Bosch Video Management System

BOSCH

en Configuration Manual

Table of contents

1 Using the Help 15
1.1 Finding information 15
1.2 Printing the Help 15
2 Introduction 17
3 System overview 20
3.1 Hardware requirements 20
3.2 Software requirements 21
3.3 License requirements 21
3.4 Supported system structures 21
4 Concepts 23
4.1 Recording settings 23
4.1.1 Basic stream settings (schedule-independent) 23
4.1.2 Stream assignment for Live 23
4.1.3 Scheduled Recording Settings 23
4.2 Config Wizard 26
4.3 Enterprise System 26
4.3.1 Scenarios 27
4.3.2 Permissions 30
4.3.3 Types of user groups 31
4.3.4 Licensing 31
4.4 Unmanaged site 31
4.4.1 Structure of CSV file for importing unmanaged sites 32
4.5 Server Lookup 33
4.5.1 Server List 35
4.6 Remote access 35
4.7 iSCSI storage pool 38
4.8 Automated Network Replenishment (ANR) 38
4.9 Dual / failover recording 40
4.10 VRM recording modes 41
4.11 Playback of VRM recording sources 44
4.12 Alarm handling 50
4.13 DVR devices 52
4.14 Mobile Video Service 53
4.15 Adding Video IP devices from Bosch 53
4.16 Region of Interest (ROI) 54
4.17 Intelligent Tracking 54
4.18 Inactivity logoff 55
4.19 Malfunction relay 55
4.20 Text data 56
4.21 Allegiant CCL commands 57
4.22 Offline Operator Client 57
4.22.1 Working with Offline Mode 57
4.23 Version independent Operator Client 60
4.23.1 Working with Compatibility Mode 60
4.24 ONVIF events 60
4.25 Viewing modes of a panoramic camera 61
4.25.1 360° panoramic camera - floor- or ceiling mounted 62
4.25.2 180° panoramic camera - floor- or ceiling mounted 63

4.25.3 360° panoramic camera - wall mounted 64
4.25.4 180° panoramic camera - wall mounted 65
4.25.5 Cropped view on a panoramic camera 66
4.26 Server-based analytics 67
4.26.1 Installing the analytics viewer application 68
5 Supported hardware 69
5.1 Installing hardware 70
5.2 Installing a KBD Universal XF keyboard 70
5.3 Connecting a Bosch IntuiKey keyboard to Bosch VMS 71
5.3.1 Scenarios for Bosch IntuiKey keyboard connections 71
5.3.2 Connecting a Bosch IntuiKey keyboard to a decoder 72
5.3.3 Updating Bosch IntuiKey keyboard firmware 73
5.4 Connecting Bosch Allegiant Matrix to Bosch Video Management System 74
5.4.1 Bosch Allegiant Connection Overview 74
5.4.2 Configuring the control channel 76
5.4.3 Bosch Allegiant Satellite System Concept 78
5.5 Allegiant CCL commands supported in Bosch VMS 78
6 Getting started 81
6.1 Installing the software modules 81
6.2 Scanning for devices 81
6.3 Using Config Wizard 85
6.4 Accessing the system 95
6.5 Using Server Lookup 96
6.6 Configuring remote access 96
6.6.1 Configuring without Enterprise System 96
6.6.2 Configuring with Enterprise System 96
6.7 Activating the software licenses 97
6.8 Starting Configuration Client 98
6.9 Configuring the language of Configuration Client 98
6.10 Configuring the language of Operator Client 98
6.11 Adding a new license 98
6.12 Maintaining Bosch VMS 99
6.13 Replacing a device 100
6.13.1 Replacing a MS / EMS 100
6.13.2 Replacing a VRM 101
6.13.3 Replacing an encoder or decoder 102
6.13.4 Replacing an Operator Client 105
6.13.5 Final tests 105
6.13.6 Recovering Divar IP 3000/7000 105
6.14 Configuring time synchronization 105
6.15 Configuring the storage media of an encoder 105
6.16 Creating an Enterprise System 106
6.16.1 Configuring the Server List for Enterprise System 107
6.16.2 Creating an Enterprise User Group 108
6.16.3 Creating an Enterprise Account 109
6.17 Configuring the mounting position of a panoramic camera 110
7 Creating an Enterprise System 112
7.1 Configuring the Server List for Enterprise System 112
7.2 Creating an Enterprise User Group 114

7.3 Creating an Enterprise Account 114

8 Configuring the Server List for Enterprise System 117

9 Configuring Server Lookup 119

9.1 Exporting the Server List 120

9.2 Importing a Server List 120

10 Adding an unmanaged site 121

10.1 Importing a configuration of unmanaged sites 121

11 Managing VRM storage 122

11.1 Synchronizing Bosch VMS configuration 122

11.2 Scanning for VRM devices 122

11.3 Adding a Primary VRM manually 123

11.4 Adding a Secondary VRM manually 123

11.5 Adding a Mirrored VRM manually 124

11.6 Adding a Failover VRM manually 124

11.7 Adding a VRM pool 125

11.8 Adding an iSCSI device 125

11.9 Configuring automatic recording mode on a pool 125

11.10 Adding a DSA E-Series iSCSI device 126

11.11 Configuring an iSCSI device 126

11.12 Moving an iSCSI system to another pool 127

11.13 Adding a LUN 128

11.14 Formatting a LUN 128

11.15 Changing the password of a VRM device 129

11.16 Configuring dual recording in the Device Tree 129

12 Preparing an ONVIF camera 130

13 Managing encoders / decoders 132

13.1 Adding an encoder to a VRM pool 132

13.2 Moving an encoder to another pool 133

13.3 Adding a live only encoder 133

13.4 Adding a local storage encoder 134

13.5 Configuring an encoder / decoder 135

13.6 Updating the device capabilities 135

13.7 Configuring failover recording mode on an encoder 136

13.8 Configuring multiple encoders / decoders 137

13.9 Changing the password of an encoder / decoder 137

13.10 Providing the destination password for a decoder 138

13.11 Configuring the storage media of an encoder 139

13.12 Adding and removing an ONVIF profile 139

13.13 Configuring ONVIF events 140

13.14 Importing an ONVIF Mapping Table file 141

13.15 Exporting an ONVIF Mapping Table file 142

14 Managing Video Streaming Gateway 143

14.1 Adding a Video Streaming Gateway device 143

14.2 Moving a VSG to another pool 144

14.3 Adding a camera to a VSG 144

14.4 Configuring multicast 145

14.5 Configuring logging 145

14.6 Adding and removing an ONVIF profile 146

14.7 Assigning an ONVIF profile 146

14.8 Configuring ONVIF events 147
14.9 Importing an ONVIF Mapping Table file 148
14.10 Exporting an ONVIF Mapping Table file 148
15 Managing various devices 150
15.1 Adding a device manually 150
15.2 Adding a VIDOS NVR 154
15.3 Configuring a decoder for use with a Bosch IntuiKey keyboard 155
15.4 Configuring the integration of a DiBos system 155
15.5 Configuring the integration of a DVR 156
15.6 Configuring a Bosch Allegiant device 157
15.7 Configuring a startup Command Script 157
15.8 Changing the network address of a workstation 157
15.9 Enabling Forensic Search on a workstation 158
15.10 Assigning an analog monitor group to a workstation 158
15.11 Configuring an analog monitor group 158
15.12 Adding a monitor wall 159
15.13 Configuring a communication device 159
15.14 Configuring a peripheral device 159
15.15 Configuring an SNMP trap receiver 160
15.16 Configuring a Bosch IntuiKey keyboard (workstation) 160
15.17 Configuring a Bosch IntuiKey keyboard (decoder) 160
15.18 Configuring an I/O module 161
15.19 Configuring an Allegiant CCL emulation 161
15.20 Adding a Mobile Video Service 162
15.21 Adding a video analytics device 162
16 Configuring video-based fire alarm detection 163
16.1 Configuring a fire detection camera 163
16.2 Adding an encoder to a VRM pool 164
16.3 Adding a live only encoder 164
16.4 Adding a local storage encoder 165
16.5 Configuring a fire event 166
16.6 Configuring a fire alarm 166
17 Configuring MIC IP 7000 connected to a VIDEOJET 7000 connect 167
18 Configuring server-based video analytics 168
18.1 Installing the alarm viewer application 168
18.2 Adding a video analytics device 169
19 Configuring the structure 170
19.1 Configuring the Logical Tree 170
19.2 Adding a device to the Logical Tree 170
19.3 Removing a tree item 170
19.4 Managing resource files 171
19.5 Adding a Command Script 172
19.6 Managing pre-configured camera sequences 172
19.7 Adding a camera sequence 174
19.8 Adding a folder 174
19.9 Adding a map 174
19.10 Adding a link to another map 175
19.11 Assigning a map to a folder 175
19.12 Managing devices on a map 176

19.13 Adding a document 176
19.14 Adding a malfunction relay 177
20 Configuring schedules 178
20.1 Configuring a Recording Schedule 178
20.2 Adding a Task Schedule 179
20.3 Configuring a standard Task Schedule 179
20.4 Configuring a recurring Task Schedule 179
20.5 Removing a Task Schedule 180
20.6 Adding holidays and exception days 180
20.7 Removing holidays and exception days 181
20.8 Renaming a schedule 181
21 Configuring cameras and recording settings 183
21.1 Copying and pasting in tables 183
21.2 Exporting the Camera Table 184
21.3 Configuring stream quality settings 184
21.4 Configuring camera properties 185
21.5 Configuring recording settings (only VRM and Local Storage) 185
21.6 Configuring recording settings (NVR only) 186
21.7 Configuring PTZ port settings 187
21.8 Configuring PTZ camera settings 188
21.9 Configuring the ROI function 188
21.10 Configuring predefined positions for the ROI function 189
21.11 Configuring the ANR function 189
21.12 Configuring dual recording in the Camera Table 189
22 Configuring events and alarms 191
22.1 Copying and pasting in tables 192
22.2 Removing a table row 192
22.3 Managing resource files 192
22.4 Configuring an event 192
22.5 Duplicating an event 193
22.6 Logging user events 193
22.7 Configuring user event buttons 194
22.8 Creating a Compound Event 194
22.9 Editing a Compound Event 195
22.10 Configuring an alarm 196
22.11 Configuring settings for all alarms 196
22.12 Configuring the pre- and post-alarm duration for an alarm 197
22.13 Triggering alarm recording with text data 197
22.14 Adding text data to continous recording 198
22.15 Protecting alarm recording 198
22.16 Configuring blinking hot spots 199
23 Configuring Command Scripts 200
23.1 Managing Command Scripts 200
23.2 Configuring a Command Script to be started automatically 201
23.3 Importing a Command Script 201
23.4 Exporting a Command Script 201
23.5 Configuring a startup Command Script 202
24 Configuring users, permissions and Enterprise Access 203
24.1 Creating a user 203

24.2 Creating a group or account 204
24.3 Creating a dual authorization group 205
24.4 Configuring LDAP settings 205
24.5 Associating an LDAP group 206
24.6 Scheduling user logon permission 206
24.7 Configuring operating permissions 207
24.8 Configuring user interface settings 207
24.9 Configuring permissions for Logical Tree 208
24.10 Configuring permissions for events and alarms 208
24.11 Configuring camera permissions 209
24.12 Configuring decoder permissions 209
24.13 Configuring various priorities 209
24.14 Copying user group permissions 210
25 Managing configuration data 211
25.1 Activating the working configuration 211
25.2 Activating a configuration 212
25.3 Exporting configuration data 212
25.4 Importing configuration data 213
25.5 Exporting configuration data to OPC 213
25.6 Checking the status of your encoders/decoders 214
25.7 Configuring SNMP monitoring 214
25.8 Creating a report 214
26 Configuration examples 215
26.1 Adding a Bosch ATM/POS bridge 215
26.2 Adding a Bosch Allegiant input alarm 216
26.3 Adding and configuring 2 Dinion IP cameras with VRM recording 216
27 Global Configuration Client windows 218
27.1 Configuration window 218
27.2 Menu commands 219
27.3 Activation Manager dialog box 220
27.4 Activate Configuration dialog box 221
27.5 Protect Devices with Global Default Password dialog box 222
27.6 License Manager dialog box 222
27.7 License Activation dialog box 223
27.8 Reports dialog boxes 223
27.8.1 Recording Schedules dialog box 223
27.8.2 Task Schedules dialog box 223
27.8.3 Cameras and Recording Parameters dialog box 223
27.8.4 Stream Quality Settings dialog box 223
27.8.5 Event Settings dialog box 224
27.8.6 Compound Event Settings dialog box 224
27.8.7 Alarm Settings dialog box 224
27.8.8 Configured Users dialog box 224
27.8.9 User Groups and Accounts dialog box 224
27.8.10 Device Permissions dialog box 224
27.8.11 Operating Permissions dialog box 224
27.9 Alarm Settings dialog box 224
27.10 Options dialog box 224
27.11 Remote Access Settings dialog box 225

27.11.1 Port Mapping Table dialog box 226
27.12 Device Monitor dialog box 226
27.13 SNMP Settings dialog box 227
27.14 License Investigator dialog box 228
28 Devices page 229
28.1 Server List / Address Book page 229
28.1.1 Add Server dialog box 230
28.2 Initial Device Scan dialog box 231
28.3 NVR & Decoder Scan dialog box 231
28.4 IP Device Configuration dialog box 231
28.5 Set IP Addresses dialog box 232
28.6 Set Display Names dialog box 233
28.7 NVRs / Failover NVRs / Redundant NVRs page 233
28.8 Vidos NVRs page 233
28.9 DiBos page 233
28.9.1 Add DiBos System dialog box 234
28.9.2 Settings page 234
28.9.3 Cameras page 234
28.9.4 Inputs page 234
28.9.5 Relays page 235
28.10 DVR (Digital Video Recorder) page 235
28.10.1 Add DVR dialog box 235
28.10.2 Settings tab 235
28.10.3 Cameras tab 236
28.10.4 Inputs tab 236
28.10.5 Relays tab 236
28.11 Matrix Switches page 236
28.11.1 Connection page 236
28.11.2 Cameras page 237
28.11.3 Outputs page 237
28.11.4 Inputs page 238
28.12 Workstation page 238
28.12.1 Settings page 238
28.12.2 Assigned Analog Monitor Groups page 240
28.13 Decoders page 240
28.13.1 Add Encoder / Add Decoder dialog box 241
28.13.2 Edit Encoder / Edit Decoder dialog box 241
28.13.3 Enter password dialog box 243
28.14 Analog Monitor Groups page 244
28.14.1 Settings page 244
28.14.2 Advanced Configuration page 245
28.15 Monitor Wall page 246
28.15.1 Add Monitor Wall dialog box 247
28.16 Communication Devices page 247
28.16.1 E-mail/SMTP Server dialog box 248
28.16.2 Add SMS Device dialog box 248
28.16.3 SMTP Server page 248
28.16.4 Send Test E-mail dialog box 249
28.16.5 GSM Settings / SMSC Settings page 249

28.17 POS + ATM page 250
28.17.1 Add Bosch ATM/POS-Bridge dialog box 251
28.17.2 Bosch ATM/POS-Bridge page 251
28.17.3 Inputs page 252
28.17.4 DTP Settings page 252
28.17.5 ATM Settings page 252
28.18 Foyer Card Readers 252
28.18.1 Add Foyer Card Reader dialog box 253
28.18.2 Settings for Foyer Card Reader page 253
28.19 Virtual Inputs page 254
28.19.1 Add Virtual Inputs dialog box 254
28.20 SNMP page 254
28.20.1 Add SNMP dialog box 255
28.20.2 SNMP Trap Receiver page 255
28.20.3 SNMP Trap Logger dialog box 255
28.21 Assign Keyboard page 256
28.22 I/O Modules page 257
28.22.1 ADAM page 257
28.22.2 Inputs page 258
28.22.3 Relays page 258
28.23 Allegiant CCL Emulation page 258
28.24 Mobile Video Service page 259
28.24.1 Add Mobile Video Service dialog box 259
28.25 Intrusion panels page 259
28.25.1 Add Intrusion Panel dialog box 260
28.25.2 Settings page 260
28.26 Video Analytics Settings page 260
28.26.1 Add Video Analytics Device dialog box 261
28.27 Bosch VMS Scan Wizard 261
28.28 VRM Devices page 263
28.28.1 Add VRM dialog box 264
28.28.2 Add Failover VRM dialog box 264
28.29 VRM Settings page 265
28.29.1 SNMP page 265
28.29.2 Accounts page 265
28.29.3 Advanced page 266
28.30 Pool page 266
28.30.1 Add Encoder / Add Decoder dialog box 267
28.30.2 Edit Encoder / Edit Decoder dialog box 268
28.30.3 Change Pool for dialog box 270
28.30.4 Add Streaming Gateway dialog box 270
28.31 iSCSI device page 271
28.31.1 Add iSCSI Device dialog box 271
28.31.2 Add DSA E-Series Device dialog box 271
28.31.3 Load Balancing dialog box 272
28.31.4 Basic Configuration page 272
28.31.5 iqn-Mapper dialog box 274
28.31.6 LUNs page 274
28.31.7 Add LUN dialog box 274

28.32 Video Streaming Gateway device page 274
28.32.1 Multicast tab (Video Streaming Gateway) 275
28.32.2 Advanced tab (Video Streaming Gateway) 275
28.32.3 Add Bosch Encoder dialog box 276
28.32.4 Add ONVIF Encoder dialog box 277
28.32.5 Add JPEG Camera dialog box 278
28.32.6 Add RTSP Encoder dialog box 279
28.33 Live Only page 279
28.34 Local Storage page 280
28.35 Unmanaged Sites page 280
28.35.1 Unmanaged Network Device page 280
28.35.2 Add Unmanaged Network Device dialog box 281
29 Bosch Encoder / Decoder page 282
29.1 Enter password dialog box 282
29.2 Unit Access page 283
29.2.1 Identification / Camera identification 283
29.2.2 Camera name 284
29.2.3 Version information 284
29.3 Date/Time page 284
29.4 Installer / Initialization menu 285
29.4.1 Application variant 285
29.4.2 Base frame rate 285
29.4.3 Camera LED 285
29.4.4 Mirror image 285
29.4.5 Flip image 285
29.4.6 Menu button 285
29.4.7 Heater 285
29.4.8 Reboot device 285
29.4.9 Factory defaults 285
29.4.10 Lens Wizard 285
29.5 Privacy Masks page 285
29.6 Recording Management page 286
29.7 Recording preferences page 287
29.8 Video Input page 287
29.9 Picture settings - Scene mode 289
29.9.1 Current mode 289
29.9.2 Mode ID 289
29.9.3 Copy mode to 289
29.9.4 Restore Mode Defaults 289
29.9.5 Scene mode factory defaults 289
29.9.6 Scene mode factory defaults 289
29.9.7 Scene mode factory defaults 290
29.10 Picture settings - Color 291
29.10.1 White balance 291
29.10.2 White balance 291
29.10.3 White balance 292
29.10.4 White balance 292
29.11 Picture settings - ALC 293
29.11.1 ALC mode 293

