices** > Right-click > Click **Add Mobile Video Service**
You can add one or more Mobile Video Service entries to your BVMS.

To add:

1. Type in the URI of your Mobile Video Service.
2. Click **OK**.

✓ Mobile Video Service and Management Server now know each other and the Mobile Video Service can receive configuration data from Management Server.

Add Mobile Video Service dialog box

URI

Type in the URI of your Mobile Video Service. Follow the syntax rules of the example:

https://www.MyDomain.org/mvs

You must start the entry always with https://, even when you did not configure an encrypted access to your Web server.

12.21 Intrusion panels page

Main window > **Devices** > Expand >
Allows you to add and configure intrusion panels from Bosch. The device must be connected and available.
When you have added an intrusion panel, the areas, points, doors, and relays are displayed in the Device Tree hierarchically.
You can remove or rename the panel, each area, each point, each door, and each relay.
When the configuration on the intrusion panel was changed, you must rescan the device to display the changes in BVMS.

Notice!
All alarm events that can occur at a point, are automatically configured as a BVMS alarm.
Example: Fire alarm

Notice!
If a door is not assigned to a point in the configuration of an intrusion panel that is added to your BVMS, an alarm from this door does not trigger a BVMS event and hence no BVMS alarm.

12.21.1 Adding an Intrusion Panel manually

Main window > **Devices** > Expand > Right-click > **Add Panel** command
Allows you to add an intrusion panel from Bosch.

To add an intrusion panel:

1. Expand , right-click and click **Add Panel**.
   The **Add Intrusion Panel** dialog box is displayed.
2. Enter the appropriate values.
3. Click **OK**.
   The intrusion panel is added to your system.

Add Intrusion Panel dialog box

Network address
Type in the IP address of the device.

Network port
Select the port number configured in the device.

Automation passcode
Type in the passcode for authenticating at the device.

12.21.2 Settings page

Main window > **Devices** > Expand > Expand > > **Settings** tab
Allows you to change the connection settings of the intrusion panel.

12.22 Video analytics page

Main window > > **Devices** > Expand >
Allows you to add video analytics and Person Identification (PID) devices.

12.22.1 Video Analytics Settings page

Main window > > **Devices** > Expand > Expand > > **Video Analytics** > **Video Analytics Settings** page
You can add a server-based video analytics device.

The credentials and the installation path to the analytics viewer application used for the video analytics device must be available.

Network address
Type in the IP address of the video analytics device. DNS name is not allowed.

User name
Type in the user name as configured in the video analytics device.

Password
Type in the password as configured in the server-based analytics device.

Analytics viewer path
Type in the relative path of the installation path of the analytics viewer application. The path is relative to `C:\Program Files (x86)\` on the computer where the viewer application is used. Example: The analytics viewer application (`AnalyticsViewer.exe`) is installed in the following directory:

`C:\Program Files (x86)\VideoAnalytics\`
Configure the following path in the **Analytics viewer path** field:

`VideoAnalytics\AnalyticsViewer.exe`

12.22.2 Adding a Video Analytics Device

Main window > > **Devices** > Right-click >**Add Video Analytics Device** command > **Add Video Analytics Device** dialog box
When adding a server-based analytics device, you type in the credentials for the new device.

To add a server-based analytics device:

1. Expand , right-click and click **Add Video Analytics Device**.
   The **Add Video Analytics Device** dialog box is displayed.
2. Enter the appropriate values.
3. Click **OK**.
   The device is added to your system.

Add Video Analytics Device dialog box

Network address
Type in the IP address of the video analytics device. DNS name is not allowed.

User name
Type in the user name as configured in the video analytics device.

Password
Type in the password as configured in the server-based analytics device.

12.22.3 Person Identification settings page

Main window > > **Devices** > Expand > Expand > **PID**> **PID** settings page

Allows you to add a Person Identification device. The device must be connected and available. You can add cameras to your Person Identification device and configure Person Identification events and alarms.

Connection
The **Connection** tab displays the network address and port number of your Person Identification device. The connection settings of a Person Identification device are read-only.

Cameras
In the **Cameras**
tab you can add cameras to your Person Identification device. The added cameras appear in a list.
Note: At first, add the appropriate cameras to the Logical Tree.

12.22.4 Adding a Person Identification device (PID)

Notice!
In the event of a central server breakdown you need to restore the BVMS configuration and the certificate Bosch VMS CA. Otherwise you can not use an existing PID without a reset, which deletes all stored persons.
We recommend to create a backup of the BVMS configuration and the certificate Bosch VMS CA.

When adding a Person Identification device, make sure the certificate that is displayed in the **Add Person Identification Device** dialog box corresponds to the PID that you want to add.

To add a Person Identification device:

1. Expand .
2. Right-click
3. Click **Add Person Identification Device**.
   The **Add Person Identification Device** dialog box is displayed.
4. Enter the appropriate values.
5. Click **View certificate...** to check, if the certificate corresponds to the PID.
6. Click **OK** to confirm.
7. Click **OK**.
   The device is added to your system.

Add Person Identification Device dialog box

Network address
Type in the IP address of the device.

Port number
Type in the port number of the device.

See also
- *Restoring access to a PID after a BVMS central server breakdown, page 171*
- *To export configuration data:, page 105*

12.22.5 Restoring access to a PID after a BVMS central server breakdown

Notice!
In the event of a central server breakdown you need to restore the BVMS configuration and the certificate Bosch VMS CA. Otherwise you can not use an existing PID without a reset, which deletes all stored persons.
We recommend to create a backup of the BVMS configuration and the certificate Bosch VMS CA.

For more information on saving the BVMS configuration refer to *To export configuration data:, page 105*. Certificates are managed outside of BVMS in the Windows application **Manage Computer Certificates**.

Notice!
Certificates contain confidential information. Protect them by doing the following:
- Set a strong password.
- Store the certificate in a restricted area, for example a non-public server.
- Make sure that only authorized personnel can access the certificate.

To create a backup of the Bosch VMS CA certificate:

1. Open the Windows application **Manage Computer Certificates**.
2. In the folder **Trusted Root Certification Authorities** select the certificate Bosch VMS CA.
3. Export the certificate with the private key by selecting **Yes, export the private key**.
4. Use the Personal Information Exchange format.
5. Set a strong password.
6. Save the certificate as a PFX file.

To restore the access to the PID from a newly installed BVMS central server:

1. Open the Windows application **Manage Computer Certificates**.
2. Import the PFX file that contains the certificate Bosch VMS CA into the folder **Trusted Root Certification Authorities** of the new central server. Include all extended properties.
3. Import the BVMS configuration backup.

See also

– *Exporting configuration data, page 104*

12.22.6 Adding cameras to a Person Identification device (PID)

You can add cameras to your Person Identification device, if they are already added to the Logical tree.

To add cameras to a Person Identification device:

1. Expand .
2. Expand .
3. Click .
4. Click the **Cameras** tab.

5. Drag the appropriate cameras from the **Logical Tree** window to the **Cameras** window.
   Or
   double-click the appropriate cameras in the **Logical Tree** window.
   The cameras are added to your Person Identification device and are displayed in the **Cameras** list.

12.22.7 Configuring camera parameters for Person Identification alarms

For each available camera you can configure camera parameters for Person Identification alarms to reduce false alarms.

Camera parameter

Name	Value information	Description
Threshold probability (%)	Default: 55 % Min: 0 % Max: 100 %	The minimum probability of positive identification of a face in order to generate a Person Identification event.
Face size (%)	Default: 7,5 % Min: 5 % Max: 100 %	The minimum size of a face to be detected compared to the size of the entire video frame.
Min. frame number	Default: 4 Min.: 1	The minimum number of consecutive video frames in which a face must appear in order to be detected.
Frames to analyze (%)	Default: 100 % Min: 10 % Max: 100 %	The percentage of frames that is analyzed to identify persons. A value of 50 % means every second frame is analyzed.

12.22.8 Configuring person groups

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

To configure person groups:

1. Select the **Person groups** tab.
2. Click to add a new person group.
3. Enter the appropriate values.
4. Click to delete a person group.

Notice!
You can not delete or change the values of the default group.

Person groups table

Person group	Type the person group name.
Alarm Color	Double-click to select the alarm color.
Alarm Title	Type the title of the alarm that will be displayed in the Operator client.

To change the values of the person groups table:

1. Double-click in the appropriate table field.
2. Change the value.

Alarm priority

You can set the alarm priority for Person Identification alarms on the **Alarms** page.

Notice!

You can set different alarm priorities for each camera of the appropriate person group.
You can also change the alarm priority of the default person group.

See also

– *Alarms page, page 300*

12.23 Access control systems page

Main window > **Devices** > Expand >

Allows you to add and configure access control systems from Bosch. The device must be connected and available. When you have added an access control system, the controller, entrances and readers are displayed in the Device Tree hierarchically.
You can remove or rename the controller, entrances and readers on the **Maps and Structure** page.
When the configuration or hierarchy for controllers, readers or doors of the access control system was changed, you must rescan the device to display the changes in BVMS.

HTTPS Certificate for Client

In order to secure the connection between the access control system and BVMS, you have to export a client certificate from the access control system and import it into BVMS. This process is described in the section **HTTPS Certificate for Client** of the access control system documentation.

Notice!

If the certificate is not added, the systems will not be able to exchange information with each other.

12.23.1 Adding an access control system

Main window > **Devices** > Expand >

To add an access control system:

1. Right-click .
2. Click **Add access control system**.
   The **Add access control system** dialog box is displayed.

Add access control system dialog box

Network address / HTTPS 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.

To test the connection:

1. Click connect.
   The BVMS Configuration Client will try to connect to the access control system and retrieve the relevant information.
2. Click OK.
   The access control system is added to your system, based on the information displayed.

12.23.2 Editing an access control system

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

To edit an access control system:

1. Right-click .
2. Click **Edit access control system**.
   The **Edit access control system** dialog box is displayed.

12.23.3 Settings page

Main window > **Devices** > Expand > > > **Settings** tab
Allows you to change the connection settings of the access control system.

12.24 VRM Devices page

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

Caution!
After you have added an iSCSI device with respective encoders to your BVMS, you must add the IQN of each encoder to this iSCSI device (valid for some iSCSI device types).
See *Configuring an iSCSI device, page 196* for details.

Caution!
Ensure that the time of the VRM computer is synchronized with the Management Server. Otherwise you can loose recordings.
Configure the time server software on the Management Server. On the VRM computer, configure the IP address of the Management Server as time server using standard Windows procedures.

See also
- *Configuring multicast, page 230*
- *Synchronizing BVMS configuration, page 184*
- *VRM Settings page, page 178*
- *Pool page, page 184*
- *iSCSI device page, page 192*
- *Changing the password of a VRM device, page 180*

12.24.1 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, page 196* 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.

See also

- *Adding a device, page 126*
- *VRM Devices page, page 174*
- *Configuring an iSCSI device, page 196*
- *Dual / failover recording, page 32*

12.24.2 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.

See also

- *Editing a VRM device, page 177*
- *Adding a Mirrored VRM manually, page 181*
- *Adding a Failover VRM manually, page 180*

12.24.3 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.

See also
– *Adding a primary or secondary VRM manually, page 176*

12.24.4 VRM Settings page

Main window > **Devices** > Expand > > **Main Settings** > **VRM Settings**

Server initiator name
Displays the iSCSI initiator name of VRM Server.

System-wide CHAP password
Enter the password that you have configured in the iSCSI storage device. The CHAP password is valid for the VRM and is sent to all devices automatically. Replay clients do not need additional configuration. You must configure the iSCSI systems manually with the CHAP password. If you are using a CHAP password, all storage systems have to be configured to use the CHAP password. Only one system wide CHAP password is supported by the VRM system.
See *Global iSCSI connection password (CHAP password): , page 123*

12.24.5 SNMP page

Main window > **Devices** > Expand > Expand > **Network** > **SNMP**

1. SNMP host address 2. SNMP host address
VRM supports the SNMP (Simple Network Management Protocol) for managing and monitoring network components, and can send SNMP messages (traps) to IP addresses. The unit supports SNMP MIB II in the unified code. If you wish to send SNMP traps, enter the IP addresses of one or two required target units here.
Some events are sent as SNMP traps only. Refer to the MIB file for descriptions.

12.24.6 Accounts page

In order to configure image posting, and to export video in MP4 file format, you must create an Account in which to save and access them. You can create a maximum of four (4) accounts.

Type
Select the type of account: **FTP** or **Dropbox**.

IP address
Enter the IP address of the server on which you wish to save the images.

User name
Enter the user name for the server.

Password
Enter the password that gives you access to the server. To verify the password, click **Check** to the right.

Check
Click to verify the password.

Path
Enter the exact path on which you wish to post the images and video on the server.

12.24.7 Advanced page

Main window > **Devices** > Expand > Expand > **Service** > **Advanced**

RCP+ logging / Debug logging / Replay logging / VDP logging / Performance logging
Activate the different logs for VRM Server and Configuration Manager.
The log files for VRM Server are stored on the computer on which VRM Server has been started, and can be viewed or downloaded with VRM Monitor.
The log files for Configuration Manager are stored locally in the following directory:
%USERPROFILE%\My Documents\Bosch\Video Recording Manager\Log

Retention time (days)
Specify the retention time for log files in days.

Complete memory dump file
Only activate this option if necessary, for example if the Technical Customer Service team requests a complete summary of the main memory.

Telnet support
Activate this option if access with the Telnet protocol is to be supported. Only activate if necessary.

Notice!
Extensive logging requires considerable CPU power and HDD capacity.
Do not use extensive logging in continuous operation.

12.24.8 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.

To enable encrypted recording:
1. Select the appropriate VRM device.
2. Click **Service**.
3. In the **Recording encryption** tab select the **Enable encrypted recording** check box.
4. Click .

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 disable/enable encrypted recording for a single VRM encoder:

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

Note: Encryption is enabled after the next block change.
To check the VRM encoders that are encrypting, refer to the **Monitoring** tab in the VRM Monitor.

12.24.9 Changing the password of a VRM device

Main window > **Devices** > Expand >

To change the password:

1. Right-click and click **Change VRM Password**.
   The **Change password** dialog box is displayed.
2. In the **Old Password** field, type in the appropriate password.
3. In the **New Password** field, type in the new password and click and repeat this entry in the second **New Password** field.

Click **OK**.

- Confirm the next dialog box.

✓ The password is changed immediately on the device.

12.24.10 Adding a VRM pool

Main window > **Devices** > Expand

To add a VRM pool:

- Right-click or and click **Add Pool**.
  A new pool is added to the system.

See also

– *iSCSI storage pool, page 192*

12.24.11 Adding a Failover VRM manually

Main window > **Devices** > Expand > Right-click > Click **Add Failover VRM** > **Add Failover VRM** 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**.

Either a Primary VRM or a Secondary VRM can take over the role of a Failover VRM. You add a Primary Failover VRM to a Primary VRM or you add a Secondary Failover VRM to a Secondary VRM.
You can add a Failover VRM device manually if you know the IP address and password. The initially selected VRM is the Master VRM for this Failover VRM.
You can add a Failover VRM device. You can either add it manually or you can select a device from a list of scanned VRM devices.
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.

To add a Failover VRM device:

1. Make the required settings for your VRM device.
2. Ensure that the correct Master VRM is selected. If not, cancel this procedure.
3. Click **OK**.

✓ The Failover VRM device is added to the selected Master VRM.

Add Failover VRM dialog box

Network address
Type in the IP address of your device or select a network address in the **Scanned VRMs** list.

Scanned VRMs
Displays the list of scanned VRM computers. To rescan, close the dialog box and display the dialog box again.

Notice!
The Failover VRM device inherits the settings that are configured in the Master VRM. If the settings of the Master VRM are changed, the settings of the Failover VRM device are changed accordingly.

See also

– *Dual / failover recording, page 32*

12.24.12 Adding a Mirrored VRM manually

Main window > **Devices** > Expand > Right-click > Click **Add Mirrored VRM** > **Add VRM** 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**.

Only a Secondary VRM can take over the role of a Mirrored VRM. You add a Mirrored VRM to a Primary VRM.
You can add a Mirrored VRM device manually if you know the IP address and password. The initially selected VRM is the Master VRM for this Mirrored VRM.

To add a Mirrored VRM device:

1. Make the required settings for your VRM device.
2. Ensure that the correct Master VRM is selected. If not, cancel this procedure.
3. Click **OK**.

The Mirrored VRM device is added to the selected 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.

Show password
Click to enable that the password is visible.

Password
Type in the password for authentication.

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.

See also

- *Adding a primary or secondary VRM manually, page 176*
- *Dual / failover recording, page 32*

12.24.13 Adding Encoders via scan

To add encoders via scan:

1. Right-click and click **Scan for Encoders**.
   The **BVMS Scan Wizard** dialog box is displayed.

2. Select the required encoders, select the desired VRM pool and click **Assign** to assign them to the VRM pool.
3. Click **Next >>**.
   The **Authenticate Devices** dialog box of the wizard is displayed.
4. Type in the password for each device that is protected by a password.
   Password check is performed automatically, when you do not enter a further character in the password field for a few seconds or you click outside the password field.
   If the passwords of all devices are identical, you can enter it in the first **Password** field. Then right-click this field and click **Copy cell to column**.
   In the **Status** column, the successful logons are indicated with .
   The failed logons are indicated with
   indicates that the device requires an initial password.
   To set the initial password, enter it in the **Password** field.
   The status changes to .
   Repeat this step for all devices that require an initial password.
   Note: As long as you have not set the initial password for all devices in the list that require an initial password, you cannot continue.
5. Click **Finish**.
   The device is added to the Device Tree.

12.24.14 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.

12.24.15 Synchronizing BVMS configuration

Main window > **Devices** > Expand > Right-click > **Synchronize BVMS Configuration** command

As of BVMS 6.0, VRM 3.50 is supported. When you do not upgrade VRM to version 3.50 during the upgrade to BVMS 6.0, recording continues but you cannot change the configuration of the old VRM.

If you upgraded your VRM software to version 3.50, you must manually synchronize the BVMS configuration.

12.25 Pool page

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

Allows you to configure recording settings valid for all devices that are collected in this storage pool.

Pool identification

Displays the pool number.

Recording preferences mode

- **Failover**
  Recordings are saved only to primary target. If it is not possible to save to this target, the recording will be saved to the target entered under secondary target.
  A failure situation is reached if the primary target does not provide storage blocks due to whatever reason: system down, network error, no capacity left.
  You can leave the second list empty. In this case no failover is possible but the number of required iSCSI sessions is reduced and no disk space on secondary target is allocated. This reduces system overhead and extends the system retention time.
- **Automatic**
  Load balancing is configured automatically. Each encoder is automatically assigned 2 iSCSI targets and blocks on these 2 iSCSI targets are assigned to the encoder.

Sanity check period (days)

Move the slider to configure the required time period. After this time period the iSCSI target is checked and blocks are reassigned if needed.

Secondary target usage

Enable or disable the use of a secondary target.

Block reservation for downtime

Enter the number of days that the assigned encoders will be recorded although the VRM Server is down.

For example, if you set 4, the encoders will be recorded during approximately 4 days of VRM Server downtime.

If your system has encoders with low bit rate, you can significantly reduce the pre-allocated disk space. This ensures a proper distribution of storage capacity and extends the retention time.

Allow LUNs larger than 2 TB

Click to enable the use of LUNs that are larger than 2 TB.

LUNs larger than 2 TB ("large LUNs") are not supported by the following devices:

- VRM devices earlier than 3.60

– VSG devices with firmware version earlier than 6.30
– Encoders with firmware version earlier than 6.30

BVMS prevents you to perform the following procedures:

– Add or move devices with firmware version earlier than 6.30 to a pool that allows large LUNs.
– Add or move devices that are currently not connected to the network, to a pool that allows large LUNs.
– Add or move an iSCSI device that contains large LUNs, to a pool that does not allow large LUNs.
– Allow large LUNs on a pool that contains devices with firmware version earlier than 6.30.
– Disable large LUNs on a pool with an iSCSI device that contains large LUNs.

Please move devices with firmware earlier than 6.30 to a pool that does not allow large LUNs.

See also

– *Adding a LUN, page 200*
– *Adding a VRM pool, page 180*

12.25.1 Configuring automatic recording mode on a pool

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

Notice:

If you have configured a failover recording mode earlier, this configuration is overwritten.

To configure:

▸ In the **Recording preferences mode** list, select **Automatic**.
After activation of the configuration the **Automatic** recording mode is active. On the **Recording Preferences** page of an encoder, the primary and the secondary target list are disabled.

Related Topics

– *Configuring failover recording mode on an encoder, page 229*

12.25.2 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:

1. Expand , expand , right-click .
   Or
   Right-click .
   Or
   Right-click .

2. Click **Add Encoder**.
   The **Add Encoder** dialog box is displayed.

3. Enter the appropriate IP address.
4. In the list, select **<Auto Detect>.**
5. Click **OK**.
   The device is added to the system.
6. 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** > Expand > Expand > Right-click > Click **Add Encoder** > **Add Encoder** dialog box
or
Main window > **Devices** > Right-click > Click **Add Encoder** > **Add Encoder** dialog box
or
Main window > **Devices** > Right-click > Click **Add Encoder** > **Add Encoder** dialog box
or
Main window > **Devices** > Expand > 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.

12.25.3 Adding an iSCSI device manually

Main window > **Devices** > > Expand > Right-click > **Add iSCSI Device** > **Add iSCSI Device** dialog box
Allows you to add an iSCSI devices to a VRM.

To add an iSCSI device:

1. Right-click and click **Add iSCSI Device**.
   The **Add iSCSI Device** dialog box is displayed.
2. Type the desired display name, the network address of an iSCSI device, and the device type and click **OK**.
   The iSCSI device is added to the selected VRM pool.
   If required, add targets and LUNs.

Add iSCSI Device dialog box

Name
Type in a display name for the device.

Network Address
Type in a valid network address of the device.

iSCSI device type
Select the appropriate device type.

Password
Type in the password for authenticating at the device.

Related Topics
– *Adding VRM Devices via scan, page 175*

12.25.4 Adding a Video Streaming Gateway manually

Main window > **Devices** > Expand >
You can add VSG devices to a VRM pool.

To add a VSG device manually:

1. Right-click and click **Add Video Streaming Gateway**.
   The **Add Video Streaming Gateway** dialog box is displayed.
2. Make the required settings for your VSG device.
3. Click **Add**.

✓ The VSG device is added to the system. The cameras assigned to this VSG device are recorded.

Add Video Streaming Gateway dialog box

Right-click > **Add Video Streaming Gateway** > **Add Video Streaming Gateway** dialog box

Name
Type in the desired display name for the device.

User name
Type in the user name used for authenticating at the device. Usually: service

Network address / port
Type 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 or the VSG instances are configured in a different order.

Default ports

VSG instance	rcpp port	HTTPS port
1	8756	8443
2	8757	8444
3	8758	8445
4	8759	8446
5	8760	8447
6	8761	8448
7	8762	8449

Password
Type in 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.

Security
The **Secure connection** check box is selected by default, if HTTPS is supported.
From VSG version 7.0, VSG supports secure connection.

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 Video Streaming Gateway** command and select or deselect the **Secure connection** check box.

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

See also
– *Editing a Video Streaming Gateway, page 204*

12.25.5 Adding a DSA E-Series iSCSI device manually

Main window > **Devices** > > Expand >
You can either add an E-Series iSCSI device that is already initialized or you add an E-Series iSCSI device that is not initialized.
You can add LUNs larger than 2 TB if the pool is enabled for large LUNs.
LUNs larger than 2 TB ("large LUNs") are not supported by the following devices:
– VRM devices earlier than 3.60
– VSG devices with firmware version earlier than 6.30
– Encoders with firmware version earlier than 6.30
BVMS prevents you to perform the following procedures:
– Add or move devices with firmware version earlier than 6.30 to a pool that allows large LUNs.

– Add or move devices that are currently not connected to the network, to a pool that allows large LUNs.
– Add or move an iSCSI device that contains large LUNs, to a pool that does not allow large LUNs.
– Allow large LUNs on a pool that contains devices with firmware version earlier than 6.30.
– Disable large LUNs on a pool with an iSCSI device that contains large LUNs.

Please move devices with firmware earlier than 6.30 to a pool that does not allow large LUNs.

To add an initialized iSCSI device:

1. Right-click and then click **Add DSA E-Series Device**.
   The **Add DSA E-Series Device** dialog box is displayed.
2. Type in the management IP address and the password.
3. Click **Connect**
   If connection is established, the fields in the **Controller** group and/or the **2nd Controller** group are filled.
4. Click **OK**.
   The device is added to the system.
   The available targets are automatically scanned and the LUNS are displayed.
   You can use the iSCSI device.
   If the pool is enabled for large LUNs, and the iSCSI device has large LUNs configured, the **Large LUN** column displays a checkmark for the affected LUNs.

To add a not initialized iSCSI device:

1. Right-click and then click **Add DSA E-Series Device**.
   The **Add DSA E-Series Device** dialog box is displayed.
2. Type in the management IP address and the password.
3. Click **Connect**
   If connection is established, the fields in the **Controller** group and/or the **2nd Controller** group are filled.
4. Click **OK**.
   The device is added to the system.
5. Click and then click .
6. Click the **Basic Configuration** tab.
7. Type in the desired LUN capacity.
   If you type in a value larger than 2 TB, you must enable your pool for LUNs larger than 2 TB.
8. Click **Initialize**.
   The LUNs are created.
9. Click **Close**.
10. Right-click the iSCSI device, and then click **Scan Target**.
    The LUNs are displayed with an unknown state.
11. Save and activate the configuration.
12. Format all LUNs.
13. If you added an iSCSI device with dual controller, remove the desired LUNs from the first controller, right-click the second controller, and click **Scan Target** to add these LUNs.

Add DSA E-Series Device dialog box

Main window > **Devices** > > Expand > Right-click > **Add DSA E-Series Device** > **Add DSA E-Series Device** dialog box

Allows you to add a DSA E-Series iSCSI device. This device type has a management IP address different from the IP address of the iSCSI storage. Via this management IP address the device is automatically detected and configured.

Name

Type in a display name for the device.

Management address

Type in the IP address for automatic configuration of the device.

Password

Type the password of this device.

DSA E-Series type

Displays the device type.

Network address iSCSI Ch

Displays the IP address of the iSCSI port of the device. If available you can select another IP address.

Management address

Displays the IP address for automatic configuration of the second controller if available. If available you can select another IP address.

Network address iSCSI Ch

Displays the IP address of the iSCSI port of the second controller if available. If available you can select another IP address.

Connect

Click to detect the settings of the device.

If connection is established, the fields in the **Controller** group and the **2nd Controller** group are filled.

See also

- *Basic Configuration page, page 197*
- *Formatting a LUN, page 201*

12.25.6 Adding Encoders via scan

To add encoders via scan:

1. Right-click and click **Scan for Encoders**.
   The **BVMS Scan Wizard** dialog box is displayed.
2. Select the required encoders, select the desired VRM pool and click **Assign** to assign them to the VRM pool.
3. Click **Next >>**.
   The **Authenticate Devices** dialog box of the wizard is displayed.
4. Type in the password for each device that is protected by a password.
   Password check is performed automatically, when you do not enter a further character in the password field for a few seconds or you click outside the password field.

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

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

The failed logons are indicated with

indicates that the device requires an initial password.

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

The status changes to .

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

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

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

12.25.7 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.

12.25.8 Configuring dual recording in the Device Tree

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

You must disable the ANR function to configure dual recording.

If you configure dual recording for one camera of a multi-channel encoder, the system ensures that the same recording target is configured for all cameras of this encoder.

You can configure dual recording by assigning encoders that are recorded by a Primary VRM to a Secondary VRM. This is for example useful when you want to assign only a part of the encoders that are recorded by a Primary VRM.

A Secondary VRM must already be added.

To configure:

1. Right-click and click **Add Encoder from Primary VRM**.
   The **Add Encoders** dialog box is displayed.
2. Click to select the desired encoders.
   When you select a pool or a VRM, all child items are automatically selected.
3. Click **OK**.
   The selected encoders are added to the Secondary VRM.

See also

- *Configuring dual recording in the Camera Table, page 294*
- *Configuring the ANR function, page 293*
- *Dual / failover recording, page 32*

12.26 Bosch Encoder / Decoder page

To configure a Bosch Encoder / Decoder, see *Bosch Encoder / Decoder / Camera page, page 217*.

12.27 iSCSI device page

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

You can either add a E-Series iSCSI device or any other supported iSCSI device.

See also

- *Adding an iSCSI device manually, page 193*
- *Adding a DSA E-Series iSCSI device manually, page 194*
- *Configuring an iSCSI device, page 196*
- *Adding a LUN, page 200*
- *Formatting a LUN, page 201*

12.27.1 iSCSI storage pool

As of VRM v.3.0, iSCSI storage pools are introduced. A storage pool is a container for one or more iSCSI storage systems that share the same load balancing properties. The encoders / IP cameras that are assigned to a storage pool, are recorded with these common load balancing settings.

A storage pool can be used to have a logical mapping of the network topology to the VRM, for example if you have two buildings, both containing storage and devices, you want to avoid routing the network traffic from one building to the other.

Storage pools can also be used to group cameras and storage systems by an important aspect of view. For example a system contains of some very important cameras and a lot of less important ones. In this case it is possible to group them into two storage pools, one with a lot of redundancy features and one with less redundancy.

You can configure the following load balancing properties for a storage pool:

- Recording preferences (**Automatic** or **Failover**)

– Secondary target usage
  Secondary target is used in case of **Failover** mode if the assigned primary target fails. If this option is turned off, the recording stops on all devices assigned to this failed primary target.
  In case of **Automatic** mode: if one target fails, VRM Server performs an automatic reassign of the related devices to other storages. If VRM Server is down while a target fails, the recording is stopped on the devices currently recording on the failed target.
– Block reservation for downtime
– Sanity check period

For each pool you can configure that this pool allows LUNs larger than 2 TB.
LUNs larger than 2 TB ("large LUNs") are not supported by the following devices:
– VRM devices earlier than 3.60
– VSG devices with firmware version earlier than 6.30
– Encoders with firmware version earlier than 6.30

BVMS prevents you to perform the following procedures:
– Add or move devices with firmware version earlier than 6.30 to a pool that allows large LUNs.
– Add or move devices that are currently not connected to the network, to a pool that allows large LUNs.
– Add or move an iSCSI device that contains large LUNs, to a pool that does not allow large LUNs.
– Allow large LUNs on a pool that contains devices with firmware version earlier than 6.30.
– Disable large LUNs on a pool with an iSCSI device that contains large LUNs.

Please move devices with firmware earlier than 6.30 to a pool that does not allow large LUNs.
If a Primary VRM has a pool that allows large LUNs, the corresponding Mirrored VRM inherits this setting and you cannot select or clear the **Allow LUNs larger than 2 TB** checkbox on the corresponding pool of the Mirrored VRM. If you have added an iSCSI device with large LUNs to a Mirrored VRM, you cannot clear the **Allow LUNs larger than 2 TB** checkbox on the corresponding pool of the Primary VRM.

See also
– *Pool page, page 184*

12.27.2 Adding an iSCSI device manually

Main window > **Devices** > > Expand > Right-click > **Add iSCSI Device** > **Add iSCSI Device** dialog box

Allows you to add an iSCSI devices to a VRM.

To add an iSCSI device:

1. Right-click and click **Add iSCSI Device**.
   The **Add iSCSI Device** dialog box is displayed.
2. Type the desired display name, the network address of an iSCSI device, and the device type and click **OK**.
   The iSCSI device is added to the selected VRM pool.
   If required, add targets and LUNs.

Add iSCSI Device dialog box

Name
Type in a display name for the device.

Network Address
Type in a valid network address of the device.

iSCSI device type
Select the appropriate device type.