29.11.2 ALC level 293
29.11.3 Saturation (av-pk) 293
29.11.4 Exposure/frame rate 293
29.11.5 Day/night 294
29.12 Encoder Regions page 294
29.13 Camera page 295
29.13.1 ALC 296
29.13.2 Scene mode 298
29.13.3 Scene Mode Scheduler 298
29.13.4 WDR 298
29.13.5 Sharpness level 299
29.13.6 Backlight Compensation 299
29.13.7 Contrast enhancement 299
29.13.8 Intelligent DNR 299
29.13.9 Intelligent defog 299
29.14 Lens page 299
29.14.1 Focus 299
29.14.2 Iris 300
29.14.3 Zoom 300
29.15 PTZ page 300
29.16 Prepositions and Tours page 301
29.17 Sectors page 301
29.18 Misc page 301
29.19 Logs page 301
29.20 Audio page 302
29.21 Relay page 302
29.22 Periphery page 303
29.22.1 COM1 303
29.23 VCA page 304
29.23.1 Motion detector (MOTION+ only) 305
29.23.2 Select Area dialog box 306
29.23.3 Tamper detection 306
29.24 Network Access page 308
29.24.1 JPEG posting 309
29.24.2 FTP server 309
29.25 DynDNS 310
29.25.1 Enable DynDNS 310
29.25.2 Provider 310
29.25.3 Host name 310
29.25.4 User name 310
29.25.5 Password 310
29.25.6 Force registration now 310
29.25.7 Status 310
29.26 Network Management 310
29.26.1 SNMP 310
29.26.2 UPnP 311
29.26.3 Quality of Service 311
29.27 Advanced page 311
29.27.1 SNMP 311

29.27.2 802.1x 312
29.27.3 RTSP 312
29.27.4 UPnP 312
29.27.5 TCP metadata input 312
29.28 Multicast page 312
29.29 Accounts 313
29.30 IP v4 Filter 314
29.31 Licenses page 314
29.32 Decoder page 314
29.32.1 Decoder profile 314
29.32.2 Monitor display 314
30 ONVIF page 316
30.1 ONVIF Encoder page 316
30.2 ONVIF Encoder Events page 317
30.2.1 Add / Rename ONVIF Mapping Table dialog box 318
30.2.2 Import Mapping Table dialog box 319
30.3 ONVIF Configuration page 319
30.3.1 Unit Access 320
30.3.2 Date / Time 320
30.3.3 User Management 321
30.3.4 Video Encoder Profile page 322
30.3.5 Audio Encoder Profile 324
30.3.6 Imaging General 325
30.3.7 Backlight Compensation 325
30.3.8 Exposure 326
30.3.9 Focus 327
30.3.10 Wide Dynamic Range 328
30.3.11 White balance 328
30.3.12 Network Access 329
30.3.13 Scopes 331
30.3.14 Relays 332
30.4 ONVIF Event Source page 332
31 Maps and Structure page 334
31.1 Resource Manager dialog box 335
31.2 Select Resource dialog box 335
31.3 Sequence Builder dialog box 336
31.4 Add Sequence dialog box 337
31.5 Add Sequence Step dialog box 337
31.6 Add URL dialog box 337
31.7 Select Map for Link dialog box 338
31.8 Malfunction Relay dialog box 338
32 Schedules page 339
32.1 Recording Schedules page 339
32.2 Task Schedules page 340
33 Cameras and Recording page 341
33.1 Cameras page 341
33.2 Scheduled Recording Settings dialog box (only VRM and Local Storage) 344
33.3 Recording settings pages (NVR only) 346
33.4 Stream Quality Settings dialog box 347

33.5 PTZ/ROI Settings dialog box 348
34 Events page 350
34.1 Debounce Settings tab 351
34.2 Settings tab for advanced map display 351
34.3 Settings tab for event configuration 352
34.4 Command Script Editor dialog box 352
34.5 Create Compound Event / Edit Compound Event dialog box 353
34.6 Select Script Language dialog box 353
34.7 Edit Priorities of Event Type dialog box 354
34.8 Select Devices dialog box 354
34.9 Text Data Recording dialog box 354
35 Alarms page 355
35.1 Alarm Settings dialog box 356
35.2 Select Image Pane Content dialog box 356
35.3 Select Resource dialog box 357
35.4 Alarm Options dialog box 357
36 User Groups page 361
36.1 New User Group/Enterprise Account dialog box 362
36.2 User Group Properties page 363
36.3 User Properties page 364
36.4 Add New Dual Authorization Group dialog box 365
36.5 Logon Pair Properties page 365
36.6 Select User Groups dialog box 366
36.7 Camera Permissions page 366
36.8 Control Priorities 367
36.9 Copy User Group Permissions dialog box 368
36.10 Decoder Permissions page 368
36.11 Events and Alarms page 369
36.12 LDAP Server Settings dialog box 369
36.13 Credentials page 371
36.14 Logical Tree page 372
36.15 Operator Features page 372
36.16 Priorities page 374
36.17 User Interface page 375
36.18 Server Access page 376
37 Troubleshooting 377
37.1 Configuring the desired language in Windows 379
37.2 Reestablishing the connection to a Bosch IntuiKey keyboard 379
37.3 Reducing the number of Allegiant cameras 379
37.4 Used ports 380
37.5 Enabling logging for ONVIF events 385
Glossary 386
Index 399

1 Using the Help

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

To use the Contents, Index, or Search:

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

To get help on a window or dialog:

- On the toolbar, click ?.

OR

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

1.1 Finding information

You can find information in the Help in several ways.

To find information in the Online Help:

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

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

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

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

Related Topics

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

Concepts, page 23 provides background information on selected issues.

Caution!
Medium risk (without safety alert symbol): Indicates a potentially hazardous situation.
If not avoided, this may result in property damage or risk of damage to the unit.
Cautionary messages should be heeded to help you avoid data loss or damaging the system.

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

1.2 Printing the Help

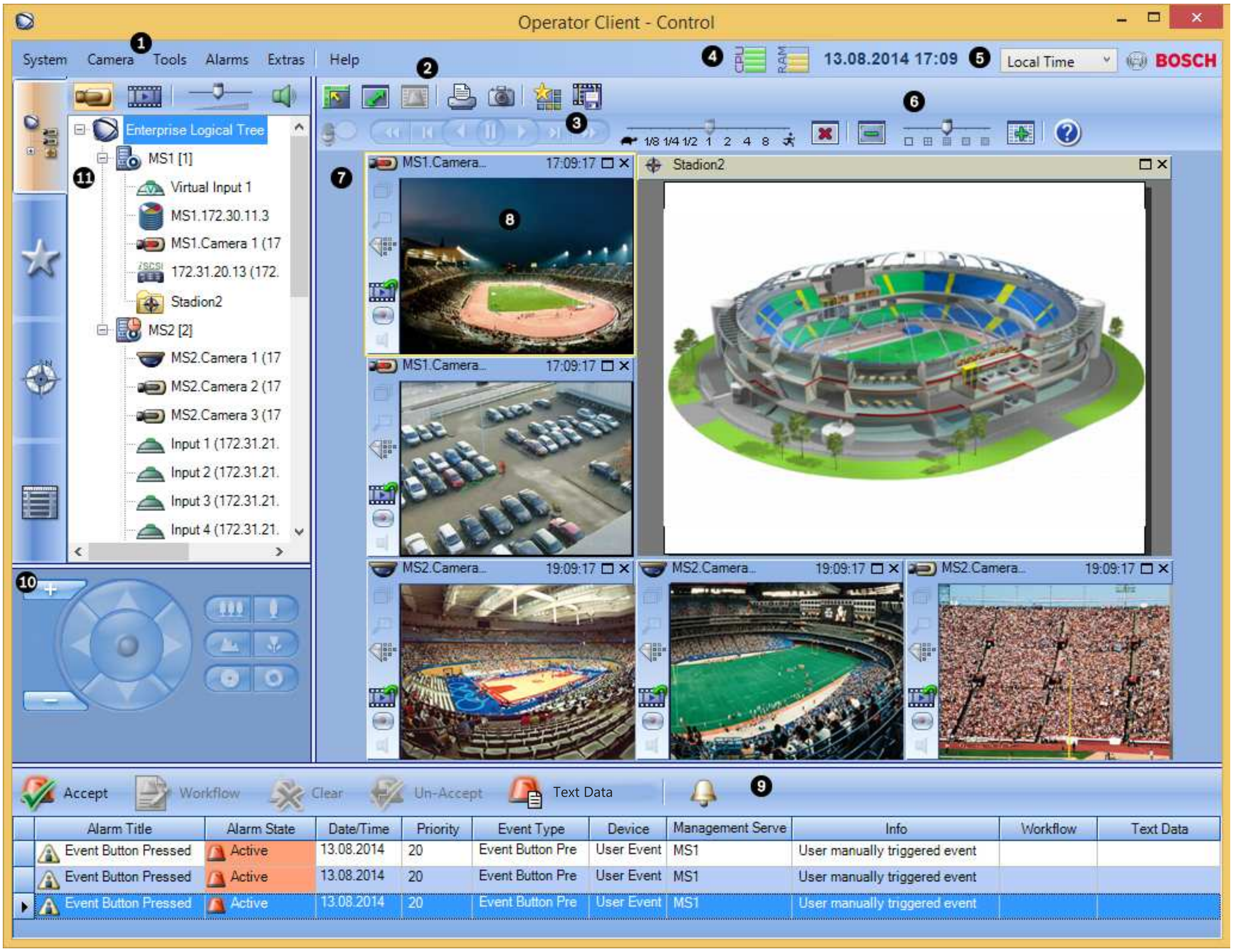
While using the Online Help, you can print topics and information right from the browser window.

To print a Help topic:

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

2 Introduction

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



	Alarm Title	Alarm State	Date/Time	Priority	Event Type	Device	Management Serve	Info	Workflow	Text Data
	Event Button Pressed	Active	13.08.2014	20	Event Button Pre	User Event	MS1	User manually triggered event		
	Event Button Pressed	Active	13.08.2014	20	Event Button Pre	User Event	MS1	User manually triggered event		
▶	Event Button Pressed	Active	13.08.2014	20	Event Button Pre	User Event	MS1	User manually triggered event		

1	Menu bar	Allows you to select a menu command.
2	Toolbar	Displays the available buttons. Point to an icon to display a tooltip.
3	Playback controls	Allows you to control instant playback or a camera sequence or alarm sequence.
4	Performance meter	Displays the CPU usage and the memory usage.
5	Time zone selector	Select an entry for the time zone to be displayed in most time related fields. Only available if at least one Management Server in the Logical Tree is located in another time zone as your Operator Client.
6	Controls for Image panes	Allows you to select the required number of Image panes and to close all Image panes.

7	Image window	Displays the Image panes. Allows you to arrange the Image panes.
8	Image pane	Displays a camera, a map, an image, a document (HTML file).
9	**Alarm List** window	Displays all alarms that the system generates. Allows you to accept or clear an alarm or to start a workflow, for example, by sending an E-mail to a maintenance person. The Alarm List is not being displayed, when the connection to the Management Server is lost.
10	**Monitors** window (only available if at least one analog monitor group has been configured)	Displays the configured analog monitor groups. Allows you to switch to the next or previous analog monitor group if available. **Note:** The **Monitors** tab is not visible if your Operator Client is connected to more than one Management Server.
	PTZ Control window	Allows you to control a PTZ camera.
11	**Logical Tree** window	Displays the devices your user group has access to. Allows you to select a device for assigning it to an Image pane.
	Favorites Tree window	Allows you to organize the devices of the Logical Tree as required.
	Bookmarks window	Allows to manage bookmarks.
	Map window	Displays a site map. Allows you to drag the map to display a particular section of the map. If activated, a map is displayed automatically for each camera displayed in an Image pane. In this case, the camera must be configured on a map.

This manual guides you through the basic steps of the configuration and operation with Bosch VMS.
For detailed help and step-by-step instructions read the Configuration Manual and the User Manual or use the Online Help.
Bosch VMS 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 (VRM recording / DiBos DVRs / iSCSI recording / VIDOS NVRs / local recording)
- 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

Bosch VMS Archive Player displays exported recordings.

3 System overview

If you plan to install and configure Bosch VMS, participate in a system training on Bosch VMS.
Refer to the Release Notes of the current Bosch VMS 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 Bosch VMS can be installed.
The Bosch VMS software modules can optionally be installed on one PC.

Important components

- 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 Bosch VMS 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 Bosch VMS live and playback Image panes to your external third-party application. The Image panes follow the Bosch VMS based user permissions.
  The Cameo SDK provides a subset of the Bosch VMS Operator Client functionalities that enables you to create applications similar to the Operator Client.
- 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 Bosch VMS. Data sheets for platform PCs are also available.

3.2 Software requirements

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

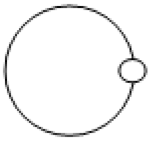
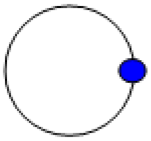
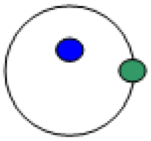
3.3 License requirements

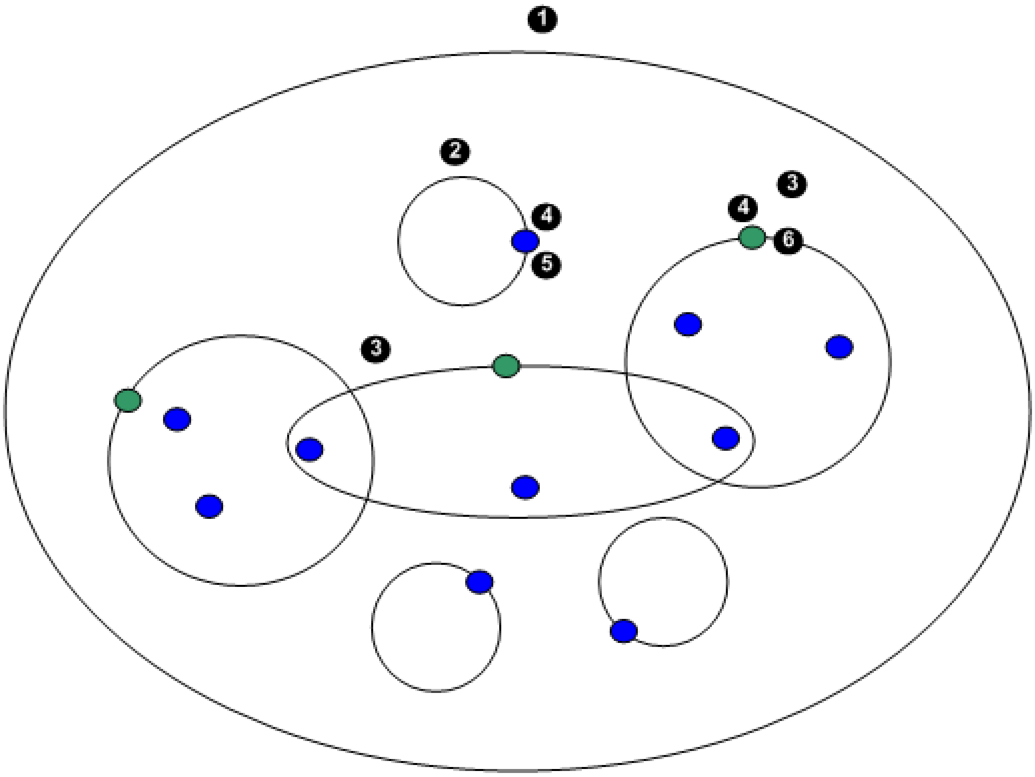
See the data sheet for Bosch VMS for the available licenses.

3.4 Supported system structures

An operator or installer can be responsible for the following system structures:

- Single server system
- Multi server system (Enterprise System)
- Multi system environment

	System with access point for logon
	Single server system, System access point: Management Server
	Enterprise System, System access point: Enterprise Management Server



1	Multi system environment	**4**	System access point: Server on which logon request of an operator or installer is processed.
2	Single server system	**5**	Management Server
3	Multi server system	**6**	Enterprise Management Server

Use cases for multi system access

The following features valid for multi system environments are available:

- Enterprise System
- Server Lookup
- Unmanaged site

An operator might want to access a multi system environment for the following reasons:

- Configure multiple systems (Server Lookup)
- Maintenance and monitoring of multiple systems (Server Lookup)
- Alert (SMS, Email 3rd party) driven on-demand monitoring of multiple systems (Server Lookup)
- Simultaneous connection to multiple servers for seamless operation of one distributed system (Enterprise System)

See also

- *Enterprise System , page 26*
- *Server Lookup , page 33*

4 Concepts

This chapter provides background information on selected issues.

4.1 Recording settings

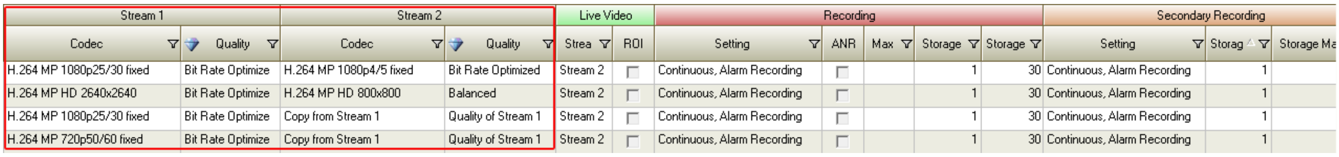
Recording settings in Bosch VMS consist of basic settings (non-scheduled) and scheduled recording settings.

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	

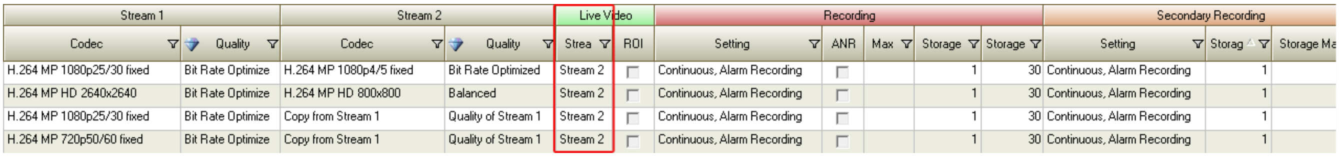
Codecs and HD resolution

Codecs are part of the basic stream settings. Bosch VMS 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	

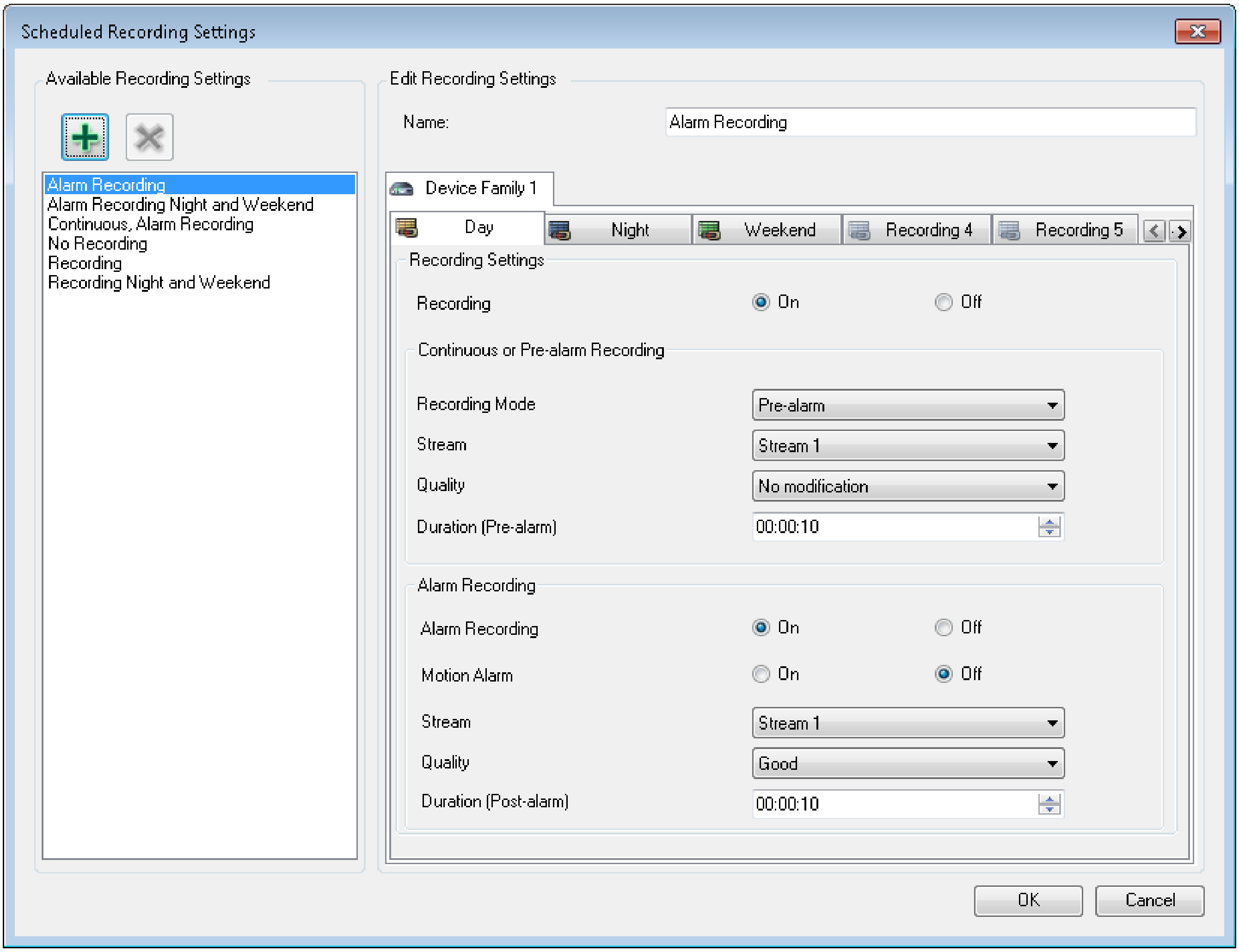
4.1.3 Scheduled Recording Settings

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 Bosch VMS.