Password
Type in the password for authenticating at the device.

Related Topics
– *Adding VRM Devices via scan, page 175*

12.27.3 Adding a DSA E-Series iSCSI device manually

Main window > **Devices** > > Expand >
You can either add an E-Series iSCSI device that is already initialized or you add an E-Series iSCSI device that is not initialized.
You can add LUNs larger than 2 TB if the pool is enabled for large LUNs.
LUNs larger than 2 TB ("large LUNs") are not supported by the following devices:
– VRM devices earlier than 3.60
– VSG devices with firmware version earlier than 6.30
– Encoders with firmware version earlier than 6.30
BVMS prevents you to perform the following procedures:
– Add or move devices with firmware version earlier than 6.30 to a pool that allows large LUNs.
– Add or move devices that are currently not connected to the network, to a pool that allows large LUNs.
– Add or move an iSCSI device that contains large LUNs, to a pool that does not allow large LUNs.
– Allow large LUNs on a pool that contains devices with firmware version earlier than 6.30.
– Disable large LUNs on a pool with an iSCSI device that contains large LUNs.
Please move devices with firmware earlier than 6.30 to a pool that does not allow large LUNs.

To add an initialized iSCSI device:

1. Right-click and then click **Add DSA E-Series Device**.
   The **Add DSA E-Series Device** dialog box is displayed.
2. Type in the management IP address and the password.
3. Click **Connect**
   If connection is established, the fields in the **Controller** group and/or the **2nd Controller** group are filled.
4. Click **OK**.
   The device is added to the system.
   The available targets are automatically scanned and the LUNS are displayed.
   You can use the iSCSI device.
   If the pool is enabled for large LUNs, and the iSCSI device has large LUNs configured, the **Large LUN** column displays a checkmark for the affected LUNs.

To add a not initialized iSCSI device:

1. Right-click and then click **Add DSA E-Series Device**.
   The **Add DSA E-Series Device** dialog box is displayed.
2. Type in the management IP address and the password.
3. Click **Connect**
   If connection is established, the fields in the **Controller** group and/or the **2nd Controller** group are filled.
4. Click **OK**.
   The device is added to the system.
5. Click and then click .
6. Click the **Basic Configuration** tab.
7. Type in the desired LUN capacity.
   If you type in a value larger than 2 TB, you must enable your pool for LUNs larger than 2 TB.
8. Click **Initialize**.
   The LUNs are created.
9. Click **Close**.
10. Right-click the iSCSI device, and then click **Scan Target**.
    The LUNs are displayed with an unknown state.
11. Save and activate the configuration.
12. Format all LUNs.
13. If you added an iSCSI device with dual controller, remove the desired LUNs from the first controller, right-click the second controller, and click **Scan Target** to add these LUNs.

Add DSA E-Series Device dialog box

Main window > **Devices** > > Expand > Right-click > **Add DSA E-Series Device** > **Add DSA E-Series Device** dialog box

Allows you to add a DSA E-Series iSCSI device. This device type has a management IP address different from the IP address of the iSCSI storage. Via this management IP address the device is automatically detected and configured.

Name

Type in a display name for the device.

Management address

Type in the IP address for automatic configuration of the device.

Password

Type the password of this device.

DSA E-Series type

Displays the device type.

Network address iSCSI Ch

Displays the IP address of the iSCSI port of the device. If available you can select another IP address.

Management address

Displays the IP address for automatic configuration of the second controller if available. If available you can select another IP address.

Network address iSCSI Ch
Displays the IP address of the iSCSI port of the second controller if available. If available you can select another IP address.

Connect
Click to detect the settings of the device.
If connection is established, the fields in the **Controller** group and the **2nd Controller** group are filled.

See also
- *Basic Configuration page, page 197*
- *Formatting a LUN, page 201*

12.27.4 Configuring an iSCSI device

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

After adding VRM devices, iSCSI devices, and encoders, perform the following tasks to ensure that video data of encoders is stored on the iSCSI devices or video data can be retrieved from these iSCSI devices:
- Execute the default configuration to create LUNs on each target of the iSCSI device. This step is optional. You do not need to perform this step on an iSCSI device with LUNs pre-configured.
- Scan the iSCSI device to add the targets and LUNs to the Device Tree after default configuration.

Note:
Not all iSCSI devices support the default configuration and automatic IQN mapping.
Prerequisite:
The iSCSI device must be configured with valid IP addresses.

To perform basic configuration of an DSA E-Series iSCSI device:

- Expand the appropriate VRM device and , click the appropriate iSCSI device .

1. Click the **Basic Configuration** tab.
2. Type in the desired LUN capacity.
   If you type in a value larger than 2 TB, you must enable your pool for LUNs larger than 2 TB.
3. Click **Initialize**.
   The LUNs are created.
4. Click **Close**.
5. Right-click the iSCSI device, and then click **Scan Target**.
   The LUNs are displayed with an unknown state.
6. Save and activate the configuration.
7. Format all LUNs.
8. If you added an iSCSI device with dual controller, remove the desired LUNs from the first controller, right-click the second controller, and click **Scan Target** to add these LUNs.

To perform basic configuration on other iSCSI devices:
1. Click the **Basic Configuration** tab.

2. Type in the desired LUN count.
3. Click **Set**.
   The LUNs are created.
4. Click **Close**.
5. Right-click the iSCSI device, and then click **Scan Target**.
   The LUNs are displayed with an unknown state.
6. Save and activate the configuration.
7. Format all LUNs.

To perform IQN mapping for other iSCSI devices:

1. Expand the appropriate VRM device and , click the appropriate iSCSI device .
2. Right-click and click **Map IQNs**.
   The iqn-Mapper dialog box is displayed and the process is started.
   The encoders that are assigned to the selected VRM device are evaluated and their IQNs are added to this iSCSI device.
3. Click to save the settings.
4. Click to activate the configuration.

See also

- *Basic Configuration page, page 197*
- *Load Balancing dialog box, page 198*
- *iqn-Mapper dialog box, page 201*
- *Formatting a LUN, page 201*

12.27.5 Basic Configuration page

Main window > **Devices** > Expand > Expand > Expand > Click > **Basic Configuration** tab

The displayed options can differ depending on the used type of iSCSI storage system.

Allows you to perform a basic configuration of your iSCSI device. You create LUNs on the iSCSI hard drive and format these LUNs.

Only displayed if the device is one of the iSCSI storage systems supported by Bosch, for example DSA or DLS 1x00.

Notice!
After the basic configuration of an E-Series the system needs many hours (or even days) to initialize. In this phase the full performance is not available and in phase 1.5 formatting can fail.

Physical capacity [GB]
Information on the total capacity of the storage system.

Number of LUNs
You can change the number of LUNs.

Notice!
If you change the number of LUNs, the entire iSCSI system is reorganized and any sequences saved on the system are lost.
Therefore, before making changes, check the recordings and back up any important sequences.

Capacity for new LUNs [GB]
This option is only displayed for E-Series.
As 256 is the maximum number of LUNs of a storage array, the LUN size should not be set to a too small value (otherwise no more LUNs can be created in the future, if an additional shelf is installed).

Target spare disks
Number of spare disks the user wants the system to have.

Actual spare disks
Number of spare disks which are currently in the system. This number can differ from the number above, e.g. if the storage system is reconfigured manually or if disks are broken.

Initialization status (%)
Additional information is displayed during initialization. When initialization is complete (100%), you will also have the opportunity to delete all LUNs again.
Note: On FAS storage systems, it can take several hours before LUNs are fully deleted. During that time, the total capacity of newly created LUNs can be reduced. You can only create new LUNs with full capacity after the old LUNs have been completely deleted.

RAID-DP (reliability focused)
Activate this option if you do not wish to use the specified RAID type RAID-4, but would prefer to use the more reliable RAID type RAID DP.

RAID 6 (reliability focused)
Activate this option if you do not wish to use the specified RAID type RAID-5, but would prefer to use the more reliable RAID type RAID 6.

Additional information
Additional information is displayed here, for example information that the storage system is not configured correctly and that therefore no setup is possible.

See also
– *Adding a DSA E-Series iSCSI device manually, page 194*

12.27.6 Load Balancing dialog box

Main window > **Devices** > Expand > Expand > Expand > Right-click > **Load Balancing...** command > **Load Balancing** dialog box

Prerequisite: Configure the **Automatic** recording mode.

Set the upper limits for the permitted bit rate and the number of simultaneous iSCSI connections for each iSCSI system. If these limits are exceeded, data is no longer being written to the iSCSI system and is lost.
For supported systems (for example Bosch RAID, NetApp, DLA), use the default values. For another device see the documentation of this device. Start testing with small values.

12.27.7 Moving an iSCSI system to another pool (Change pool...)

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

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

To move:

1. Right-click / /

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

12.27.8 LUNs page

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

>

Allows you to add, remove, or format LUNs, and to view information on the LUNs.

Add
Click to display the **Add LUN** dialog box.

Remove
Click to remove the selected rows. To select a row, click the row header on the left side. Each row represents a LUN.
A message box is displayed.

Format LUN
Click to format the selected LUN. A message box is displayed.

Format
Click the check box to select the LUN and then click **Format LUN**.

LUN
Displays the name of the LUN.

Size [GB]
Displays the maximal capacity of the LUN.

Large LUN
Each cell displays whether this is a LUN larger than 2 TB or not.

State
Displays the state of the LUN.

Progress
Displays the progress of the formatting process.

See also

- *Pool page, page 184*
- *Adding a LUN, page 200*
- *Adding VRM Devices via scan, page 175*

12.27.9 Adding a LUN

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

Usually the network scan adds the desired iSCSI devices with their targets and LUNs automatically. If your network scan did not work correctly or you want to configure your iSCSI device offline before it is actually integrated into your network, you configure a target in your iSCSI device and on this target you configure one or more LUNs.

You can add LUNs larger than 2 TB if the pool is enabled for large LUNs.

LUNs larger than 2 TB ("large LUNs") are not supported by the following devices:

- VRM devices earlier than 3.60
- VSG devices with firmware version earlier than 6.30
- Encoders with firmware version earlier than 6.30

BVMS prevents you to perform the following procedures:

- Add or move devices with firmware version earlier than 6.30 to a pool that allows large LUNs.
- Add or move devices that are currently not connected to the network, to a pool that allows large LUNs.
- Add or move an iSCSI device that contains large LUNs, to a pool that does not allow large LUNs.
- Allow large LUNs on a pool that contains devices with firmware version earlier than 6.30.
- Disable large LUNs on a pool with an iSCSI device that contains large LUNs.

Please move devices with firmware earlier than 6.30 to a pool that does not allow large LUNs.

To add:

1. If required, click to select **Allow LUNs larger than 2 TB**.
2. Right-click and click **Scan Target**.
   The target is added.
3. Click the target.
   The **LUNs** page is displayed.
4. Click **Add**.
   The **Add LUN** dialog box is displayed.
5. Enter the desired LUN number and click **Ok**.
   The LUN is added as a new row in the table.
   Repeat this step for each desired LUN.

Notes:

- To remove a LUN, click **Remove**.
  The video data remains on this LUN.
- To format a LUN, click **Format LUN**.
  All data on this LUN is removed!

Add LUN dialog box

Main window > **Devices** > Expand > Expand > Expand > Expand > > Click **Add**

Allows you to add a LUN.

Id

Enter the ID of the desired LUN.

See also

- *Pool page, page 184*
- *LUNs page, page 199*

12.27.10 Formatting a LUN

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

You format a LUN to prepare it for the first use.

Notice!

All data on the LUN is lost after formatting.

To configure:

1. Select the desired LUN and, in the **Format** column, click to check.
2. Click **Format LUN**.
3. Read the displayed message carefully and confirm the message if desired.
   The selected LUN is formatted. All data on this LUN is lost.

See also

- *LUNs page, page 199*

12.27.11 iqn-Mapper dialog box

Main window > **Devices** > Expand > Expand > Expand > Right-click > **Map IQNs**

Allows you to start the IQN mapping process.

See also

- *Adding VRM Devices via scan, page 175*
- *Configuring an iSCSI device, page 196*

12.28 Video Streaming Gateway device page

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

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

Allows you to add and configure the following encoder types:

- Bosch encoders
- ONVIF encoders
- JPEG encoders
- RTSP encoders

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.

If you add a new VSG version 7.0 or higher, the **Secure connection** check box is selected by default.

To change secure or unsecure connection, use the **Edit Video Streaming Gateway** command and select or deselect the **Secure connection** check box.

See also

- *Editing a Video Streaming Gateway, page 204*
- *ONVIF page, page 232*

12.28.1 Adding a Video Streaming Gateway manually

Main window > **Devices** > Expand >

You can add VSG devices to a VRM pool.

To add a VSG device manually:

1. Right-click and click **Add Video Streaming Gateway**.
   The **Add Video Streaming Gateway** dialog box is displayed.
2. Make the required settings for your VSG device.

3. Click **Add**.
✓ The VSG device is added to the system. The cameras assigned to this VSG device are recorded.

Add Video Streaming Gateway dialog box

Right-click > **Add Video Streaming Gateway** > **Add Video Streaming Gateway** dialog box

Name
Type in the desired display name for the device.

User name
Type in the user name used for authenticating at the device. Usually: service

Network address / port
Type 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 or the VSG instances are configured in a different order.

Default ports

VSG instance	rcpp port	HTTPS port
1	8756	8443
2	8757	8444
3	8758	8445
4	8759	8446
5	8760	8447
6	8761	8448
7	8762	8449

Password
Type in 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.

Security
The **Secure connection** check box is selected by default, if HTTPS is supported.
From VSG version 7.0, VSG supports secure connection.

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 Video Streaming Gateway** command and select or deselect the **Secure connection** check box.

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

See also

– *Editing a Video Streaming Gateway, page 204*

12.28.2 Editing a Video Streaming Gateway

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

To change secure/unsecure connection:

1. Right- click .
2. Click **Edit Video Streaming Gateway**.
   The **Edit Video Streaming Gateway** 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.

See also

– *Adding a Video Streaming Gateway manually, page 202*

12.28.3 Adding a camera to a VSG

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

You can add the following devices to your VSG:

– Encoders from Bosch
– ONVIF cameras
– JPEG cameras
– RTSP encoders

If you added VSG encoders offline, you can refresh their state.

To add:

1. Right-click , point to **Add Encoder/camera** and click the desired command.
2. Make the required settings in the dialog box for adding the device.
3. Click **OK**.

The device is added.

To refresh:

▸ Right-click the desired encoder and click **Refresh state**.
  The properties of the device are retrieved.

See also

– *Add Bosch Encoder dialog box, page 205*
– *Add ONVIF Encoder dialog box, page 206*

– *Add JPEG Camera dialog box, page 207*
– *Add RTSP Encoder dialog box, page 208*

12.28.4 Add Bosch Encoder dialog box

Main window > **Devices** > Expand > Expand > Expand > Right-click > **Add Encoder/camera** > **Bosch Encoder** command

You can add an encoder from Bosch to your VSG device.

Name
Type in the desired display name for the device.

Network address
Type in the network address of the device.

Type
Displays the detected device type, if supported.

User name
Type in the user name used for authenticating at the device. Usually: service

Password
Type in 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.

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

Properties
Click to enable the desired features available for this device.

Audio	Click to activate audio if available for this device.
PTZ	Click to activate PTZ if available for this device.
Camera protocol	TCP Used for transmission in the Internet and / or for lossless data transmission. Ensures that no data packet gets lost. Bandwidth requirement can be high. Use if the device is located behind a Firewall. Does not support multicast. UDP Used for connectionless and lightweight data transmission in private networks. Data packets can get lost. Bandwidth requirement can be low. Supports multicast.
Use video input 1 - **Use video input 4**	Click to select the video inputs if you configure a multichannel device.

See also
– *Adding a camera to a VSG, page 204*

12.28.5 Add ONVIF Encoder dialog box

Main window > **Devices** > Expand > Expand > Expand > Right-click > **Add Encoder/camera** > **Add ONVIF Encoder** command

or

Main window > **Devices** > Right-click > **Add ONVIF Encoder** command

You can add an ONVIF encoder to your VSG device or as a live only encoder.
You must configure the used profile for recording and live in the Camera Table.

From BVMS 10.0, ONVIF encoder events can be retrieved from VSG or ONVIF encoder directly. If you add a new ONVIF encoder, the **retrieve ONVIF events from VSG (Profile S, T)** check box is selected by default and Profile T is supported.
The following features are only supported, if an ONVIF encoder is added to your system via a VSG device:

- If ONVIF encoder events are retrieved from VSG, default ONVIF events are already mapped.
- The Operator can switch relays on or off in the Operator Client.

Notice!
Retrieving ONVIF events from VSG is only available from VSG version 7.0. If you migrate to BVMS version 10.0, existing ONVIF encoder events are retrieved from ONVIF encoder directly. You have to update the VSG to version 7.0.

Name
Type in the desired display name for the device.

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

User name
Type in the user name used for authenticating at the device. Usually: service

Password
Type in 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.

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

Secure connection
You can activate the secure connection of live video transferred from an ONVIF encoder to your VSG device.

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

Notice!
Port 443 is set by default. You can edit the port number to match the configured HTTPS port on the encoder.
The configured port number will not be remembered.

Properties

Device type	Displays the retrieved device type.
Manufacturer	Displays the retrieved manufacturer name.
Model	Displays the retrieved model name.
Firmware version	Displays the retrieved firmware version.
Auxiliary commands	If the check box is selected, auxiliary commands are supported.
Number of video input channels	Enter the number of desired video inputs.
Number of audio input channels	Enter the number of desired audio inputs.
Number of alarm inputs	Enter the number of desired alarm inputs.
Number of relays	Enter the number of desired relays.
Assigned Gateway channel(s)	Enter the number of desired gateway channels.
Camera protocol	Select the desired camera protocol.
Use video input {0}	Select the check box to use the appropriate video input.

Notice!
The **Video Streaming Gateway settings** options are not available for ONVIF encoder, that are added as live only encoder.

See also
– *Adding a camera to a VSG, page 204*

12.28.6 Add JPEG Camera dialog box

Main window > **Devices** > Expand > Expand > Expand > Right-click > **Add Encoder/camera** > **JPEG camera** command

You can add a JPEG camera to your VSG device.

Name
Type in the desired display name for the device.

URL
Enter the URL of your JPEG camera / RTSP camera.
For a JPEG camera from Bosch, type in the following string:

```
http://<ip-address>/snap.jpg?jpegCam=<channel_no.>
```

For an RTSP camera from Bosch, type in the following string:

```
rtsp://<ip-address>/rtsp_tunnel
```

User name
Type in the user name used for authenticating at the device. Usually: service

Password
Type in 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.

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

Properties

Number of video input channels	Enter the number of available video inputs if available.
Frame rate [ips]	Enter the desired frame rate.

See also
– *Adding a camera to a VSG, page 204*

12.28.7 Add RTSP Encoder dialog box

Main window > **Devices** > Expand > Expand > Expand > Right-click > **Add Encoder/camera** > **RTSP camera** command
You can add an RTSP encoder to your VSG device.

Name
Type in the desired display name for the device.

URL
Enter the URL of your JPEG camera / RTSP camera.
For a JPEG camera from Bosch, type in the following string:

```
http://<ip-address>/snap.jpg?jpegCam=<channel_no.>
```

For an RTSP camera from Bosch, type in the following string:

```
rtsp://<ip-address>/rtsp_tunnel
```

User name
Type in the user name used for authenticating at the device. Usually: service

Password
Type in 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.

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

Properties

Number of video input channels	Enter the number of available video inputs if available.

See also
– *Adding a camera to a VSG, page 204*

12.28.8 Moving a VSG to another pool (Change pool)

Main window > **Devices** > Expand > Expand > > >
You move a device from one pool to another within the same VRM device without any recording loss.

To move:

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

12.28.9 Configuring multicast (multicast tab)

Main window > **Devices** > Expand > Expand > Expand >
For each camera assigned to a Video Streaming Gateway device 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** > Expand > 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).
Type in `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.

12.28.10 Configuring logging (advanced tab)

Main window > **Devices** > Expand > Expand > Expand > > **Service** tab > **Advanced** tab
Allows you to activate logging for Video Streaming Gateway.
The log files are usually stored in the following path:

```
C:\Program Files (x86)\Bosch\Video Streaming Gateway\log
```

From VSG version 7.0, the log files are usually stored in the following path:

```
C:\ProgramData\Bosch\VSG\log
```

Note: If you upgrade to VSG 7.0 or newer, previous log files are automatically moved to this location.
Log files from older VSG versions are usually stored in the following path:

```
C:\Program Files (x86)\Bosch\Video Streaming Gateway\log
```

Advanced tab

RCP+ logging
Click to enable RCP+ logging.

Debug logging
Click to enable debug logging.

RTP logging
Click to enable RTP logging.

Retention time (days)
Select the desired number of days.

Complete memory dump file
Only activate this option if necessary, for example if the Technical Customer Service team requests a complete summary of the main memory.

Telnet support
Activate this option if access with the Telnet protocol is to be supported. Only activate if necessary.

Notice!
Extensive logging requires considerable CPU power and HDD capacity.
Do not use extensive logging in continuous operation.

12.29 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 ONFIV encoder, see *ONVIF page, page 232*.

See also

- *Adding a live only encoder, page 218*
- *Scanning for devices, page 84*
- *Bosch Encoder / Decoder / Camera page, page 217*
- *ONVIF page, page 232*
- *Configuring multicast, page 230*

12.29.1 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.
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.

12.29.2 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:

1. Expand , expand , right-click .
   Or
   Right-click .
   Or
   Right-click .
2. Click **Add Encoder**.
   The **Add Encoder** dialog box is displayed.
3. Enter the appropriate IP address.
4. In the list, select **<Auto Detect>.**
5. Click **OK**.
   The device is added to the system.
6. 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** > Expand > Expand > Right-click > Click **Add Encoder** > **Add Encoder** dialog box
or
Main window > **Devices** > Right-click > Click **Add Encoder** > **Add Encoder** dialog box
or
Main window > **Devices** > Right-click > Click **Add Encoder** > **Add Encoder** dialog box
or
Main window > **Devices** > Expand > 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.

12.29.3 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:
1. In the **Enter user name** list, select destination password.
2. In the **Enter password for user** field, type in the new password.
3. Click **OK**.

✓ The password is changed immediately on the device.

See also
– *Changing the password of an encoder / decoder (Change password / Enter password), page 146*

12.30 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.

See also

- *Configuring multicast, page 230*
- *Adding a local storage encoder, page 219*
- *Bosch Encoder / Decoder / Camera page, page 217*
- *Scanning for devices, page 84*

12.31 Unmanaged Site page

Main window > **Devices** > Expand >

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

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

Site name

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

Description

Type in a description for this site.

Time zone

Select the appropriate time zone for this unmanaged site.

See also

- *Unmanaged site, page 27*
- *Adding an unmanaged site manually, page 214*
- *Importing unmanaged sites, page 215*
- *Configuring the time zone, page 216*

12.31.1 Adding an unmanaged site manually

Main window > **Devices** >

To create:

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

A new unmanaged site is added to the system.

See also
- *Unmanaged site, page 27*
- *Unmanaged Site page, page 214*

12.31.2 Importing unmanaged sites

Main window > **Devices** >

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

To import:

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

12.31.3 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.

12.31.4 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 27* for details.

Password:
Type the valid password if available. See *Unmanaged site, page 27* for details on user credentials.

See also
– *Unmanaged site, page 27*

12.31.5 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.

See also
– *Unmanaged Site page, page 214*

13 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, refer to the appropriate device manuals.
The count of items below an entry is displayed in square brackets.

To configure an encoder:

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

To configure a decoder:

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

See the Online Help for the pages for details.

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

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

Most of the settings on the encoder / decoder pages are active immediately after you click . If you click another tab without clicking and changes have occurred, two corresponding message boxes are displayed. Confirm them both if you want to save.
To change the passwords of an encoder right-click the device icon and click **Change password...**.

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

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

- Click a tab to display the corresponding property page.

To add encoders via scan:

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

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

   The failed logons are indicated with

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

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

See also

– *Scanning for devices, page 84*

13.1 Adding an encoder to a VRM pool

To add encoders to a VRM pool, see *Adding Encoders via scan, page 182*.

See also

– *Adding a device, page 126*

13.2 Adding a live only encoder

To add a live only encoder via scan, see *Adding live only devices via scan, page 211*.

See also
- *Adding a device, page 126*
- *Live Only page, page 211*

13.3 Adding a local storage encoder

To add local storage encoders via scan, see *Local Storage page, page 213*.

See also
- *Adding a device, page 126*
- *Local Storage page, page 213*

13.4 Editing an Encoder

13.4.1 Encrypting live video (Edit Encoder)

Main window > **Devices** > Expand > Expand > Expand > Click > **Edit Encoder** dialog box

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

Main window > **Devices** > Expand > Click > **Edit Encoder** dialog box

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.

See also
- *Configuring multicast, page 230*
- *Edit Encoder / Edit Decoder dialog box, page 220*

13.4.2 Updating the device capabilities (Edit Encoder)

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

or

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

or

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

or

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

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

To update:

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

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

See also

– *Edit Encoder / Edit Decoder dialog box, page 220*

13.4.3 Edit Encoder / Edit Decoder dialog box

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

or

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

or

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

or

Main window > **Devices** > Expand > Expand > Right-click > Click **Edit 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.

See also

- *Encrypting live video (Edit Encoder), page 219*
- *Updating the device capabilities (Edit Encoder), page 220*

13.5 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.

See also

– *Verification of authenticity , page 59*

13.5.1 Configuring the authentication

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

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 .

13.5.2 Uploading a certificate

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

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 .

13.5.3 Downloading a certificate

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

or

Main window > **Devices** > Expand >

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.

13.5.4 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`.

13.6 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:

1. In the **Enter user name** list, select destination password.
2. In the **Enter password for user** field, type in the new password.
3. Click **OK**.

✓ The password is changed immediately on the device.

See also

– *Changing the password of an encoder / decoder (Change password / Enter password), page 224*

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

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

or

Main window > **Devices** > >

or

Main window > **Devices** > >

or

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

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.

See also

– *Providing the destination password for a decoder (Authenticate...), page 223*

13.8 Moving an encoder to another pool (Change Pool)

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

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

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

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

To move:

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

Change pool dialog box

Allows you to change the pool assignment of a device.

Current Pool:

Displays the number of the pool which the selected device is currently assigned to.

New Pool:

Select the desired pool number.

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

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

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

Notice!

An encoder can only be replaced by an encoder with the same amount of channels.

To recover recordings from a replaced encoder

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

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

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.

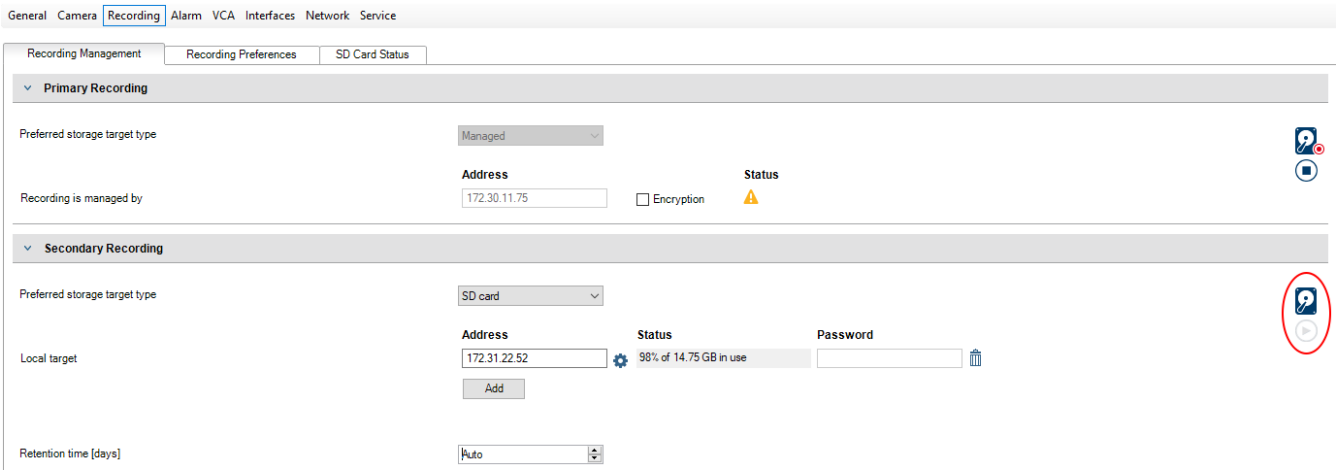
Authenticate
Click to authenticate at the device with the credentials entered above.

13.10 Configuring encoders / decoders

13.10.1 Configuring the storage media of an encoder

Main window > **Devices** > Expand > Expand > > > **Advanced Settings** > **Recording Management**

Note: Ensure that the desired cameras of this encoder are added to the Logical Tree.
You must configure the storage media of an encoder to use the ANR function.
Note: If you want to configure the storage media of an encoder that has already been added to your system and is recorded via VRM, ensure that secondary recording is stopped:



The ANR function only works on encoders with firmware version 5.90 or later. Not all encoder types support ANR even if the correct firmware version is installed.

To configure the storage media of an encoder:

1. Under **Secondary Recording**, in the **Preferred storage target type** list, select the storage media. Depending on the device type, different media are available.
2. If required, click the ... button to format the storage media.
   After the successful formatting process, the storage media is ready for use with the ANR function.
3. Configure the ANR function for this encoder on the **Cameras and Recording** page.

See also

- *Recording Management page, page 229*
- *Configuring the ANR function, page 293*

13.10.2 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.

13.10.3 Configuring failover recording mode on an encoder

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

Prerequisites: On the **Pool** page, in the **Recording preferences mode** list, select **Failover**. If **Automatic** is selected, the settings are performed automatically and cannot be configured.
If you want to use a secondary target for both automatic or failover mode: On the **Pool** page, in the **Secondary target usage** list, select **On**.
It is recommended to configure at least 2 iSCSI devices for failover mode.

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

Related Topics
– *Configuring automatic recording mode on a pool, page 185*

13.10.4 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.

See also
– *Configuring the storage media of an encoder, page 226*

13.10.5 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.

See also
– *Pool page, page 184*

13.11 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).
Type in `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.

See also
– *Encrypting live video (Edit Encoder), page 219*

14 ONVIF page

Main window > **Devices** > Expand >

or

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

See also

- *Video Streaming Gateway device page, page 202*
- *Live Only page, page 211*

14.1 Adding an live only ONVIF device via scan

To add live only ONVIF devices via scan:

1. Right-click and click **Scan for Live Only ONVIF 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
5. Click **Finish**.
   The device is added to the Device Tree.

14.2 ONVIF Encoder page

Main window > **Devices** > Expand > Expand > Expand > Expand > > > **ONVIF Encoder** tab

or

Main window > **Devices** > Expand > > > **ONVIF Encoder** tab

Displays information on a live only ONVIF encoder added to your BVMS.

Name
Displays the name of the ONVIF device. You can rename it in the Device Tree directly.

Network Address
Displays the IP address of the device.

Manufacturer
Displays the manufacturer name.

Model
Displays the model name.

Video Inputs
Enter the number of cameras connected to this encoder.

Audio Inputs
Enter the number of audio inputs connected to this encoder.

Alarm Inputs
Enter the number of alarm inputs connected to this encoder.

Relays
Enter the number of relays connected to this encoder.

See also
- *ONVIF Encoder Events page, page 233*
- *Adding a live only encoder, page 218*
- *Configuring an ONVIF mapping table, page 237*

14.3 ONVIF Encoder Events page

From BVMS 10.0, ONVIF encoder events can be retrieved from VSG or ONVIF encoder directly. If you add a new ONVIF encoder, the **retrieve ONVIF events from VSG (Profile S, T)** check box is selected by default and Profile T is supported.
The following features are only supported, if an ONVIF encoder is added to your system via a VSG device:
- If ONVIF encoder events are retrieved from VSG, default ONVIF events are already mapped.
- The Operator can switch relays on or off in the Operator Client.

Notice!
Retrieving ONVIF events from VSG is only available from VSG version 7.0. If you migrate to BVMS version 10.0, existing ONVIF encoder events are retrieved from ONVIF encoder directly. You have to update the VSG to version 7.0.

Main window > **Devices** > Expand > Expand > Expand > Expand > > **ONVIF Encoder Events** tab

or

Main window > **Devices** > Expand > > **ONVIF Encoder Events** tab

You have to map ONVIF events to BVMS events, if ONVIF encoder events are retrieved from ONVIF encoder directly. This ensures that you later can configure ONVIF events as BVMS alarms.

Notice!
If ONVIF encoder events are retrieved from VSG, default ONVIF events are already mapped.

Mapping Table
You can create or edit a Mapping Table.

Click to display the **Add Mapping Table** dialog box.

Click to display the **Rename Mapping Table** dialog box.

Click to remove the Mapping Table with all rows.

Click or to import or export an ONVIF Mapping Table.

Events and Alarms
Select a BVMS event for mapping with an ONVIF event.

Add row
Click to add a row to the Mapping Table.
When multiple rows are available, an event occurs if one row is true.

Remove row
Click to remove the selected row from the Mapping Table.

ONVIF Topic
Type in or select a string, for example:

```
tns1:VideoAnalytics/tnsaxis:MotionDetection
```

ONVIF Data Name
Type in or select a string.

ONVIF Data Type
Type in or select a string.

ONVIF Data Value
Type in or select a string or number.

If ONVIF events are retrieved from VSG, the following events are mapped to VSG by default:
- **Global Change - Detected**
- **Global Change - Not detected**
- **Motion Detection** - **Motion Detected**
- **Motion Detection** - **Motion Stopped**
- **Reference Image Check** - **Deadjusted**
- **Reference Image Check** - **Adjusted**
- **Video Loss** - **Video Signal Lost**
- **Video Loss** - **Video Signal OK**
- **Video Loss** - **Video Signal State Unknown**

- **Video Signal Too Blurry - Video signal OK**
- **Video Signal Too Blurry - Video signal not OK**
- **Video Signal Too Bright** - **Video Signal OK**
- **Video Signal Too Bright** - **Video Signal Not OK**
- **Video Signal Too Dark** - **Video Signal OK**
- **Video Signal Too Dark** - **Video Signal Not OK**
- **Video Signal Too Noisy** - **Video Signal OK Video Signal Not OK**
- **Relay State** - **Relay Opened**
- **Relay State** - **Relay Closed**
- **Relay State** - **Relay Error**
- **Input State** - **Input Opened**
- **Input State** - **Input Closed**
- **Input State** - **Input Error**

See also
- *ONVIF event mapping, page 52*
- *Configuring an ONVIF mapping table, page 237*

14.3.1 Adding and removing an ONVIF profile

Main window > **Devices** > Expand > Expand > Expand > Expand > > **ONVIF Encoder Events** tab

or

Main window > **Devices** > Expand > > **ONVIF Encoder Events** tab

You can add, remove or change ONVIF profiles for a selected encoder.

To add:
1. Click **Add...**.
2. In the **Add Profile** dialog box, type a name for the profile.
3. Click **Next >**.
4. In the next dialog box, select the desired camera.
5. Click **Next >**.
6. In the next dialog box, select the desired non-recording encoder profile.
7. Click **Save**.
   The new profile is saved.
   The settings of this profile are filled with the values from the selected encoder profile.
   You can change these values if required.

To remove:
- In the list, select a profile and click **Remove**.

To change:
1. In the list, select a profile.
2. Change the settings as required.

14.3.2 Exporting an ONVIF mapping table file

Main window > **Devices** > Expand > Expand > Expand > Expand > > > **ONVIF Encoder Events** tab

or

Main window > **Devices** > Expand > > **ONVIF Encoder Events** tab

You can export an ONVIF Mapping Table as a file (OMF file). The Mapping Table is saved for the selected encoder model.

To export:

1. Click .
2. Type in a filename and click **Save**.
   The ONVIF Mapping Table is exported as OMF file for the selected encoder model.

See also

– *ONVIF Encoder Events page, page 233*

14.3.3 Importing an ONVIF mapping table file

Main window > **Devices** > Expand > Expand > Expand > Expand > > > **ONVIF Encoder Events** tab

or

Main window > **Devices** > Expand > > **ONVIF Encoder Events** tab

You can import an ONVIF Mapping Table available as a file (OMF file).

Released ONVIF Mapping files are stored in the following directory of Configuration Client:

– `%programdata%\Bosch\VMS\ONVIF`

If the same Mapping Table name is already imported, an error message is displayed.

If a newer version of this file is imported, a warning is displayed. Click **OK** if you want to import this file. Otherwise click **Cancel**.

To import:

1. Click .
2. Select the desired file and click **Open**.
   The **Import Mapping Table** dialog box is displayed.
3. Make the appropriate settings.
4. Click **OK** .

Import Mapping Table dialog box

Main window > **Devices** > Expand > Expand > Expand > Expand > Expand > > > **ONVIF Encoder Events** tab >

or

Main window > **Devices** > Expand > > **ONVIF Encoder Events** tab >

Manufacturer
Displays the manufacturer name this Mapping Table is valid for.

Model
Displays the model name this Mapping Table is valid for.

Description
Displays further information for example on tested camera models.

Mapping Table name
Displays the name of the Mapping Table. Change this name if it is already in use in BVMS.
You can select one of the following options to decide to which ONVIF encoders you want to apply the Mapping Table.

Apply only to selected ONVIF encoder

Apply to all ONVIF encoders of the listed models

Apply to all ONVIF encoders of the manufacturer
Existing ONVIF event mapping is continued. You cannot import OMT files from earlier BVMS versions.

14.3.4 Configuring an ONVIF mapping table

Main window > **Devices** > Expand > Expand > Expand > Expand > Expand > > > **ONVIF Encoder Events** tab

or

Main window > **Devices** > Expand > > **ONVIF Encoder Events** tab

You configure Mapping Tables for mapping ONVIF events to BVMS events.
You configure a Mapping Table for all ONVIF encoders of the same model or all ONVIF encoders from the same manufacturer.

Click to update ONVIF encoders that were added offline with the event mapping of an already added ONVIF encoder with the same manufacturer and/or model name.
For multichannel encoders you can configure the event sources, for example a specific camera or a relay.

To create a Mapping Table:

1. Click .
   The **Add Mapping Table** dialog box is displayed.
2. Type in a name for the Mapping Table.
3. In the **Manufacturer** and the **Model** lists, select the entries if desired.
   When you select **<none>** in both lists, the event mapping is only valid for this device.
   When you select **<none>** in the **Model** list and the manufacturer name in the **Manufacturer** list, the event mapping is valid for all devices with the same manufacturer.
   When you select the available entries in both lists, the event mapping is valid for all devices with the same manufacturer and model.
4. Click **OK**.
   You can now edit the Mapping Table, for example add a row to the **Motion Detected** event.

To edit a Mapping Table:

1. Click .
   The **Rename Mapping Table** dialog box is displayed.
2. Change the desired entries.

To add or remove event mappings:

1. In the **Mapping Table** list, select the desired name.
2. To add a row: Click **Add row**.
3. In the row, select the desired entries.
   When multiple rows are available, an event is triggered when only one of the rows is true.
4. To remove a row: Click **Remove row**.

To remove a Mapping Table:

1. In the **Mapping Table** list, click the name of the event mappings that you want to remove.
2. Click .

To configure an event source:

1. Expand and click or or .
2. Click the **ONVIF Event Source** tab.
3. In the **Trigger Event** column, activate the event configured in this row.
4. Select the desired event definitions.

Add / Rename ONVIF Mapping Table dialog box

Main window > **Devices** > Expand > Expand > Expand > Expand > > **ONVIF Encoder Events** tab > or

or

Main window > **Devices** > Expand > > **ONVIF Encoder Events** tab > or

Allows you to add a Mapping Table. If this Mapping Table shall serve as a template for future ONVIF encoders of the same manufacturer and model, select the correct entries.

Mapping Table name
Type in name for easy identification.

Manufacturer
Select an entry if required.

Model
Select an entry if required.

See also
- *Enabling logging for ONVIF events, page 359*
- *ONVIF event mapping, page 52*
- *ONVIF Encoder Events page, page 233*
- *ONVIF Event Source page, page 252*

14.4 ONVIF Configuration page

Main window > **Devices** > Expand > Expand > Expand > Expand > > > **ONVIF Configuration** tab

or

Main window > **Devices** > Expand > > **ONVIF Configuration** tab

You can select multiple ONVIF encoders and change settings on the **Video Encoder Profile** page. The changed settings are valid for all selected devices.

This page is only available for ONVIF encoders.

Notice!
Limitations of ONVIF configuration
Settings which you perform on these pages, are possibly not executed correctly because they are not supported by your camera. Supported ONVIF cameras were tested only with default settings.

14.4.1 Unit Access

Main window > **Devices** > Expand > Expand > Expand > Expand > > > **ONVIF Configuration** tab > **Main Settings** tab > **Unit Access** tab

or

Main window > **Devices** > Expand > > **ONVIF Configuration** tab > **Main Settings** tab > **Unit Access** tab

Manufacturer
Displays the manufacturer name of the selected encoder.

Model
Displays the model name of the selected encoder.
Note: If you want to export any event mappings into a ONVIF Mapping file select this model name as file name.

Hardware ID
Displays the hardware ID of the selected encoder.

Firmware version
Displays the firmware version of the selected encoder.
Note: Please ensure with the BVMS compatibility list whether the firmware version is correct.

Serial number
Displays the serial number of the selected encoder.

MAC address
Displays the MAC address of the selected encoder.

ONVIF version
Displays the ONVIF version of the selected encoder.
For BVMS, the ONVIF version 2.0 is required.

14.4.2 Date / Time

Main window > **Devices** > Expand > Expand > Expand > Expand > > > **ONVIF Configuration** tab > **Main Settings** tab > **Date/Time** tab

or

Main window > **Devices** > Expand > > **ONVIF Configuration** tab > **Main Settings** tab > **Date/Time** tab

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

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

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

14.4.3 User Management

Main window > **Devices** > Expand > Expand > Expand > Expand > > **ONVIF Configuration** tab > **Main Settings** tab > **User Management** tab

or

Main window > **Devices** > Expand > > **ONVIF Configuration** tab > **Main Settings** tab > **User Management** tab

These user settings are used for 3rd party applications such as direct Web Client access to encoders.

Following user roles for the access of 3rd party applications are supported:

- **Anonymous**: This role has unlimited access only to those devices where no users from other roles (**User**, **Operator**, **Administrator**) are registered. On the devices with at least one above mentioned user, the anonymous user has the right only to view time settings.
- **Administrator** (not supported by Configuration Client): This role has access to all application sections and features, the rights to reboot the device, reset settings and update firmware as well as create other users with different access rights.

The first user created on the device must be **Administrator**.

For differences in Operator's and User's default access rights of the **Operator** role and the **User** role, see the following table.

ONVIF Configuration Section or Feature	Operator	User
Identification	VIEW	HIDDEN
Time Settings	VIEW	VIEW
Network Settings	VIEW	VIEW
Users	HIDDEN	HIDDEN
Relays Settings	CHANGE	VIEW
Live Video (including rtsp-link)	CHANGE	CHANGE
Video Streaming	CHANGE	VIEW
Profiles	CHANGE	VIEW

CHANGE - Change current and create new settings.
VIEW - Settings are not hidden, but it is not permitted to change and create them.
HIDDEN - Certain settings or even the whole sections are hidden.

Users
Lists the available users of the device.

Password
Type in a valid password.

Confirm password
Confirm the typed in password.

Role
Select the desired role for the selected user. Access rights are adapted accordingly.

14.4.4 Video Encoder Profile page

Main window > **Devices** > Expand > Expand > Expand > Expand > > > **ONVIF Configuration** tab > **Camera** tab > **Video Encoder Profile** tab

or

Main window > **Devices** > Expand > > **ONVIF Configuration** tab > **Camera** tab > **Video Encoder Profile** tab

Profiles are rather complex and include a number of parameters that interact with one another, so it is generally best to use the pre-defined profiles. Only change a profile if completely familiar with all the configuration options.

Profiles

Click the desired name.

Notice!

The profiles configured here can be selected in Configuration Client.

In the main window, click **Cameras and Recording** and click or .

The default setting ´<Automatic>´ can be changed to one of the listed and configured profiles

Note: Take care when using actively more than 1 profile of a single device that certain performance restrictions apply and possibly the camera automatically restricts the quality of a stream in overload situations.

Name

You can enter a new name for the profile here. The name is then displayed in the list of available profiles in the Active profile field.

Encoding

Select the desired codec.

Resolution

Select the desired resolution for the video image.

Quality

This parameter allows you to reduce the load on the channel by means of reducing the picture definition. The parameter is set with the help of the slider bar: The left most position corresponds to the highest picture definition, the right most - to the lowest load on the video channel.

Frame rate limit

Frame rate (frame per second) denotes how many frames per second are captured by the video camera connected to the device. This parameter is shown just for information.
If an encoding interval is provided the resulting encoded frame rate is reduced by the given factor.

Bit rate limit

The less the bit rate is, the less the final video file size. But when the bit rate is considerably reduced, the program will have to use stronger compression algorithms, which also reduces video quality.

Select the maximum output bit rate in kbps. This maximum data rate is not exceeded under any circumstances. Depending on the video quality settings for the I- and P-frames, this fact can result in individual images being skipped.
The value entered here should be at least 10% greater than the typical target data bit rate.

Encoding interval
Encoding interval (number of frames) denotes at which rate the frames coming from the camera are encoded. For example, when encoding the interval comprises 25, it means that 1 frame from 25 captured per second is encoded and transmitted to the user. The maximum value reduces the load on the channel but may cause skipping information from the frames that were not encoded. Reducing the encoding interval increases the frequency of picture update as well as the load on the channel.

GOP length
GOP length is possible to edit only in case the encoder is H.264 or H.265. This parameter denotes the length of the picture group between the two key frames. The higher this value is, the less the load to the network is, but the video quality is affected.
An entry of 1 indicates that I-frames are continuously generated. An entry of 2 indicates that every second image is an I-frame, and 3 only every third frame, and so on. The frames in between are encoded as P-frames or B-frames.

Session timeout
The RTSP session timeout for the related video stream.
The session timeout is provided as a hint for keeping RTSP session by a device.

Multicast - IP address
Enter a valid multicast address to be operated in multicast mode (duplication of the data stream in the network).

With a 0.0.0.0 setting, the encoder for the stream operates in multi-unicast mode (copying of data stream in device). The camera supports multi-unicast connections for up to five simultaneously connected receivers.

Duplication of data places a heavy demand on the CPU and can lead to impairment of the image quality under certain circumstances.

Multicast - Port
Select the RTP multicast destination port. A device may support RTCP. In this case the port value shall be even to allow the corresponding RTCP stream to be mapped to the next higher (odd) destination port number as defined in the RTSP specification.

Multicast - TTL
A value can be entered to specify how long the multicast data packets are active on the network. If multicast is to be run via a router, the value must be greater than 1.

Notice!
Multicast operation is only possible with the UDP protocol. The TCP protocol does not support multicast connections.
If the device is operated behind a Firewall, select TCP (HTTP port) as the transfer protocol.
For use in a local network, select UDP.

14.4.5 Audio Encoder Profile

Main window > **Devices** > Expand > Expand > Expand > Expand > > > **ONVIF Configuration** tab > **Camera** tab > **Audio Encoder Profile** tab

or

Main window > **Devices** > Expand > > >**ONVIF Configuration** tab > **Camera** tab > **Audio Encoder Profile** tab

Profiles are rather complex and include a number of parameters that interact with one another, so it is generally best to use the pre-defined profiles. Only change a profile if completely familiar with all the configuration options.

Encoding

Select the desired encoding for the audio source if available:

- **G.711 [ITU-T G.711]**
- **G.726 [ITU-T G.726]**
- **AAC [ISO 14493-3]**

Bit rate

Select the desired bit rate, for example 64 kbps, for transmitting the audio signal.

Sample rate

Enter the output sample rate in kHz, for example 8 kbps.

Session timeout

The RTSP session timeout for the related audio stream.

The session timeout is provided as a hint for keeping RTSP session by a device.

14.4.6 Imaging General

Main window > **Devices** > Expand > Expand > Expand > Expand > > > **ONVIF Configuration** tab > **Camera** tab > **Imaging General** tab

or

Main window > **Devices** > Expand > > >**ONVIF Configuration** tab > **Camera** tab > **Imaging General** tab

Brightness

Adjust the image brightness to your working environment.

Color saturation

Adjust the color saturation in the image to make the reproduction of colors on your monitor as realistic as possible.

Contrast

You can adapt the contrast of the video image to your working environment.

Sharpness

Adjust the sharpness in the image.

A low value makes the picture less sharp. Increasing sharpness brings out more detail. Extra sharpness can enhance the details of license plates, facial features and the edges of certain surfaces but can increase bandwidth requirements.

IR cut-off filter
Select the state of the IR cut-off filter.
The AUTO state lets the exposure algorithm handle when the IR cut-off filter is switched.

14.4.7 Backlight Compensation

Main window > **Devices** > Expand > Expand > Expand > Expand > > > **ONVIF Configuration** tab > **Main Settings** tab > **Backlight compensation** tab

or

Main window > **Devices** > Expand > >**ONVIF Configuration** tab > **Main Settings** tab > **Backlight compensation** tab

Depending on the device model you can configure here parameters for the backlight compensation.

Mode
Select **Off** to switch off backlight compensation.
Select **On** to capture details in high-contrast and extremely bright-dark conditions.

Level
Enter or select the desired value.

14.4.8 Exposure

Main window > **Devices** > Expand > Expand > Expand > Expand > > > **ONVIF Configuration** tab > **Main Settings** tab > **Exposure** tab

or

Main window > **Devices** > Expand > >**ONVIF Configuration** tab > **Main Settings** tab > **Exposure** tab

Depending on the device model you can configure here parameters for the exposure.

Mode
Select **Auto** to enable the exposure algorithm on the device. The values in the following fields are used by the algorithm:

- **Priority**
- **Window**
- **Min. exposure time**
- **Max. exposure time**
- **Min. gain**
- **Max. gain**
- **Min. iris**

Select **Manual** to disable the exposure algorithm on the device. The values in the following fields are used by the algorithm:

- **Exposure time**
- **Gain**
- **Iris**

Priority
Configure the exposure priority mode (low noise/frame rate).

Window
Define a rectangular exposure mask.

Min. exposure time
Configure the minimum exposure time period [µs].

Max. exposure time
Configure the maximum exposure time period [µs].

Min. gain
Configure the minimum sensor gain range [dB].

Max. gain
Configure the maximum sensor gain range [dB].

Min. iris
Configure the minimum attenuation of input light affected by the iris [dB]. 0dB maps to a fully opened iris.

Max. iris
Configure the maximum attenuation of input light affected by the iris [dB]. 0dB maps to a fully opened iris.

Exposure time
Configure the fixed exposure time [µs].

Gain
Configure the fixed gain [dB].

Iris
Configure the fixed attenuation of input light affected by the iris [dB]. 0dB maps to a fully opened iris.

14.4.9 Focus

Main window > **Devices** > Expand > Expand > Expand > Expand > > **ONVIF Configuration** tab > **Main Settings** tab > **Focus** tab

or

Main window > **Devices** > Expand > >**ONVIF Configuration** tab > **Main Settings** tab > **Focus** tab

Depending on the device model you can configure here parameters for the focus.
This page allows for moving the lens in an absolute, a relative or in a continuous way. Focus adjustments through this operation turn off the autofocus. A device with support for remote focus control usually supports control through this move operation. The focus position is represented with a certain numeric value. The state of the focus can be one of the following:

MOVING
OK
UNKNOWN
Additionally error information can be displayed, for example a positioning error indicated by the hardware.

Mode
Select **Auto** to enable the lens to automatically focus at any time according to the objects in the scene. The values in the following fields are used by the algorithm:
– **Near limit**
– **Far limit**
Select **Manual** to adjust the focus manually. The values in the following fields are used by the algorithm:
– **Default speed**

Default speed
Configure the default speed for focus move operation (when the speed parameter not is present).

Far limit
Configure the near limit for focus lens [m].

Far limit
Configure the far limit for focus lens [m].

14.4.10 Wide Dynamic Range

Main window > **Devices** > Expand > Expand > Expand > Expand > Expand > > **ONVIF Configuration** tab > **Main Settings** tab > **Wide Dynamic Range** tab
or
Main window > **Devices** > Expand > >**ONVIF Configuration** tab > **Main Settings** tab > **Wide Dynamic Range** tab
Depending on the device model you can configure here parameters for the wide dynamic range.

Mode
Enter or select the desired value.

Level
Enter or select the desired value.

14.4.11 White balance

Main window > **Devices** > Expand > Expand > Expand > Expand > Expand > > **ONVIF Configuration** tab > **Main Settings** tab > **White Balance** tab
or

Main window > **Devices** > Expand > >**ONVIF Configuration** tab > **Main Settings** tab > **White Balance** tab

Depending on the device model you can configure here parameters for the white balance.

Mode

Auto mode allows the camera to continually adjust for optimal color reproduction using an average reflectance method or in an environment with natural light sources.

In Manual mode the Red, Green, and Blue gain can be manually set to a desired position

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

- indoor light sources and for colored LED light illumination
- sodium vapor light sources (street lighting)
- for any dominant color in the image for example, the green of a football pitch or of a gaming table

R-gain

In Manual white balance mode, adjust the Red gain slider to offset the factory white point alignment (reducing Red, increases Cyan).

B-gain

In Manual white balance mode, adjust the Blue gain slider to offset the factory white point alignment (reducing Blue, increases Yellow).

14.4.12 Network Access

Main window > **Devices** > Expand > Expand > Expand > Expand > > **ONVIF Configuration** tab > **Network** tab > **Network Access** tab

or

Main window > **Devices** > Expand > >**ONVIF Configuration** tab > **Network** tab > **Network Access** tab

Here you can configure various network settings.

Ethernet IPv4

DHCP

If a DHCP server is employed in the network for the dynamic assignment of IP addresses, you can activate acceptance of IP addresses automatically assigned to the encoder.

BVMS uses the IP address for the unique assignment of the encoder. The DHCP server must support the fixed assignment between IP address and MAC address, and must be appropriately set up so that, once an IP address is assigned, it is retained each time the computer is restarted.

Subnet mask

Type in the appropriate subnet mask for the set IP address.

If DHCP server is enabled, the subnet mask is automatically assigned.

Default gateway

If you want the module to establish a connection to a remote location in a different subnet, type in the IP address of the gateway here. Otherwise leave the field empty (0.0.0.0).

Ethernet IPv6

DHCP
Enter or select the desired value.

IP address
Displays the IPv6 address of the device, provided by the DHCP server.

Prefix length
Displays the prefix length of the device, provided by the DHCP server.

Default gateway
Displays the default gateway of the device, provided by the DHCP server.

Host name
Enter or select the desired value.

DNS
Using a DNS server, the device can resolve an address indicated as a name. Enter the IP address of the DNS server here.

NTP servers
Type in the IP address of the desired time server or let the DHCP server do this for you. The encoder can receive the time signal from a time server using various time server protocols, and then use it to set the internal clock. The module polls the time signal automatically once every minute. Enter the IP address of a time server here. This supports a high level of accuracy and is required for special applications.

HTTP ports
Select a different HTTP browser port if required. The default HTTP port is 80. If you want to allow only secure connections via HTTPS, you must deactivate the HTTP port.
Note: Not supported by BVMS.

HTTPS ports
Note: Not supported by BVMS.
If you want to grant access on the network via a secure connection, select an HTTPS port if necessary. The default HTTPS port is 443. Select the **Off** option to deactivate HTTPS ports; only unsecured connections will now be possible.

Default gateway
Enter or select the desired value.

RTSP ports
If necessary, select a different port for the exchange of the RTSP data. The standard RTSP port is 554. Select **Off** to deactivate the RTSP function.

Zero configuration address
Enable or disable the zero configuration discovery of the selected camera.
Zero configuration is an alternative method to DHCP and DNS for assigning IP addresses to cameras. It automatically creates a usable IP network address without configuration or special servers.
Note: In the ONVIF standard only the service discovery of zero configuration is used. Alternatively without zero configuration the network must provide services, such as DHCP or DNS.
Otherwise configure the network settings of each IP camera manually.

ONVIF discovery mode
If enabled, the camera can be scanned in the network. This includes its capabilities.

If disabled, the camera does not send any discovery messages to avoid denial-of-service attacks.
We recommend disabling the discovery after adding the camera to the configuration.
Enter or select the desired value.

Enable DynDNS
Alllows for enabling DynDNS.
A dynamic Domain Name Service (DNS) allows you to select the unit via the Internet using a host name, without having to know the current IP address of the unit. To do this, you must have an account with one of the dynamic DNS providers and you must register the required host name for the unit on that site.

Note:
For information about the service, registration process and available host names refer to the DynDNS provider on dyndns.org.

Type
Enter or select the desired value.

Name
Type in the name of your DynDNS user account.

TTL
Enter or select the desired value.

14.4.13 Scopes

Main window > **Devices** > Expand > Expand > Expand > Expand > > **ONVIF Configuration** tab > **Network** tab > **Scopes** tab

or

Main window > **Devices** > Expand > > **ONVIF Configuration** tab > **Network** tab > **Scopes** tab

You can add or remove scopes to your ONVIF device with URIs having the following format:

```
onvif://www.onvif.org/<path>
```

The following example illustrates the usage of the scope value. This is just an example, and not at all an indication of what type of scope parameter to be part of an encoder configuration. In this example we assume that the encoder is configured with the following scopes:

```
onvif://www.onvif.org/location/country/china
onvif://www.onvif.org/location/city/bejing
onvif://www.onvif.org/location/building/headquarter
onvif://www.onvif.org/location/floor/R5
onvif://www.onvif.org/name/ARV-453
```

You can give the device a detailed location and device name to identify it within your list of devices.
The table shows the basic capabilities and other properties of the device, which are standardized:

Category	Defined values	Description
type	video_encoder	Te device is a network video encoder device.
	Ptz	The device is a PTZ device.
	audio_encoder	The device provides audio encoder support.
	video_analytics	The device supports video analytics.
	Network_Video_Transmitter	The device is a network video transmitter.
	Network_Video_Decoder	The device is a network video decoder.
	Network_Video_Storage	The device is a network video storage device.
	Network_Video_Analytic	The device is a network video analytics device.
location	Any character string or path value.	Not supported by BVMS.
hardware	Any character string or path value.	A string or path value describing the hardware of the device. A device shall include at least one hardware entry into its scope list.
name	Any character string or path value.	The searchable name of the device. This name is displayed in the Device and the Logical Tree.

The scope name, model, manufacturer determine how the device appears in the Device Tree and the ONVIF Encoder Identification and Main Settings.

14.4.14 Relays

Main window > **Devices** > Expand > Expand > Expand > Expand > > > **ONVIF Configuration** tab > **Interfaces** tab > **Relay** tab

Main window > **Devices** > Expand > > **ONVIF Configuration** tab > **Interfaces** tab > **Relay** tab

The physical idle state of a relay output can be configured by setting the idle state to **open** or **closed** (inversion of the relay behavior).

The available digital outputs oft he device are listed with their name, e.g.:

- **AlarmOut_0**
- **AlarmOut_1**

For any event mapping of relays within BVMS use the names listed here.

Mode

The relay can work in two relay modes:

- **Bistable**: After setting the state, the relay remains in this state.
- **Monostable**: After setting the state, the relay returns to its idle state after the specified delay time.

Idle state

Select **Open** if you want the relay to operate as a normally open contact, or select **Closed** if the relay is to operate as a normally closed contact.

Delay time
Set the delay time . After this time period, the relay switches back to its idle state if configured in the **Monostable** mode.
If you like to test any configurations related to a relay status change, click **Activate** or **Deactivate** to switch the relay. You can check the configured camera relay events for correct functioning: Status display of the relay icon in Logical Tree, Events in Alarm List or Event Log.

Activate
Click to switch the relay to the configured idle state.
Deactivate
Click to switch the relay to the configured non-idle state.

14.5 ONVIF Event Source page

Main window > **Devices** > Expand > Expand > Expand > Expand > Expand > > **ONVIF Event Source** tab
or
Main window > **Devices** > Expand > Expand > > **ONVIF Event Source** tab
or
Main window > **Devices** > Expand > Expand > Expand > Expand > Expand > > **ONVIF Event Source** tab
or
Main window > **Devices** > Expand > Expand > > **ONVIF Event Source** tab
or
Main window > **Devices** > Expand > Expand > Expand > Expand > Expand > > **ONVIF Event Source** tab
or
Main window > **Devices** > Expand > Expand > > **ONVIF Event Source** tab
You can configure ONVIF events of a source (video channel, input or relay). An activated event definition is added to the Mapping Table of the encoder.
For example for a multichannel encoder, you configure for which camera a **Motion Detected** event is triggered.

Trigger Event
Activate this event.

ONVIF Topic
Type in or select a string.

ONVIF Source Name
Type in or select a string.

ONVIF Source Type
Type in or select a string.

ONVIF Source Value
Type in or select a string.

See also
- *ONVIF event mapping, page 52*
- *Configuring an ONVIF mapping table, page 237*

14.6 Assigning an ONVIF profile

Main window > **Cameras and Recording** >

You can assign an ONVIF Media Profile token to an ONVIF camera.
You can assign either for live video or for recording.

To assign a live video token:
- In the **Live Video** - **Profile** column, select the desired entry.

To assign a recording token:
- In the **Recording** - **Profile** column, select the desired entry.

See also
- *Cameras page, page 276*

15 Maps and Structure page

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

Main window > **Maps and Structure**

Permissions can get lost. If you move a group of devices, these devices loose their permission settings. You must set the permissions on the **User groups** page again.

Displays the Device Tree, the Logical Tree, and the map window.

Allows you to introduce a structure for all the devices in your BVMS. Your structure is displayed in the Logical Tree.

Allows you to perform the following tasks:

- Configuring the Full Logical Tree
- Managing resource files, assigning them to nodes
- Creating hotspots on a map
- Creating a malfunction relay

Resource files can be:

- Site map files
- Document files
- Web files
- Audio files
- Command Scripts
- Camera sequence files

Hotspots can be:

- Cameras
- Inputs
- Relays
- Command Scripts
- Sequences
- Links to other maps
- Readers of an access control system

Icons

	Displays a dialog box for managing resource files.
	Displays a dialog box for adding or managing Command Scripts to the Logical Tree.
	Displays a dialog box for adding or editing a camera sequence file.
	Creates a folder in the Logical Tree.
	Displays a dialog box for adding map resource files.
	Displays a dialog box for adding a document file (HTML, HTM, TXT, URL, MHT).
	Displays a dialog box for adding a link to an external application.

	Displays a dialog box for adding a malfunction relay.

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 .

15.1 Resource Manager dialog box

Main window > **Maps and Structure** > > **Resource Manager** dialog box

Allows you to manage resource files.

You can manage the following file formats:

- DWF files (map resource files)
  For use in Operator Client, these files are converted to a bitmap format.
- HTML files (HTML documents, e.g. action plans)
- MP3 (audio file)
- TXT files (text files)
- URL files (contain links to web pages or Intelligent Insights widgets)
- MHT files (Web archives)
- WAV (audio file)
- EXE

Click to display a dialog box for importing a resource file.

Click to display the **Add URL** dialog box.