Scheduled Recording Settings

Available Recording Settings

- Alarm Recording
- Alarm Recording Night and Weekend
- Continuous, Alarm Recording
- No Recording
- Recording
- Recording Night and Weekend

Edit Recording Settings

Name: Alarm Recording

Device Family 1

Day | Night | Weekend | Recording 4 | Recording 5

Recording Settings

Recording ● On ○ Off

Continuous or Pre-alarm Recording

Recording Mode: Pre-alarm

Stream: Stream 1

Quality: No modification

Duration (Pre-alarm): 00:00:10

Alarm Recording

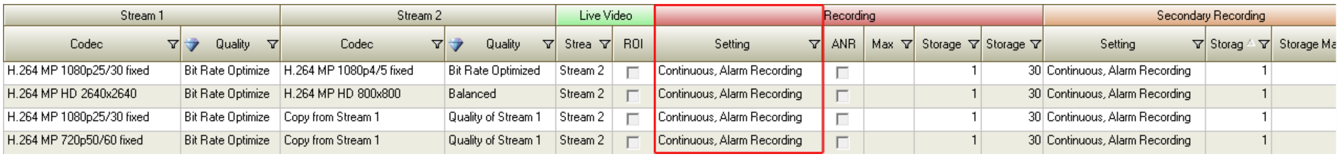
Alarm Recording ● On ○ Off

Motion Alarm ○ On ● Off

Stream: Stream 1

Quality: Good

Duration (Post-alarm): 00:00:10



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. Bosch VMS 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 85*

4.3 Enterprise System

The target of a Bosch VMS Enterprise System is to enable a user of Operator Client to simultaneously access multiple Management Servers.

See also

- *Creating an Enterprise System, page 106*
- *Configuring the Server List for Enterprise System, page 107*

- *Configuring users, permissions and Enterprise Access, page 203*
- *Accessing the system, page 95*

4.3.1 Scenarios

The following three scenarios are covered.

- **Scenario 1**: A dedicated server plays the role of Enterprise Management Server. This server has the only task to manage the simultaneous access of an Operator Client workstation to multiple Management Servers.

An Operator Client workstation logs on to Enterprise Management Server. After successful logon the user of Operator Client has access to the devices of all configured Management Servers according to the permissions in his Enterprise User Group.

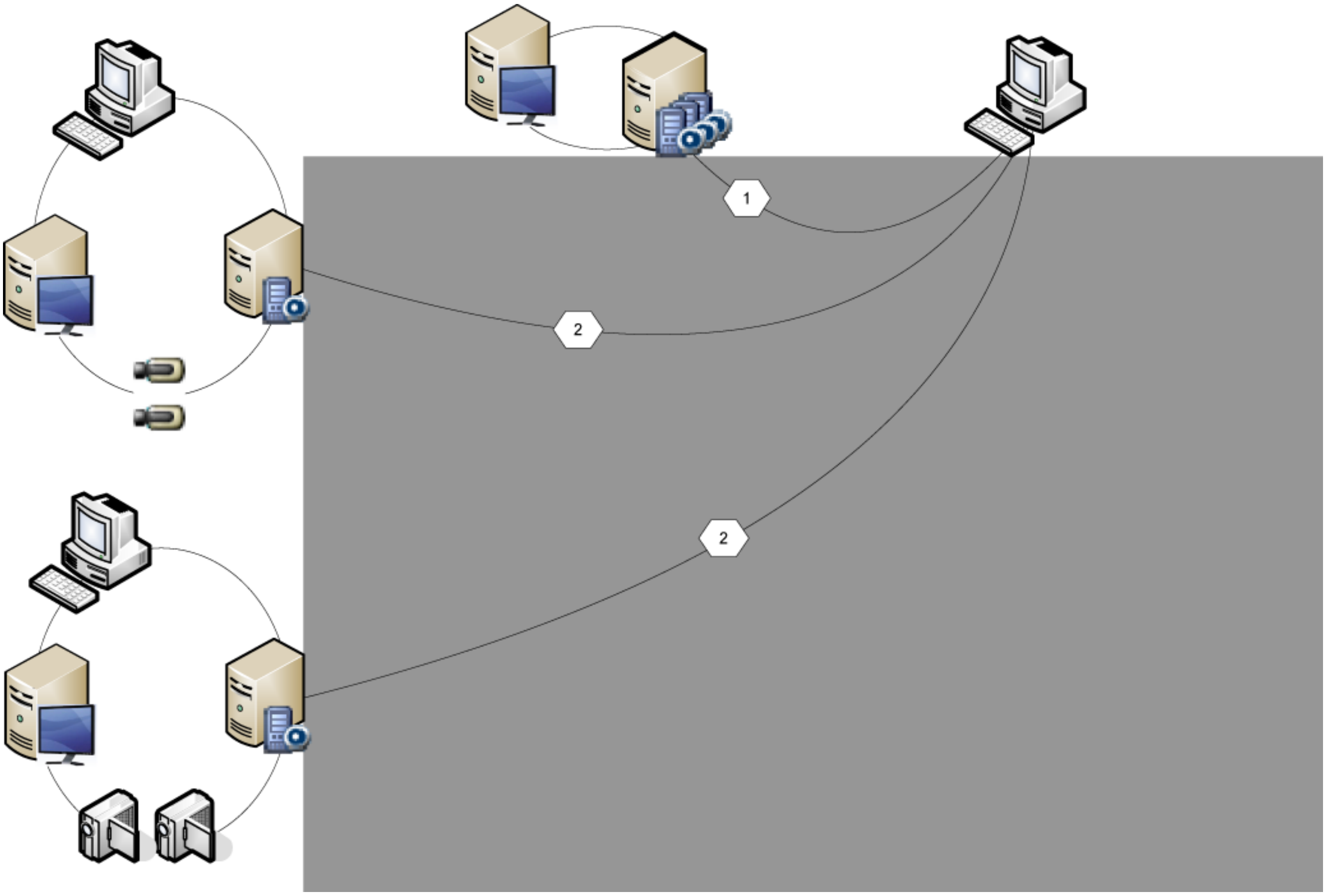


Figure 4.1: Enterprise Scenario 1

	Management Server
	Operator Client

	Configuration Client
	IP camera / encoder
	Enterprise Management Server

- **Scenario 2**: Combination of Enterprise Management Server and Management Server role. In this case the own Management Server must also be part of the Enterprise Management Server configuration.

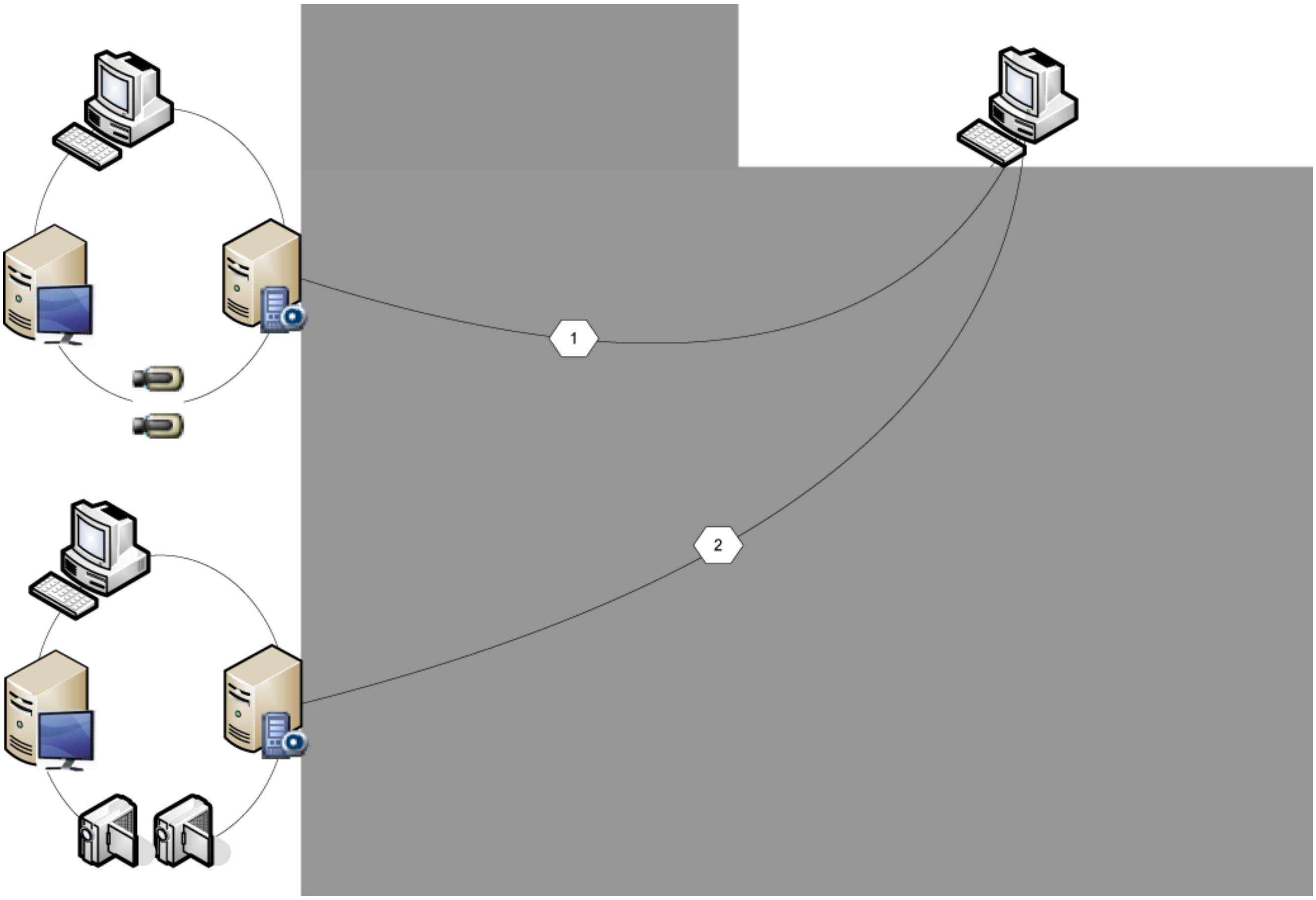
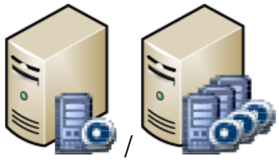


Figure 4.2: Enterprise Scenario 2

	Management Server / Enterprise Management Server
	Operator Client
	Configuration Client
	IP camera / encoder

- **Scenario 3**: The classic client-server architecture remains supported.

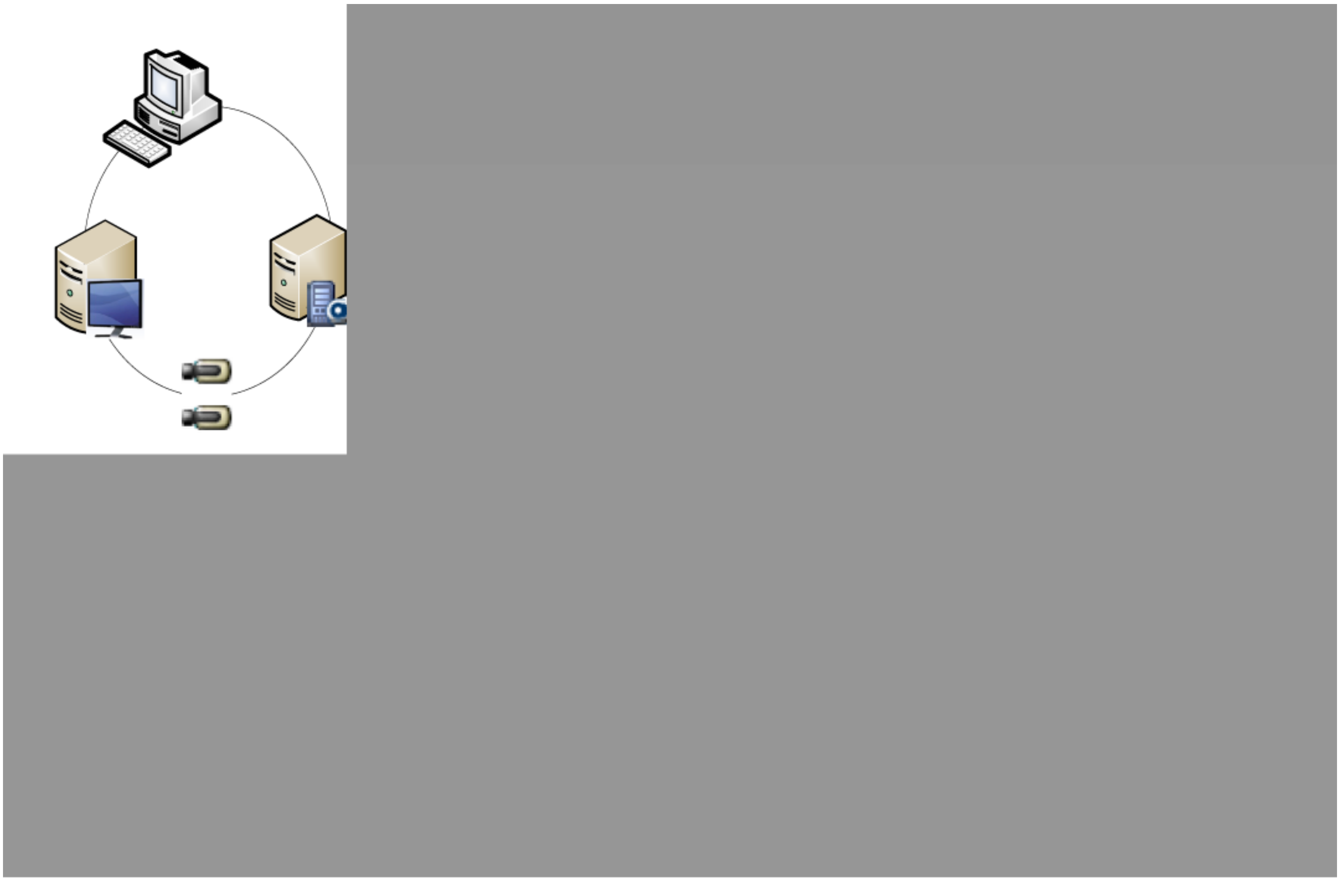


Figure 4.3: Classic Scenario 3

	Management Server
	Operator Client
	Configuration Client
	IP camera / encoder

4.3.2 Permissions

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.

4.3.3 Types of 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

4.3.4 Licensing

Bosch VMS Enterprise (MBV-BENT) version license is required at each Enterprise Management Server to enable the feature.
For each Management Server assigned to one or more Enterprise User Groups, 1 license (MBV-XSUB) is required.
To update an existing MBV-BPRO Base license to an Enterprise System, you need an Enterprise Upgrade license (MBV-FEUP).
Each Workstation connecting to an Enterprise Management Server requests one MBV-XWST that is licensed at Enterprise Management Server. No additional MBV-XWST license is required on each Management Server if accessed via Enterprise Management Server.

4.4 Unmanaged site

Operator Client
The user of Operator Client of system A can connect to another system B. System B is called unmanaged site, indicated by 📍. The user can for example perform the following tasks on the video network devices of system B:

- Display live and playback.
- Export video.

- Delete video.
- Protect and unprotect video.
- Create and print a snapshot.

Configuration Client

In the Device Tree of Configuration Client of Bosch VMS A, you can add a system B to an unmanaged site item. You add system B as a network device.

You can add the following device types as system B:

- DVR
- DIVAR IP 3000/7000
- Bosch VMS

You can add an unmanaged site to the Logical Tree multiple times, for example to folders configured as maps.

If port mapping is enabled in the remote access settings of system B then the public network address can also be used in the settings of the unmanaged network device configured in system A.

Credentials for an unmanaged site

When adding a network device to an unmanaged site, you must type in the IP address and select the correct device type of this network device. It is optional to enter credentials for this network device. IP address and the credentials are not checked from within Configuration Client.

When the user of Operator Client connects to an unmanaged site, the credentials that were entered in Configuration Client, are used for logon to the network devices of this unmanaged site if available. If no credentials are available in the configuration, the credentials of the current Operator Client logon are automatically used.

Security considerations

When a user of Operator Client in system A accesses system B via unmanaged site access, keep the following security related considerations in mind:

- All user actions on cameras of system B performed in system A, are not logged on both the systems.
- Operator Client of system A does not enforce the operating permissions configured in system B.
- Operator Client of system A enforces the device permissions configured in system B.
- If an administrator of system A knows a valid user account of system B, system B cannot prevent system A from connecting to system B as an unmanaged network device.

Limitations

For supported video network devices and limitations, see the Bosch VMS datasheet.

See also

- *Adding an unmanaged site, page 121*

4.4.1 Structure of CSV file for importing unmanaged sites

You can prepare a CSV file for importing unmanaged sites in Bosch VMS.

Mandatory field in the CSV file is the definition headline at line 4.

All information above the “definition headline” is ignored during import.

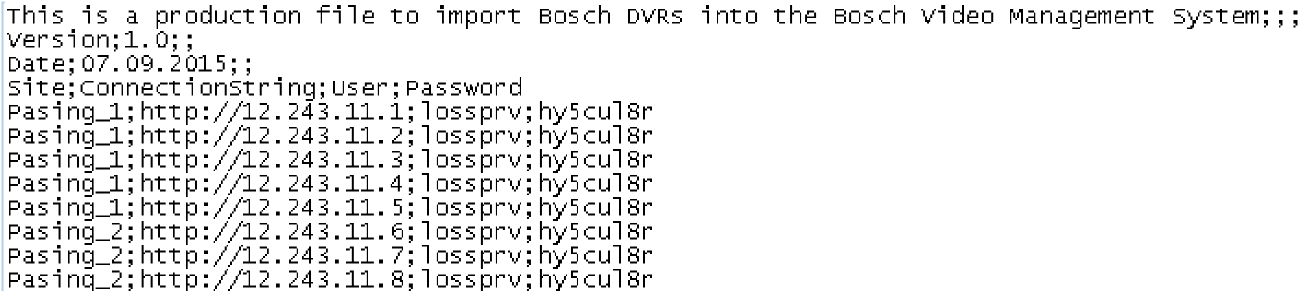
The definition headline defines the mapping of the columns to the unmanaged sites in Bosch VMS.