Click to display the **Link to External Application** dialog box.

Click to remove the selected resource file.

Click to rename the selected resource file.

Click to display a dialog box for replacing the selected resource file with another one.

Click to display a dialog box for exporting the selected resource file.

See also

- *Managing resource files, page 261*

15.2 Select Resource dialog box

Main window > **Maps and Structure** >

Allows you to add a map file in DWF format to the Logical Tree.

Select a resource file:

Click a filename to select a map file. The content of the selected file is displayed in the preview pane.

Manage...

Click to display the **Resource Manager** dialog box.

See also

- *Adding a map, page 264*
- *Assigning a map to a folder, page 265*
- *Adding a document, page 266*

15.3 Sequence Builder dialog box

Main window > **Maps and 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.

See also
- *Monitor Wall page, page 150*
- *Managing pre-configured camera sequences, page 262*

15.4 Add Sequence dialog box

Main window > **Maps and Structure** > > **Sequence Builder** dialog box >
Allows you to configure the properties of a camera sequence.

Sequence name:
Type an appropriate name for the new camera sequence.

Logical number:
For using with a Bosch IntuiKey keyboard, enter a logical number for the sequence.

Dwell time:
Enter the appropriate dwell time.

Cameras per step:
Enter the number of cameras in each step.

Steps:
Enter the appropriate number of steps.

See also
- *Managing pre-configured camera sequences, page 262*

15.5 Add Sequence Step dialog box

Main window > **Maps and Structure** > > **Add Step** button
Allows you to add a step with a new dwell time to an existing camera sequence.

Dwell time:
Enter the appropriate dwell time.

See also
- *Managing pre-configured camera sequences, page 262*

15.6 Add URL dialog box

Main window > **Maps and Structure** > >

Allows you to add an HTTP Internet address (URL) or an HTTPS Internet Address such as Intelligent Insights widgets to your system. You can add this URL to the Logical Tree as a document. The user can display an Internet page or an Intelligent Insights widget in his Operator Client.

Name

Type a display name for the URL.

URL

Type the URL.

For secure connection only

User

Type the user name for the HTTPS URL.

Password:

Type the password for the HTTPS URL.

Show password

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

See also

– *Adding a document, page 266*

15.7 Select Map for Link dialog box

Main window > **Maps and Structure** > Select a map folder in the Logical Tree > On the map, right-click and click **Create Link**

Allows you to select a map for creating a link to another map.

Click another map to select.

Select

Click to insert the link to the selected map.

See also

– *Adding a link to another map, page 265*

15.8 Malfunction Relay dialog box

Main window > **Maps and Structure** > > **Malfunction Relay** dialog box

You can add a malfunction relay to your system. You define the relay that is to be used as malfunction relay and you configure the events that can trigger the malfunction relay.
The relay must already be configured in the Logical Tree.

Malfunction Relay

In the list, select the desired relay.

Events...
Click to display the **Events selection for Malfunction Relay** dialog box.

See also
- *Adding a malfunction relay, page 267*
- *Malfunction relay, page 47*

15.9 Link to External Application dialog box

Main window > **Maps and Structure** > > **Resource Manager** dialog box >
> **Link to External Application** dialog box
Allows you to add a link to an external application. The link must be valid on the workstation where this link is used.

Notice!
An external application that starts with a splash screen will not work as expected.
An external application which shares functions with Operator Client, will not work as expected and can, under rare circumstances, lead to a crash of Operator Client.

Name
Type in a name for the link that is displayed in the Logical Tree.

Path
Type in or browse the path to the external application. This path must be valid on the workstation where the user of Operator Client uses this link.

Arguments
If required, type in arguments for the command that executes the external application.

16 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.

See also
- *Resource Manager dialog box, page 255*
- *Select Resource dialog box, page 256*
- *Sequence Builder dialog box, page 256*
- *Add Sequence dialog box, page 257*
- *Add Sequence Step dialog box, page 257*
- *Add URL dialog box, page 258*
- *Select Map for Link dialog box, page 258*
- *Malfunction Relay dialog box, page 258*
- *Link to External Application dialog box, page 259*

16.1 Configuring the Logical Tree

See also
- *Maps and Structure page, page 254*

16.2 Adding a device to the Logical Tree

Main window > **Maps and Structure**

To add a device:

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

See also
- *Maps and Structure page, page 254*

16.3 Removing a tree item

Main window > **Maps and Structure**

To remove a tree item from the Logical Tree:

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

See also

– *Maps and Structure page, page 254*

16.4 Managing resource files

Main window > **Maps and Structure** >

or

Main window > **Alarms** >

You can import resource files in the following formats:

– DWF files (2 D, map resource files)
  For use in Operator Client, these files are converted to a bitmap format.
– HTML files (map document files)
– MP3 (audio file)
– TXT files (Command Scripts or camera sequences)
– MHT files (Web archives)
– URL files (links to Web pages)
– HTTPS URL files (links to Intelligent Insights widgets)
– WAV (audio file)

The imported resource files are added to a database. They are not linked to the original files.

Notice!
After each of the following tasks:
Click to save the settings.

To import a resource file:

1. Click .
   The **Import Resource** dialog box is displayed.
2. Select one or more files.
3. Click **Open**.
   The selected files are added to the list.
   If a file has already been imported, a message box is displayed.
   If you decide to import an already imported file again, a new entry is added to the list.

To remove a resource file:

1. Select a resource file.
2. Click .
   The selected resource file is removed from the list.

To rename a resource file:

1. Select a resource file.
2. Click .
3. Enter the new name.
   The original file name and creation date persists.

To replace the content of a resource file:

1. Select a resource file.
2. Click .
   The **Replace Resource** dialog box is displayed.
3. Select a file with the appropriate content and click **Open**.
   The resource name persists, the original file name is exchanged with the new file name.

To export a resource file:

1. Select a resource file.
2. Click .
   A dialog box for selecting a directory is displayed.
3. Select the appropriate directory and click **OK**.
   The original file is exported.

See also

– *Select Resource dialog box, page 256*

16.5 Adding a Command Script

Main window > **Maps and Structure**

Before you can add a Command Script, you must have Command Script files imported or created.

If required, see *Configuring Command Scripts, page 100* for details.

To add a Command Script file:

1. Select a folder where you want to add the new Command Script.
2. Click . The **Select Client Script** dialog box is displayed.
3. Select a file in the list.
4. Click **OK**.
   A new Command Script is added under the selected folder.

See also

– *Select Resource dialog box, page 256*

16.6 Managing pre-configured camera sequences

Main window > **Maps and Structure**

You can perform the following tasks for managing camera sequences:

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

– Remove a step from camera sequence
– Delete a camera sequence

Notice!
When the configuration is changed and activated, a camera sequence (pre-configured or automatic) usually is continued after restart of the Operator Client.
But in the following cases the sequence is not continued:
A monitor where the sequence is configured to be displayed has been removed.
The mode of a monitor (single/quad view) where the sequence is configured to be displayed has been changed.
The logical number of a monitor where the sequence is configured to be displayed is changed.

Notice!
After each of the following tasks:
Click to save the settings.

To create a camera sequence:
1. In the Logical Tree, select a folder where you want to create the camera sequence.
2. Click .
   The **Sequence Builder** dialog box is displayed.
3. In the **Sequence Builder** dialog box, click .
   The **Add Sequence** dialog box is displayed.
4. Enter the appropriate values.
5. 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:
1. Select the desired camera sequence.
2. Click **Add Step**.
   The **Add Sequence Step** dialog box is displayed.
3. Make the appropriate settings.
4. Click **OK**.
   A new step is added to the camera sequence.

To remove a step from a camera sequence:
- Right-click the desired camera sequence and click **Remove Step**.
  The step with the highest number is removed.

To delete a camera sequence:
1. Select the desired camera sequence.
2. Click . The selected camera sequence is removed.

See also
– *Sequence Builder dialog box, page 256*

– *Add Sequence dialog box, page 257*
– *Add Sequence Step dialog box, page 257*

16.7 Adding a camera sequence

Main window > **Maps and Structure**

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

To add a camera sequence:

1. In the Logical Tree, select a folder where you want to add the new camera sequence.
2. Click . The **Sequence Builder** dialog box is displayed.
3. In the list, select a camera sequence.
4. Click **Add to Logical Tree**. A new is added under the selected folder.

See also

– *Sequence Builder dialog box, page 256*

16.8 Adding a folder

Main window > **Maps and Structure**

To add a folder:

1. Select a folder where you want to add the new folder.
2. Click . A new folder is added under the selected folder.
3. Click to rename the folder.
4. Type the new name and press ENTER.

See also

– *Maps and Structure page, page 254*

16.9 Adding a map

Main window > **Maps and Structure**

Before you can add a map, you must have map resource files imported.

To import a map resource file see *Managing resource files, page 261* for details.

To add a map:

1. Ensure that the map resource file that you want to add has already been imported.
2. Select a folder where you want to add the new map.
3. Click . The **Select Resource** dialog box is displayed.
4. Select a file in the list.
   If the required files are not available in the list, click **Manage...** to display the **Resource Manager** dialog box for importing files.

5. Click **OK**.

   A new map is added under the selected folder.
   The map is displayed.
   All devices within this folder are displayed in the upper left corner of the map.

See also
– *Select Resource dialog box, page 256*

16.10 Adding a link to another map

Main window > **Maps and Structure**

After you have added at least two maps, you can add a link on one map to the other so that the user can click from one map to a linked one.

To add a link:

1. Click a map folder in the Logical Tree.
2. Right-click the map and click **Create Link**.
   The **Select Map for Link** dialog box is displayed.
3. In the dialog box, click a map .
4. Click **Select**.
5. Drag the item to the appropriate place on the map.

See also
– *Select Map for Link dialog box, page 258*

16.11 Assigning a map to a folder

Main window > **Maps and Structure**

Before you can assign maps, you must have map resource files imported.
If required, see *Managing resource files, page 261* for details.

To assign a map resource file:

1. Right-click a folder and click **Assign Map**.
   The **Select Resource** dialog box is displayed.
2. Select a map resource file in the list.
3. Click **OK**. The selected folder is displayed as .
   The map is displayed in the map window.
   All items within this folder are displayed in the upper left corner of the map.

See also
– *Maps and Structure page, page 254*
– *Select Resource dialog box, page 256*

16.12 Managing devices on a map

Main window > **Maps and Structure**

Before you can manage devices on a map you must add a map or assign a map to a folder and add devices to this folder.

Notice!

After each of the following tasks:

Click to save the settings.

To place items on a map:

1. Select a map folder.
2. Drag devices from the Device Tree to the map folder.
   The devices of a map folder are located on the left upper corner of the map.
3. Drag the items to the appropriate places on the map.

To remove an item in the Logical Tree only from the map:

1. Right-click the item on the map and click **Invisible**.
   The item is removed from the map.
   The item remains in the Logical Tree.
2. To make it visible again, right-click the device in the Logical Tree and click **Visible In Map**.

To remove an item from the map and from the Full Logical Tree:

- Right-click the item in the Logical Tree and click **Remove**.
  The item is removed from the map and from the Logical Tree.

To change the icon for the orientation of a camera:

- Right-click the item, point to **Change Image**, and then click the appropriate icon.
  The icon changes accordingly.

To change the color of an item:

- Right-click the item and click to **Change Color**. Select the appropriate color.
  The icon changes accordingly.

To bypass / unbypass a device on a map:

1. Right-click the certain device on the map.
2. Click **Bypass** / **Unbypass**.

Notice!

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

See also

- *Configuring bypass of devices, page 267*
- *Maps and Structure page, page 254*

16.13 Adding a document

Main window > **Maps and Structure**

You can add text files, HTML files (including MHT files), URL files (containing an Internet address) or HTTPS URL files (for example containing an Intelligent Insights widget) as documents. And you can add a link to another application.
Before you can add a document, you must have document files imported.
To import document files see *Managing resource files, page 261* for details.
To add a map document file / to add an Intelligent Insights **widget:**

1. Ensure that the document file that you want to add has already been imported.
2. Select a folder where you want to add the new document.
3. Click . The **Select Resource** dialog box is displayed.
4. Select a file in the list. If the required files are not available in the list, click **Manage...** to display the **Resource Manager** dialog box for importing files.
5. Click **OK**. A new document is added under the selected folder.

See also

- *Select Resource dialog box, page 256*
- *Managing resource files, page 261*

16.14 Adding a malfunction relay

Main window > **Maps and Structure** > > **Malfunction Relay** dialog box

To add:

1. In the **Malfunction Relay** list, select the desired relay.
2. Click **Events...**
   The **Events selection for Malfunction Relay** dialog box is displayed.
3. Click to select the desired events that can trigger the malfunction relay.
4. Click **OK**.
   The malfunction relay is added to the system.

See also

- *Malfunction Relay dialog box, page 258*

16.15 Configuring bypass of devices

Main window > **Maps and Structure**

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

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

To bypass / unbypass a device in the Logical Tree or in the Device Tree:

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

To bypass / unbypass a device on a map:

See *Managing devices on a map, page 266*

Notice!

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

See also

– *Managing devices on a map, page 266*

17 Schedules page

Main window >

Allows you to configure Recording Schedules and Task Schedules.

Click to rename the selected Recording or Task Schedule.

Recording Schedules

Displays the Recording Schedules Tree. Select an entry for configuring.

Task Schedules

Displays the Task Schedules Tree. Select an entry for configuring.

Add

Click to add a new Task Schedule.

Delete

Click to delete the selected Task Schedule.

See also

- *Configuring schedules, page 271*

17.1 Recording Schedules page

Main window > > Select an item in the Recording Schedules tree

Allows you to configure Recording Schedules.

Weekdays

Click to display the Schedule Table for weekdays. The time periods of all configured Recording Schedules are displayed.

Drag the pointer to select the time periods for the selected schedule. All selected cells get the color of the selected schedule.

The 24 hours of the day are displayed horizontally. Every hour is divided into 4 cells. One cell represents 15 minutes.

Holidays

Click to display the Schedule Table for holidays.

Exception Days

Click to display the Schedule Table for exception days.

Add

Click to display a dialog box for adding the required holidays or exception days.

Delete

Click to display a dialog box for removing holidays or exception days.

See also

- *Configuring a Recording Schedule, page 271*
- *Adding holidays and exception days, page 273*
- *Removing holidays and exception days, page 274*
- *Renaming a schedule, page 274*

17.2 Task Schedules page

Main window > > Select an item in the Task Schedules tree

Allows you to configure the available Task Schedules. You can configure a standard or a recurring pattern.

Standard

Click to display the Schedule Table for configuring standard Task Schedules. If you configure a Standard Pattern, no Recurring Pattern is valid for the selected schedule.

Recurring

Click to display the Schedule Table for configuring a recurring pattern for the selected Task Schedule. For example, you configure a schedule for every second Tuesday of every month or for the 4th of July of every year. If you configure a recurring pattern, no standard pattern is valid for the selected Task Schedule.

Weekdays

Click to display the Schedule Table for weekdays.

Drag the pointer to select the time periods for the selected schedule. The selected cells are displayed in the color of the selected schedule.

The 24 hours of the day are displayed horizontally. Every hour is divided into 4 cells. One cell represents 15 minutes.

Holidays

Click to display the Schedule Table for holidays.

Exception Days

Click to display the Schedule Table for exception days.

Clear All

Click to clear the time periods of all available days (weekdays, holidays, exception days).

Select All

Click to select the time periods of all available days (weekdays, holidays, exception days).

Add...

Click to display a dialog box for adding the required holidays or exception days.

Delete...

Click to display a dialog box for deleting holidays or exception days.

Recurrence Pattern

Click the frequency with which you want the Task Schedule to recur (Daily, Weekly, Monthly, Yearly) and then select the corresponding options.

Day Pattern

Drag the pointer to select the time period(s) for the recurring pattern.

See also

- *Adding a Task Schedule, page 272*
- *Configuring a standard Task Schedule, page 272*
- *Configuring a recurring Task Schedule, page 272*
- *Removing a Task Schedule, page 273*
- *Adding holidays and exception days, page 273*
- *Removing holidays and exception days, page 274*
- *Renaming a schedule, page 274*

18 Configuring schedules

Main window > **Schedules**

There are two schedule types available:

- Recording Schedules
- Task Schedules

You can configure a maximum of 10 different Recording Schedules in the Recording Schedule Table. In these segments the cameras can behave differently. For example, they can have different frame rate and resolution settings (to be configured in the **Cameras and Recording** page). In every point in time, exactly one Recording Schedule is valid. There are no gaps and no overlaps.

You configure Task Schedules for scheduling various events which can occur in your system (to be configured in the **Events** page).

See glossary for definitions of Recording Schedules and Task Schedules.

The schedules are used in other pages of the Configuration Client:

- **Cameras and Recording** page
  Used to configure recording.
- **Events** page
  Used to determine when events cause logging, alarms, or execution of Command Scripts.
- **User groups** page
  Used to determine when the members of a user group can log on.

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

See also

- *Recording Schedules page, page 269*
- *Task Schedules page, page 270*

18.1 Configuring a Recording Schedule

Main window > **Schedules**

You can add exception days and holidays to any Recording Schedule. These settings override the normal weekly settings.

The sequence of decreasing priority is: exception days, holidays, weekdays.

The maximum number of Recording Schedules is 10. The first three entries are configured by default. You can change these settings. Entries with the gray icon do not have a time period configured.

Recording Schedules share the same weekdays.

Each Standard Task Schedule has its own weekdays patterns.

To configure a Recording Schedule:

1. In the **Recording Schedules** tree, select a schedule.

2. Click the **Weekdays** tab.
3. In the **Schedule Table** field, drag the pointer to select the time periods for the selected schedule. The selected cells are displayed in the color of the selected schedule.

Notes:

– You can mark a time period on a weekday of a Recording Schedule with the color of another Recording Schedule.

See also

– *Recording Schedules page, page 269*

18.2 Adding a Task Schedule

Main window > **Schedules**

To add a Task Schedule:

1. Click **Add**.
   A new entry is added.
2. Enter the appropriate name.
3. Click **Standard** for a standard Task Schedule or **Recurring** for a recurring Task Schedule. If you change the setting, a message box is displayed. Click **OK** if you want to change the schedule type.
   A standard Task Schedule is displayed as , a recurring Task Schedule as .
4. Make the appropriate settings for the selected schedule.

See also

– *Task Schedules page, page 270*

18.3 Configuring a standard Task Schedule

Main window > **Schedules**

Each standard Task Schedule has its own weekdays patterns.

To configure a standard Task Schedule:

1. In the **Task Schedules** tree, select a standard Task Schedule.
2. Click the **Weekdays** tab.
3. In the **Schedule Table** field, drag the pointer to select the time periods for the selected schedule.

See also

– *Task Schedules page, page 270*

18.4 Configuring a recurring Task Schedule

Main window > **Schedules**

Each recurring Task Schedule has its own day pattern.

To configure a recurring Task Schedule:

1. In the **Task Schedules** tree, select a recurring Task Schedule .

2. In the **Recurrence Pattern** field, click the frequency with which you want the Task Schedule to recur (**Daily**, **Weekly**, **Monthly**, **Yearly**) and then make the corresponding settings.
3. In the **Start date:** list, select the appropriate start date.
4. In the **Day Pattern** field, drag the pointer to select the appropriate time period.

See also
– *Task Schedules page, page 270*

18.5 Removing a Task Schedule

Main window > > Select an item in the **Task Schedules** tree

To remove a Task Schedule:
1. In the **Task Schedules** tree, select an item.
2. Click **Delete**.
   The Task Schedule is deleted. All items that are assigned to this schedule, are not scheduled.

See also
– *Task Schedules page, page 270*

18.6 Adding holidays and exception days

Main window > **Schedules**

Notice!
You can configure empty exception days and holidays. Exception days and holidays replace the schedule of the corresponding week day.
Example:
Old configuration:
Weekday schedule configured to be active from 9:00 to 10:00
Exception day schedule configured to be active from 10:00 to 11:00
Result: activity from 10:00 to 11:00
Same behavior is valid for holidays.

You can add holidays and exception days to a Recording Schedule or to a Task Schedule.
Recording Schedules share the same holidays and exception days.
Each standard Task Schedule has its own holidays or exception days patterns.

To add holidays and exception days to a schedule:
1. In the **Recording Schedules** or **Task Schedules** tree, select a schedule.
2. Click the **Holidays** tab.
3. Click **Add**.
   The **Add Holiday(s)** dialog box is displayed.
4. Select one or more holidays and click **OK**.
   The selected holidays are added to the Schedule Table.
5. Drag the pointer to select the appropriate time period (this is not possible for Recording Schedules).
   The selected cells are cleared and vice versa.

6. Click the **Exception Days** tab.
7. Click **Add**.
   The **Add Exception Day(s)** dialog box is displayed.
8. Select one or more special days and click **OK**.
   The selected exception days are added to the Schedule Table.
9. Drag the pointer to select the appropriate time period (this is not possible for Recording Schedules).
   The selected cells are cleared and vice versa.
   The sorting order of the added holidays and exception days is chronological.

Notes:

– You can mark a time period on a holiday or exception day of a Recording Schedule with the color of another Recording Schedule.

See also

– *Recording Schedules page, page 269*
– *Task Schedules page, page 270*

18.7 Removing holidays and exception days

Main window > **Schedules**

You can remove holidays and exception days from a Recording Schedule or a Task Schedule.

To remove holidays and exception days from a Task Schedule:

1. In the **Recording Schedules** or **Task Schedules** tree, select a schedule.
2. Click the **Holidays** tab.
3. Click **Delete**.
   The **Select the holidays to delete** dialog box is displayed.
4. Select one or more holidays and click **OK**.
   The selected holidays are removed from the Schedule Table.
5. Click the **Exception Days** tab.
6. Click **Delete**.
   The **Select the exception days to delete.** dialog box is displayed.
7. Select one or more exception days and click **OK**.
   The selected exception days are removed from the Schedule Table.

See also

– *Recording Schedules page, page 269*
– *Task Schedules page, page 270*

18.8 Renaming a schedule

Main window >

To rename a schedule:

1. In the **Recording Schedules** or **Task Schedules** tree, select an item.
2. Click .
3. Enter the new name and press ENTER. The entry is renamed.

See also

- *Recording Schedules page, page 269*
- *Task Schedules page, page 270*

19 Cameras and Recording page

Main window > **Cameras and Recording**

Displays the Camera Table page or a Recording Table page.

Allows you to configure camera properties and recording settings.

Allows you to filter the cameras that are displayed according to their type.

Icons

	Click to copy recording settings from one Recording Schedule to another.
	Click to display the **Stream Quality Settings** dialog box.
	Click to display the **Scheduled Recording Settings** dialog box.
	Click to display the dialog box for configuring a selected PTZ camera.
	Displays all available cameras regardless of their storage device.
	Click to change the Camera Table according to the selected storage device.
	Displays the corresponding Camera Table. No recording settings are available because these cameras are not recorded in BVMS.

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

To cancel filtering, click .

19.1 Cameras page

Main window > **Cameras and Recording** > Click an icon to change the Cameras page according to the desired storage device, for example

Displays various information on the cameras available in your BVMS.

Allows you to change the following camera properties:

- Camera name
- Assignment of an audio source
- Logical number
- PTZ control, if available

- Live quality (VRM and Live / Local Storage)
- Recording settings profile
- Minimum and maximum storage time
- Region of Interest (ROI)
- Automated Network Replenishment
- Dual Recording

▸ Click a column title to sort the table by this column.

Camera - Encoder
Displays the device type.

Camera - Camera
Displays the name of the camera.

Camera - Network Address
Displays the IP address of the camera.

Camera - Location
Displays the location of the camera. If the camera is not assigned to a Logical Tree yet, **Unassigned Location** is displayed.

Camera - Device Family
Displays the name of the device family to which the selected camera belongs.

Camera - Number
Click a cell to edit the logical number that the camera received automatically when it was detected. If you enter an already used number, a corresponding error message is displayed. The logical number is "free" again when the camera is removed.

Audio
Click a cell to assign an audio source to the camera.
If an alarm occurs with low priority and with a camera that has audio configured, this audio signal is played even when an alarm with higher priority is currently being displayed. But this is only true, if the high priority alarm has no audio configured.

Stream 1 - Codec / Stream 2 - Codec (only VRM and Local Storage)
Click a cell to select the desired codec for encoding the stream.

Stream 1 - Quality / Stream 2 - Quality
Select the desired quality of the stream used for live or recording. You configure quality settings in the **Stream Quality Settings** dialog box.

Stream 1 - Active platform / Stream 2 - Active platform
Shows the name of the platform settings within the **Stream Quality Settings** dialog box. This column is read only and indicates which profile settings will be written to the encoder.

Notice!
Applicable only if the stream quality profiles quiet, standard or busy are selected:
The value **Active platform** changes if you change the codec of the selected camera. The target bit rate is adjusted automatically and the name of the platform settings is displayed.

Live Video - Stream (only VRM and Live Only and Local Storage)
Click a cell to select the stream for a VRM or a local storage / live only encoder.

Live Video - Profile (only available for ONVIF cameras)
Click a cell to browse for the available live profile tokens of this ONVIF camera.
If you select the **<Automatic>** entry, the stream with the highest quality is automatically used.

Live Video - ROI
Click to enable Region of Interest (ROI). This is only possible if in the **Quality** column the H.264 MP SD ROI or H.265 MP SD ROI item is selected for stream 2 and stream 2 is assigned to Live Video.
Note: If stream 1 is used for Live for a specific workstation then the Operator Client running on this workstation cannot enable ROI for this camera.

is automatically enabled in the table.

Recording - Setting
Click a cell to select the required recording setting. You configure the available recording settings in the **Scheduled Recording Settings** dialog box.

Recording - Profile (only available for ONVIF cameras)
Click a cell to browse for the available recording profile tokens of this ONVIF camera. Select the desired entry.

Recording - ANR
Select a check box to enable the ANR function. You can only enable this function, if the encoder has an appropriate firmware version and an appropriate device type.

Recording - Max Pre-Alarm Duration
Displays the calculated maximum pre-alarm duration for this camera. This value can help you in calculating the required storage capacity of the local storage medium.

Notice!
If a Mirrored VRM is already configured for an encoder, you cannot change any settings for this encoder in the **Secondary Recording** columns.

Secondary Recording - Setting (only available if a Secondary VRM is configured)
Click a cell to assign a scheduled recording setting to the dual recording of this encoder. Depending on your configuration it can happen that the configured stream quality for secondary recording is not valid. The stream quality configured for primary recording is then used instead.

Secondary Recording - Profile (only available for ONVIF cameras)
Click a cell to browse for available recording profile tokens of this ONVIF camera.

(Only visible when you click **All**)
Select a check box to activate PTZ control.

Note:
For port settings refer to COM1.

Port (Only visible when you click **All**)
Click a cell to specify which encoder serial port is used for PTZ control. For a PTZ camera connected to a Bosch Allegiant system, you can select **Allegiant**. For such a camera you do not need to use a trunk line.

Protocol (Only visible when you click **All**)
Click a cell to select the appropriate protocol for the PTZ control.

PTZ Address (Only visible when you click **All**)
Type the address number for the PTZ control.

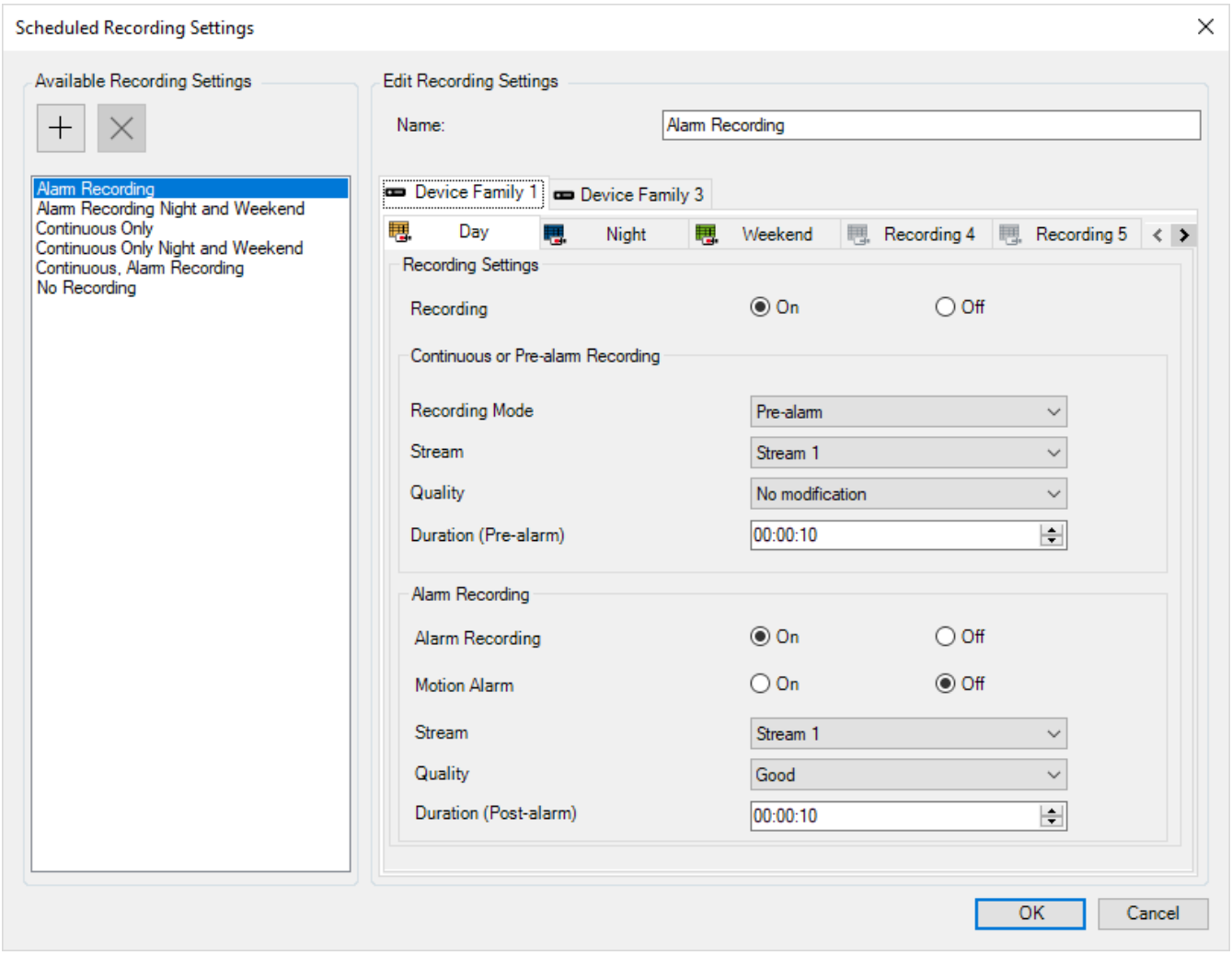
Recording - Storage Min Time [days]
Secondary Recording - Storage Min Time [days] (only VRM and Local Storage)
Click a cell to edit the minimum number of days that video data from this camera is retained. Recordings younger than this number of days are not deleted automatically.

Recording - Storage Max Time [days]
Secondary Recording - Storage Max Time [days] (only VRM and Local Storage)
Click a cell to edit the maximum number of days that video data from this camera is retained. Only recordings older than this number of days are deleted automatically. 0 = unlimited.

See also
- *Configuring dual recording in the Camera Table, page 294*
- *Configuring PTZ camera settings, page 291*
- *Configuring PTZ port settings, page 291*
- *Configuring stream quality settings, page 288*
- *Copying and pasting in tables, page 287*
- *Configuring the ANR function, page 293*
- *Exporting the Camera Table, page 288*
- *Assigning an ONVIF profile, page 294*
- *Configuring the ROI function, page 292*

19.2 Scheduled Recording Settings dialog box (only VRM and Local Storage)

Main window > **Cameras and Recording** >
Allows you to configure schedule-dependent recording settings for each available device family. A device family is available when at least one encoder of this device family has been added to the Device Tree. In the **Cameras** table, you assign such a recording setting to each camera.
You use the Recording Schedules configured on the **Schedules** page.
Note: Switching on or off the normal recording is valid for all device families.



Available Recording Settings

Select a pre-defined recording setting to change its properties. You can add or delete a user-defined setting.

Name:

Type in a name for the new recording setting.

Select the desired device family to configure the recording settings valid for this device family.

For the selected device family, select a Recording Schedule to configure the recording settings.

Recording

Switch on or off the normal recording (continuous and prealarm).

Recording Mode

Select the desired recording mode.

The following items are available:

- **Continuous**
- **Pre-alarm**

Stream

Select the desired stream used for normal recording.

Note: It depends on the device family which streams are available.

Quality
Select the desired stream quality used for normal recording. The available quality settings are configured in the **Stream Quality Settings** dialog box.

Duration (pre-alarm)
Enter the desired recording time before an alarm. You enter the time in the format hh.mm.ss.
Note: Only enabled when **Pre-alarm** is selected.

Notice!
For pre-alarm settings between 1 and 10 s, the pre-alarms are automatically stored on the RAM of the encoder if enough RAM space is available, otherwise on the storage.
For pre-alarm settings greater than 10 s, pre-alarms are stored on the storage.
The storage of pre-alarms on the RAM of the encoder is only available for firmware version 5.0 or later.

Alarm Recording
Allows you to switch on or off the alarm recording for this camera.

Motion Alarm
Allows you to switch on or off alarm recording triggered by motion.

Stream
Select the stream used for alarm recording.
Note: It depends on the device family which streams are available.

Quality
Select the desired stream quality used for alarm recording. The available quality settings are configured in the **Stream Quality Settings** dialog box.
Only for devices belonging to Device Family 2 or 3: When you select the **No modification** entry, alarm recording uses the same quality as used for continuous/prealarm recording. We recommend using the **No modification** entry. When you select a stream quality for alarm recording, only the values for image encoding interval and target bit rate are modified according to the settings in this stream quality. The other quality settings are used that are configured in the quality setting assigned to the continuous/prealarm recording.

Duration (post-alarm)
Enter the desired alarm recording time. You enter the time in the format hh.mm.ss.

See also
- *Copying and pasting in tables, page 287*
- *Configuring recording settings (only VRM and Local Storage), page 289*

19.3 Recording settings pages (NVR only)

Main window > **Cameras and Recording** > > Click a Recording Schedule tab (for example)

Allows you to configure the recording settings for all encoders assigned to your system's NVR.
The displayed Recording Schedules are configured in **Schedules**.
Only those columns are described that are not part of a Camera Table.

- Click a column title to sort the table by this column.

Continuous Recording
In the **Quality** column, click a cell to disable recording or to select the stream quality of stream 1.
In the column, select a check box to activate audio.

Live/Pre-event Recording
In the **Quality** column, click a cell to select the stream quality of the live view (required for instant playback) and the pre-event recording (required for motion and alarm recording) mode of stream 2. If dual streaming is active on this encoder, you can select stream 1 to use for live or pre-event recording.
In the column, select a check box to activate audio.

Motion Recording
In the **Quality** column, click a cell to disable recording or to select the stream quality of stream 1.
In the column, click a cell to activate audio.
In the **Pre-event [s]** column, click a cell to select the recording time before the motion event in seconds.
In the **Post-event [s]** column, click a cell to select the recording time after the motion event in seconds.

Alarm Recording
In the **Quality** column, click a cell to select the stream quality of stream 1.
To enable alarm recording, configure a corresponding alarm.
In the column, select a check box to activate audio.
In the **Pre-event [s]** column, click a cell to select the time before the alarm in seconds.
In the **Post-event [s]** column, click a cell to select the time after the alarm in seconds.

See also
- *Copying and pasting in tables, page 287*
- *Configuring recording settings (NVR only), page 290*
- *Copying recording settings (NVR only), page 293*

19.4 Copy Recording Settings dialog box (NVR only)

Main window > **Cameras and Recording** > Click an icon for recording device, for example > Click a Recording Schedule tab (for example) >
Allows you to copy recording settings from one Recording Schedule to another.

Copy all
Click to copy all recording settings of the selected schedule to another schedule.

Copy current selection
Click to copy only the recording settings of the selected table rows to another schedule.

See also
- *Copying recording settings (NVR only), page 293*

19.5 Stream Quality Settings dialog box

Main window > **Cameras and Recording** >

Allows you to configure stream quality profiles that you can later assign on the **Cameras and Recording** page to cameras or in the **Scheduled Recording Settings** dialog box.
A stream quality combines video resolution, frame rate, maximum bandwidth, and video compression.

Stream Qualities

Select a predefined stream quality and click to add a new stream quality on the basis of the predefined stream quality. When you select a single stream and click , this stream quality setting is copied as a childless top level node.

Click to delete a selected stream quality. You cannot delete the stream quality settings.
The list displays all available predefined stream quality settings. We recommend assigning a stream quality with the same name as the platform of the camera.
The following profiles for stream qualities are available:
Image optimized: The settings are optimized for image quality. This can burden the network.
Bit rate optimized: The settings are optimized for low bandwidth. This can reduce the image quality.
Balanced: The settings offer a compromise between optimal image quality and optimal bandwidth usage.

The following profiles for stream qualities are available since BVMS 9.0 to support the Intelligent Streaming feature of Bosch cameras:
Cloud optimized 1/8 FR: The settings are optimized for low bandwidth and identically for all camera types.
PTZ optimized: The settings are optimized for PTZ cameras.
Image optimized quiet / standard / busy
Bit rate optimized quiet / standard / busy
Balanced quiet / standard / busy

Scene type categories:
quiet: The settings are optimized for images with low activity. 89% static scene, 10% normal scene, 1 % busy scene.
standard: The settings are optimized for images with medium activity. 54% static scene, 35% normal scene, 11 % busy scene.
busy: The settings are optimized for images with high activity. 30% static scene, 55% busy scene, 15% crowded scene.
The percentage values are related to a distribution during a day.

By default the Balanced standard profile is assigned.

Notice!
For each combination of camera platform (CPP3-CPP7.3) and for each of the available resolutions a specific setting exists to be able to set the correct bit rates for the cameras. The profile has to be selected manually with the corresponding scene type for each camera.

Notice!
If doing an update installation the new profiles have to be selected manually to become active. The old profiles remain.

Name
Displays the name of the stream quality. When you add a new stream quality, you can change the name.

SD video resolution
Select the desired video resolution. For an HD quality you configure the SD quality of stream 2.

Image encoding interval
Move the slider or type the appropriate value.
The system helps you in calculating the corresponding value for IPS.
With the image encoding interval you configure the interval at which images are encoded and transmitted. If 1 is entered, all images are encoded. Entering 4 means that only every fourth image is encoded, the following three images are skipped - this can be particularly advantageous with low bandwidths. The lower the bandwidth the higher this value should be to achieve best-quality video.

GOP structure
Select the structure you require for the Group-of-Pictures (GOP). Depending on whether you place higher priority on having the lowest possible delay (IP frames only) or using as little bandwidth as possible, you choose IP, IBP or IBBP. (GOP selection is not available on some cameras.)

Note:
B-frames are only supported by cameras up to a resolution of 1080 p and from firmware 6.40.

Target bit rate [Kbps]
Move the slider or type the appropriate value.
You can limit the data rate for the encoder to optimize usage of bandwidth in your network. The target data rate should be set according to the desired picture quality for typical scenes with no excessive motion.
For complex images or frequent changes of image content due to frequent movements, this limit can be temporarily exceeded up to the value you enter in the **Maximum bit rate [Kbps]** field.

Maximum bit rate [Kbps]
Move the slider or type the appropriate value.
With the maximum bit rate you configure the maximum transmission speed which cannot be exceeded.
You set a bit rate limit to be able to reliably determine the appropriate disk space for storage of the video data.
Depending on the video quality settings for the I- and P-Frames, this fact can result in individual images being skipped.
The value entered here must be at least 10% higher than the value entered in the **Target bit rate [Kbps]** field. If the value entered here is too low, it will automatically be adjusted.

I-frame Distance
This parameter allows you to set the intervals in which the I-Frames are coded. Click **Automatic** to insert I-Frames as necessary. An entry of 1 indicates that I-Frames are continuously generated. An entry of 2 indicates that only every second image is an I-Frame, and 3 only every third image etc. The I-Frames in between are coded as P-Frames.

Frame Quality Level
Here you can set a value between 0 and 100 for both the I-Frames and the P-Frames. The lowest value results in the highest quality and the lowest frame refresh rate. The highest value results in the highest frame refresh rate and the lowest image quality.
The lower the available transmission bandwidth, the higher adjust the quality level to maintain high quality of the video.

Note:
You adjust the video quality dependent on the motion and level of detail in the video. If you check the **Automatic** check boxes, the optimum relationship between motion and image definition is automatically adjusted.

VIP X1600 XFM4 Settings
Allows you to configure the following H.264 settings for the VIP X 1600 XFM4 encoder module.
H.264 deblocking filter: Select to improve visual quality and prediction performance by smoothing the sharp edges.
CABAC: Select to activate high efficient compression. Uses a large amount of processing power.

See also
– *Configuring stream quality settings, page 288*

19.6 PTZ/ROI Settings dialog box

Main window > **Cameras and Recording** > > Select a PTZ camera >
Allows you to configure a PTZ camera or a ROI camera.
For a ROI camera no auxiliary commands are available.

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

Icons

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

Predefined Positions tab
Click to display the table with the predefined positions.

Nr
Displays the number of the predefined position.

Name
Click a cell to edit the name of the predefined position.

Aux Commands tab (only for PTZ cameras)
Click to display the table with the auxiliary commands.
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.

See also
- *Configuring PTZ port settings, page 291*
- *Configuring PTZ camera settings, page 291*

20 Configuring cameras and recording settings

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.

See also

– *Cameras page, page 276*
– *Scheduled Recording Settings dialog box (only VRM and Local Storage), page 279*
– *Stream Quality Settings dialog box, page 283*
– *PTZ/ROI Settings dialog box, page 285*
– *Copy Recording Settings dialog box (NVR only), page 282*

20.1 Copying and pasting in tables

You can configure many objects simultaneously within a Camera Table, an Event Configuration Table, or an Alarm Configuration Table.

You can copy the configurable values of a table row in other rows:

– Copy all values of a row to other rows.
– Copy only one value of a row to another row.
– Copy the value of one cell to a complete column.

You can copy the values in two different ways:

– Copy into the clipboard and then paste.
– Direct copy and paste.

You can determine in which rows to paste:

– Copy in all rows.
– Copy in selected rows.

To copy and paste all configurable values of a row into another row:

1. Right-click the row with the desired values and click **Copy Row**.
2. Click the row heading of the row that you want to modify.
   To select more than one row press the CTRL key and point to the other row headings.
3. Right-click the table and click **Paste**.
   The values are copied.

To copy and paste one value of a row into another row:

1. Right-click the row with the desired values and click **Copy Row**.
2. Right-click the cell that you want to modify, point to **Paste Cell to**, and click **Current Cell**.
   The value is copied.

To copy all configurable values directly:

1. Click the row heading of the row that you want to modify.
   To select more than one row press the CTRL key and point to the other row headings.

2. Right-click the row with the desired values, point to **Copy Row to**, and click **Selected Rows**.
   The values are copied.

To copy one value directly:

1. Click the row heading of the row that you want to modify.
   To select more than one row press the CTRL key and point to the other row headings.
2. Right-click the cell with the desired value, point to **Copy Cell to**, and click **Selection in Column** .
   The value is copied.

To copy a value of a cell to all other cells in this column:

- Right-click the cell with the desired value, point to **Copy Cell to**, and click **Complete Column**.
  The value is copied.

To duplicate a row:

- Right-click the row and click **Add Duplicated Row**.
  The row is added below with a new name.

See also

- *Cameras page, page 276*
- *Scheduled Recording Settings dialog box (only VRM and Local Storage), page 279*
- *Events page, page 295*
- *Alarms page, page 300*

20.2 Exporting the Camera Table

Main window > **Cameras and Recording**
Or
Main window > **Cameras and Recording** > Click an icon to change the Cameras page according to the desired storage device, for example
Displays various information on the cameras available in your BVMS.
You can export the Camera Table into a CSV file.

To export:

1. Right-click anywhere in the Camera Table and click **Export table...**.
2. In the dialog box, type in an appropriate filename.
3. Click **Save**.
   The selected Camera Table is exported in a csv file.

20.3 Configuring stream quality settings

To add a stream quality settings entry:

1. Click to add a new entry in the list.
2. Type in a name.

To remove a stream quality settings entry:

- Select an entry in the list and click to delete the entry.
  You cannot delete default entries.

To rename a stream quality settings entry:

1. Select an entry in the list.
2. Enter the new name in the **Name** field.
   You cannot rename default entries.
3. Click **OK**.

To configure stream quality settings:

1. Select an entry in the list.
2. Make the appropriate settings.

20.4 Configuring camera properties

Main window > **Cameras and Recording** >

To change camera properties:

1. In the **Camera** column, click a cell and type a new name for the camera.
   This name is displayed in all other places where cameras are listed.
2. Make the appropriate settings in the other columns.

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

See also

– *Cameras page, page 276*

20.5 Configuring recording settings (only VRM and Local Storage)

Main window > **Cameras and Recording** >

You can configure the recording settings of all devices that are added to the VRM Devices item in the Device Tree.

Note: For recording, ensure that the corresponding VRM or local storage is properly configured.

VRM: **Devices** > Expand >

Local Storage: **Devices** > Expand >

To add a recording settings entry:

1. Click to add a new entry in the list.
2. Type in a name.

To remove a recording settings entry:

- Select an entry in the list and click to delete the entry.
  You cannot delete default entries.

To rename a recording settings entry:

1. Select an entry in the list.

2. Enter the new name in the **Name:** field.
   You cannot rename default entries.
3. Click **OK**.

To configure recording settings:

1. Select an entry in the list.
2. Make the appropriate settings and click **OK**.
3. Click or .
4. In the **Recording** column, select the desired recording setting for each encoder.

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

See also

– *Scheduled Recording Settings dialog box (only VRM and Local Storage), page 279*

20.6 Configuring recording settings (NVR only)

Main window > **Cameras and Recording** > Click > Click a Recording Schedule tab (for example)

Before you configure the recording settings, configure the stream quality levels.

Note: For recording, ensure that the corresponding NVR is configured properly (**Devices** > Expand > > **Disk Storage** tab).

Notice!

For all encoders, live view settings are also used for pre-event recording.

For encoders that support dual-streaming, the settings for live/pre-event recording, motion recording, and alarm recording are all configured independently.

For encoders that support only a single stream (e.g., the VideoJet 8004), live viewing and recording use the same stream. In this case, the recording settings take priority, so the live view uses the stream quality settings for continuous, motion, and alarm recording. You can enter a setting for live/pre-event only if continuous recording is disabled.

You can switch the live stream from stream 2 (default) to stream 1 for a workstation (**Devices** > Expand > > **Settings** tab > **Override settings from "Cameras and Recording" page**) or for an encoder. This setting does not affect pre-event recording.

To configure recording settings:

1. In the column of **Continuous Recording**, select the desired stream quality or disable continuous recording.
2. In the column, select a check box to activate audio.
3. In the column of **Live/Pre-event Recording**, select the desired stream quality or select stream 1.
4. In the column, select a check box to activate audio.

5. In the column of **Motion Recording**, select the desired stream quality or disable motion recording.
6. In the column, select a check box to activate audio.
7. In the **Pre-event [s]** column, click a cell and type the appropriate time.
8. In the **Post-event [s]** column, click a cell and type the appropriate time.
9. In the column of **Alarm Recording**, select the desired stream quality or disable alarm recording.
10. In the column, select a check box to activate audio.
11. In the **Pre-event [s]** column, click a cell and type the appropriate time.
12. In the **Post-event [s]** column, click a cell and type the appropriate time.

Notice!
If pre-event time for motion recording and pre-event time for alarm recording differ, the higher value is used for both.
If the configured pre-event time would overlap a preceding alarm or motion recording, the pre-event recording starts after the preceding recording is finished.

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

See also
– *Cameras page, page 276*

20.7 Configuring PTZ port settings

Main window > **Devices** > Expand > Expand > > **Interfaces** tab > **Periphery** tab

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.

20.8 Configuring PTZ camera settings

Main window > **Cameras and Recording** >

First configure the port settings of your PTZ camera before you can configure the PTZ camera settings. Otherwise the PTZ control is not working in this dialog box.
You can remove menu items of the context menu displayed on a PTZ camera hotspot on a map.

To configure the control of a camera:

1. In the Camera Table, select the required encoder.
2. To activate the control of a camera: In the column, select the check box.
3. Click the button.
   The dialog box for configuring PTZ settings is displayed.
4. Remove the prepositions that you do not want to be displayed as context menu items on a map.
5. Make the appropriate settings.
6. Click **OK**.

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

See also

- *PTZ/ROI Settings dialog box, page 285*
- *Configuring PTZ port settings, page 291*

20.9 Configuring the ROI function

Main window > **Cameras and Recording** >

You can enable the ROI function for a fixed HD camera.
You must configure stream 2 for live video and you must configure the H.264 MP SD ROI or H.265 MP SD ROI codec for stream 2.
Ensure that stream 2 is used for live video on each workstation where ROI is to be used.

To enable ROI:

1. In the **Stream 2** - **Codec** column, select the H.264 MP SD ROI or H.265 MP SD ROI codec.
2. In the **Live Video** - **Stream** column, select **Stream 2**.
3. In the **Live Video** - **ROI** column, click to select the check box.

To disable ROI:

1. In the **Live Video** - **ROI** column, click to disable the check box.
2. In the **Stream 2** - **Codec** column, select the desired codec.

See also

- *Cameras page, page 276*

20.10 Configuring predefined positions for the ROI function

Main window > **Cameras and Recording** >

You can configure the predefined positions for using ROI like for a PTZ camera. You cannot configure Aux commands for ROI.

To configure:

1. In the Camera Table, select the desired camera for which ROI is enabled.
2. Click .
   The **PTZ/ROI Settings** dialog box is displayed.
3. In the **Predefined Positions** tab, define predefined positions as required.
4. Click **OK**.

See also

– *PTZ/ROI Settings dialog box, page 285*

20.11 Copying recording settings (NVR only)

Main window > **Cameras and Recording** > Click an icon for recording device (for example) > Click a Recording Schedule tab (for example)

You can copy recording settings from one Recording Schedule to another.

To copy the recording settings of a selected table row:

1. Select a table row you with the desired recording settings.
2. Click . The **Copy Recording Settings** dialog box is displayed.
3. In the list, select a Recording Schedule where you want the settings to copy to.
4. Click **Copy current selection**.
5. Click **OK**. The recording settings of the selected table row are copied.

To copy all recording settings of a Recording Schedule:

1. Click . The **Copy Recording Settings** dialog box is displayed.
2. In the list, select a Recording Schedule where you want the settings to copy to.
3. Click **Copy all**.
4. Click **OK**. The recording settings of all table rows are copied.

See also

– *Copy Recording Settings dialog box (NVR only), page 282*

20.12 Configuring the ANR function

Main window > **Cameras and Recording** >

Before you enable the ANR function, you must add the storage media of an encoder to the desired encoder and configure this storage media.

You must disable dual recording for the encoder to configure ANR.

The ANR function only works on encoders with firmware version 5.90 or later. Not all encoder types support ANR even if the correct firmware version is installed.

To enable:

- In the row of the desired camera, in the **ANR** column, select the checkbox.

See also

– *Configuring dual recording in the Camera Table, page 294*

– *Cameras page, page 276*

– *Configuring the storage media of an encoder, page 226*

20.13 Configuring dual recording in the Camera Table

Main window > **Cameras and Recording** >

You must disable the ANR function to configure dual recording.

If you configure dual recording for one camera of a multi-channel encoder, the system ensures that the same recording target is configured for all cameras of this encoder.

To configure:

1. In the **Secondary Recording** - **Target** column, click a cell of the desired encoder and then click the desired pool of a Secondary VRM.
   Automatically all cameras of the affected encoder are configured to be recorded to the selected Secondary VRM.
2. In the **Setting** column, select a scheduled recording setting.

See also

– *Configuring dual recording in the Device Tree, page 191*
– *Configuring the ANR function, page 293*
– *Dual / failover recording, page 32*
– *Cameras page, page 276*

20.14 Managing Video Streaming Gateway

See also

– *Video Streaming Gateway device page, page 202*
– *Add Bosch Encoder dialog box, page 205*
– *Add ONVIF Encoder dialog box, page 206*
– *Add JPEG Camera dialog box, page 207*
– *Add RTSP Encoder dialog box, page 208*

20.14.1 Assigning an ONVIF profile

Main window > **Cameras and Recording** >

You can assign an ONVIF Media Profile token to an ONVIF camera.

You can assign either for live video or for recording.

To assign a live video token:

▸ In the **Live Video** - **Profile** column, select the desired entry.

To assign a recording token:

▸ In the **Recording** - **Profile** column, select the desired entry.

See also

– *Cameras page, page 276*

21 Events page

Main window > **Events**

Displays the Event Tree with all available events and an Event Configuration Table for each event. The events are grouped by their type, for example, all camera recording events like continuous recording or alarm recording are grouped under Recording Mode.

The available events are grouped beyond their corresponding devices. A state change of a device is displayed beyond as . All other events are displayed under device dependant groups as .

You can configure for each event:

– Trigger an alarm according to a schedule (not available for all events).
– Log the event according to a schedule. An event is displayed in the Event List of the Operator Client if it is logged.
– Execute a Command Script according to a schedule (not available for all events).
– For events of type : Adding text data to recording.

If the event occurs, your settings are executed.

You can create a Compound Event which combines several events with Boolean expressions.

▸ Click a tree item to display the corresponding Event Configuration Table.

Click to duplicate an event. Use it to generate multiple alarms for a certain event.

Click to delete a duplicated or a Compound Event.

Click to rename the selected Compound Event.

Click to display a dialog box for creating Compound Events using Boolean expressions of other events (maximum 10).

Compound Events are added to the Event Configuration Table.

Click to edit the selected Compound Event.

Click to display a dialog box for creating and editing Command Scripts.

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 .

See also

– *Configuring events and alarms, page 307*
– *Configuring Command Scripts, page 100*
– *Options dialog box (Settings menu), page 122*

– *Configuring blinking hotspots, page 315*

21.1 Debounce Settings tab

Note: For some events the Debounce Settings tab is not available due to technical limitations.
Allows you to configure debounce settings for the selected event.

Debounce time
During the entered time period all further events are ignored.

Event state priority
For an event state you can assign a priority setting.

Edit Priorities
Click to display a dialog box for configuring a priority setting.

Add Setting
Click to add a row for configuring a debounce setting that is deviating from the debounce settings for all devices.

Remove Setting
Click to remove a selected row. To select a row click the left row header.

21.2 Settings tab for advanced map display

The configuration of the color states on maps is only possible when you click to check the **Enable advanced state display (hot spot coloring in maps depending on state)** option or the **Enable advanced alarm display (hotspot coloring in maps depending on alarm)** option in the **Options** dialog box.

For each event or alarm, you can configure the background color and the behavior (blinking or not blinking) for hotspots. For example you can configure for a event or alarm of a device that its device icon on a map starts blinking when the state of this device changes.
Additionally you can configure the display priority for all hotspots. This is required when different events occur for the same device. (1 = highest priority)
The configured color is valid for all hotspots with the same display priority. You can change color, behavior and priority at any event or alarm: The changed color and behavior is used for all hotspots of all other events or alarms which have the same priority.

Enable color states on maps
Click to enable that the hotspots of the devices belonging to this event are displayed with colored background and can blink on maps.

Display priority on map:
Click the arrows to change the priority for the hotspots of the devices belonging to this event.

Background color on map:
Click the color field to select the background color used for the hotspots of the devices belonging to this event.
Note: All state events of all devices with the same priority have the same color.

Blinking
Click to enable blinking of the hotspots of the devices belonging to this event.

21.3 Settings tab for event configuration

Device
Displays the name of the device or schedule.

Network
Displays the IP address of the corresponding IP device.

Trigger Alarm
Click a cell to select a Recording or Task Schedule for triggering an alarm.
Select **Always** if you want the alarm to be triggered independently from the point in time.
Select **Never** if you do not want the alarm to be triggered.

Log
In the **Schedule** column, click a cell to select a Recording or Task Schedule for logging.
Select **Always** if you want the event to be logged independently from the point in time.
Select **Never** if you do not want the event to be logged.

Script
In the **Script** column, click a cell to select a Command Script.
In the **Schedule** column, click a cell to select a Recording or Task Schedule for executing a Command Script.
Select **Always** if you want the Command Script to be executed independently from the point in time.
Select **Never** if you do not want the Command Script to be executed.

Text Data Recording
You can configure that text data is added to the continuous recording of a camera.
Note: This column is available only for events that contain text data, for example: **ATM/POS Devices** > **ATM Input** > **Data Input**

21.4 Command Script Editor dialog box

Main window > **Events** >
Allows you to create and edit Command Scripts.

Click to save the changed settings.

Click to restore the saved settings.

Click to check the code of a script.

Click to create a scriptlet file.

Click to delete a scriptlet file.

Click to display a dialog box for importing a script file.

Click to display a dialog box for exporting a script file.

Click to convert an existing script to the other available script language. All existing script text is deleted.

Click to display the Online Help for BVMS Script API.

Click to display the Online Help for BVMS.

Click to close the **Command Script Editor** dialog box.

See also

– *Configuring Command Scripts, page 100*

21.5 Create Compound Event / Edit Compound Event dialog box

Main window > **Events** >

Allows you to create or modify a Compound Event.

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 .

Event name:

Type the required name for the Compound Event.

Event States:

Select the state change that shall be part of a Compound Event.

Objects:

Select one or more of the available objects of the selected event state. This state and the selected object appear in the Compound Event Tree, as immediate child of the root operator.

Compound Event:

Allows you to build compound events in the Compound Event Tree. All immediate children of a Boolean operator (AND, OR) are combined by this operator.

See also

– *Creating a Compound Event, page 310*
– *Editing a Compound Event, page 311*

21.6 Select Script Language dialog box

Main window > **Events** >

Allows you to set the script language for your Command Scripts.

You cannot change the script language for existing Command Scripts.

Script Language:

Select the required script language.

See also

– *Configuring Command Scripts, page 100*

21.7 Edit Priorities of Event Type dialog box

Main window > **Events** > **Debounce Settings** tab > **Edit Priorities** button

You can configure priorities for the different state changes of an event type if applicable, for example Virtual Input Closed and Virtual Input Opened. A state change with higher priority overrides the debounce time of another state change with lower priority.

Name of Priority:

Type in a name for the priority setting.

State Value

Displays the names of the event states of the select event.

State Priority

Enter the desired priority. 1=highest priority, 10=lowest priority.

21.8 Select Devices dialog box

Main window > **Events** > or > **Debouce Settings** tab > **Add Setting** button

Select

Select the check box for the desired entry and click **OK** to add a row in the **Devices with Deviating Debounce Settings** table.

21.9 Text Data Recording dialog box

Main window > **Events** > In the Event Tree select **Data Input** (text data must be available, for example: **Foyer Card Reader Devices** > **Foyer Card Reader** > **Card Rejected**) > **Text Data Recording** column > ...

You can configure the cameras for which text data is added to the continuous recording.

See also

– *Triggering alarm recording with text data, page 313*

22 Alarms page

Main window > **Alarms**

Displays the Event Tree and an Alarm Configuration Table for each event. Only the events configured on the **Events** page are displayed.

In the tables you configure for each event how an alarm triggered by this event is displayed and which cameras are recorded and displayed when this alarm occurs.

Some events are configured as alarms by default, e.g., a system error.

For the following events you cannot configure an alarm:

- Change of a recording mode
- Change of an alarm state
- Most of the user actions, e.g. PTZ action

Click to display the **Resource Manager** dialog box.

Displays a dialog box to set alarm settings valid for this Management Server.

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 Alarm Configuration Table.

Device

Displays the device of the event condition selected in the Events Tree.

Network Address

Displays the IP address of the corresponding IP device.

Device

In the **Priority** column, click in a cell to type the alarm priority for the selected alarm (**100** is low priority, **1** is high priority). In the **Title** column, click in a cell to type the title of the alarm to be displayed in BVMS, for example in the Alarm List. In the **Color** column, click in a cell to display a dialog box for selecting a color for the alarm to be displayed in the Operator Client, for example in the Alarm List.

Alarm Identity

In one of the **1-5** columns, click ... in a cell to display a dialog box for selecting a camera.

You can only select a camera that was added to the Logical Tree in **Maps and Structure**.

You can configure the number of available Alarm Image panes in the **Alarm Settings** dialog box.

In the **Audio File** column, click ... in a cell to display a dialog box for selecting an audio file that is played in case of an alarm.

Alarm Options

Click ... in a cell to display the **Alarm Options** dialog box.

See also

- *Alarm handling, page 43*

22.1 Alarm Settings dialog box

Main window > **Alarms** >

Alarm Settings tab

Max. image panes per alarm:
Enter the maximum count of Alarm Image panes to be displayed in case of an alarm.

Auto-clear time:
Enter the number of seconds until an alarm is automatically cleared.
This only applies for alarms that are set to **Auto-clear alarm after configured time ('Alarm Settings' dialog box)** in the **Alarms** page.

Multi-row alarm display in alarm image window
Select the check box to enable the multi-row alarm mode of the alarm image window.

Notice!
For existing alarm configurations the Multi-row Alarm mode is on, for new alarm configurations the default value is off and the Single View mode is active.

Set the duration limit for state-triggered alarm recordings:
Select the check box to enable a duration limit for state-triggered alarm recordings. Enter the number of minutes for the duration of alarm recording. The alarm recording stops automatically after the defined time.
The user can enter a duration time between 1 and 1440 minutes.
When an alarm triggers a recording with a configured duration limit:

- If the alarm is retriggered before the timeout is reached, then the recording continues with the timeout restarting from 0.
- If the alarm is cancelled before the timeout is reached, then the recording continues to the configured post alarm timeout.

Monitor groups tab

Display order in case of same alarm priority
Select the desired entry for sorting alarms of the same priority according to their time stamp.

Show blank screen
Click to configure that on a monitor not being used for alarm display nothing is shown.

Continue live display
Click to configure that on a monitor not being used for alarm display live display is shown.

See also

- *Configuring settings for all alarms, page 312*

22.2 Select Image Pane Content dialog box

Main window > **Alarms** > or > **Alarm Identity** column > Click ... in one of the **1-5** columns

Allows you to select the Logical tree item that is displayed and recorded (if the item is a camera) in case of the selected alarm.

Notice!
A map displayed in an Alarm Image pane is optimized for display and contains only the initial view of the basic .dwf file.

Search Item
Enter text to find an item in the Logical Tree.

Find
Click to find the camera with the entered search text in its description.

Live
Click to determine that the live image of the camera is displayed in case of an alarm.

Instant playback
Click to determine that instant playback of the camera is displayed.
The rewind time for alarm instant playback is configured on the **Operator Features** page, see *Operator Features page, page 327*.

Pause playback
Select the check box to display the alarm instant playback camera with paused instant playback. The user can start instant playback if needed.

Loop playback
Select the check box to display the alarm instant playback camera with looped instant playback.
The duration of looped instant playback in the alarm cameo is rewind time plus the duration of the alarm state plus rewind time.