Possible values are:

- `Site`: Creates a site. This is only allowed to appear once per line.
- `ConnectionString`: Creates a Device by connecting to the specified URI.

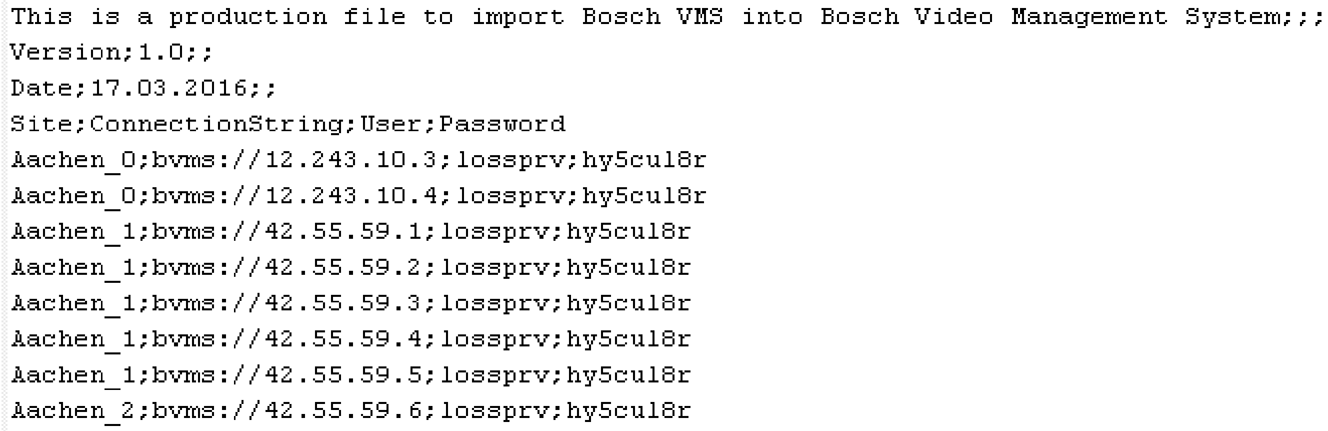
- `User`: The user name for authentication. This field can be empty.
- `Password`: The password for authentication. This field can be empty.

Below the definition headline, each line represents one device.



```
This is a production file to import Bosch DVRs into the Bosch Video Management System;;;
Version;1.0;;
Date;07.09.2015;;
Site;ConnectionString;User;Password
Pasing_1;http://12.243.11.1;lossprv;hy5cul8r
Pasing_1;http://12.243.11.2;lossprv;hy5cul8r
Pasing_1;http://12.243.11.3;lossprv;hy5cul8r
Pasing_1;http://12.243.11.4;lossprv;hy5cul8r
Pasing_1;http://12.243.11.5;lossprv;hy5cul8r
Pasing_2;http://12.243.11.6;lossprv;hy5cul8r
Pasing_2;http://12.243.11.7;lossprv;hy5cul8r
Pasing_2;http://12.243.11.8;lossprv;hy5cul8r
```

For importing another Bosch VMS, use a CSV file like in the following example.



```
This is a production file to import Bosch VMS into Bosch Video Management System;;;
Version;1.0;;
Date;17.03.2016;;
Site;ConnectionString;User;Password
Aachen_0;bvms://12.243.10.3;lossprv;hy5cul8r
Aachen_0;bvms://12.243.10.4;lossprv;hy5cul8r
Aachen_1;bvms://42.55.59.1;lossprv;hy5cul8r
Aachen_1;bvms://42.55.59.2;lossprv;hy5cul8r
Aachen_1;bvms://42.55.59.3;lossprv;hy5cul8r
Aachen_1;bvms://42.55.59.4;lossprv;hy5cul8r
Aachen_1;bvms://42.55.59.5;lossprv;hy5cul8r
Aachen_2;bvms://42.55.59.6;lossprv;hy5cul8r
```

See also

- *Importing a configuration of unmanaged sites, page 121*

4.5 Server Lookup

A single user of Configuration Client or Operator Client may want to connect to multiple system access points sequentially. This access is called Server Lookup. System access points can be Management Server or Enterprise Management Server.

Server Lookup supports you in locating system access points by their names or descriptions.

The user retrieves the list of system access points during logon. He needs to connect to the server hosting the configuration with **Server List / Address Book**.

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.

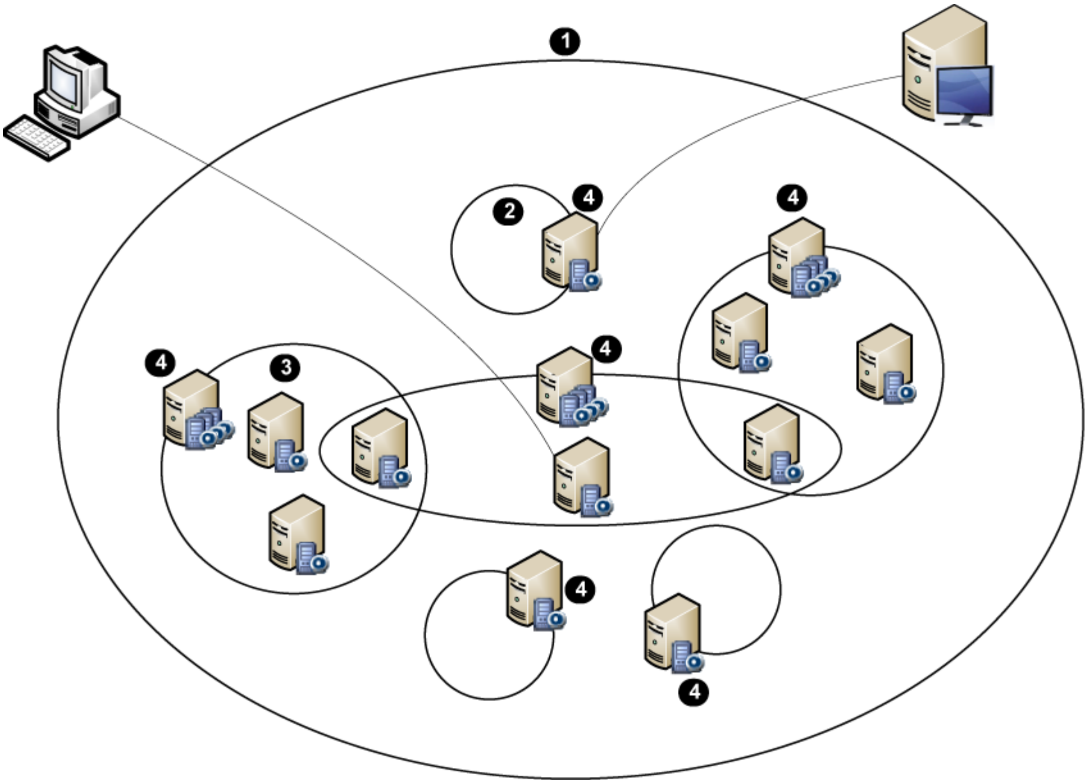
As of Bosch VMS 5.5:

A user of Operator Client can log on to a Management Server with another version. The operator can display the Server List / Address Book of this server.

If the server has a newer version than the client, the client is updated automatically by No-touch deployment if the last successful connection of the client has been established to this server before its upgrade.

You can add further columns in the Server List according to your requirements. The user then has more search criteria to find a specific server in the Server Lookup dialog box. The added columns are also visible on the **Server Access** page (Main window > **User Groups** > **Enterprise User Group** tab > > **Server Access** tab).

The following image shows an example for Server Lookup in a multi system environment:



1	Multi system environment		Enterprise Management Server
2	Single server system		Management Server
3	Multi server system		Operator Client
4	System access point: Server on which logon request of Operator Client or Configuration Client is processed.		Configuration Client

When a client logs on to Enterprise Management Server, it is possible to get access to all Management Servers of this Enterprise System simultaneously.

See also

- *Configuring Server Lookup , page 119*
- *Server List / Address Book page, page 229*

- *Using Server Lookup, page 96*
- *Exporting the Server List, page 120*
- *Importing a Server List, page 120*

4.5.1 Server List

You can export or import a CSV file with a Server List and all configured properties. If you import a CSV file with a Server List, all previously configured servers in the **Server List / Address Book** page are overwritten with the servers in the CSV file. But if you import a server with the name of an already configured server, the settings of the **Server Access** page are retained (Main window > **User Groups** > **Enterprise User Group** tab > > **Server Access** tab).

When you edit the exported CSV file in Microsoft Excel, save the file as CSV file type (Windows ANSI), not as Unicode file type. When using an external editor for editing the exported CSV file, make sure that this editor can save your CSV file with Windows ANSI character encoding or with UTF-8 (with BOM) character encoding. Windows ANSI encoding is used for all Western European languages, UTF-8 is used for all other languages.

The list separator that is configured in the Regional Settings of your Operating System, is used as separator for the CSV file. Windows 7 as an example:

- Click **Start** > **Control Panel** > **Region and Language** > **Additional Settings** > In the **List separator:** list, select the desired character.

4.6 Remote access

> **Caution!**
> 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 364*
- *Changing the password of an encoder / decoder, page 137*
- *Changing the password of a VRM device, page 129*

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

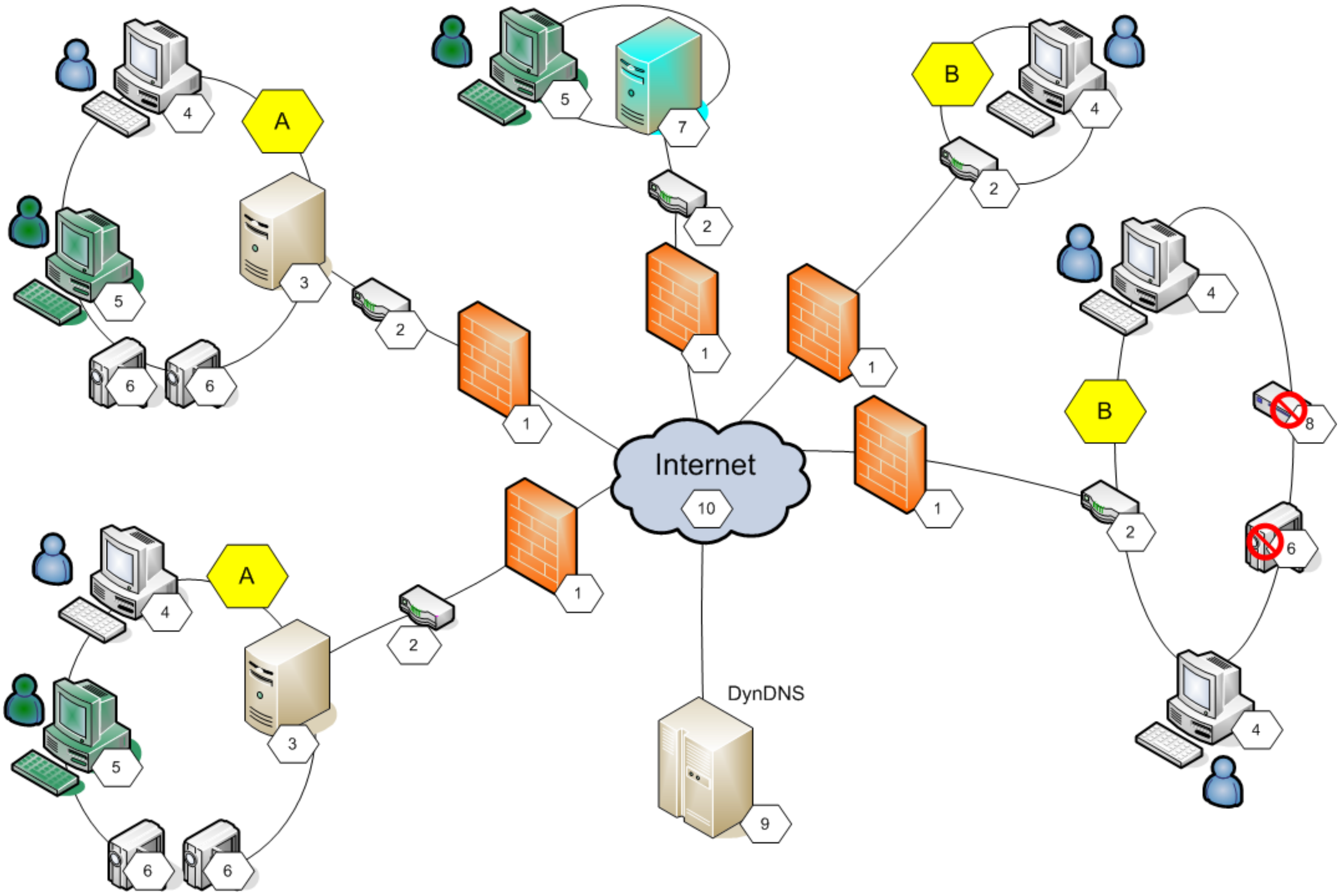
Multiple networks with private (local) network addresses can be accessed simultaneously or sequentially by Operator Client computers via public interfaces (routers). Task of the router is to translate the incoming public network traffic to the corresponding private network address.

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:

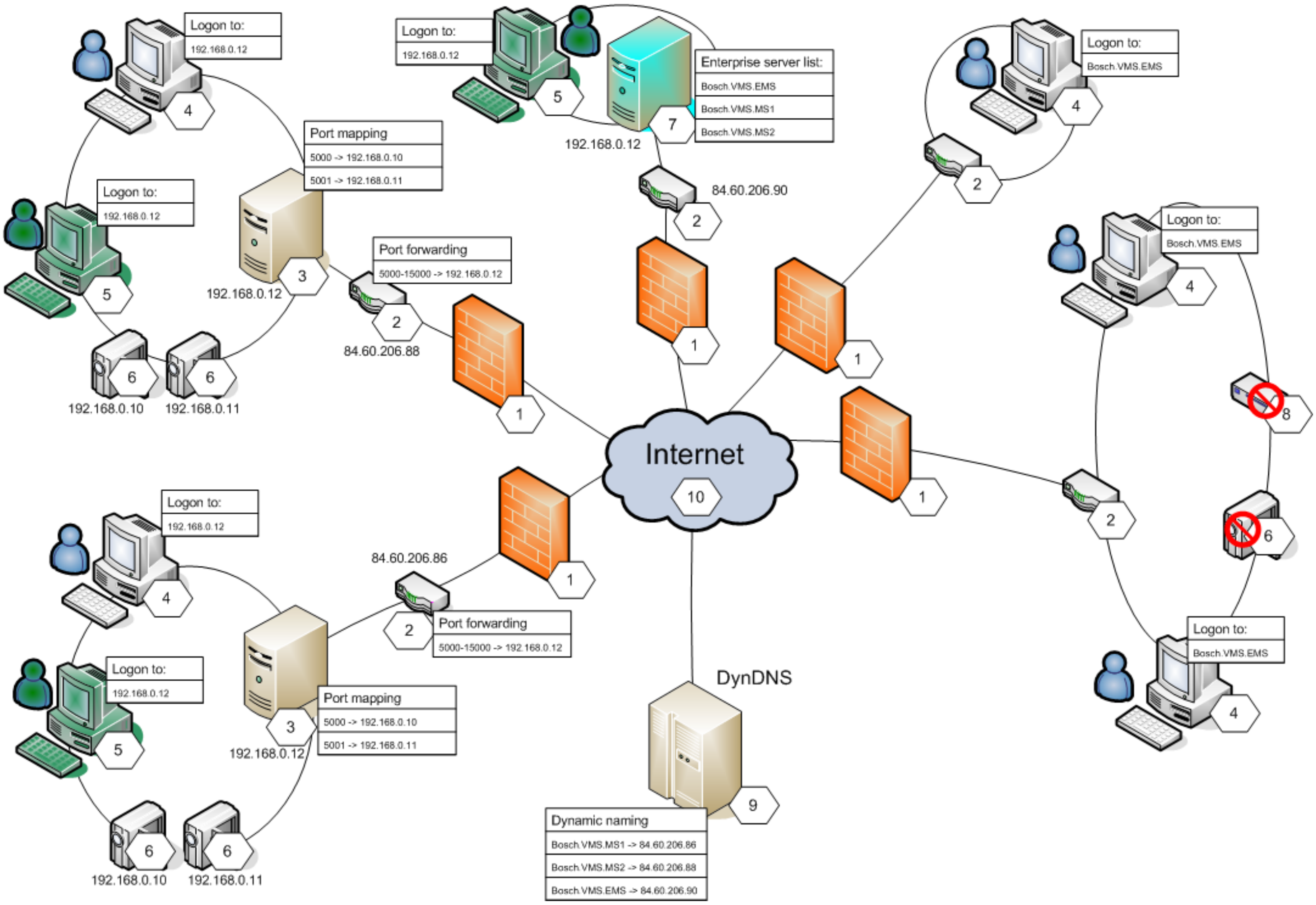
- Playback of local storage
- ONVIF
- DiBos
- Direct iSCSI replay

The following image shows an example of remote access to Bosch VMS 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 Bosch VMS 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 Bosch VMS environment.

See also

- *Configuring remote access, page 96*
- *Remote Access Settings dialog box, page 225*
- *Port Mapping Table dialog box, page 226*

4.7 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

Notice!
As of Bosch VMS v. 4.5.5, multiple storage pools per VRM are supported.

See also

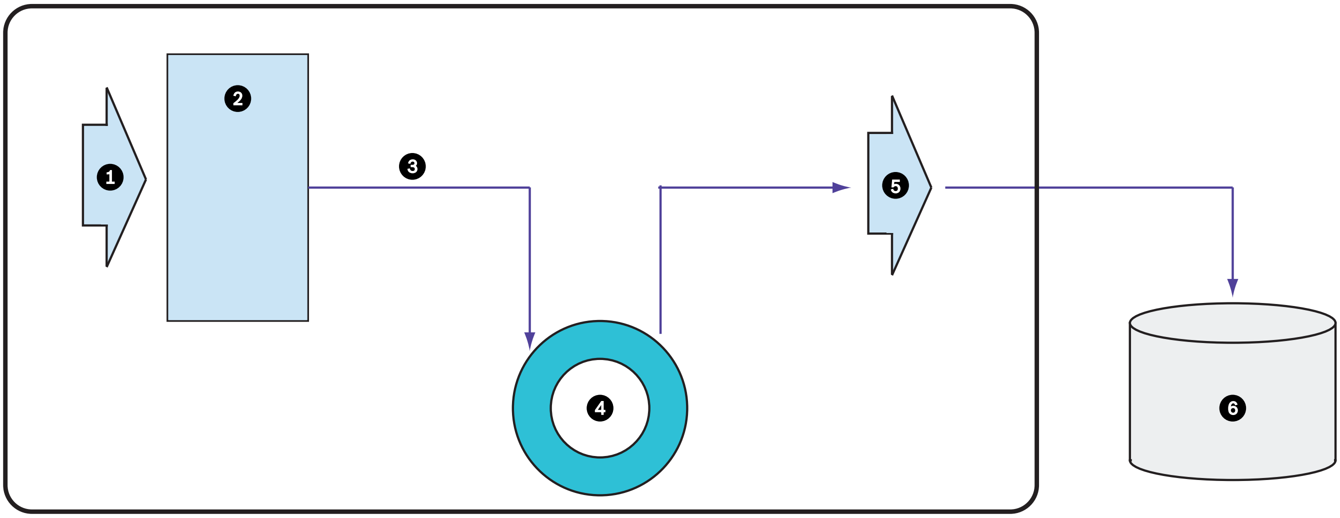
- *Pool page, page 266*

4.8 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.
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 126*
- *Configuring the storage media of an encoder, page 105*
- *Configuring the ANR function, page 189*

4.9 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.