Record this camera
Select the check box to enable alarm recording for this camera in case of an alarm. If an alarm is triggered, this camera is recorded in alarm recording quality. The duration of the recording is the duration of the alarm state plus pre- and post-alarm time. This setting directly changes the setting for alarm recording in the **Alarm Options** dialog box and vice versa.

See also
- *Operator Features page, page 327*
- *Configuring an alarm, page 312*

22.3 Select Resource dialog box

Main window > **Alarms** > or > **Alarm Identity** column > **Audio File** column > Click ...
Allows you to select an audio file that is played in case of an alarm.

Play
Click to play the selected audio file.

Pause
Click to pause the selected audio file.

Stop
Click to stop the selected audio file.

Manage...
Click to display the **Resource Manager** dialog box.

See also
- *Configuring an alarm, page 312*
- *Managing resource files, page 308*

22.4 Alarm Options dialog box

Main window > **Alarms** > or > **Alarm Options** column > ...

Allows you to configure the following settings for alarms:
- Cameras that start recording in case of an alarm.
- Enabling protection for these alarm recordings.
- Enabling and configuring deviating alarm duration settings.
- Triggering PTZ commands in case of alarm.
- Notifications that are sent in case of an alarm.
- Workflow that has to be processed in case of an alarm.
- Assigning cameras that are displayed in monitor groups in case of an alarm.

Cameras tab

Nr	Displays the camera number as configured on the **Cameras and Recording** page.
Name	Displays the camera name as configured on the **Cameras and Recording** page.
Location	Displays the location as configured on the **Maps and Structure** page.
Record	Select a check box to enable alarm recording for this camera in case of an alarm. If an alarm is triggered, this camera is recorded in alarm recording quality. The duration of the recording is the duration of the alarm state plus pre- and post-alarm time. This setting directly changes the setting for alarm recording in the **Select Image Pane Content** dialog box and vice versa.
Protect Recording	Select a check box to protect the alarm recording of this camera.
Deviating Alarm Duration Settings	The check box is automatically enabled when you enable the **Record** check box and when the camera supports ANR.
Auxiliary Command	Click a cell to select an auxiliary command to be executed in case of an alarm. Entries in this list are only available for a PTZ camera.
Predefined Position	Click a cell to select a predefined position to be set in case of an alarm. Entries in this list are only available for a PTZ camera.

Notifications tab

E-mail	Select the check box to send an e-mail in case of an alarm.

Server:	Select an e-mail server.
Recipients:	Type the e-mail addresses of the recipients separated by commas (example: name@provider.com).
SMS	Select the check box to send an SMS in case of an alarm.
Device:	Select an SMS device.
Recipients:	Type the mobile numbers of the recipients.
Text:	Type the text of the notification.
Information:	Select the check box to add the corresponding information to the notification text. **Note:** For an e-mail the date of the time zone of the Management Server is used.

Workflow tab

Record only alarm	Select the check box to specify that the camera is only recorded and not being displayed in case of this alarm. This check box is only active if the **Record** check box on the **Cameras** tab is selected.
Auto-clear alarm after configured time ('Alarm Settings' dialog box)	Select the check box to specify that this alarm is automatically cleared.
Auto-clear alarm when event state changes back to normal	Select the check box to specify that this alarm is automatically cleared when the event that triggers this alarm changes its state. The alarm will not be cleared automatically if it is accepted and unaccepted.
Prevent alarm clearing while triggering state lasts	Select the check box to prevent that this alarm is deleted as long as the cause for the alarm exists.
Suppress duplicate alarms in alarm list	Select the check box to avoid alarms for the same event type and device being duplicated in the Alarm List of BVMS Operator Client. As long as an alarm is active (in alarm state **Active** or **Accepted**), no further alarms for the same event type and device are displayed in the Alarm List. **Note:** – Events are still logged in the logbook. – Please be aware that all alarm actions triggered by this alarm (for example sending an SMS, starting alarm recording etc.) are not retriggered. After the alarm has been cleared and a new alarm has been triggered for the same device and by the same event type, the new alarm appears again in the Alarm List and all alarm actions set for this alarm are triggered again.

	– This check box is preselected for person identification alarms.
Show action plan	Select the check box to enable the workflow that must be processed in case of an alarm.
Resources...	Click to display the **Resource Manager** dialog box. Select a document with a description of the corresponding workflow.
Display a comment box	Select the check box to enable displaying a comment box in case of an alarm. In this comment box the user can type comments on the alarm.
Force the operator to process the workflow	Select the check box to force the user to process the workflow. If selected, the user cannot clear the alarm until he has entered a comment on the alarm.
Execute the following Client Script when alarm is accepted:	Select a Client Command Script that is executed automatically, when the user accepts an alarm.

Monitor Group tab

1...10	In a numbered column, click a cell and select a camera from the Logical Tree. This camera will be displayed in the assigned monitor in case of an alarm
Clear Table	Click to remove all camera assignments to monitor groups.
Alarm title	Select the check box to configure that the title of the alarm is displayed on the monitors as an on-screen display.
Alarm time	Select the check box to configure that the time of the alarm is displayed on the monitors as an on-screen display.
Alarm date	Select the check box to configure that the date of the alarm is displayed on the monitors as an on-screen display.
Alarm camera name	Select the check box to configure that the name of the alarm camera is displayed on the monitors as an on-screen display
Alarm camera number	Select the check box to configure that the number of the alarm camera is displayed on the monitors as an on-screen display.
Only on 1st monitor	Select the check box to configure that the title and the time of the alarm is displayed only on the first monitor of the monitor group as an on-screen display.

Deviating Alarm Duration Settings tab

The settings on this tab are only available if ANR is enabled for this camera.

Use profile settings	Click to enable this setting. For this camera the pre-alarm and post-alarm duration settings are used that are configured in the **Scheduled Recording Settings** dialog box.
Override settings	Click to enable the following settings for pre-alarm and post-alarm duration.
Duration (pre-alarm)	Available for all events.
Duration (post-alarm)	Only available for events.

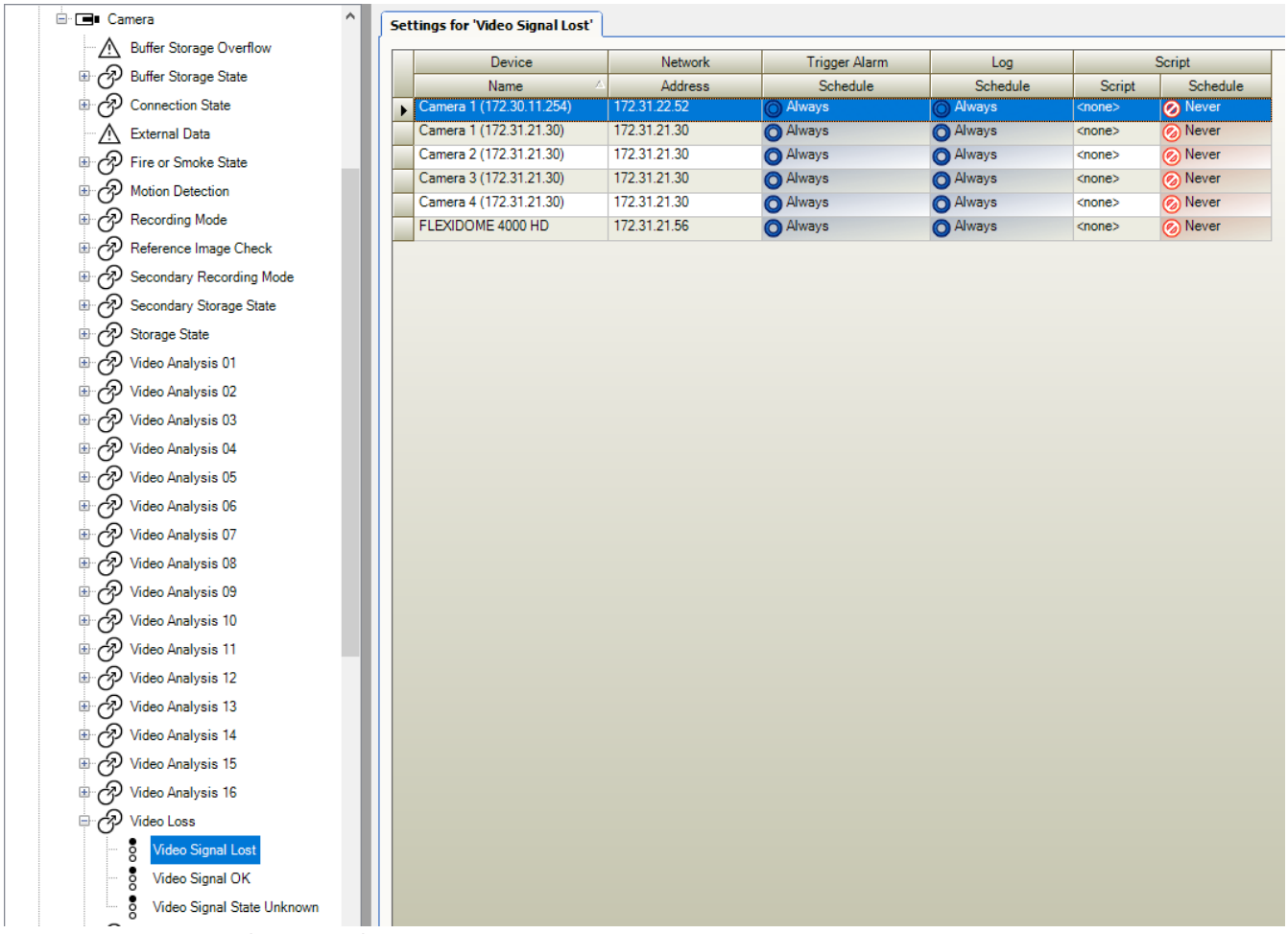
See also

- *Triggering alarm recording with text data, page 313*
- *Configuring an alarm, page 312*
- *Configuring the pre- and post-alarm duration for an alarm, page 313*

23 Configuring events and alarms

Main window > **Events**
or
Main window > **Alarms**

This chapter provides information on how to configure events and alarms in your system.
The available events are grouped beyond their corresponding devices.
In the **Events** page, you configure when an event in your BVMS triggers an alarm, executes a Command Script, and is logged.
Example (part of an Event Configuration Table):



This example means:
If the video signal of the selected camera gets lost, an alarm is triggered, the event is logged, and no script is executed.
In **Alarms**, you define how an alarm is displayed, and which cameras are displayed and recorded in case of an alarm.
Some system events are configured as alarms by default.

– Click to save the settings.

– Click to undo the last setting.

– Click to activate the configuration.

See also

– *Debounce Settings tab, page 296*
– *Settings tab for advanced map display, page 296*
– *Settings tab for event configuration, page 297*
– *Command Script Editor dialog box, page 297*
– *Create Compound Event / Edit Compound Event dialog box, page 298*
– *Select Script Language dialog box, page 298*
– *Edit Priorities of Event Type dialog box, page 299*
– *Select Devices dialog box, page 299*
– *Text Data Recording dialog box, page 299*
– *Alarm Settings dialog box, page 301*
– *Select Image Pane Content dialog box, page 301*
– *Alarm Options dialog box, page 303*

23.1 Copying and pasting in tables

You can configure many objects simultaneously within a Camera Table, an Event Configuration Table, or an Alarm Configuration Table with a few clicks.
For detailed information, see *Copying and pasting in tables, page 287*.

23.2 Removing a table row

Main window > **Alarms**

You can only remove a table row that you or another user have added, i.e. you can delete duplicated events or Compound Events.
Compound Events are located in the Event Tree under **System Devices** > **Compound Events**.

To remove a table row:

1. Select the row.
2. Click .

See also

– *Events page, page 295*

23.3 Managing resource files

For detailed information see:

– *Managing resource files, page 261*.

23.4 Configuring an event

Main window > **Events**

To configure an event:

1. In the tree, select an event or event state, for example **System Devices** > **Authentication** > **Operator Authentication Rejected**.
   The corresponding Event Configuration Table is displayed.
2. In the **Trigger Alarm** - **Schedule** column, click a cell and select the appropriate schedule.
   The schedule determines when the alarm is triggered.
   Select one of the Recording Schedules or Task Schedules that you have configured in the **Schedules** page.
3. In the **Log** - **Schedule** column, click a cell and select the appropriate schedule.
   The schedule determines when the event is logged.
4. In the **Script** - **Script** column, click a cell and select an appropriate Command Script.
5. In the **Script** - **Schedule** column, click a cell and select the appropriate schedule.
   The schedule determines when the event triggers the start of the Command Script.

See also

– *Events page, page 295*

23.5 Duplicating an event

Main window > **Events**

You can duplicate an event to trigger different alarms for a particular event.

To duplicate an event:

1. In the tree, select an event condition. The corresponding Event Configuration Table is displayed.
2. Select a table row.
3. Click . A new table row is added below. It has the default settings.

See also

– *Events page, page 295*

23.6 Logging user events

Main window > **Events** > Expand **System Devices** > **User Actions**

You can configure the logging behavior of several user actions for each available user group individually.

Example:

To log user events:

1. Select a user event to configure its logging behavior, e.g. **Operator Logon**.
   The corresponding Event Configuration Table is displayed.
   Each user group is displayed in the **Device** column.
2. If available: In the **Trigger Alarm** - **Schedule** column, click a cell and select the appropriate schedule.
   The schedule determines when the alarm that is supposed to notify the user is triggered.
   You can select one of the Recording Schedules or Task Schedules that you have configured in **Schedules**.

3. In the **Log** - **Schedule** column, click a cell and select the appropriate schedule.
   The schedule determines when the event is logged.
   In the example, the Operator logon of the Admin Group and the Power User Group are not logged whereas the Operator logon of the Live User Group are logged during **Day** schedule.

See also
– *Events page, page 295*

23.7 Configuring user event buttons

Main window > **Events**

You can configure the user event buttons available in the Operator Client. You can configure that one or more user event buttons are not displayed in the Operator Client.
On the **User groups** page, you configure that the user event buttons are only available in the Operator Client of the corresponding user group.

To configure user event buttons:

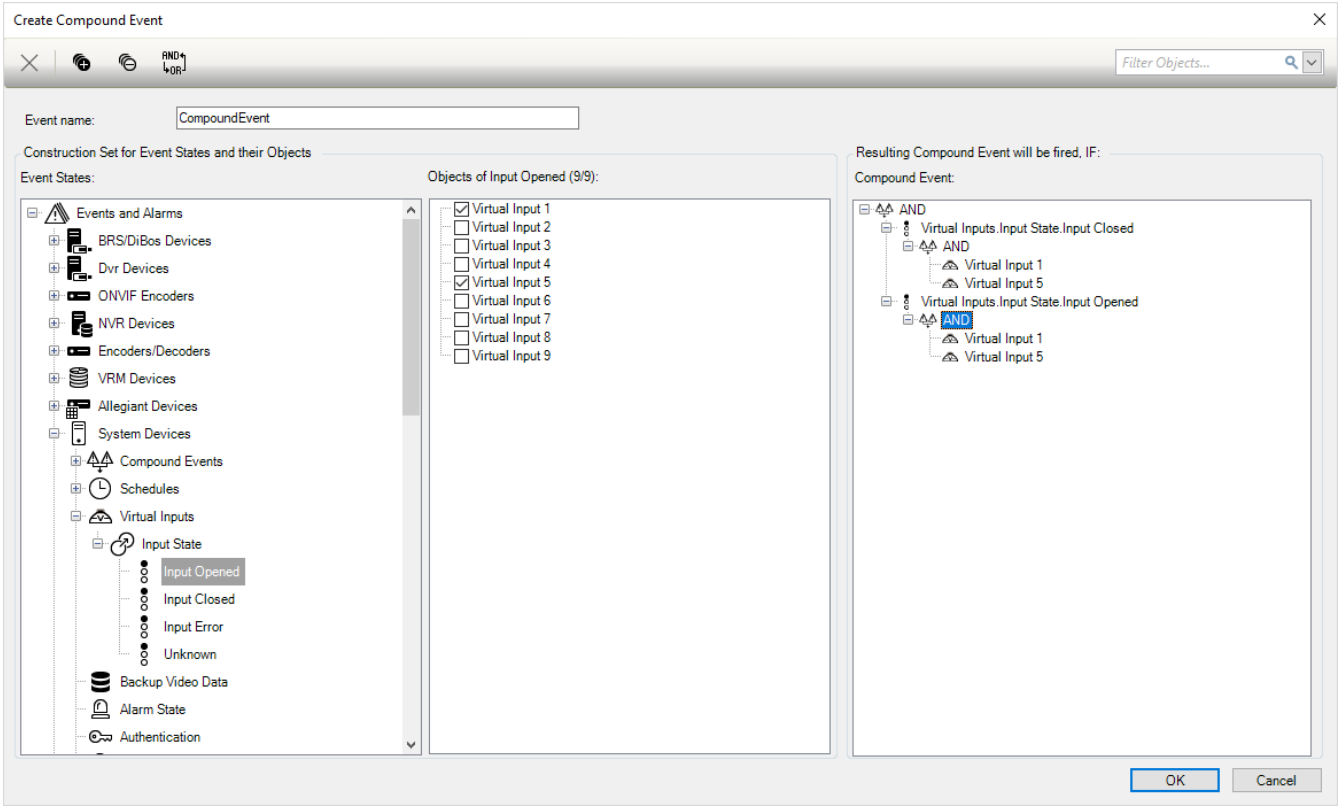
1. In the tree, select **System Devices** > **Operator Client Event Buttons** > **Event Button Pressed**.
   The corresponding Event Configuration Table is displayed.
2. Select a user event button to configure its behavior.
3. In the **Trigger Alarm** - **Schedule** column, click a cell and select the appropriate schedule.
   The schedule determines when the alarm that is supposed to notify the user is triggered.
4. In the **Log** - **Schedule** column, click a cell and select the appropriate schedule.
   The schedule determines when the event is logged.
   Selecting **Never** makes the user event button unavailable in the Operator Client of all user groups that have the user event button permission.
5. In the **Script** - **Script** column, click a cell and select an appropriate Command Script.
6. In the **Script** - **Schedule** column, click a cell and select the appropriate schedule.
   The schedule determines when the Command Script is executed.

See also
– *Events page, page 295*

23.8 Creating a Compound Event

Main window > **Events** >

You create a Compound Event. You can combine only state changes and their objects. Objects can be for example schedules or devices. You can combine both the state changes and their objects with the Boolean expressions AND and OR.
Example: You combine the connection states of an IP camera and a decoder. The Compound Event shall only occur when both the devices loose their connection. In this case you use the AND operator for the two objects (the IP camera and the decoder) and for the two connection states **Video Signal Lost** and **Disconnected**.



To create a Compound Event:

1. In the **Event name:** field, enter a name for the Compound Event.
2. In the **Event States:** field, select an event state.
   The available objects are displayed in the **Objects:** field.
3. In the **Objects:** field select device as required.
   The corresponding event and the selected devices are added to the Compound Event pane.
4. In the **Compound Event:** field, right-click a Boolean operation and change it where required.
   A Boolean operation defines the combination of its immediate child elements.
5. Click **OK**.
   The new Compound Event is added to the Event Configuration Table. You find it in the Event Tree below **System Devices**.

See also

– *Events page, page 295*

23.9 Editing a Compound Event

Main window > **Events**

You can change a previously created Compound Event.

To edit a Compound Event:

1. In the Event Tree, expand **System Devices** > **Compound Event State** > **Compound Event is True**.

2. In the Event Configuration Table, in the **Device** column, right-click the required Compound Event and click **Edit**.
   The **Edit Compound Event** dialog box is displayed.
3. Make the required changes.
4. Click **OK**.
   The Compound Event is changed.

See also
– *Events page, page 295*

23.10 Configuring an alarm

Main window > **Alarms**

Before configuring an alarm you must configure the trigger in **Events**.

To configure an alarm:

1. In the tree, select an alarm, for example **System Devices** > **Authentication** > **Operator Authentication Rejected**.
   The corresponding Alarm Configuration Table is displayed.
2. In the **Priority** column, click ... in a cell to type the alarm priority for the selected alarm (100 is low priority, 1 is high priority).
   In the **Title** column, click ... in a cell to type the title of the alarm to be displayed in BVMS, for example in the Alarm List.
   In the **Color** column, click ... in a cell to display a dialog box for selecting a color for the alarm to be displayed in the Operator Client, for example in the Alarm List.
3. In the 1-5 columns, click ... in a cell to display the **Select Image Pane Content** dialog box. Make the required settings.
4. In the **Audio File** column, click ... in a cell to display a dialog box for selecting an audio file that is played in case of an alarm.
5. In the **Alarm Options** column, click ... in a cell to display the **Alarm Options** dialog box.
6. Make the required settings.

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

See also
– *Configuring an event, page 308*
– *Alarms page, page 300*
– *Select Image Pane Content dialog box, page 301*
– *Alarm Options dialog box, page 303*

23.11 Configuring settings for all alarms

Main window > **Alarms**

You can set the following alarm settings that are valid for this Management Server:
– Number of Image panes per alarm
– Auto-clear time
– Manual alarm recording time
– Multi-row alarm display in alarm image window

– Duration limit for state-triggered alarm recordings
– Configure the behavior of all monitor groups

To configure all alarms:

1. Click .
   The **Alarm Settings** dialog box is displayed.
2. Make the appropriate settings.

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

▸ Click **OK**.

See also

– *Alarm Settings dialog box, page 301*

23.12 Configuring the pre- and post-alarm duration for an alarm

For configuring pre-alarm and post-alarm duration settings you need a camera that supports ANR and firmware 5.90 or later must be installed.

Main window > **Cameras and Recording** >

▸ For the desired camera, click to enable **ANR**.

Main window > **Events**

▸ Configure the desired event for the ANR activated camera.

Main window > **Alarms**

1. Configure an alarm for this event.
2. Select or
3. In the **Alarm Options** column click ...
   The **Alarm Options** dialog box is displayed.
4. In the **Record** column, select the check box of the ANR enabled camera to enable alarm recording.
   The check box in the **Deviating Alarm Duration Settings** column is selected automatically.
5. Click the **Deviating Alarm Duration Settings** tab.
6. Configure the alarm duration settings as required.

See also

– *Alarm Options dialog box, page 303*

23.13 Triggering alarm recording with text data

Main window > **Alarms**

You can trigger alarm recording with text data.

Before configuring an alarm you must configure an event that contains text data.

Example: **Events** > In the Event Tree select (text data must be available, for example: **Foyer Card Reader Devices** > **Foyer Card Reader** > **Card Rejected**)

Notice!
Configure the debounce time for the selected event to 0.
This ensures that no text data is lost.

To configure alarm recording:

1. In the tree, select an alarm, for example **ATM/POS Devices** > **ATM Input** > **Data Input**. The corresponding Alarm Configuration Table is displayed.
2. Make the required settings.
3. In the **Alarm Options** column, click ... in a cell to display the **Alarm Options** dialog box.
4. Click the **Cameras** tab and click to select the **Record** checkbox.

See also

- *Alarm Options dialog box, page 303*
- *Text Data Recording dialog box, page 299*

23.14 Adding text data to continous recording

Main window > **Events** > In the Event Tree select **Data Input** (text data must be available, for example: **Foyer Card Reader Devices** > **Foyer Card Reader** > **Card Rejected**) > **Text Data Recording** column > ...
You can add text data to continuous recording.

23.15 Protecting alarm recording

Main window > **Alarms**
Before configuring an alarm you must configure an event in **Events**.

To configure alarm recording:

1. In the tree, select an alarm, for example **ATM/POS Devices** > **ATM Input** > **Data Input**. The corresponding Alarm Configuration Table is displayed.
2. Make the required settings.
3. In the **Alarm Options** column, click ... in a cell to display the **Alarm Options** dialog box.
4. Click the **Cameras** tab and click to select the **Record** checkbox.
1. Select the **Protect Recording** checkbox.

See also

- *Alarm Options dialog box, page 303*

23.16 Configuring blinking hotspots

Notice!
A blinking hotspot can only be configured for an event OR an alarm.

Main window > **Events**
or
Main window > **Alarms**

For each event or alarm, you can configure the background color and the behavior (blinking or not blinking) for hotspots. For example you can configure for a event or alarm of a device that its device icon on a map starts blinking when the state of this device changes.
Additionally you can configure the display priority for all hotspots. This is required when different events occur for the same device. (1 = highest priority)
The configured color is valid for all hotspots with the same display priority. You can change color, behavior and priority at any event or alarm: The changed color and behavior is used for all hotspots of all other events or alarms which have the same priority.
The configuration of the color states on maps is only possible when you click to check the **Enable advanced state display (hot spot coloring in maps depending on state)** option or the **Enable advanced alarm display (hotspot coloring in maps depending on alarm)** option in the **Options** dialog box.

To configure a blinking hotspot for an event:

1. In the tree, select an event state ( ), for example **Encoders/Decoders** > **Encoder Relay** > **Relay State** > **Relay Opened**.
   The corresponding Event Configuration Table is displayed.
2. Click **Enable color states on maps**.
3. In the **Display priority on map:** field, enter the desired priority.
4. Click the **Background color on map:** field to select the desired color.
5. If desired, click to enable **Blinking**.

To configure a blinking hotspot for an alarm:
See chapter *Device , page 300* on the *Alarms page, page 300*.

Notice!
Only if the alarm is on the alarm list, the hotspot blinks.

The device icons on a map blink in the same color configured for the alarm or event.

See also

- *Events page, page 295*
- *Options dialog box (Settings menu), page 122*

23.17 Configuring events and alarms for an access control system

You can configure the following events:

- Access denied
- Access granted
- Access requested

Access requested events

These events allow a BVMS operator to manually grant or deny access to a person via an access control system. You can configure alarm recording, text data recording or additional information to this event.

Access requested events are only sent to BVMS, if the option **Additional verification** is set on each reader of the access control system. In the BVMS event configuration the **Access requested** events sent by the readers always trigger an alarm in BVMS.

Notice!

We recommend to set the highest priority (1) for the **Access requested** alarms. This ensures that the alarms automatically pop-up and receive the necessary attention of the operator.

24 User Groups page

Main window > **User groups**

Allows you to configure user groups, Enterprise User Groups and Enterprise Access.

The following user group is available by default:

– Admin Group (with one Admin user).

User Groups tab

Click to display the pages available for configuring the rights of the standard user group.

Enterprise User Group tab (only available with valid Enterprise license)

Click to display the pages available for configuring the permissions of an Enterprise User Group.

Enterprise Access tab (only available with valid Enterprise license)

Click to display the pages available for adding and configuring Enterprise Access.

User/user group options

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.
	Displays a dialog box for copying permissions from a selected user group to another user group.
	Click to display the pages available for configuring the permissions of this group.
	Click to display the page available for configuring the properties of this user.
	Click to display the page available for configuring the properties of this logon pair.
	Click to display the pages available for configuring the permissions of this dual authorization group.

Activating user name changes and password changes

Click to activate password changes.

Click to activate user name changes.

Notice!
User name changes and password changes are reverted after a configuration rollback.

Permissions on an Enterprise System
For an Enterprise System you configure the following permissions:
– Operating permissions of Operator Client defining the user interface for operating in the Enterprise System, for example the user interface of the alarm monitor.
Use an Enterprise User Group. Configure it on the Enterprise Management Server.
– Device permissions that should be available for operating in an Enterprise Management Server are defined on each Management Server.
Use Enterprise Accounts. Configure it on each Management Server.

Permissions on a single Management Server
For managing the access to one of the Management Servers, use the standard user group. You configure all permissions on this Management Server in this user group.
You can configure dual authorization user groups for standard user groups and for Enterprise User Groups.

Type	Contains	Available configuration settings	Where do you configure?
User group	Users	– Operating and device permissions	– Management Server
Enterprise User Group	Users	– Operating permissions – Per Management Server: Name of the corresponding Enterprise Access Accounts with logon credentials	– Enterprise Management Server
Enterprise Account	-	– Device permissions – Account password	– Management Server
Dual authorization user group	User groups	– See user groups	– See user groups
Enterprise dual authorization	Enterprise User Groups	– See Enterprise User Groups	– See Enterprise User Groups

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

To cancel filtering, click .

24.1 User Group Properties page

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

Main window > **User groups** > **Enterprise User Group** tab > > **Operating Permissions** tab > **User Group Properties** tab
Allows you to configure the following settings for the selected user group:
– Logon schedule
– Association of an LDAP user group

Description:
Type an informative description for the user group.

Language
Select the language of the Operator Client.

Logon schedule
Select a task or recording schedule. The users of the selected group can only log on to the system in the times defined by this schedule.

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.

LDAP groups
Displays the available LDAP user groups. You configure LDAP groups in the **LDAP Server Settings** dialog box.

Search for Groups
Click to display the available LDAP user groups in the **LDAP groups** list. To find user groups you must make the appropriate settings in the **LDAP Server Settings** dialog box.

Settings
Click to display the **LDAP Server Settings** dialog box.

Associate Group
Click to associate the selected LDAP group with this user group.

Clear Group
Click to clear the **Associated LDAP group** field. The association of the LDAP group to the BVMS user group is removed.

See also
– *Configuring LDAP settings, page 342*
– *Associating an LDAP group, page 342*
– *Scheduling user logon permission, page 343*

24.2 User Properties page

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

or

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

Allows you to configure a new user in a standard user group or in an Enterprise 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.

24.3 Logon Pair Properties page

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

or

Main window > **User groups** > **Enterprise User Group** tab > **New enterprise dual authorization group** >

Allows you to modify a pair of user groups to a dual authorization group. The users of the first user group are the users that must log on in the first dialog box for logging on, the users of the second user group confirm the logon.

Select Logon Pair
In each list, select a user group.

Force dual authorization
Select the check box to force each user to log on only together with a user of the second user group.

See also
– *Adding a logon pair to dual authorization group, page 340*

24.4 Camera Permissions page

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

Main window > **User groups** > **Enterprise Access** 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.

Manual Recording
Select a check box to allow manual recording (alarm recording).
You can select or clear this check box only when the manual alarm recording is enabled on the **Operator Features** page.

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.

24.5 Control Priorities page

Main window > **User groups** > **User Groups** tab > > **Device Permissions** tab > **Control priorities** tab
or

Main window > **User groups** > **Enterprise Access** tab > > **Device Permissions** tab > **Control priorities** tab

Control priorities
Move the appropriate slider to the right to decrease the priority for acquiring PTZ controls and Bosch Allegiant trunk lines. A user with a high priority can lock the PTZ controls or the control of a trunk line for users with lower priorities. You set the timeout for locking PTZ control on the **Timeout in min.** field. The default setting is 1 minute.

Timeout in min.
Enter the time period in minutes.

See also
– *Configuring various priorities, page 344*

24.6 Copy User Group Permissions dialog box

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

Main window > **User groups** > **Enterprise User Group** tab > >
Allows you to select user group permissions to be copied to selected user groups.

Copy from:
Displays the selected user group. Its permissions are to be copied to another user group.

Settings to Copy
Select a check box to select the desired user group permissions for copying.

Copy to:
Select a check box to specify the user group where to copy the selected user group permissions to.

See also
– *Copying user group permissions, page 345*

24.7 Decoder Permissions page

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

Main window > **User groups** > **Enterprise Access** tab > > **Device Permissions** tab > **Decoder Permissions** tab
Allows you to configure the decoders that the users of this group have access to.

Decoder
Displays the available decoders.
Click the check box to give the user group access to this decoder.

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

24.8 Events and Alarms page

Main window > **User groups** > **User Groups** tab > > **Device Permissions** tab > **Events and Alarms** tab
or

Main window > **User groups** > **Enterprise Access** tab > > **Device Permissions** tab > **Events and Alarms** tab

Allows to configure the permissions for the Events Tree, for example you set the events the user group is authorized or not authorized to use.
You cannot change these settings for a default user group.
For each event there is at least one device. For example, for the **Video Loss** event the available cameras are the devices. For an event like **Backup Finished** the corresponding device is **Time Controlled Backup**. Hence, a device can be a software process.