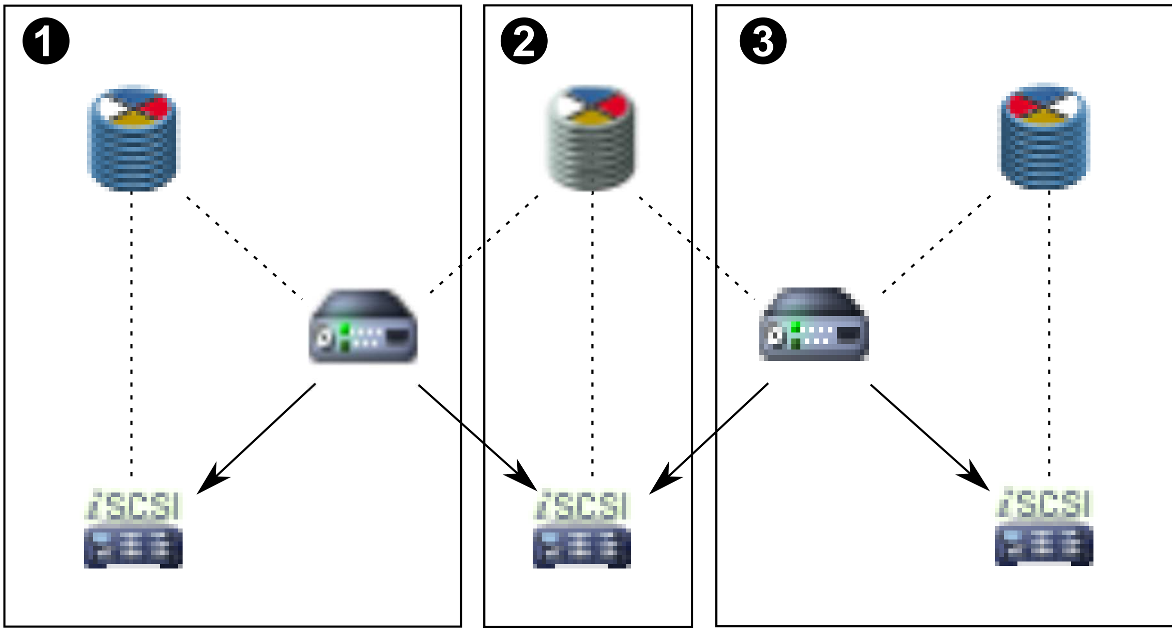
A Secondary VRM can manage the secondary recording for multiple Primary VRMs.

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	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 189*
- *Adding a Primary VRM manually, page 123*
- *Adding a Secondary VRM manually, page 123*
- *Adding a Mirrored VRM manually, page 124*
- *Adding a Failover VRM manually, page 124*
- *Cameras page, page 341*

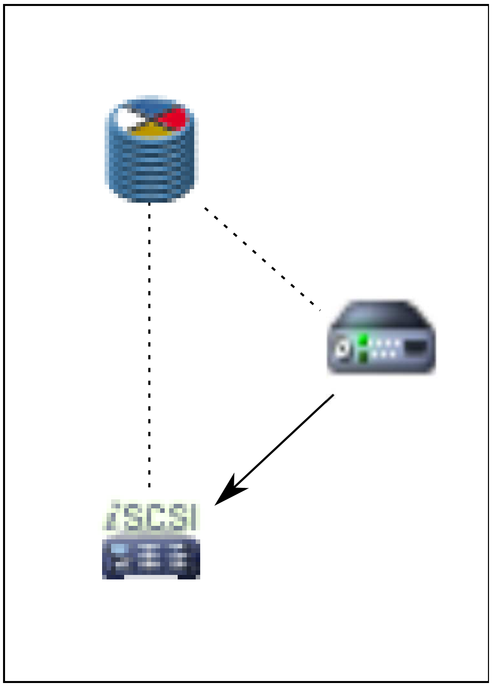
4.10 VRM recording modes

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

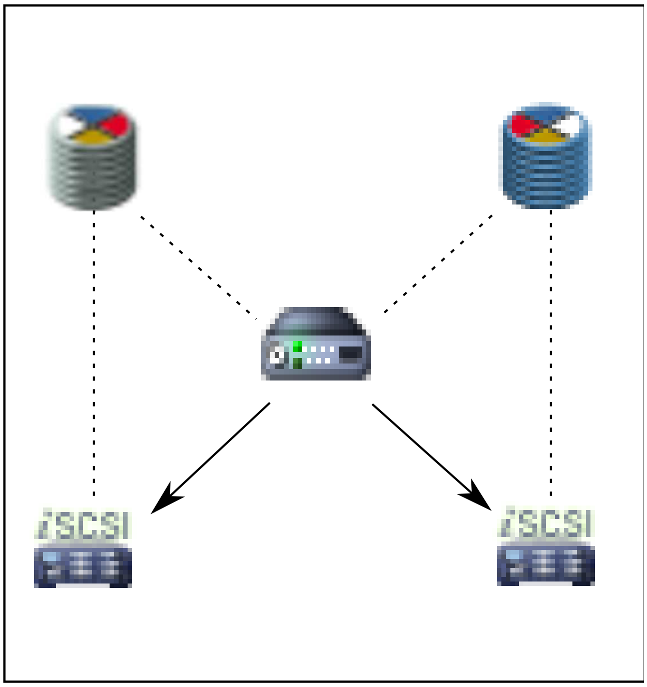
For ANR recording, see chapter *Automated Network Replenishment (ANR), page 38*.

Primary VRM recording



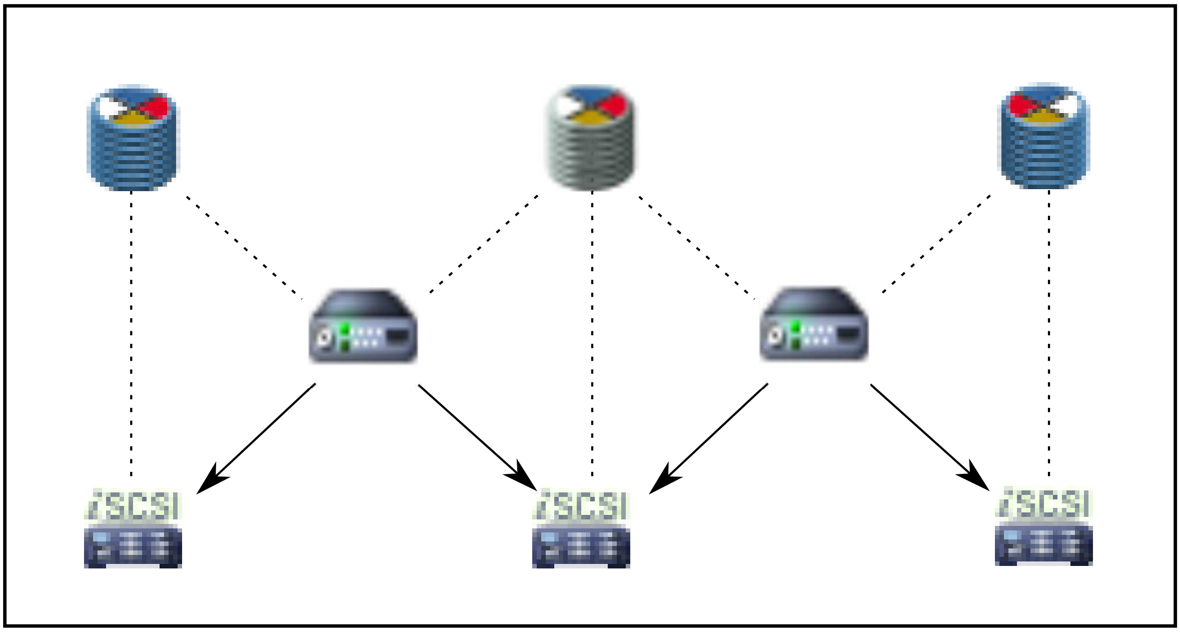
	Primary VRM	....	Control connection
iSCSI	iSCSI storage device	→	Video stream
	Encoder		

Mirrored VRM recording



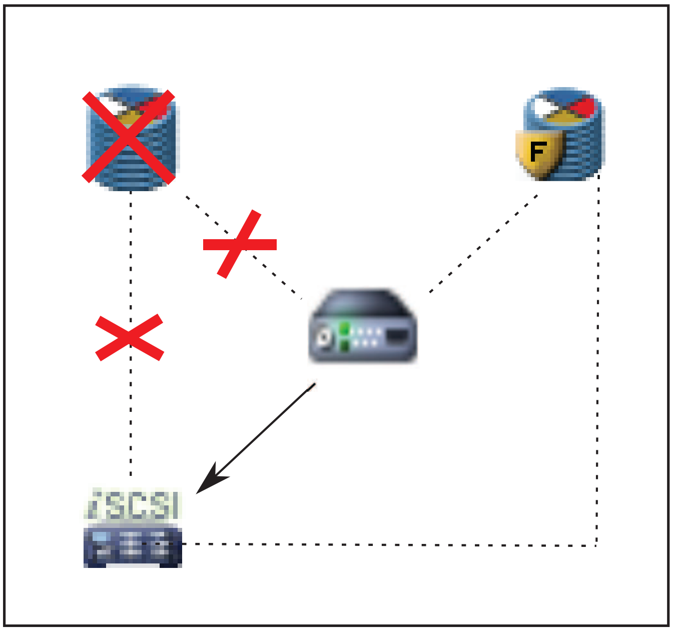
	Primary VRM		Secondary VRM
iSCSI	iSCSI storage device	....	Control connection
	Encoder	→	Video stream

Secondary VRM recording



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

Failover VRM recording



	Primary VRM		Secondary VRM

iSCSI	iSCSI storage device	F	Primary Failover VRM
	Encoder	F	Secondary Failover VRM
....	Control connection	➤	Video stream

4.11 Playback of VRM recording sources

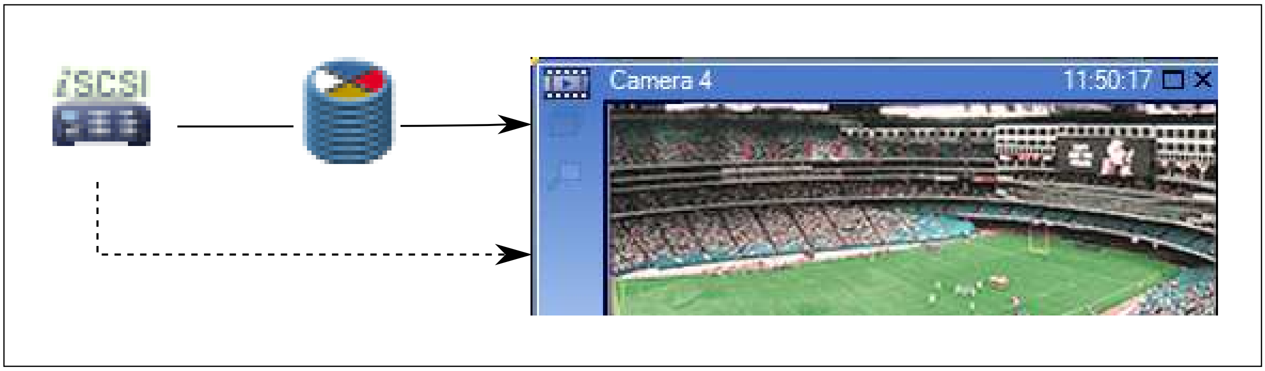
The following graphics show Image panes with playback from all possible VRM recording sources. Each graphic displays the storage device, the VRM instance (if available), and a section of an Image pane as example of the playback. If applicable, the recording source is indicated by an appropriate icon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

– *Playback of single recording, page 44*
– *Playback of dual VRM recording, page 45*
– *Playback of Primary VRM recording with optional Failover VRM, page 46*
– *Playback of Secondary VRM recording with optional Failover VRM, page 48*
– *Automatic Network Replenishment, page 50*

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.

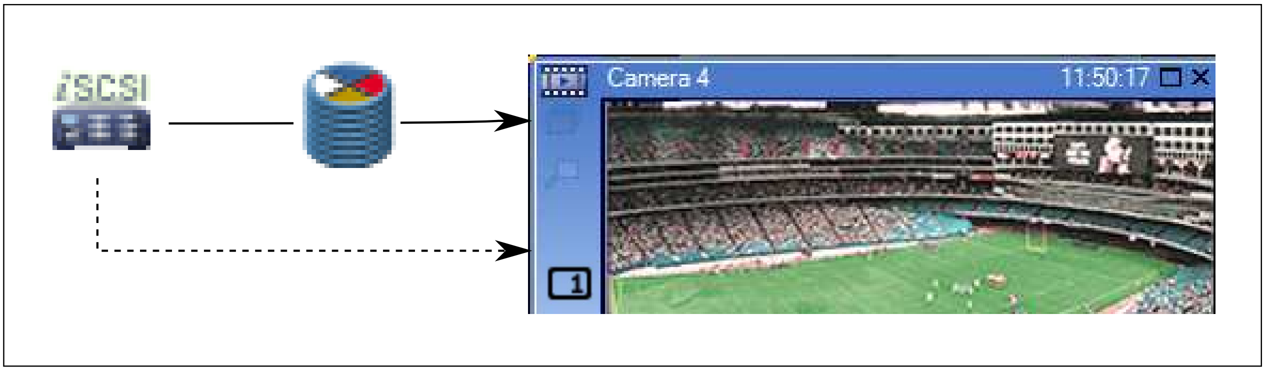


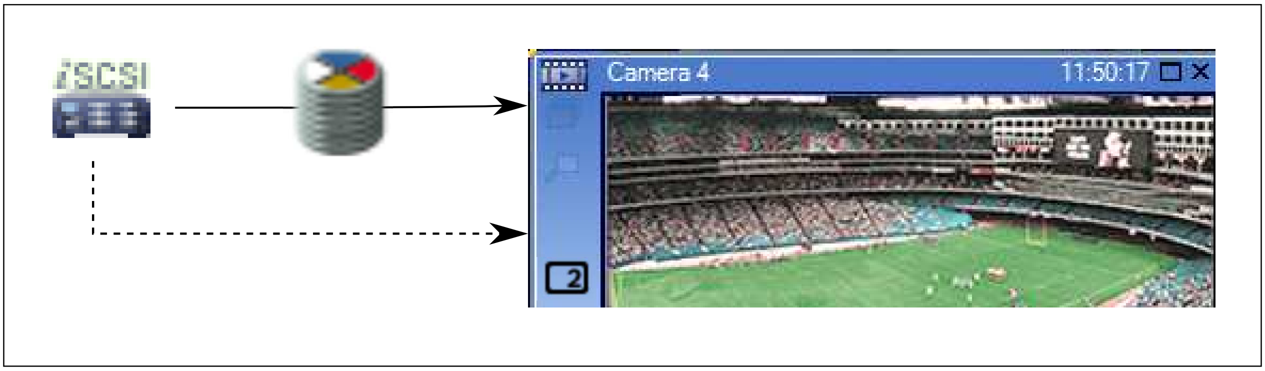
iSCSI	iSCSI storage device
	Primary VRM

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.

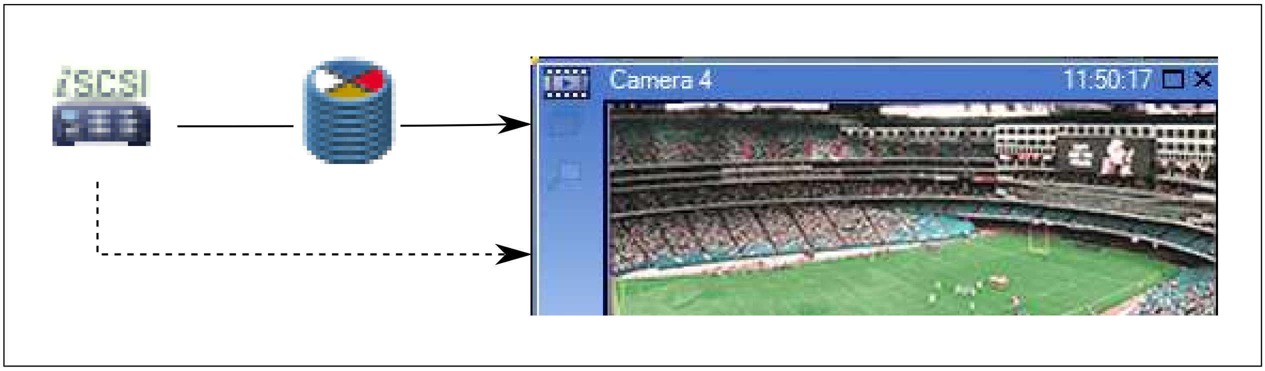




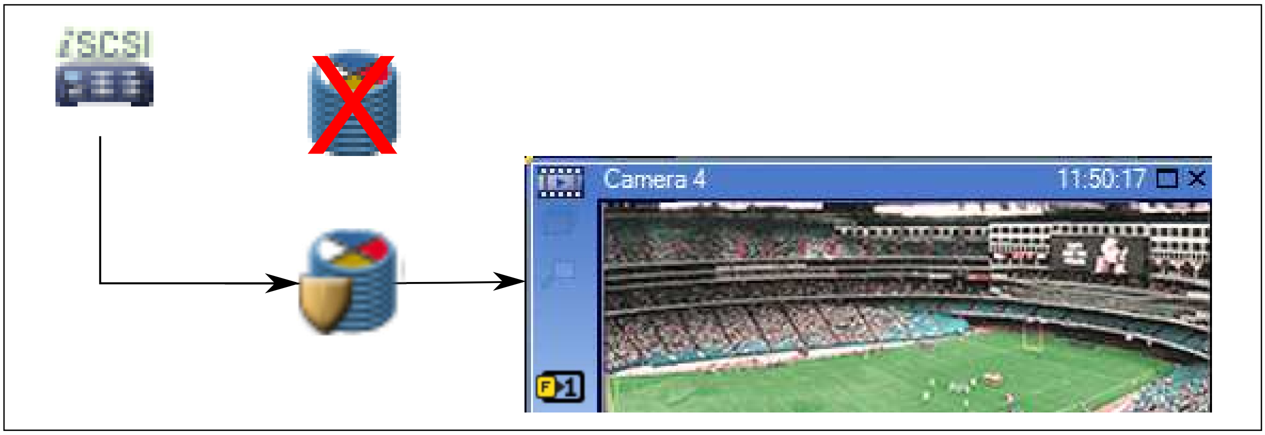
iSCSI	iSCSI storage device
	Primary VRM
	Secondary VRM

Playback of Primary VRM recording with optional Failover VRM

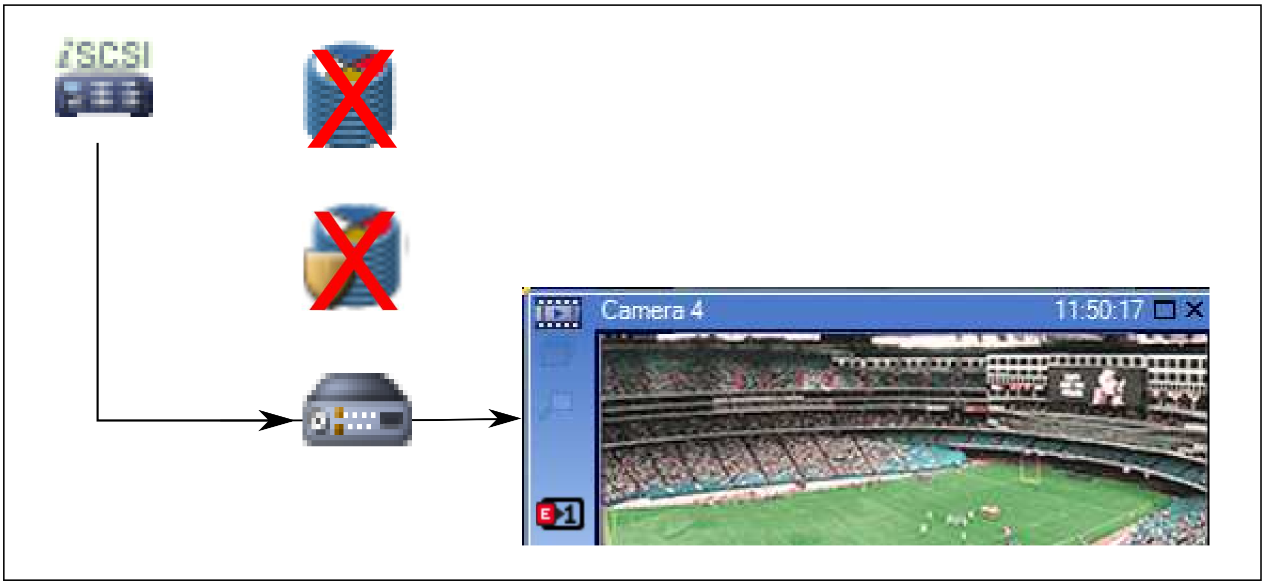
While the Primary VRM is working, it provides playback. The Failover VRM runs in idle state. If configured for this workstation, playback is provided directly by the iSCSI storage device. If a Secondary VRM or ANR recording is configured, you can switch the recording source.



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:

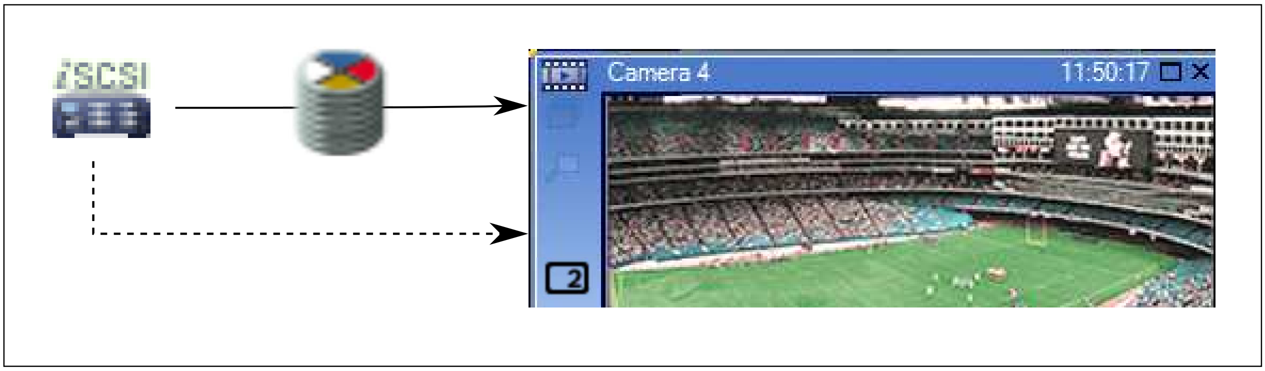


iSCSI	iSCSI storage device
	Primary VRM
F	Primary Failover VRM
	Encoder

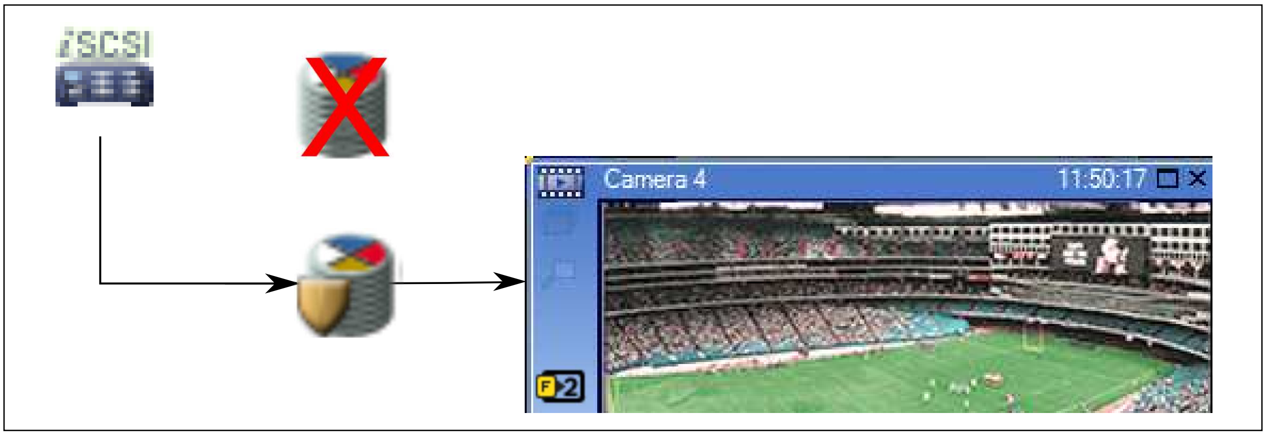
Encoder playback can only access a limited recording period.

Playback of Secondary VRM recording with optional Failover VRM

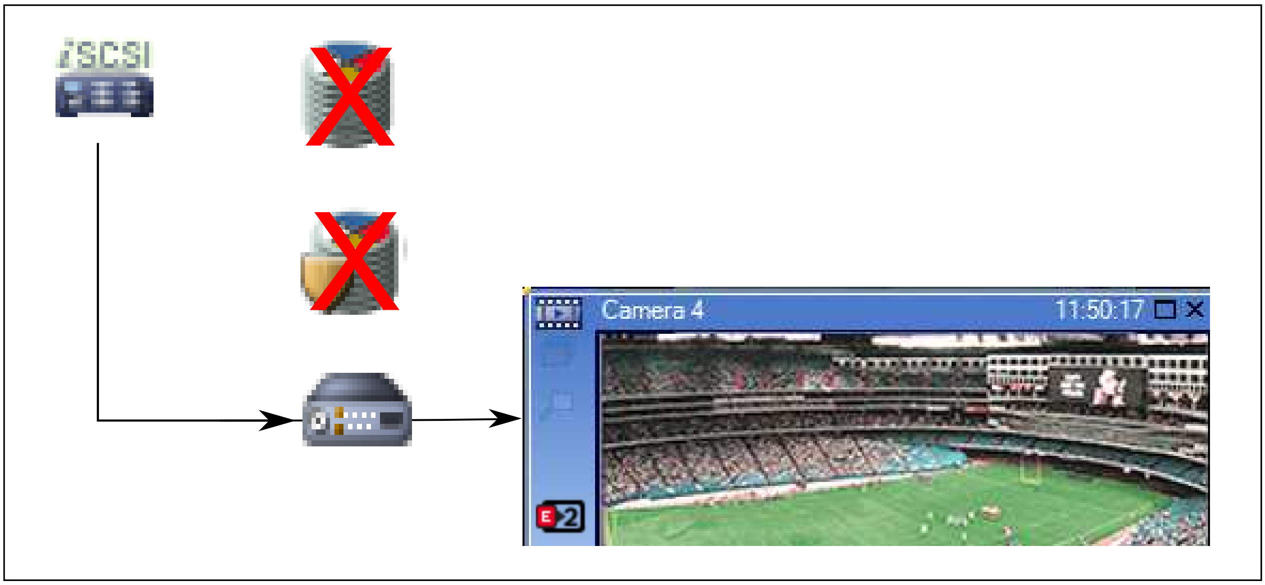
While the Secondary VRM is working, it provides playback. The Failover VRM runs in idle state. If configured for this workstation, playback is provided directly by the iSCSI storage device.



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

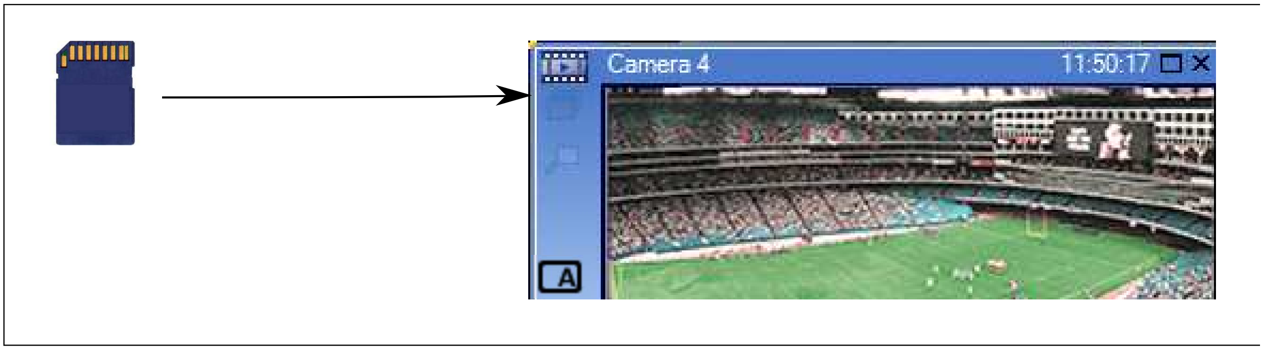
	Primary VRM
F	Secondary Failover VRM
	Encoder

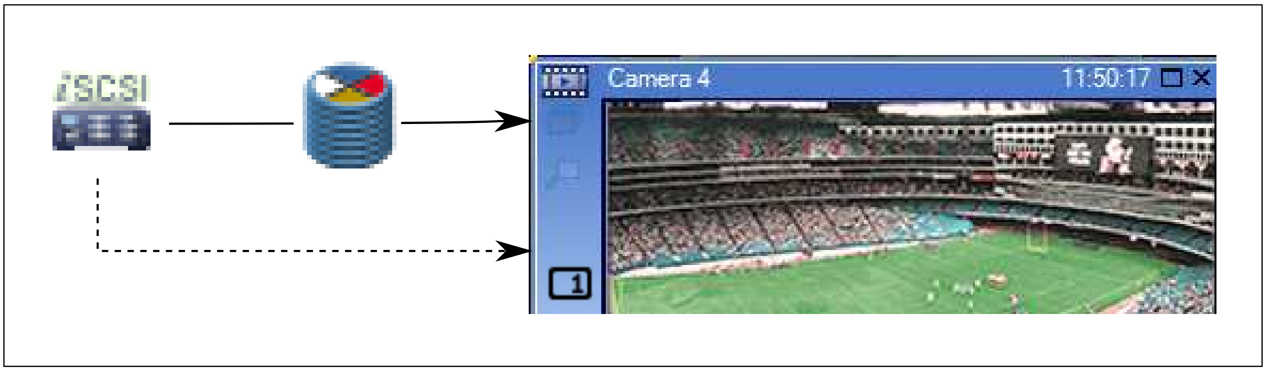
Encoder playback can only access a limited recording period.

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 card

4.12 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 and optionally on analog monitors. 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 analog 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 an analog 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 an analog monitor group, each alarm can call up cameras on a row of analog monitors. The number of cameras in the row is limited by the number of columns in the analog 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 analog 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 analog monitor groups with control buttons in the **Monitors** window of the Operator Client workstation display. Analog monitors in alarm are indicated by red icons with blinking "LEDs".
   The alarm title, time, and date can be optionally be displayed on all analog 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.

See also

– *Configuring the pre- and post-alarm duration for an alarm, page 197*

4.13 DVR devices

This chapter gives background information on the DVR devices that you can integrate in Bosch VMS.
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 Bosch VMS, these encoders / IP cameras are not detected by the Bosch VMS 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 Bosch VMS and these encoders / IP cameras are already added to Bosch VMS, a warning is displayed. Remove these encoders / IP cameras from the DVR or from Bosch VMS.
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.

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

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 235*
– *Configuring the integration of a DVR, page 156*

4.14 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 Bosch VMS.

Internet Information Service
Configure the settings for Internet Information Service on the computer where you plan to install MVS for Bosch VMS.

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, Bosch VMS Setup to install Mobile Video Service aborts.
You select the Mobile Video Service component for installation during Bosch VMS 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, page 162*
- *Mobile Video Service page, page 259*

4.15 Adding Video IP devices from Bosch

As of Bosch VMS 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 a device manually, page 150*
- *Updating the device capabilities, page 135*
- *Add Encoder / Add Decoder dialog box, page 241*
- *Edit Encoder / Edit Decoder dialog box, page 241*

4.16 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.
The ROI feature is available on the Nevada and A5 HW platform with firmware version 5.60 or higher.
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** 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 341*
- *Camera Permissions page, page 366*

4.17 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.

4.18 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 Bosch VMS 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, page 224*
- *Operator Features page, page 372*

4.19 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 177*
- *Malfunction Relay dialog box, page 338*

4.20 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 197*
- *Text Data Recording dialog box, page 354*

4.21 Allegiant CCL commands

You use CCL commands for switching IP cameras or encoders to IP decoders both configured in Bosch VMS. You cannot use CCL commands to directly control analog cameras or the Allegiant matrix itself.

The Allegiant CCL emulation starts an internal Bosch VMS service that translates CCL commands of the Matrix Switch into Bosch VMS. 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 Bosch VMS cannot be controlled with these commands.

4.22 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 Bosch VMS 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 Bosch VMS V5.5 an Operator Client workstation can work offline with a configuration of Bosch VMS V5.0.5.

Caution!

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.

Caution!

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

4.22.1 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 Bosch VMS V3.0 we will show a more user friendly Image pane informing the user about the impossibility to display this camera right now.
- AMG:
  It is not possible to drag cameras on the AMG 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
  - AnalogMonitorMananger
  - 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 Bosch VMS 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 Bosch VMS 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).

4.23 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

4.23.1 Working with Compatibility Mode

This feature is available in versions later than 5.5.

A Bosch VMS 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 Bosch VMS version than the Operator Client workstation.

4.24 ONVIF events

Intended use

Intended use is the mapping of ONVIF events to Bosch VMS events. ONVIF events can then trigger Bosch VMS 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 Bosch VMS Scan Wizard or are added manually.

When you add an ONVIF encoder to the Bosch VMS 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 Bosch VMS.
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 ONVIF events, page 140*
- *Enabling logging for ONVIF events, page 385*
- *ONVIF Encoder Events page, page 317*

4.25 Viewing modes of a panoramic camera

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

- Circle view
- Panorama view
- Cropped view

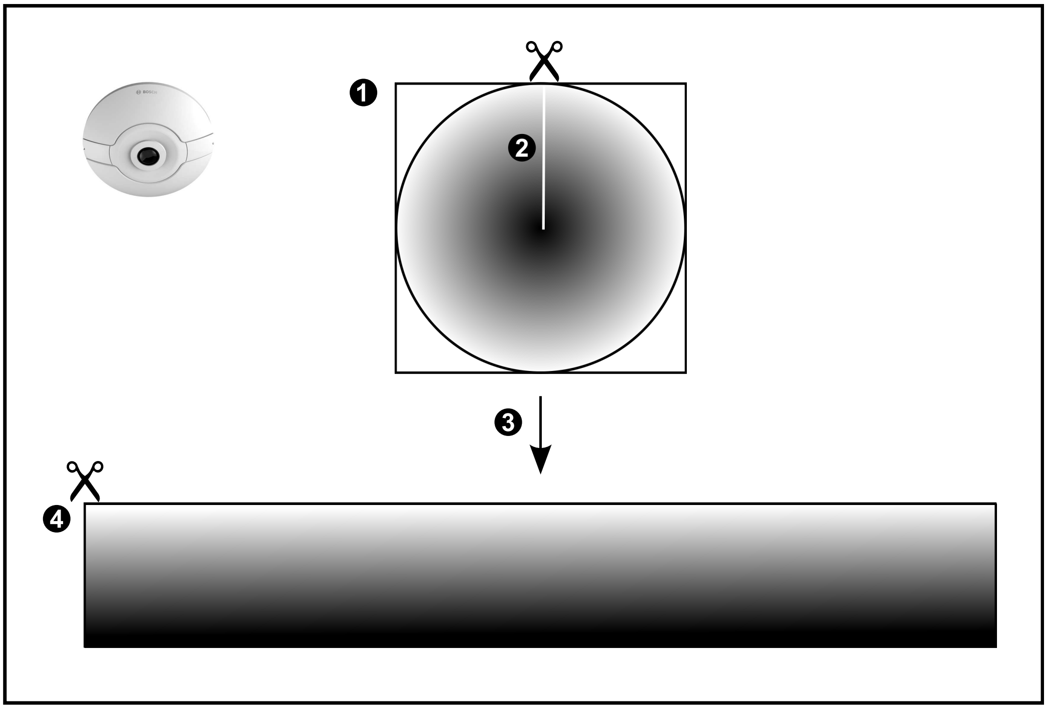
Panorama and cropped view modes are created by the dewarping process in Bosch VMS. Edge dewarping is not used.
The administrator must configure the mounting position of a panoramic camera in Configuration Client.
You can resize the Image pane of a camera as required. The Image pane ratio is not restricted to the 4:3 or 16:9 aspect ratio.