1. Expand a tree item and click the required check boxes for enabling the events. In the **Access** column, select the check box of a device to enable the events of this device. The access to the devices is configured on the **Camera** page and on the **Camera Permissions** page.
2. To enable or disable all events at once, select or clear the **Events and Alarms** check box.

24.9 LDAP Server Settings dialog box

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

Main window > **User groups** > **Enterprise User Group** tab > > **Operating Permissions** tab > **User Group Properties** tab > **Settings** button

You enter the LDAP server settings that are configured outside of BVMS. You will need the assistance of your IT administrator who set up the LDAP server for the following entries.
All fields are mandatory except the fields in the **Test User / User Group** group box.

LDAP Server Settings

LDAP Server
Type the name of the LDAP server.

Port
Type the port number of the LDAP server (default 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.

See also
– *Configuring LDAP settings, page 342*

24.10 Credentials page

Main window > **User groups** > **Enterprise Access** tab > > **Device Permissions** tab > **Credentials** tab

Configure the credentials of an Enterprise Account on a Management Server.

You configure Enterprise Access on each Management Server that is member of your Enterprise System. The Enterprise Management Server uses this credential to grant access to the devices of this Management Server for the Operator Client that logs on as a user of an Enterprise User Group.

Description:

Type in a description for the desired Enterprise Account.

Strong password policy

The **Strong password policy** check box is pre-selected for all newly created user groups.

We highly recommend to keep this setting to enhance the protection of your computer against unauthorized 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: ! $ # %).

Enter new password: / Confirm password

Type in and confirm the password for this Management Server.

See also

- *Strong password policy , page 336*
- *Creating an Enterprise Account, page 338*

24.11 Logical Tree page

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

or

Main window > **User groups** > **Enterprise Access** tab > > **Device Permissions** tab > **Logical Tree** tab

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.

See also
– *Configuring device permissions, page 344*

24.12 Operator Features page

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

Main window > **User groups** > **Enterprise User Group** tab > > **Operating Permissions** tab > **Operator Features** tab

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.

Allegiant trunk lines
Select the check box to allow accessing Bosch Allegiant trunk lines.
Control priorities page: In the **Control priorities** field, you can set the priority for acquiring Bosch Allegiant trunk lines.

Print and save
Select the check box to allow printing and saving video, maps and documents.

Alarm processing
Select the check box to allow alarm processing.

Interrupt the windows screen saver for incoming alarms
Select the check box to ensure that an incoming alarm is displayed even when the screen saver is active. If the screen saver requires a user name and password for being interrupted, this setting has no effect.

Alarm display
Select the check box to allow alarm display. If you select this option, the **Alarm processing** is deactivated simultaneously.

Playback
Select the check box to allow various playback features.

Export video
Select the check box to allow exporting video data.

Export MOV / ASF video
Select the check box to allow exporting video data in ASF and MOV format.

Protect video
Select the check box to allow protecting video data.

Unprotect video
Select the check box to allow both protecting and unprotecting video data.

Notice!
Configure the permissions for restricting and unrestricting or a user account on your DIVAR AN device as required. Create a user in BVMS with the same credentials and configure the permissions for restricting and unrestricting accordingly.
Display of restricted video is not affected and must be configured separately.

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.

Access to video that has been recorded in periods when the user group has not been allowed to log on
Select the check box to allow accessing the described video data.

Logbook access
Select the check box to allow accessing the Logbook.

Erase text data from logbook entries (for erasing person-related data)
Select the check box to allow erasing text data from logbook entries.

Operator event buttons
Select the check box to allow user event buttons in the Operator Client.

Close Operator Client
Select the check box to allow closing the Operator Client.

Minimize Operator Client
Select the check box to allow minimizing the Operator Client.

Audio Intercom
Select the check box to allow the user to speak on the loudspeakers of an encoder with audio-in and audio-out function.

Manual alarm recording
Select the check box to allow manual alarm recording.

Access VRM monitor
Select the check box to allow access to the VRM Monitor software.

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.

Arm intrusion panel areas
Select the check box to allow a user of Operator Client to arm areas configured in an intrusion panel that is part of your BVMS configuration.

Force arm intrusion panel areas
Select the check box to allow a user of Operator Client to force the arming of areas configured in an intrusion panel that is part of your BVMS configuration.

Disarm intrusion panel areas
Select the check box to allow a user of Operator Client to disarm areas configured in an intrusion panel that is part of your BVMS configuration.

Silence bells for intrusion panel areas
Select the check box to allow a user of Operator Client to switch off alarm sirens of areas configured in an intrusion panel that is part of your BVMS configuration.

Bypass intrusion panel points
Select the check box to allow a user of Operator Client to change the state of a point configured in an intrusion panel to the **Point bypassed** state. A bypassed point cannot send an alarm. When the state is changed back to **Point unbypassed**, a pending alarm is sent if available

Unlock intrusion panel doors
Select the check box to allow a user of Operator Client to unlock a door configured in an intrusion panel.

Secure and unsecure intrusion panel doors
Select the check box to allow a user of Operator Client to secure and unsecure a door configured in an intrusion panel.

Cycle intrusion panel doors
Select the check box to allow a user of Operator Client to cycle a door configured in an intrusion panel.

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

Display order in case of same alarm priority
Select the appropriate value to configure the order of Alarm Image panes in the Alarm Display of Operator Client.

Instant playback rewind time:
Enter the number of seconds for the duration of alarm instant playback.

Repeat alarm audio:
Select the check box and enter the number of seconds after an alarm sound is repeated.

Limit access to recorded video to the last n minutes:
Select the check box to limit the access to recorded videos.
In the list, enter the number of minutes.

Enforce automatic Operator logoff after this time of inactivity:
Select the check box to enable the automatic logoff of Operator Client after the configured time period.

See also
– *Inactivity logoff, page 46*

24.13 Priorities page

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

Main window > **User groups** > **Enterprise User Group** tab > > **Operating Permissions** tab > **Priorities** tab

Allows you to configure the timeout for explicit PTZ locking. You can set the priorities for PTZ control and the display of incoming alarms.

Automatic popup behavior

Move the slider to adjust the priority value of Live Image window or Playback Image window. This value is required for incoming alarms to decide whether this alarm is automatically displayed in the Alarm Image window.

For example: If you move the slider for Live Image window to 50 and for the Playback Display to 70 and an alarm comes in with a priority of 60, the alarm is only automatically displayed if the user has Playback Display active. The alarm is not automatically displayed when the user has Live Display active.

See also

– *Configuring various priorities, page 344*

24.14 User Interface page

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

Main window > **User groups** > **Enterprise User Group** 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.

Alarm Monitor

Select the Alarm monitor which can display either Live and Alarm Mode or only Alarm Mode.

Monitor 1 - 4

In the corresponding list of each monitor, select the required entry.

- For the Control monitor the entry **Control** is preselected and cannot be changed.
- For the Alarm monitor you can select one of the following entries:
  - **Live video and alarm content**
  - **Alarm content only**
- For the remaining monitors you can select one of the following entries:
  - **Live video only**
  - **Map and document**
  - **Two maps and document**
  - **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**
- **Alarm content only**
- **Live video and alarm content**
- **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.

24.15 Server Access page

Main window > **User groups** > **Enterprise User Group** tab > > **Server Access** tab
You configure the server access on an Enterprise Management Server.
You enter the name of the Enterprise Account and its password for each Management Server of your Enterprise System. This account is configured on each Management Server.

Management Server
Displays the name of the Management Server that you configured on this Enterprise Management Server.

Network Address
Displays the private IP address or DNS name of the Management Server.

Server Number
Displays the number of the Management Server. This number is used by a Bosch IntuiKey keyboard to select the desired Management Server.

Access
Click to check when you want to grant access to the Management Server. This Management Server is now an Enterprise Management Server.

Enterprise Account
Type the name of the Enterprise Account that has been configured on the Management Server.

Enterprise Account Password
Click to display a dialog box for typing the password of the Enterprise Account that has been configured on the Management Server.

Server Description
Displays the descriptive text for this server.
Further columns are displayed if they have been added to the Server List.

See also
- *Creating a group or account, page 337*
- *Creating an Enterprise System, page 96*
- *Configuring the Server List for Enterprise System, page 96*

24.16 Configuration Permissions page

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

Main window > **User groups** > **Enterprise User Group** tab > > **Operating Permissions** tab > **Configuration Permissions** tab
Allows you to configure various user permissions for the Configuration Client.
Permission to start the Configuration Client implies read-only access.

Logon Permissions
Select the check box to allow logon to Configuration Client application.

Device Tree
In this section you can specify the permissions on the **Devices** page. Select the check box for the respective permission.

Maps and Structure
In this section you can specify the permissions on the **Maps and Structure** page. Select the check box of the respective permission.

Schedules
In this section you can specify the permissions on the **Schedules** page. Select the check box of the respective permission.

Cameras and Recording
In this section you can specify the permissions on the **Cameras and Recording** page. Select the check box of the respective permission.

Events
In this section you can specify the permissions on the **Events** page. Select the check box of the respective permission.

Alarms
In this section you can specify the permissions on the **Alarms** page. Select the check box of the respective permission.

User Groups
In this section you can specify the permissions for configuring user groups. Select the check box of the respective permission.

Notice!
To select the **Configure User Groups** check box and the **Configure Users** check box are mutually exclusive options for security reasons.

Menu commands
In this section you can specify the permissions for configuring menu commands. Select the check box of the respective permission.

Reports
In this section you can specify the permissions for configuring reports. Select the check box of the respective permission.

24.17 User Group Permissions page

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

Main window > **User groups** > **Enterprise User Group** tab > > **Operating Permissions** tab > **User Group Permissions** tab
Allows you to assign in which user groups the users of a specific user group can add new users.

Notice!
You can only assign user group permissions to a user group, to which you have assigned the permission to configure users before. You assign this permission on the **Configuration Permissions** page.

Notice!
The users of a standard user group are not allowed to add new users to the Admin Group. This check box is not active.

See also
– *Configuration Permissions page, page 332*

24.18 Account policies page

Main window > **User groups** > **User Groups** tab > > **Security** tab > **Account policies** tab
or

Main window > **User groups** > **Enterprise User Group** tab > > **Security** tab > **Account policies** tab

Allows you to configure settings for users and passwords.

Strong password policy
Select the check box to enable the password policy.
For more information see: *Configuring users, permissions and Enterprise Access, page 336*

Notice!
The **Strong password policy** setting is only applied to the users if the check box is selected in the corresponding user group.
We highly recommend to keep this setting to enhance the protection of your computer against unauthorized access.

Minimum password length
This setting determines the least number of characters that can make up a password for a user account.
Select the check box to enable the setting and enter the minimum value.

Maximum password age in days
This setting determines the period of time (in days) that a password can be used before the system requires the user to change it.
Select the check box to enable the setting and enter the minimum value.

Number of used passwords in history
This setting determines the number of unique new passwords that must be associated with a user account before an old password can be reused.
Select the check box to enable the setting and enter the minimum value.

Maximum invalid logon attempts
This setting enables blocking an account after a specific number of logon attempts.
Select the check box to enable the setting and enter the minimum value.

Notice!
If the maximum value of invalid logon attempts is exceeded, the account is disabled and has to be activated again.

Notice!
The count of invalid logon attempts get reset upon successful login.

Notice!
The **Maximum invalid logon attempts** check box is disabled for the Admin Group.

Disable offline client
Select the check box to disable logon to an offline client.
The **Disable offline client** check box is automatically selected, if the **Maximum invalid logon attempts** check box is selected.

Additional information
From BVMS 9.0 on the following **Account policies** settings apply as default:
- The **Strong password policy** check box is pre-selected.
- The **Minimum password length** check box is pre-selected. The default value is 10.
- The **Maximum password age in days** check box is not pre-selected. The default value is 90.
- The **Number of used passwords in history** check box is not pre-selected. The default value is 10.
- The **Maximum invalid logon attempts** check box is not pre-selected. The default value is 1.
- The **Disable offline client** check box is not pre-selected.

25 Configuring users, permissions and Enterprise Access

Main window > **User groups**

This chapter provides information on how to configure user groups, Enterprise User Groups and Enterprise Access.

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

The following rules apply:

- A user can only be the member of one user group or Enterprise User Group.
- You cannot change the settings of a default user group.
- This user group has access to all the devices of the Full Logical Tree and is assigned the **Always** schedule.
- For accessing the Windows user groups of a domain, LDAP user groups are used.
- 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.

See also

- *Account policies page, page 334*
- *User Group Properties page, page 319*
- *User Properties page, page 319*

- *Logon Pair Properties page, page 320*
- *Camera Permissions page, page 321*
- *Control Priorities page, page 322*
- *Copy User Group Permissions dialog box, page 323*
- *Decoder Permissions page, page 323*
- *Events and Alarms page, page 324*
- *LDAP Server Settings dialog box, page 324*
- *Credentials page, page 326*
- *Logical Tree page, page 326*
- *Operator Features page, page 327*
- *Priorities page, page 330*
- *User Interface page, page 330*
- *Server Access page, page 331*

25.1 Creating a group or account

Main window > **User groups**

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

25.1.1 Creating a standard user group

Main window > **User groups**

To create a standard user group:

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

See also

- *User Group Properties page, page 319*
- *Operator Features page, page 327*
- *Priorities page, page 330*
- *User Interface page, page 330*

25.1.2 Creating an Enterprise User Group

Main window > **User groups**

You perform the task of creating an Enterprise User Group for an Enterprise System on the Enterprise Management Server.

You create an Enterprise User Group with users to configure their operating permissions. These operating permissions are available on an Operator Client that is connected to the Enterprise Management Server. An example of an operating permission is the user interface of the alarm monitor.

To create an Enterprise User Group:

1. Click the **Enterprise User Group** tab.
   Note: The **Enterprise User Group** tab is only available if the appropriate license is available and if one or more Management Server computers are configured in **Devices** > **Enterprise System** > **Server List / Address Book**.
2. Click .
   The **New enterprise user group** dialog box is displayed.
3. Type in the name and a description.
4. Click **OK**.
   The Enterprise User Group is added to the corresponding tree.
5. Right-click the new Enterprise group and click **Rename**.
6. Enter the desired name and press ENTER.
7. On the **Operating Permissions** page, configure the operating permissions and server access for the configured Management Server computers as required.

See also

- *User Group Properties page, page 319*
- *Operator Features page, page 327*
- *Priorities page, page 330*
- *User Interface page, page 330*
- *Server Access page, page 331*

25.1.3 Creating an Enterprise Account

Main window > **User groups**

Notice!
At least one device must be configured in the Device Tree before you can add an Enterprise Account.

You perform the task of creating an Enterprise Account on a Management Server. Repeat this task on each Management Server that is a member of your Enterprise System.
You create an Enterprise Account to configure the device permissions for an Operator Client using an Enterprise System.

To create an Enterprise Account:

1. Click the **Enterprise Access** tab.
2. Click .
   The **New enterprise account** dialog box is displayed.
3. Type in the name and a description.

4. 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.
5. Click **OK**.
   A new Enterprise Account is added to the corresponding tree.
6. Right-click the new Enterprise Account and click **Rename**.
7. Enter the desired name and press ENTER.
8. On the **Device Permissions** page, configure the credentials and the device permissions as required.

See also
- *Strong password policy , page 336*
- *Credentials page, page 326*
- *Logical Tree page, page 326*
- *Events and Alarms page, page 324*
- *Control Priorities page, page 322*
- *Camera Permissions page, page 321*
- *Decoder Permissions page, page 323*

25.2 Creating a user

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

Main window > **User groups** > **Enterprise User Group** tab
You create a user as a new member of an existing standard user group or Enterprise User Group.

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

To create a user:

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

See also
- *User Properties page, page 319*
- *Strong password policy , page 336*
- *User Groups page, page 317*

25.3 Creating a dual authorization group

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

Main window > **User groups** > **Enterprise User Group** tab
You can create a dual authorization for a standard user group or for an Enterprise User Group. For Enterprise Access, a dual authorization is not available.
You select two user groups. The members of these user groups are the members of the new dual authorization group.

To create a dual authorization group:

1. Click .
   The **New dual authorization group** dialog box respectively the **New enterprise dual authorization group** dialog box is displayed.
2. Type in a name and a description.
3. Click **OK**.
   A new dual authorization group is added to the corresponding tree.
4. Right-click the new dual authorization group and click **Rename**.
5. Enter the desired name and press ENTER.

See also
- *Adding a logon pair to dual authorization group, page 340*
- *User Group Properties page, page 319*
- *Operator Features page, page 327*
- *Priorities page, page 330*
- *User Interface page, page 330*

25.4 Adding a logon pair to dual authorization group

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

Main window > **User groups** > **Enterprise User Group** tab > **New enterprise 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

See also
- *Creating a dual authorization group, page 340*
- *Logon Pair Properties page, page 320*

25.5 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.

See also

- *User Groups page, page 317*
- *User Properties page, page 319*
- *Strong password policy , page 336*

25.6 Configuring LDAP settings

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

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

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

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

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

To configure LDAP settings:

1. Click the **User Group Properties** tab.
2. In the **LDAP Properties** field, make the appropriate settings.

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

25.7 Associating an LDAP group

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

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

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

To associate an LDAP group:

1. Click the **User Group Properties** tab.
2. In the **LDAP Properties** field, click **Settings**.
   The **LDAP Server Settings** dialog box is displayed.
3. Enter the settings of your LDAP server and click **OK**.

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

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

25.8 Scheduling user logon permission

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

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

You can limit the members of a user group or Enterprise User Group to log on to their computers at specified time periods.
You cannot change these settings for a default user group.

To schedule logging on:

1. Click the **User Group Properties** tab.
2. In the **Logon schedule** list, select a schedule.

25.9 Configuring operating permissions

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

Main window > **User groups** > **Enterprise User Group** 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 or Enterprise User Groups.

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

See also
- *User Group Properties page, page 319*
- *Operator Features page, page 327*
- *Priorities page, page 330*
- *User Interface page, page 330*
- *Server Access page, page 331*

25.10 Configuring device permissions

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

Main window > **User groups** > **Enterprise Access** 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 or Enterprise Accounts.

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

See also
- *Logical Tree page, page 326*
- *Events and Alarms page, page 324*
- *Control Priorities page, page 322*
- *Camera Permissions page, page 321*
- *Decoder Permissions page, page 323*

25.11 Configuring various priorities

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

Main window > **User groups** > **Enterprise User Group** tab
or

Main window > **User groups** > **Enterprise Access** tab
You can configure the following priorities:
- For standard user groups and **Enterprise User Group**: You can configure the alarm priorities for Live Mode and Playback Mode.
- For standard user groups and **Enterprise Access**: You can configure the priorities for acquiring PTZ controls and Bosch Allegiant trunk lines.
  You can configure a time period for PTZ locking, i.e. a user with higher priority can take over the camera control from a user with a lower priority and locks it for this time period.

To configure live and playback priorities:

1. Select a standard user group or an Enterprise User Group.
2. Click **Operating Permissions** .
3. Click the **Priorities** tab.
4. In the **Automatic popup behavior** field, move the sliders as required.

To configure priorities for PTZ and Bosch Allegiant trunk lines:

1. Select a standard user group or an Enterprise Account.
2. Click **Device Permissions** tab.
3. Click the **Control priorities** tab.
4. In the **Control priorities** field, move the sliders as required.
5. In the **Timeout in min.** list, select the required entry.

See also

- *Control Priorities page, page 322*
- *Priorities page, page 330*

25.12 Copying user group permissions

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

or

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

or

Main window > **User groups** > **Enterprise Access** tab

You can copy permissions from one group or account to another. You must have configured at least 2 groups or accounts.

To copy permissions:

1. In the User Groups tree, select a group or account.
2. Click .
   The **Copy User Group Permissions** dialog box is displayed.
3. Select the appropriate permissions and the appropriate target group or account.
4. Click **OK**. The group permissions of this group are copied to the other group or account. The dialog box is closed.

26 Configuring video-based fire alarm detection

For configuring a video-based fire alarm you must perform the following steps:

1. Configure a fire detection on your fire detection camera.
   You use the Webpage of the camera for this configuration.
   For detailed information on configuring a fire detection camera, see
   – *Configuring a fire detection camera, page 346*
2. Add this fire detection camera to the system. You can add the fire detection camera to a VRM pool, as a live only encoder, or as a local storage encoder.
   For detailed information on adding a camera, see
   – *Adding an encoder to a VRM pool, page 347*
   – *Adding a live only encoder, page 218*
   – *Adding a local storage encoder, page 219*
3. Configure a fire event for this camera.
   – *Configuring a fire event, page 349*
4. Configure the alarm for the fire event.
   – *Configuring a fire alarm, page 349*

See also

- *Adding an encoder to a VRM pool, page 347*
- *Adding a live only encoder, page 218*
- *Adding a local storage encoder, page 219*
- *Configuring a fire event, page 349*
- *Configuring a fire alarm, page 349*

26.1 Configuring a fire detection camera

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

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

Main window > **Devices** > >
or

Main window > **Devices** > >

For configuring a video-based fire alarm, you must first configure the fire detection on the fire detection camera.

For details see the Operation Manual of your fire detection camera.

To configure:

1. Right-click the device icon and click **Show webpage in browser**.
2. Click **Configuration**.
3. On the navigation pane, expand **Alarm** and click **Fire detection**.
4. Perform the desired settings.

26.2 Adding an encoder to a VRM pool

To add encoders to a VRM pool, see *Adding Encoders via scan, page 347*.

See also

– *Adding a device, page 126*

26.3 Adding Encoders via scan

To add encoders via scan:

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

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

26.4 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.
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.

26.5 Adding local storage encoders via scan

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.

26.6 Configuring a fire event

Main window > **Events**

To configure:

1. In the tree, select **Encoders/Decoders > Camera > Fire or Smoke State** > **Fire or Smoke detected**.
   The corresponding Event Configuration Table is displayed.
2. In the **Trigger Alarm** - **Schedule** column, click a cell and select the appropriate schedule.
   The schedule determines when the alarm is triggered.
   Select one of the Recording Schedules or Task Schedules that you have configured in the **Schedules** page.
3. Make the required settings.

Note: You can use the same procedure for the other available fire events.

26.7 Configuring a fire alarm

Main window > **Alarms**

To configure:

1. In the tree, select **Encoders/Decoders > Camera > Fire or Smoke State** > **Fire or Smoke detected**.
   The corresponding Alarm Configuration Table is displayed.
2. Make the required settings.

27 Configuring MIC IP 7000 connected to a VIDEOJET 7000 connect

For operating a MIC IP 7000 camera connected to a VIDEOJET 7000 connect, you must perform the following configuration for proper working.

Before you add the MIC IP camera to BVMS, perform the following tasks:

1. Reset both the MIC IP 7000 camera and the VIDEOJET 7000 connect device to the factory default settings on the Web page of each device.
2. Set the MIC IP 7000 camera to the **MIC IP Starlight 7000 HD-VJC-7000** variant.
3. Configure the MIC IP 7000 camera and the VIDEOJET 7000 connect device according to the documentation delivered with the devices.
4. If you want to use ANR, execute the ANR Setup Utility for the VIDEOJET 7000 connect device.
   Perform this task on a computer being member of the same network as the VIDEOJET 7000 connect device.
   You find the ANR Setup Utility on the product catalog page for the VIDEOJET 7000 connect device.

Perform this procedure to add and configure the MIC IP 7000 camera in BVMS:

1. In the Device Tree, add only the MIC IP 7000 camera.
   You cannot add the VIDEOJET 7000 connect device to BVMS.
2. Right-click the just added camera and click **Edit Encoder**.
   The **Edit Encoder** dialog box is displayed.
   The device capabilities are automatically retrieved according to the variant configured above.
3. If required, configure ANR on the **Cameras and Recording** page.

28 Troubleshooting

This chapter contains information on how to handle known problems using BVMS Configuration Client.

Problems after updating Bosch Video Management System

Issue	Cause	Solution
The NVR does not record after updating Bosch Video Management System.	The connection between NVR and Management Server was lost after the update. The update can potentially have changed the BVMS database on the Management Server. The NVR must “know” these changes.	Reestablish the connection between NVR and Management Server.

Problems during installation

Issue	Cause	Solution
Setup displays wrong characters.	The Windows language settings are not correct.	*Configuring the desired language in Windows, page 353*
Setup stops with a message that OPC Server cannot be installed.	OPC Server files cannot be overwritten.	Uninstall OPC Core Components Redistributable and restart BVMS Setup.
The software cannot be uninstalled by executing Setup.		Start Control Panel > Add/ Remove Programs and uninstall BVMS.

Problems immediately after starting the application

Issue	Cause	Solution
BVMS displays the wrong language.	Windows is not switched to the desired language.	*Configuring the language of Configuration Client, page 83* or *Configuring the language of Operator Client, page 83*
The logon dialog box of Operator Client shows the wrong language.	Although you have changed the language for Operator Client in Configuration Client, the language for the logon dialog box of Operator Client depends on the Windows language.	*Configuring the desired language in Windows, page 353*

Problems with display language

Issue	Cause	Solution
Some display texts in Configuration Client or Operator Client are in a foreign language, usually English.	The OS language of the computer where the Management Server is installed, is often English. Hence, when the BVMS database is generated on this computer, many display texts are created in English. They remain unchanged regardless of the Windows language of an Operator Client computer. To avoid such language discrepancies, install Management Server software on a computer with the desired Windows interface language.	Do not change this.

Problems with Bosch IntuiKey keyboard

Issue	Cause	Solution
The Bosch IntuiKey keyboard triggers an alarm and the softkey display displays Off Line.	The connection to the workstation is lost. Either the cable is damaged or unplugged, or the workstation has been reset.	*Reestablishing the connection to a Bosch IntuiKey keyboard, page 353*

Problems with the settings in the recording control of your soundcard

Issue	Cause	Solution
Feedbacks occur when using a microphone for Intercom functionality.	In the recording control of your soundcard the microphone must be selected, not the stereo mix (or something else). Operator Client checks its configuration file during startup and changes the settings in the recording control accordingly. This configuration file contains a default entry which might not match your system configuration. This setting is restored during each start of Operator Client.	Change the setting in the configuration file of Operator Client to microphone.

Crashing Configuration Client

Issue	Cause	Solution
Configuration Client crashes.	If there are many cameras configured in an Allegiant file which are not connected to Bosch Video Management System, you can reduce this number. This avoids unnecessary system load.	See *Reducing the number of Allegiant cameras, page 353*.

Crashing Operator Client

Issue	Cause	Solution
Operator Client crashes.	DiBos Web client is installed and has been started on the computer where Operator Client is installed.	Uninstall the DiBos Web client.

28.1 Configuring the desired language in Windows

If you want to change the display language for the setup of BVMS, you must switch the language in your Windows. For activating the language settings the computer is restarted after performing the following steps.

To configure the desired language:

1. Click **Start**, click **Control Panel**, and then double-click **Regional and Language Options**.
2. Click the **Advanced** tab, under **Language for non-Unicode programs**, select the desired language.
3. Click **OK**.
4. In each of the next message boxes, click **Yes**.
   Your computer is restarted.

28.2 Reestablishing the connection to a Bosch IntuiKey keyboard

1. Plug in the cable again or wait until the workstation is online.
   The Off Line message disappears.
2. Press the Terminal softkey to enter BVMS.

28.3 Reducing the number of Allegiant cameras

You need the Allegiant Master Control Software to edit the Allegiant file.

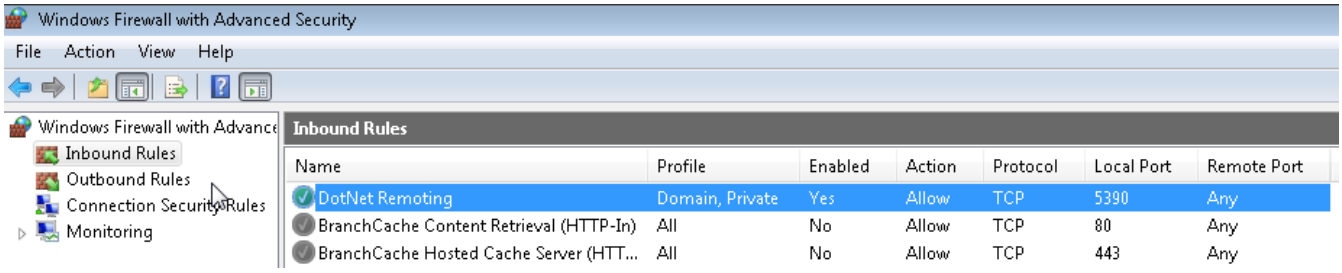
To reduce the number of Allegiant cameras:

1. Start the Master Control Software.
2. Open the Allegiant file.
3. Click the Camera tab.
4. Mark the cameras that are not required.
5. On the Edit menu, click Delete.
6. Save the file. The file size remains unchanged.
7. Repeat the last step for monitors that you do not need. Click the Monitors tab.
8. Import this file in Bosch Video Management System (refer to *Adding a device, page 126*).

28.4 Used ports

This section lists for all components of BVMS the ports that must be open within a LAN. Do not open these ports to the Internet! For operation via Internet use secure connections like VPN or Remote Access.
Each table lists the local ports that must be open on the computer where the server is installed or on the router/level 3 switch that is connected to the hardware.
On a Windows Firewall, configure an Inbound Rule for each open port.
Allow all outgoing connections for all BVMS software applications.

Example for a simple Inbound Rule in Windows 7 Firewall



Management Server / Enterprise Management Server ports

Server (Listener)	Protocol	Inbound ports	Client (Requester)	Remark
Management Server	UDP	123	Encoder	TimeServer NTP
Management Server	TCP	5322	Operator Client,	SSH connection
Management Server	TCP	5389	ONVIF device	ONVIF proxy, event notification
Management Server	TCP	5390	Operator Client, Configuration Client, BVMS SDK Application	.NET Remoting
Management Server	TCP	5392	Operator Client, Configuration Client, Mobile Video Service	WCF, gateway.push.apple.com
Management Server	TCP	5393	Operator Client, VRM, MVS	Data-Access-Service
Management Server	TCP	5395	Configuration Client, Operator Client	User preferences, File transfer
Management Server	UDP	12544	SNMP client	BVMS SNMP get port

Video Recording Manager ports

Server (Listener)	Protocol	Inbound ports	Client (Requester)	Remark
VRM	TCP	554	RTSPclient	Retrieve RTSP stream

Server (Listener)	Protocol	Inbound ports	Client (Requester)	Remark
VRM	TCP	1756	Management Server, Configuration Client	via RCP+
VRM	UDP	1757	Management Server, Operator Client	Scan Target Broadcast
VRM	UDP	1758	Management Server, Configuration Client	Scan Response
VRM	UDP	1800	Management Server, Operator Client	Scan Target Multicast
VRM	TCP	80	Operator Client	Primary VRM playback via http
VRM	TCP	443	Operator Client	Primary VRM playback via https
VRM	TCP	81	Operator Client	Secondary VRM playback via http
VRM	TCP	444	Operator Client	Secondary VRM playback via https

Mobile Video Service ports

Server (Listener)	Protocol	Inbound ports	Client (Requester)	Remark
Mobile Video Service	TCP	80	Management Server, Operator Client, Configuration Client, HTML Client, Mobile Apps	Access via http
Mobile Video Service	TCP	443	Management Server, Operator Client, Configuration Client, HTML Client, Mobile Apps	Access via https
Mobile Video Service	TCP	2195	Apple Push Notification	Mac iOS
Mobile Video Service	UDP	1064-65535	Encoder, VRM	
Mobile Video Service transcoder	TCP	5382	Mobile Video Service mobile provider	Media stream
Mobile Video Service transcoder	TCP	5385	Mobile Video Service mobile provider	Media stream
Mobile Video Service BVMS provider	TCP	5383	Operator Client	Media stream
Mobile Video Service mobile provider	TCP	5384	HTML Client, Mobile Apps	Media stream

Server (Listener)	Protocol	Inbound ports	Client (Requester)	Remark
Mobile Video Service transcoder	TCP	5385	Mobile Video Service mobile provider	Media stream

iSCSI Storage System ports

Configure port forwarding at the connected router for this device.

Server (Listener)	Protocol	Inbound ports	Client (Requester)	Remark
iSCSI storage system	TCP	3260	Encoder, VRM, Configuration Client	

Bosch Video Streaming Gateway ports

Server (Listener)	Protocol	Inbound ports	Client (Requester)	Remark
Bosch Video Streaming Gateway	TCP	8756-8762	VRM, Management Server, Configuration Client	RCP +
Bosch Video Streaming Gateway	TCP	8080-8086	VRM, Management Server, Configuration Client, Operator Client	HTTP
Bosch Video Streaming Gateway	TCP	8443-8449	VRM, Management Server, Configuration Client, Operator Client	HTTPS
Bosch Video Streaming Gateway	TCP	1757	VRM Configuration Client	Scan Target Broadcast
Bosch Video Streaming Gateway	TCP	1758	VRM Configuration Client	Scan Response
Bosch Video Streaming Gateway	TCP	1800	VRM Configuration Client	Scan Target Multicast
Bosch Video Streaming Gateway	UDP	1064-65535	Encoder, VRM	

ONVIF camera ports

Configure port forwarding at the connected router for this device.

Server (Listener)	Protocol	Inbound ports	Client (Requester)	Remark
ONVIF camera	TCP	80	Management Server, VSG, Configuration Client, Operator Client	Access via http

Server (Listener)	Protocol	Inbound ports	Client (Requester)	Remark
ONVIF camera	TCP	443	Management Server, VSG, Configuration Client, Operator Client	Access via https
ONVIF camera	RTSP	554	Management Server, VSG, Configuration Client, Operator Client	

BVMS Operator Client / Cameo SDK ports

Server (Listener)	Protocol	Inbound ports	Client (Requester)	Remark
Operator Client	TCP	5394	BVMS SDK Application, BIS	.NET Remoting
Operator Client	UDP	1024-65535	Encoder, VRM	
Operator Client	TCP	443	Encoder	Remote access, encrypted live view

Encoder ports

Configure port forwarding at the connected router for this device.

Server (Listener)	Protocol	Inbound ports	Client (Requester)	Remark
Encoder	TCP	1756	Decoder, Management Server, VRM, Operator Client, Configuration Client, BVMS SDK Application	via RCP+
Encoder	UDP	1757	Decoder, Management Server, Operator Client	Scan Target
Encoder	UDP	1758	Decoder, Management Server, Operator Client	Scan Response
Encoder	UDP	1800	Decoder, Management Server, Operator Client	Scan Target Multicast
Encoder	TCP	80	Operator Client, BVMS SDK Application, VSG	Access via http
Encoder	TCP	443	Operator Client, BVMS SDK Application, VSG	Access via https
Encoder	UDP	123	Management Server, VRM	SNTP
Encoder	UDP	161	Management Server, VRM	SNMP
Encoder	TCP	554	Operator Client, BVMS SDK Application, VSG	RTSP streaming
Encoder	TCP	3260	Encoder (outbound)	iSCSI recording

Optional encoder ports

Server (Listener)	Protocol	Inbound ports	Client (Requester)	Remark
FTP	TCP	21		
SSDP	UDP	1900		
UPNP	UDP	3702		
SRTSP	UDP	9554		
RTSP send	UDP	15344, 15345		

BVMS Decoder ports

Configure port forwarding at the connected router for this device.

Server (Listener)	Protocol	Inbound ports	Client (Requester)	Remark
Decoder	TCP	1756	Management Server, Operator Client, Configuration Client, BVMS SDK Application	via RCP+
Decoder	UDP	1757	Management Server, Operator Client	Scan Target
Decoder	UDP	1758	Management Server, Operator Client	Scan Response
Decoder	UDP	1800	Management Server, Operator Client	Multicast Network Scan Target
Decoder	TCP	80	Operator Client	Access via http
Decoder	TCP	443	Operator Client	Access via https
Decoder	UDP	1024-65535	Encoder	Streaming ports
Decoder	UDP	123	Management Server, VRM	SNTP
Decoder	UDP	161	Management Server, VRM	SNMP

BRS/DiBos ports

Server (Listener)	Protocol	Inbound ports	Client (Requester)	Remark
DiBos 8.7 / BRS 8.10	TCP	808	Management Server, Configuration Client	Web Service For DiBos v. 8.7 a patch is needed.
Alternative:				
BRS/DiBos	TCP	135	Operator Client, Management Server, Configuration Client	DCOM, used when Web Service does not work or the used DiBos version does not support Web Service Firewall must be disabled

Server (Listener)	Protocol	Inbound ports	Client (Requester)	Remark
BRS/DiBos	UDP	135	Operator Client, Management Server, Configuration Client	DCOM, used when Web Service does not work or the used DiBos version does not support Web Service Firewall must be disabled

DVR ports

Configure port forwarding at the connected router for this device.

Server (Listener)	Protocol	Inbound ports	Client (Requester)	Remark
DVR	TCP	80	Management Server, Configuration Client, Operator Client	Access via http

Barco Monitor Wall

Server (Listener)	Protocol	Inbound ports	Client (Requester)	Remark
Barco Monitor Wall	TCP	1756	Management Server, Operator Client, Configuration Client, BVMS SDK Application	via RCP+
Barco Monitor Wall	UDP	1757	Management Server, Operator Client	Scan Target
Barco Monitor Wall	UDP	1758	Management Server, Operator Client	Scan Response
Barco Monitor Wall	UDP	1800	Management Server, Operator Client	Multicast Network Scan Target

28.5 Enabling logging for ONVIF events

You can enable logging for ONVIF events for example when you encounter problems with receiving BVMS events. Logging then helps you to find the issue.

To enable logging:

1. Open the file `%programfiles(x86)%\Bosch\VMS\AppData\Server\CentralServer\BVMSLogCfg.xml` in an appropriate editor, for example Notepad. Run the Notepad application as administrator.
2. Navigate to the line containing the following string:
   `Add logging for onvif events of a device by network address`
   The commented lines contain a brief explanation.
3. As the logger name, type in `OnvifEvents.<Networkaddress>`.
   Type in only `OnvifEvents` to log the events for all ONVIF devices.

4. As level value, type in `DEBUG` for all incoming and outgoing events.
   Type in `INFO` for all outgoing events.
   Type in `WARN` or `ERROR` to disable.

The following lines show an example for logging the events from device 172.11.122.22 with all outgoing and incoming events:

```
<logger name="OnvifEvents.172.11.122.22" additivity="false">
<level value = "DEBUG"/>
<appender-ref ref="OnvifRollingFileAppender"/>
</logger>
```

See also

- *Configuring an ONVIF mapping table, page 237*
- *ONVIF event mapping, page 52*

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.

Alarm Image window

Image window for displaying one or more Alarm Image panes.

Alarm List

Window in Bosch Video Management System used to display a list of active alarms.

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

area

A group of detection devices connected to the security system.

ASF

Advanced Systems Format; Microsoft Windows media audio and video format.

ATM

Automatic Teller Machine

Authorization Number

Number that you receive from Bosch for the software licenses you have ordered. You must enter the Authorization Number in the Bosch Security System Software License Manager to obtain the Activation Key. Additionally you need the computer signature to activate the purchased licenses.

B-frame

Bidirectional frame. Part of a video compression method.

BIS

Building Integration System

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.

BRS

Bosch Recording Station. Video recording and management software.

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.

CCL emulation

Emulation of the Command Console Language used for controlling an Allegiant matrix. You can use this set of commands to switch a BVMS IP camera / encoder to a BVMS IP decoder. You cannot control old analog cameras or the Allegiant matrix itself directly.

Command Script

Macro, that the administrator can program to build an automatic action like positioning a PTZ camera or send E-mails. For that functionality Bosch Video Management System provides a specific set of commands. Command Scripts are divided into Client Scripts and Server Scripts. Client Scripts are used on client workstations to execute certain tasks that can run on a client workstation. Server Scripts are executed

automatically by an event that was triggered in the system. They get arguments provided by the event like date and time. A Command Script can consist of several scriptlets. You can create a Command Script using the following scripting languages: C#, VB.Net. Command Scripts are executed in response to events or alarms automatically according to a schedule (Server Scripts only), manually from the Logical Tree, or manually from icons or on maps.

Compound Event

Combination of different events. The combination uses Boolean expressions, i.e. AND and OR. You can combine only state changes, for example the change of a connection state to disconnected or the activation of a schedule.

debounce time

Time period starting with the occurrence of an event. During this time period usually no other event of the same type is accepted. This prevents for example that a switching sensor creates a large number of events. For events with several states, you can configure a different priority setting for each state. The following examples help you in getting a deeper understanding of the concept of debounce time. Example 1 deals with events creating the same state: The System Info event occurs and the configured debounce time starts. During this time another System Info event occurs. This System Info event is not accepted as a new event. Example 2 deals with events creating different states with the same priority: A Motion Detected event occurs and the configured debounce time starts. During this time, the Motion Stopped event with the same priority occurs. The Motion Stopped event is not accepted as a new event. Example 3 also deals with events creating different states with the same priority: The state of a virtual input is on. The state priorities for both state changes are identical. At a specific point in time, the virtual input is switched off, the debounce time is started. During this debounce time the virtual input is switched on. This state change is not accepted as a new event because it has the same priority. After the debounce time has elapsed, the virtual input is in another state. The switch-on gets the time stamp of the end of the debounce time and no new debounce time starts. Example 4 deals with events with different priorities creating different states: The Motion Detected event occurs and the configured debounce time starts. During this time the Motion Stopped event with a higher priority occurs. The Motion Stopped event is accepted as a new event but the debounce time does not start again. Example 5 also deals with events with different priorities creating different states: The state of a virtual input is off. The state priority for switched on is "5", for switched off is "2". At a specific point in time, the virtual input is switched on (prio "5"), the debounce time is started. During this debounce time the virtual input is switched off (prio "2"). This state change is accepted as a new event because it has a higher priority. The debounce time of the first switch-on is continued. Further state changes are not accepted during this debounce time.

decoder

Changes a digital stream to an analog stream.

Device Family

Bosch encoders / IP cameras can belong to one of the following device families: Device Family 1, Device Family 2, Device Family 3. Devices of Device Family 1 can only record stream 1. Devices of Device Family 2 can record stream 1 or stream 2. Devices of Device Family 3 can record stream 1, stream 2 or I-Frame only.

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.

Dual streaming

Dual streaming allows an incoming data stream to be encoded simultaneously according to two different, individually configured settings. This creates two data streams: one for live and pre-event recording, the other for continuous, motion, and alarm recording.

duplex

Term used to define the direction of data transmission between two parties. Half-duplex allows data transmission in both directions but not simultaneously. Full-duplex allows simultaneous data transmission.

DVR

Digital Video Recorder

Dwell time

Preset amount of time a camera is displayed in an Image window until the next camera is displayed during a camera sequence.

DWF

Design Web Format. Used to display technical drawings on a computer monitor.

DynDNS

Dynamic Domain Name System. A DNS host service that holds IP addresses ready in a database. Dynamic DNS allows you to connect to the device via the Internet using the host name of the device. See DNS.

Edge dewarping

Dewarping performed in the camera itself.

Encoder

Changes an analog stream to a digital stream, e.g., to integrate analog cameras in a digital system like Bosch Video Management System. Some encoders can have a local storage like a flash card, a USB hard disk, or they can store their video data on iSCSI devices. IP cameras have an encoder built in.

Enterprise Access

Enterprise Access is a feature of BVMS which consists of one or more Enterprise Accounts. Each Enterprise Account contains device permissions to devices of a particular Management Server.

Enterprise Account

Enterprise Account is an authorization that enables a user of Operator Client to connect to the devices of a Management Server being part of an Enterprise System. In an Enterprise Account, all permissions for the devices of this Management Server are configured. Operator Client can simultaneously connect to all Management Server computers that are part of this Enterprise System. This access is either controlled by the membership to an Enterprise User Group, and is controlled by the device permissions configured in the Enterprise Account for this Management Server.

Enterprise Management Server

Enterprise Management Server is a BVMS Management Server hosting the configuration of Enterprise User groups. You need one or more

Enterprise User Groups referring to one or more servers computers. The roles of Enterprise Management Server and Management Server can be combined in one configuration.

Enterprise System

Enterprise System is a feature of Bosch Video Management System that allows a user of Operator Client to access multiple Management Server computers simultaneously.

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.

Event

A circumstance or state that is linked to an alarm and/or an action. Events can arise from many sources such as cameras, archivers, directories, digital inputs, etc. They can include start-recording states, loss of signal states, disk full messages, user logons, digital input triggers, etc.

Failover VRM

Software in the BVMS environment. Takes over the task of the assigned Primary VRM or Secondary VRM in case of failure.

GSM

Global System for Mobile Communication. Standard for digital mobile phones.

H.264

Standard for encoding (compressing) digital audio and video for multimedia applications. This standard includes different profiles that can be manufacturer-dependent. The following profiles are available: Baseline, Baseline+, Main Profile. Baseline (not used in Bosch Video Management System) supports 2 CIF. Baseline+ supports 4 CIF and provides a better image quality than Baseline. Main Profile supports 4 CIF and provides a high efficient compression algorithm called CABAC (Context-adaptive binary arithmetic coding). This serves for high quality encoding for storage.

H.265

H.265 is a video compression standard defined by ISO2 and ITU3 and ratified on the 29th of October, 2014. It is seen as the successor of MPEG-4 AVC (Advanced Video Codec), also called H.264, to address the compression of resolutions from 4K and ultra HD up to 36 megapixels.

Hotspot

Mouse sensitive icon on a map. Hotspots are configured in Configuration Client. Hotspots can be for example cameras, relays, inputs. The operator uses it for localizing and selecting a device in a building. If configured, hotspots can display a blinking background color when a specific state event or alarm occurs.

I-frame

Intra frame. Part of a video compression method. Contains the information of a complete image, unlike P- or B-frames that contain information of the changes compared to the previous or next frame.

Image pane

Used for displaying live and recorded video of a single camera, a map, or an HTML file.

Image pane bar

Toolbar of an Image pane.

Image window

Container for Image panes, structured by an Image window pattern.

Instant playback

Plays the recorded image of the selected camera in an Image pane on the live screen. The start time (number of seconds in the past, or rewind time) can be configured.

Intelligent Tracking

Intelligent Tracking is a software process running on a camera that allows the camera to follow a selected object.

Intercom functionality

Used to talk on the loudspeakers of an encoder. This encoder must have audio-in and audio-out. The Intercom functionality can be granted per user group.

intrusion control panel

Generic name for the core device in a Bosch intrusion (burglary) security system. Keypads, modules, detectors, and other devices connect to the control panel.

IPS

Images per second. Number of video images transmitted or recorded per second.

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.

JPEG

Joint Photographic Expert Group

JPEG

Joint Photographic Experts Group. Encoding process for still images.

LDAP

Lightweight Directory Access Protocol. Network protocol running over TCP / IP that allows accessing directories. A directory can be for example a list of user groups and their access rights. Bosch Video Management System uses it to get access to the same user groups as MS Windows or another enterprise user management system.

Live Mode

Logbook

Container for logging all events in Bosch Video Management System.

Logical number

Logical numbers are unique IDs assigned to each device in the system for ease of reference. Logical numbers are only unique within a particular device type. Typical use of logical numbers are Command Scripts.

Logical Tree

Tree with a customized structure of all the devices. The Logical Tree is used in the Operator Client to select cameras and other devices. In the Configuration Client, the "Full Logical Tree" is configured (on the Maps and Structure page) and tailored for each user group (on the User Groups page).

LUN

Logical Unit Number. Used in the iSCSI environment to address an individual disk drive or a virtual partition (volume). The partition is part of a RAID disk array (the iSCSI target).

Management Server

BVMS server managing devices.

Master Control Software

Software used as interface between Bosch Video Management System and an Allegiant device. Version 2.8 or greater is used.

MHT

Also called 'Web Archive'. File format that can save all HTML and image files of an Internet site in one file. To avoid problems we recommend to create MHT files with Internet Explorer 7.0 or higher only.

Mirrored VRM

Software in the BVMS environment. Special case of a Secondary VRM. Ensures that the recording performed by a Primary VRMs is additionally and simultaneously performed to another iSCSI target with the same recording settings.

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.

MOV

File extension of the default video format used by QuickTime Player from Apple.

multipath

Technique in computer storage to have multiple physical paths defined that connect the data server to one storage target (using different controllers, buses switches or the like) as failover or load balancing solution (redundancy, efficiency).

multipathing

Usage of computer storage multipath technique.

Network monitoring

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

No-touch deployment

Method for automatic downloading, installing and running .NET applications without changing the registry or shared system components. With Bosch Video Management System, no-touch deployment is used for updating the Operator Clients from the Management Server. The update takes place if a new version is stored on the Management Server and when each user is logging on to the Operator Client. If you work with one Operator Client against multiple Management Server computers, no-touch deployment uses only the software version stored on the Management Server where the Operator Client has last logged on successfully. When you try to log on to another Management Server with a different application version, this one displays the Management Server as not online because the software versions do not match.

NVR

Bosch Network Video Recorder; computer in the Bosch Video Management System storing audio and video data, acting as Failover NVR, or as Redundant NVR. This NVR is different from the VIDOS NVR which can be integrated in Bosch Video Management System.

OID

Object Identifier. Term in the SNMP environment. Determines a MIB variable.

ONVIF

Open Network Video Interface Forum. Global standard for network video products. ONVIF conformant devices are able to exchange live video, audio, metadata, and control information and ensure that they are automatically discovered and connected to network applications such as video management systems.

Operator Client

Component of Bosch Video Management System that provides the user interface for system monitoring and operation.

Operator Client workstation

Computer in the Bosch Video Management System environment for viewing live and playback video and for configuration tasks. Operator Client is installed on this computer.

Panoramic camera

Camera with a 360° or 180° view angle.

P-frame

Predicted frame. Part of a video compression method.

PID

Person identification device. It extracts characteristics of a person from an image, for example the face. It runs special algorithms that are able to identify a person within a video stream.

point

A detection device connected to the security system. Points show on the keypad individually and with custom text. The text might describe a single door, motion sensor, smoke detector, or an protected space such as UPSTAIRS or GARAGE.

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).

Port mapping

Port mapping allows remote computers to connect to a specific computer or service within a private local area network (LAN).

POS

Point of sale.

Primary VRM

Synonym for VRM.

PTZ camera

Camera with pan, tilt, and zoom function.

RAID

Redundant array of independent disks. Used for organizing two or more hard disks as if they were one drive. On such a drive data is shared or replicated. This is used to achieve greater capacity, reliability, and speed.

RCP

Remote Control Protocol

Recording Schedule

Used for scheduling recording and for scheduling some events like starting backup or limiting log on. Recording Schedules cannot have gaps or overlaps. It also determines the video recording quality.

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.

Remote access

Remote access allows to connect different private networks to public networks. Multiple networks with private (local) network addresses can be accessed simultaneously or sequentially by Operator Client computers via public interfaces (routers). Task of the router is to translate the incoming public network traffic to the corresponding private network address. The users of Operator Client can access Management Server or Enterprise Management Server and their devices via remote access.

Rewind time

Number of seconds when an Image pane is switched to instant playback.

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.

RTP

Real-Time Transport Protocol; a transmission protocol for real-time video and audio

RTSP

Real Time Streaming Protocol. A network protocol which allows to control the continuous transmission of audio-visual data or software over IP-based networks.

scopes

Scope is a term used in the field of ONVIF cameras. It is a parameter used for probing an ONVIF device. Usually the parameter contains a URI like the following: onvif://www.onvif.org/

<path>. The parameter <path> can be for example video_encoder or audio_encoder. One ONVIF device can have multiple scopes. This URI denominates the task area of the device.

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.

Server Lookup

Access method for a user of Configuration Client or Operator Client to sequentially connect to multiple system access points. A system access point can be a Management Server or an Enterprise Management Server.

Skimming

Sabotage of a foyer card reader. A skimming device reads the card data of the magnetic stripe without the knowledge of the cardholder.

SNMP

Simple Network Management Protocol. IP based protocol that allows to get information from networking devices (GET), to set parameters on network devices (SET) and to be notified about certain events (EVENT).

Task Schedule

Used for scheduling events which can occur in Bosch Video Management System, for example executing a Command Script. In Events you assign Task Schedules to events. For scheduling events you can also use Recording Schedules. With a standard Task Schedule you configure time periods for every day of the week, for holidays, and for exception days. With a recurring Task Schedule you configure recurring time periods. They can recur every day, every week, every month, or every year.

TCP

Transmission Control Protocol

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.

Trap

Term in the SNMP environment for an unrequested message from a monitored device (agent) to the network monitoring system (manager) about an event in this device.

Trunk line

Analog outputs of an analog matrix that are connected to an encoder device. Thereby matrix video sources can be used in the Bosch Video Management System.

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.

URI

Uniform Resource Identifier. String for identifying a network resorce. Each URI consists of scheme, authority, path, query, fragment. Only scheme and fragment are mandatory for Mobile Video Service. Example: http:<scheme>// example.com<authority>/over/therepath>? name=ferret<query>#nose<fragment>

URL

Uniform Resource Locator

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.

VCA

Video content analysis: computer analyis of video streams to determine what is happening at the scene being monitored. See also Intelligent Video Analytics

Video Analytics

Video analytics is a software process that compares a camera image with the stored images of specific persons or objects. In case of a match, the software triggers an alarm.

Video resolution

Specification of horizontal and vertical pixels transferred with video signals. PAL: 1CIF = 352 x 288 2CIF = 704 x 288 4CIF = 704 x 576 QCIF = 176 x 144 NTSC 1CIF = 352 x 240 2CIF = 704 x 240 4CIF = 704 x480 QCIF = 176 x120 HD 720p = encoded 1280 x 720 1080p = encoded 1920 x 1080

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.

WAN

Wide Area Network.

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

Access control systems 173
access denied
  Allegiant CCL emulation 165
accessing the Help 14
acquire PTZ control 344
activate 103
  Bosch Video Management System 86
  previous configuration 104
activation 106
  configuration 103
  delayed 103, 114
add Bosch Allegiant input alarm 109
add Bosch ATM/POS bridge 108
add BVIP decoder 143, 185, 212
add BVIP encoder 45, 143, 145, 185, 211, 212, 221
add encoder 182, 190, 218, 347
add pool
  VRM 180
add text data to continuous recording 299
add unmanaged site 214, 215, 216
add video analytics device 169
add VRM 175
additional data
  text data 48
alarm map 301
alarm priority 344
alarm recording 301, 313, 314
alarm recording mode 279, 289
alarm sequence 301, 313
alarms
  sort order 301
Allegiant
  CCL emulation 127, 166
  control channel 68, 70
  firmware version 61, 62
  Network Host program 69
  PTZ camera 278
  Satellite System 70
  too many cameras 353
Allegiant CCL commands 70
Allegiant CCL emulation 165
  access denied 165
Allegiant CCL Emulation page 165
Allegiant file 353
Allegiant matrix 126, 137
all-in-one system 23
analog matrix 137
analog monitor group 122, 126
ANR 94, 226, 278
ASF 327
aspect ratio 16/9 330
ATM POS device 126
Audio Intercom functionality 328
automatic alarm popup behavior 44
automatic display of alarms 44
automatic logoff 123
automatic recording mode 184
automatic relogon 103
automatic restart 103

B

basic configuration 196
blinking device icons 296, 315
Bosch IntuiKey keyboard 61, 62, 63, 65, 126, 139, 148, 162
Bosch Script API help 100
Bosch Video Management System 16
  activate 86
  GUI language 352
  licensing 86
  Online Help 14
  overview 16
  update 351
BVIP decoder 92, 220
  add 143, 185, 212
BVIP device
  password 146, 217, 224
  Web page 218
BVIP encoder 92, 220
  add 45, 143, 185, 211, 212
BVIP encoder:add 145, 221
bypass
  point 329

C

CABAC 285
camera round 254, 257, 262
camera sequence 254, 257, 262
CCL emulation 166
CCTV keyboard 162
  connection loss 352
change IP address 125, 143, 227
change network address 143, 227
change password 146, 180, 217, 224, 320
change pool 225
CHAP password 178

chattering sensors 312
Client Command Script
alarm accepted 305
executed on startup 101, 102, 141
CLL commands 165
codecs 289
Command Script 254, 262
Bosch Script API help 100
export 101
import 101
Commercial Type Number 119
Compatibility Mode 51
Compound Events 295, 310
configuration data
export 104
configuration data to OPC
export 105
Configuration Wizard
Mobile Video Service 23
configure VRM recording 109
connecting
Allegiant matrix and BVMS 66
Bosch IntuiKey keyboard and BVMS 63
connection string 122
control of a camera 110, 289
copy and paste 287
crash
Configuration Client 353
Operator Client 353
create
Command Script 100
customized events 295, 310

D

data sheet 18
DCZ keyboard 162
decoder
Bosch IntuiKey keyboard 148
decoder:destination password 213, 223
decoupled 49
default configuration 196
default IP address 115
default password 103, 115
default stream 139, 277
delayed activation 103, 114
delete user 320
destination password 213, 223
device capabilities
update 92, 220
device monitor 106
device replacement 88, 89
Device Tree 125, 177, 254
Devices pane 254
devices without password protection 103
DiBos
version 61, 62
DiBos device 126
digital keyboard 162
digital video recorder 126
disable enforced password protection 115
disconnected 49
dome camera 285, 291
DSA E-Series 189, 190, 194, 195
DTP3N 157
dual authorization 321
dual recording 32, 191, 294
dual streaming 141
duplicate IP addresses 115
duplicating an event 309
DVR device 134
DynDNS 29

E

E-mail device 126
empty password 103
encoder
add 182, 190, 218, 347
Web page 218
encoder:failover recording mode 229
encoding on NVRs 125, 177
enforced password protection 115
Enterprise Management Server 332
Enterprise System 25, 96
examples 108
add Bosch Allegiant input alarm 109
add Bosch ATM/POS bridge 108
configure VRM recording 109
exception days 273
export
ASF 327
Camera Table 288
Command Script 101
configuration data 104
configuration data to OPC 105

F

failover recording mode 184
encoder 229
Failover VRM 32, 128, 181

filtering 116, 117, 125, 126, 255, 276, 295, 298, 300, 318
finding
devices 116, 117, 125, 126, 255, 276, 295, 298, 300, 318
information in the Help 14
fire detection camera 346
Firewall 205
firmware upgrade
Bosch IntuiKey keyboard 65
Forensic Search 110, 139, 140, 142

G

global alarm settings 312
global default password 82, 103, 115
GUI language 352

H

H.264 285
H.264 deblocking filter 285
HD cameras 330
help 14
holidays 273
hotspots 254
HTML files 254

I

I/O modules 126
import
Command Script 101
resource files 261
inactivity 123
Independent Operator Client 48
initial camera 150
Intercom functionality 328
interface settings
VIP XD 148
intrusion panel 167, 168
IntuiKey keyboard 162
IP address
change 125, 143, 227
duplicates 115
iPad 166, 167
iPhone 166, 167
IQN mapping 196
iSCSI device 196
iSCSI password 178
iSCSI storage pool 174, 192
iSCSI storage system 192

K

KBD Universal XF keyboard 61, 62, 126, 139

L

language 352
Configuration Client 122
Operator Client 319
large LUN 184, 188, 194, 199, 200
Large LUNs 184
licensing
Bosch Video Management System 86
Config Wizard 82
Stratus server 86
link to map 265
Logbook database 122
connection string 122
logging 179, 309, 312
logging ONVIF events 359
Logical Tree 260, 305
LUNS
larger than 2 TB 184

M

malfunction relay 47
Management Server 18, 25, 49
manual recording 51, 301, 313
map
blinking hot spots 296, 315
map link 265
maps 254
menu commands 112
MIC IP 7000 350
Mobile Video Service 23, 166
monitor group 149, 301, 305
add 149
initial camera 149
OSD 149
quad view 149
single view 149
startup camera 149
move device 199, 209, 225
multi monitor mode 330
multicast 205
multi-select 260

N

network address
change 143, 227
network monitoring device 126
new DiBos devices 133, 135, 136
no password 103
NVR 18

O

offline 49, 320

Offline Mode 48
online application Help 14
ONVIF logging 359
ONVIF Media profile 277
OPC Server 351
Operator Client 17, 260

P

panoramic camera
viewing modes 53
password 146, 217, 224
password change 146, 180, 217, 224, 320
password missing 103
peripheral device 126
permissions 254, 260
Person identification
Add cameras to person identification device 171
Adding a person identification device 170
Person identification device 170
point
bypass 329
pool
change 225
move device 199, 209, 225
VRM 180, 225
pooling 174, 192
port forwarding 29
port mapping 29, 123
post-alarm time 279
post-event time 279, 289
post-event time 281
pre-alarm time 279
pre-event time 279, 289
pre-event time 281
previous configuration 104
Primary Failover VRM 181
Primary VRM 32, 128, 176
printing the Help 14
profile 283
protect alarm recording 314
PTZ blocking 323, 330, 344
PTZ camera 285, 291
Allegiant 278
PTZ control
blocking 323, 330, 344
push-to-talk 328

Q

quad view 149

R

RAM recording 279
recording mode
automatic 184
failover 184
Recording preferences 230
recording quality 283
recording settings 20
Recording Table 276
redundant recording 32
Redundant VRM 32, 128, 181
refresh states 112, 116, 117, 125
Region of Interest 45, 278, 292, 322
relay
malfunction 47
Release Notes 18
remote access 29, 96, 123, 130
Remote export 51
remove prepositions 291
remove user 320
replace content 261
resource files 261
import 261
ROI 45, 278, 292, 322
routed access 129

S

scan
across subnets 122
encoders 128
in subnets 122
live only encoders 128
local storage encoders 128
VRM 128
scan for conflicting IP addresses 115
scheduled recording settings 20
Secondary Failover VRM 181
secondary recording 191, 294
Secondary VRM 32, 128, 176
sequence 257
Server ID 89
Server initiator name 178
Server List
add columns 97, 130
delete columns 97, 130
Server Lookup 130
Server Network 214, 215, 216
silence bells 329
SMS device 126

SNMP settings 121
SNMP traps
get 121
send 121
software update 351
sort order
alarms 301
states 112, 116, 117, 125
status 106
Stratus server
licensing 86
stream 277, 281
switch off alarm sirens 329
synchronization 94
synchronize
VRM configuration 184
system requirements 18

T

Target data rate 284
time server 94
time synchronization 94
time zone 214, 215
too many Allegiant cameras 353
transcoding service 166, 167
trigger text data recording 314

U

UHD cameras 142
unreliable network 166
update 351
device capabilities 92, 220
user
delete 320
remove 320
user event button 309, 310

V

verify authenticity 222
video analytics 169
Video Streaming Gateway 126
VIDEOJET 7000 connect 350
viewing modes of panoramic camera 53
VIP X1600 XFM4 285
VIP XD 61
half-duplex mode 148
interface settings 148
quad view 149
virtual input 126
VPN 29
VRM
add 175
add pool 180
Failover 32, 128, 181
pool 180, 225
Primary 32, 128, 176
Primary Failover 181
Redundant 32, 128, 181
Secondary 32, 128, 176
Secondary Failover 181
VRM 3.50 184
VRM storage pool 174, 192

W

WAN 29, 123
Web client 167
WLAN 166, 167
workstation 122

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Netherlands
www.boschsecurity.com
© Bosch Security Systems B.V., 2019