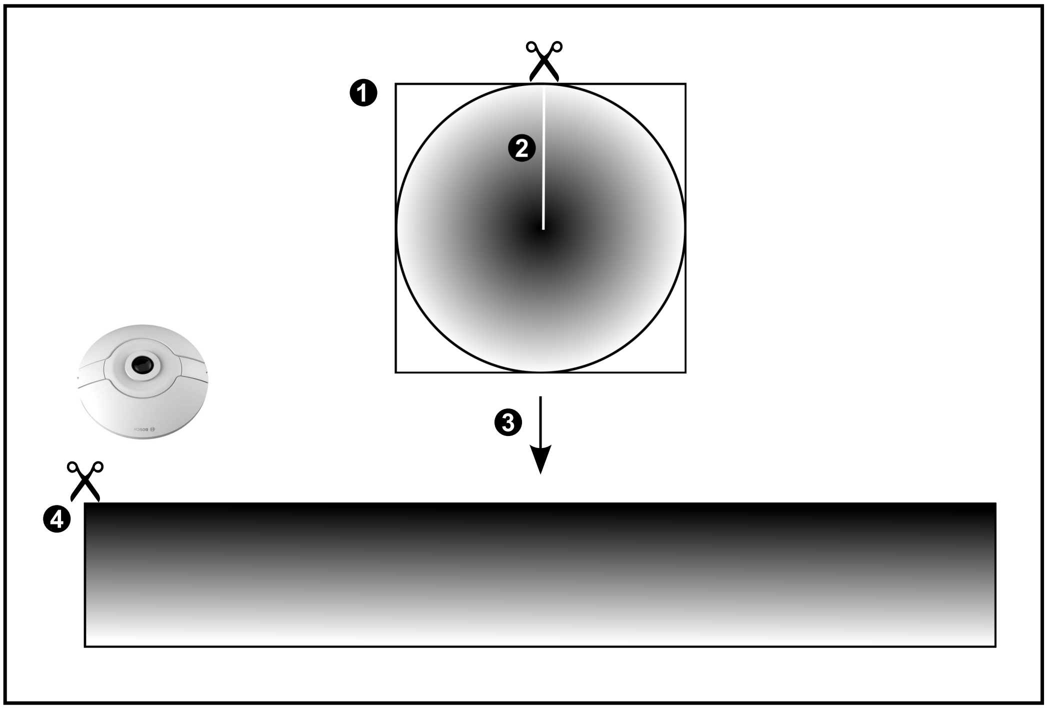
See also

- *Configuring the mounting position of a panoramic camera, page 110*

4.25.1 360° panoramic camera - floor- or ceiling mounted

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

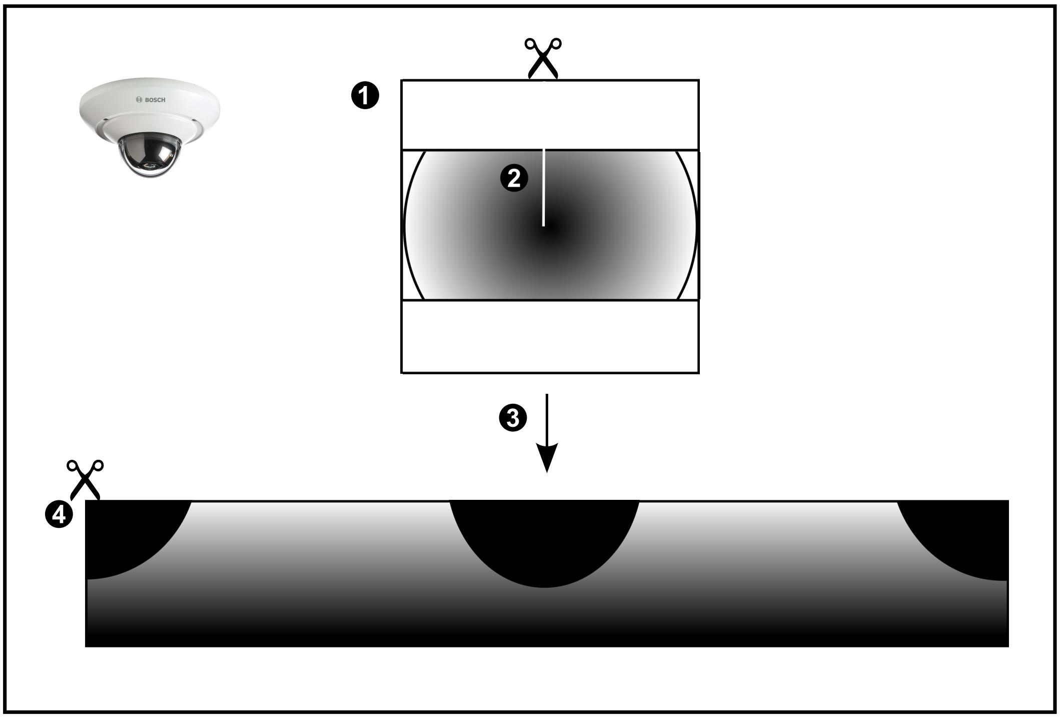


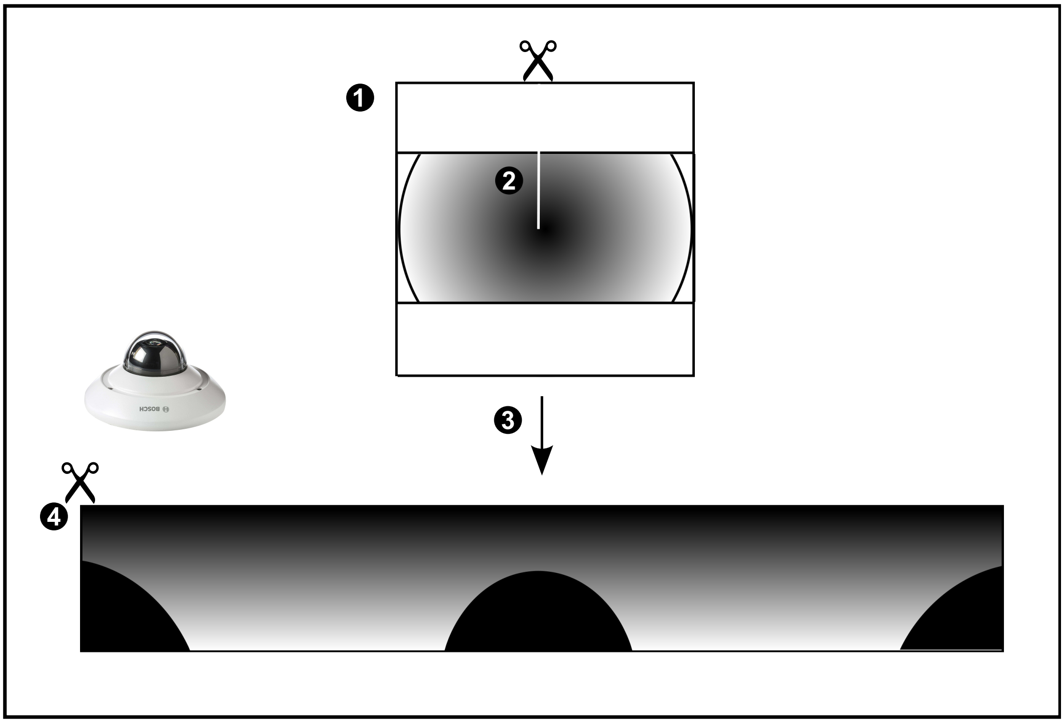


1	Full circle image	3	Dewarping
2	Snipping line (operator can change its position when not zoomed in)	4	Panorama view

4.25.2 180° panoramic camera - floor- or ceiling mounted

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

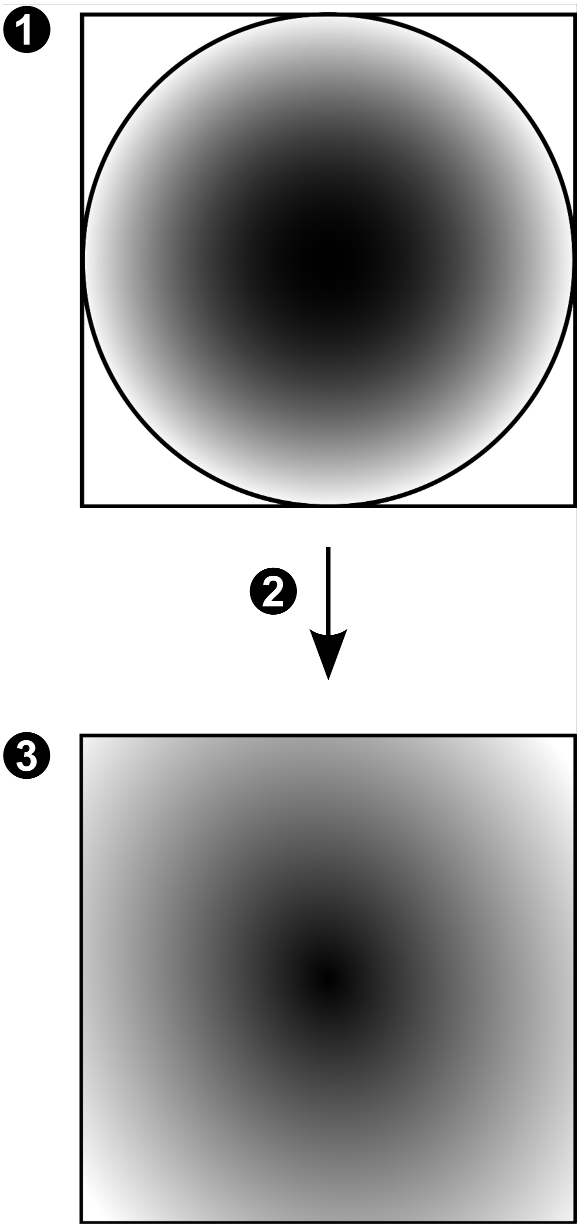




1	Full circle image	3	Dewarping
2	Snipping line (operator can change its position when not zoomed in)	4	Panorama view

4.25.3 360° panoramic camera - wall mounted

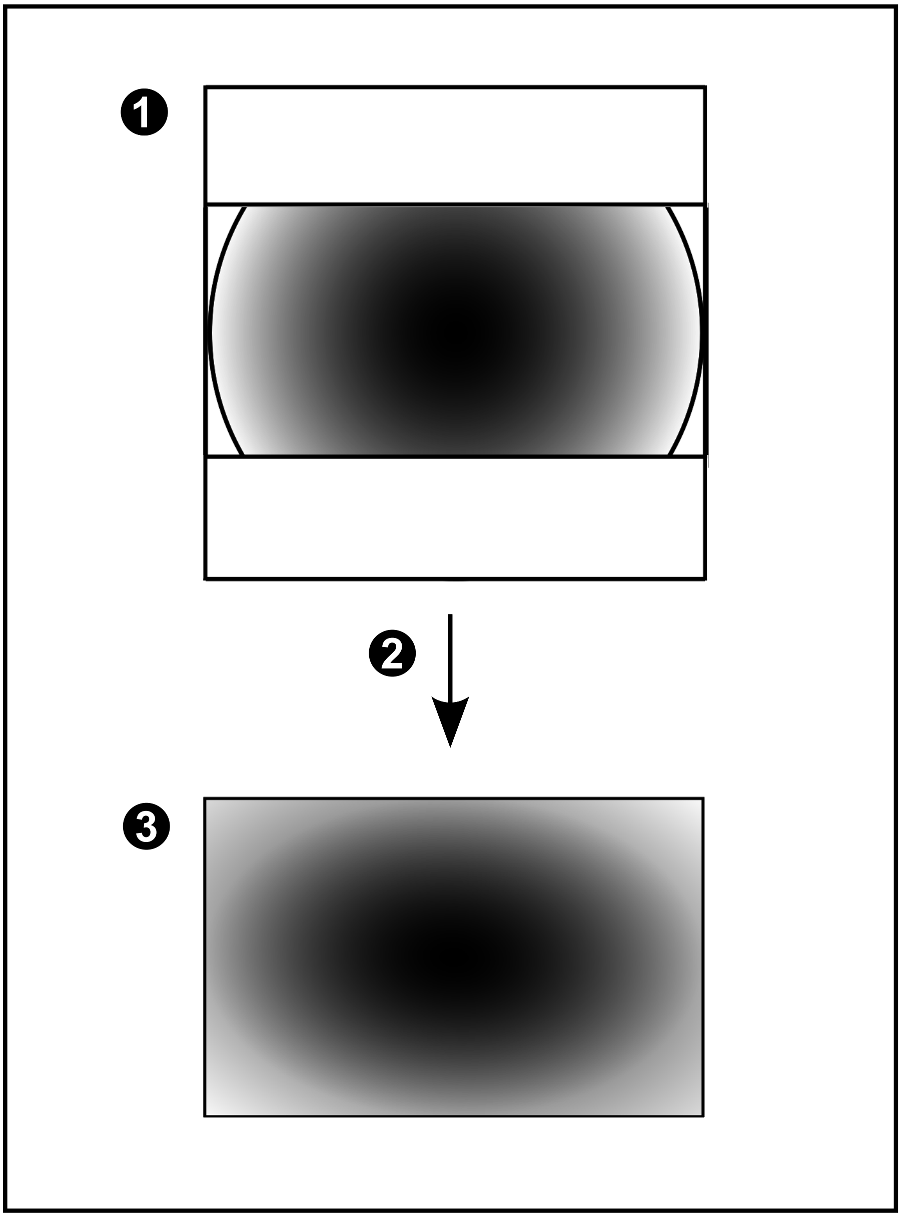
The following figure illustrates the dewarping of a 360° camera which is wall mounted.



1	Full circle image	3	Panorama view
2	Dewarping		

4.25.4 180° panoramic camera - wall mounted

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

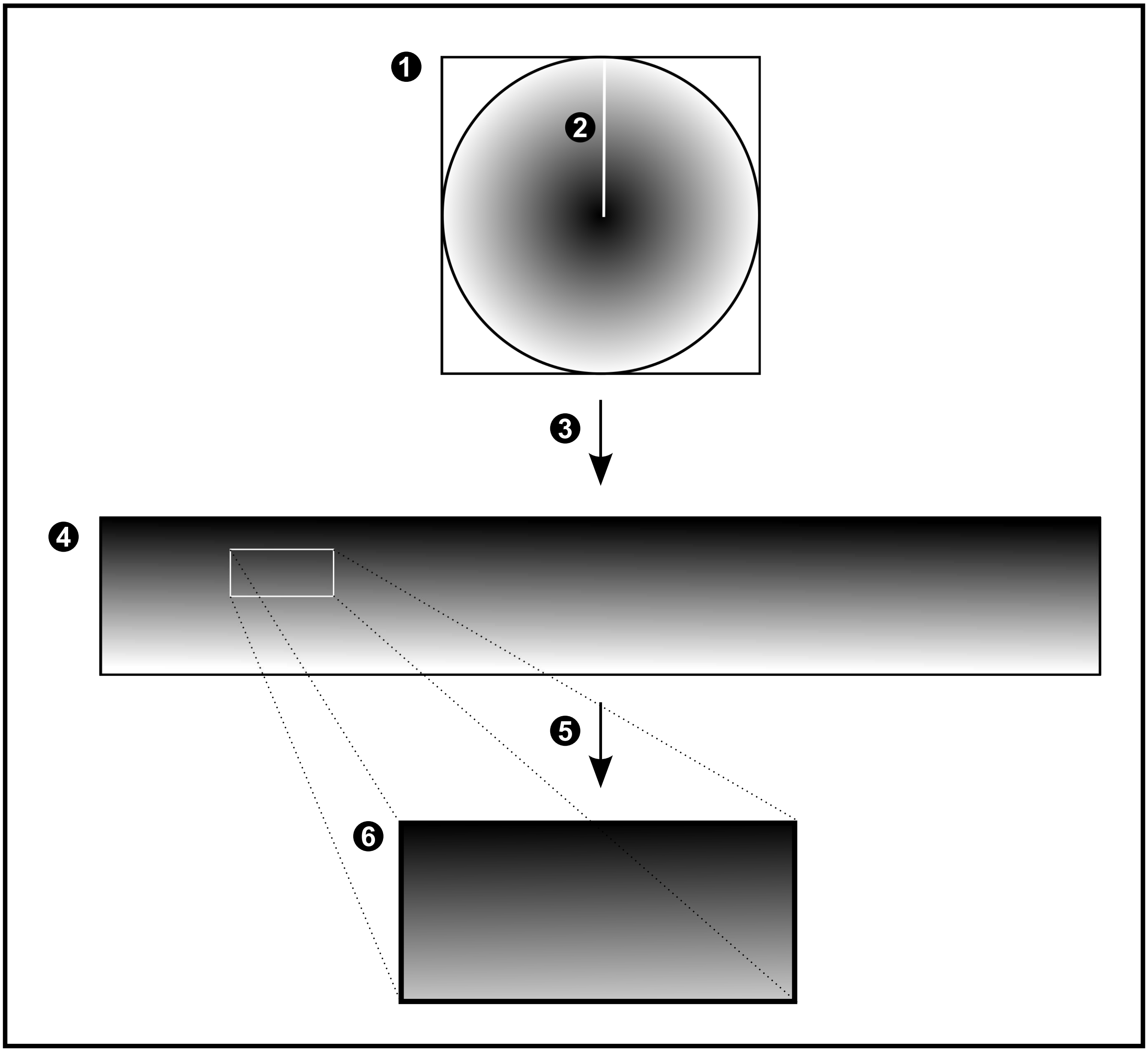


1	Full circle image	3	Panorama view
2	Dewarping		

4.25.5 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

4.26 Server-based analytics

The user of Operator Client can display the Ganetec analytics viewer application in the Live Image window. This analytics viewer application displays the results of video analytics, for example face detection. The video analytics is performed on the Bintelan Analytics Platform from Ganetec.

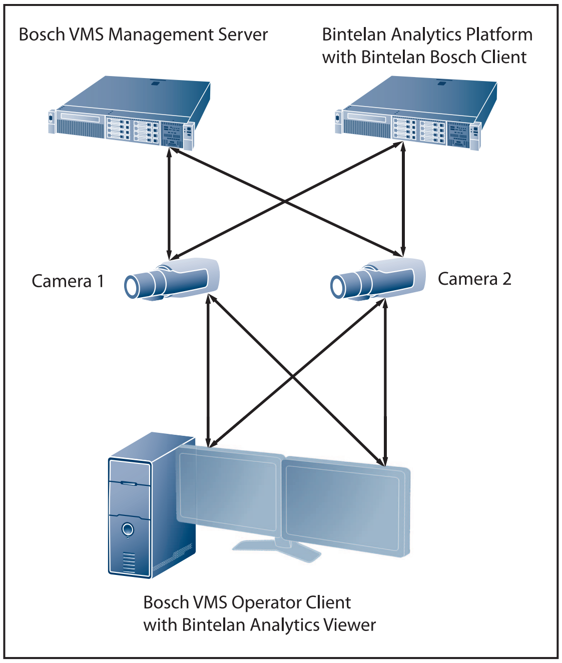
With Bintelan Analytics Platform, the following analytics algorithms are available:

- Face detection
- Face recognition
- Number plate detection
- Number plate recognition

Perform the following steps to configure video analytics:

1. Install the analytics viewer application of the video analytics on each Bosch VMS workstation to be used for analytics. Take a note containing the path to the analytics viewer application.
   For detailed information on installing the analytics viewer application, see: *Installing the analytics viewer application, page 68*.
2. Add the cameras to the Device Tree that you want to use as analytics cameras.
   These cameras are automatically retrieved when the Bintelan Analytics Platform connects with your Bosch VMS Management Server.
3. Add a video analytics device to the Device Tree of Configuration Client.
   For detailed information on adding a video analytics device, see: *Adding a video analytics device, page 162*.
4. In the video analytics device, configure the path to the analytics viewer application. A default path of the analytics viewer application is pre-configured.
5. Configure the IP address of the Bintelan Analytics Platform.
6. Use the Bintelan Bosch Client application on the Bintelan Analytics Platform for connecting with Bosch VMS Management Server.
   Type in the IP address of this Management Server.
7. Add the video analytics device to the Logical Tree.
8. Configure an alarm for the **External Data** event for the desired video analytics cameras.
9. The user of Operator Client drags the video analytics device to an Image pane.
10. When an alarm occurs, an external data alarm entry is displayed in the Alarm List.
11. The user selects this entry in the Alarm List.
    An image with the matched person or object is displayed in the analytics viewer application.

The following graphic shows an example of a server-based analytics scenario:


Bosch VMS Management Server
Bintelan Analytics Platform with Bintelan Bosch Client
Camera 1
Camera 2
Bosch VMS Operator Client with Bintelan Analytics Viewer

The Bintelan Analytics Platform must be configured properly to be able to connect with Bosch VMS.
You must install the analytics viewer application on each Operator Client workstation used for video analytics. Additionally configure the IP address of the Bintelan Analytics Platform in Configuration Client and the IP address of the Bosch VMS Management Server in the Bintelan Analytics Platform.
You configure the analytics viewer application in the Device Tree of Configuration Client.

See also

- *Adding a video analytics device, page 162*
- *Installing the analytics viewer application, page 68*

4.26.1 Installing the analytics viewer application

For displaying the Ganetec analytics viewer application, the software must be installed in the directory configured in Configuration Client.
For installation, you need the BintelanClient_BoschAlarmViewer.exe from the Ganetec Web page or from the Bosch Online Product Catalog.
Perform the installation on each Operator Client workstation where you want to use the analytics viewer application.

To install:

1. Double-click the Setup.
2. Follow the instructions on the screen.
   Note: The installation directory for the analytics viewer application must be below `%ProgramFiles(x86)%\VideoAnalytics`.

5 Supported hardware

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

You can connect the following hardware to Bosch VMS:

- 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
- Analog monitors
  Connected to a decoder, to a Bosch Allegiant matrix, to a Bosch VMS Client workstation
- BRS / DiBos devices (see the data sheet for Bosch VMS 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 Bosch VMS workstation.
- Bosch IntuiKey keyboard
  Connected to the COM port of a Bosch VMS 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 analog 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 Bosch VMS are also connected to this device.

5.1 Installing hardware

Bosch VMS 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 (analog 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

Refer to the Instructions Manual delivered with your KBD-Universal XF keyboard available on the online product catalog.
Install manufacturer's driver before attaching the keyboard.

Documentation and software for Bosch Security Systems products can be found in the online product catalogue as follows:

▸ Open any browser > enter www.boschsecurity.com > select your region and your country > start a search for your product > select the product in the search results to show the existing files.

You can connect the following hardware to Bosch VMS:

- 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
- Analog monitors
  Connected to a decoder, to a Bosch Allegiant matrix, to a Bosch VMS Client workstation
- BRS / DiBos devices (see the data sheet for Bosch VMS 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 Bosch VMS

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 Bosch VMS workstation (scenario 1) or to a hardware decoder (e.g. VIP XD, scenario 2).
If you connect the keyboard to a Bosch VMS 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 Bosch VMS 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 Bosch VMS workstation

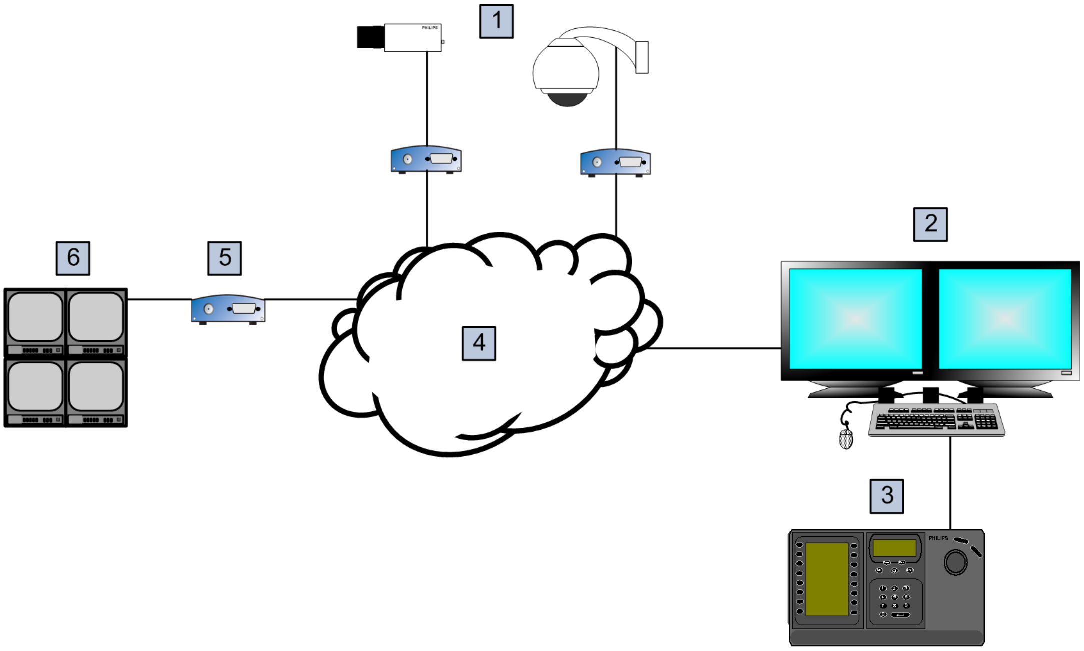


Figure 5.4: Scenario 1: Bosch IntuiKey keyboard connected to a Bosch Video Management System workstation

1	Various cameras connected to network via encoders
2	Bosch VMS workstation
3	Bosch IntuiKey keyboard
4	Bosch VMS network

5	Decoder
6	Analog monitors

Bosch IntuiKey keyboard connected to a decoder

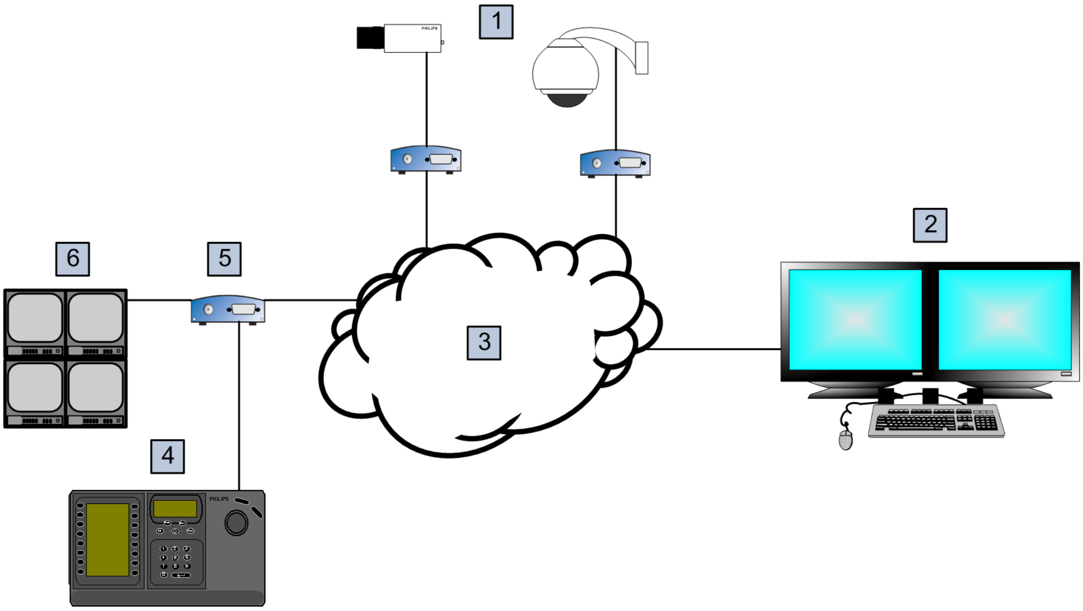


Figure 5.5: Scenario 2: Bosch IntuiKey keyboard connected to a decoder

1	Various cameras connected to network via encoders
2	Bosch VMS workstation
3	Bosch VMS network
4	Bosch IntuiKey keyboard
5	Decoder
6	Analog monitors

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

- *Assign Keyboard page, page 256*

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

- *Configuring a Bosch IntuiKey keyboard (workstation), page 160*
- *Configuring a Bosch IntuiKey keyboard (decoder), page 160*
- *Configuring a decoder for use with a Bosch IntuiKey keyboard, page 155*

See also

- *Assign Keyboard page, page 256*

5.3.2 Connecting a Bosch IntuiKey keyboard to a decoder

Configuring the decoder

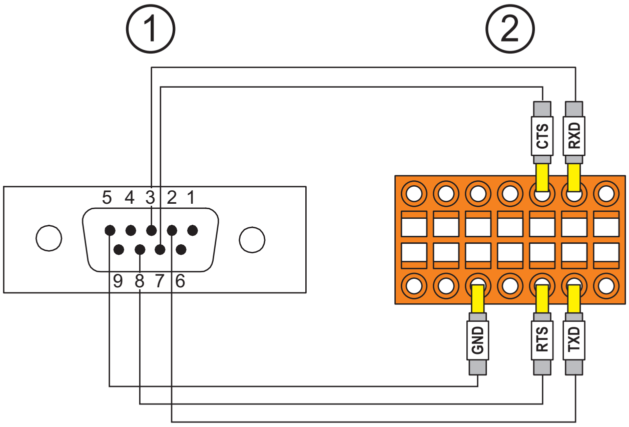
See *Configuring a decoder for use with a Bosch IntuiKey keyboard, page 155* for details.

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	
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 Bosch Video Management System

The Bosch VMSAllegiant 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 analog monitors connected to IP decoders.

Bosch VMS 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 Bosch VMS. So, for example, if a defective coax cable results in video loss in the Allegiant, an immediate notification is sent to Bosch VMS. Also, you can program Bosch VMS to respond to Allegiant alarms.

5.4.1 Bosch Allegiant Connection Overview

To achieve a connection between Bosch VMS and an Allegiant matrix switching system, you configure a control channel between the Bosch VMS 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.

Local connection

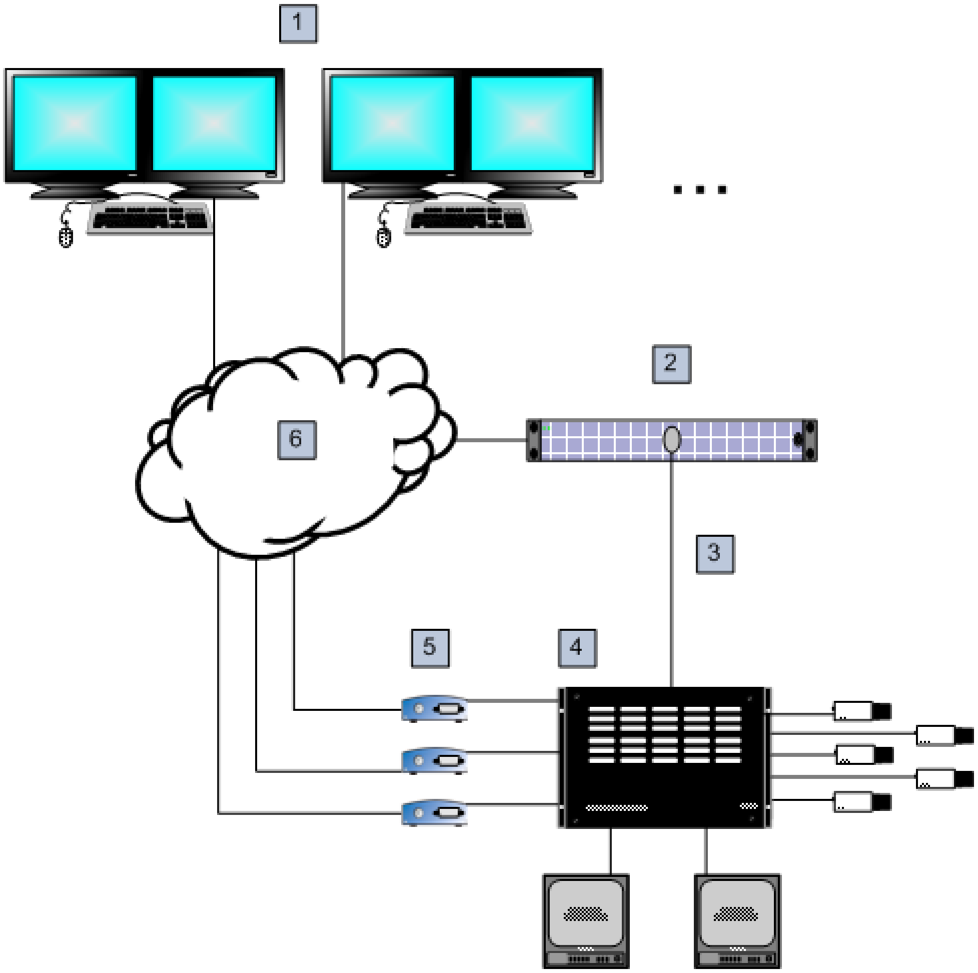


Figure 5.6: Bosch Video Management System local connection to a Bosch Allegiant matrix switch

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

Remote connection

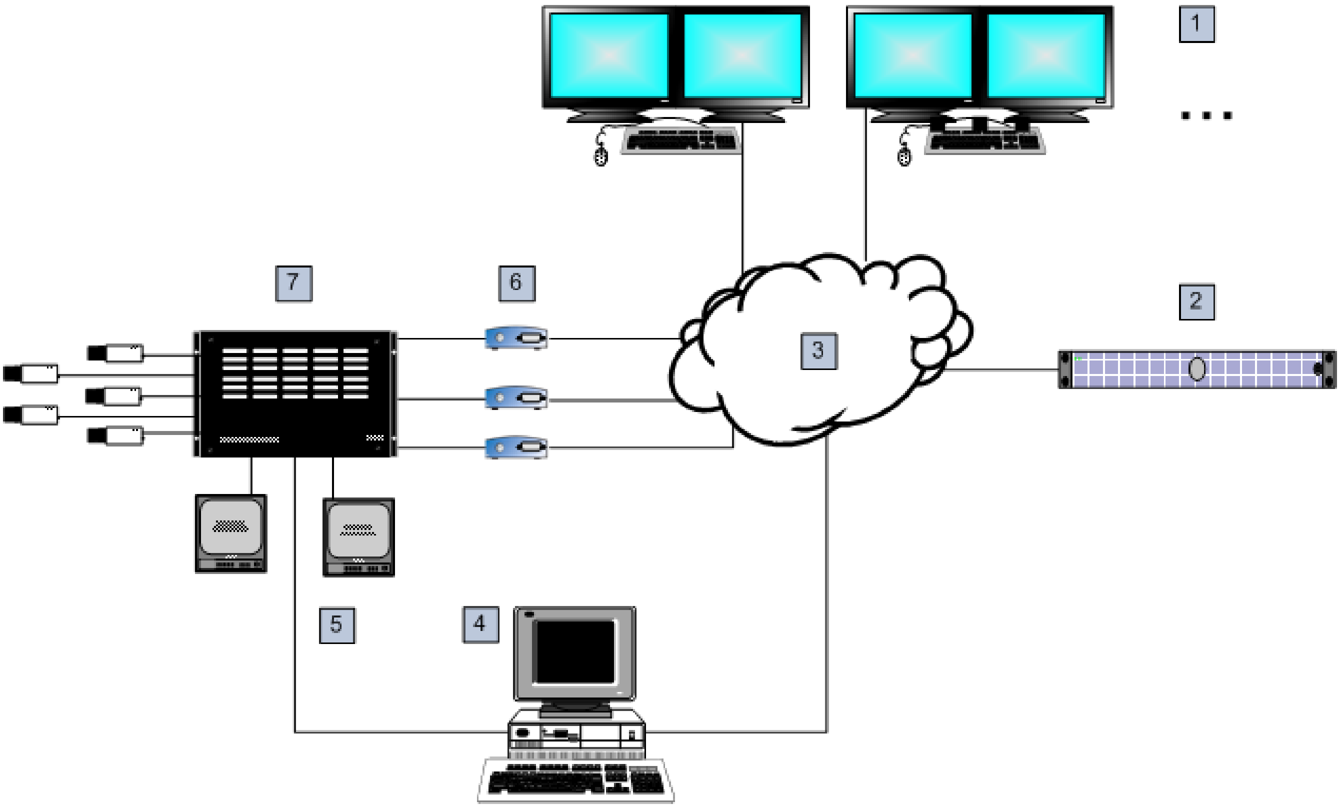


Figure 5.7: Bosch Video Management System remote connection to a Bosch Allegiant matrix switch

1	Bosch VMS 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 Bosch VMS
- Configuring user names

Wiring

To configure the control channel between Bosch VMS 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 Bosch VMS 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 Bosch VMS 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 Bosch VMS

1. Start the Bosch VMS Management Server service, start the Configuration Client, and add the Allegiant device by adding this configuration file (see *Adding a device manually, page 150* for the step-by-step instruction).
2. Ensure that the Allegiant Master Control Software configuration file used in Bosch VMS matches the current Allegiant configuration.
   Bosch VMS 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 236*

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

- *Configuring a Bosch Allegiant device, page 157*

See also

- *Matrix Switches page, page 236*

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 Bosch VMS 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.

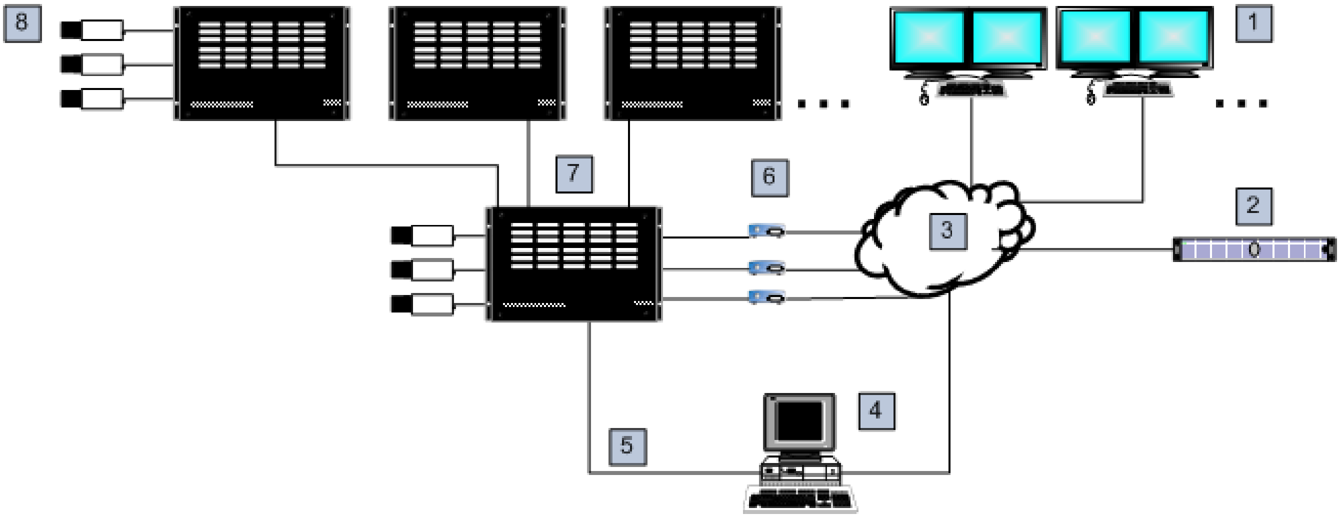


Figure 5.8: Bosch Allegiant system extended with Satellite switches

1	Bosch VMS 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 Bosch VMS

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 Bosch VMS.
-ALARM	Deactivate an alarm	Closes a virtual input in Bosch VMS.
System		
TC8x00>HEX	Set Hexadecimal Mode	

Supported command	**Description**	**Remarks**
Switching/Sequence		
TC8x00>DECIMAL	Set Decimal Mode	

6 Getting started

This chapter provides information on how to get started with Bosch VMS.

6.1 Installing the software modules

Caution!
Close Configuration Client before you start the Bosch VMS Setup.

Caution!
Do not install DiBos Web client on any Bosch VMS computer.

Install every software module on the computer that is supposed to be used for this module.

To install:

1. Insert the product CD-ROM.
2. Start Setup.exe or start the Bosch VMS Setup on the Welcome screen.
3. In the next dialog box, select the modules to be installed on this computer.
4. Follow the instructions on the screen.

6.2 Scanning for devices

Main window > **Devices**

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

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

See also

- *To add VRM devices via scan:, page 81*
- *To add encoders via scan:, page 82*
- *To add Bosch live only devices via scan:, page 82*
- *To add ONVIF live only devices via scan:, page 83*
- *To add local storage encoders via scan:, page 83*
- *To add VSG devices via scan:, page 83*
- *To add DVR devices via scan:, page 84*
- *To add VIDOS NVRs via scan:, page 84*

To add VRM devices via scan:

1. Right-click and click **Scan for VRM Devices**.
   The **Bosch VMS Scan Wizard** dialog box is displayed.
2. Select the desired check boxes for the devices that you want to add.

3. In the **Role** list, select the desired role.
   It depends on the current type of the VRM device which new role you can select.
   If you select **Mirrored** or **Failover**, the next configuration step is additionally required.
4. Click **Next >>**.
   The **Authenticate Devices** dialog box of the wizard is displayed.
5. Type in the password for each device that is protected by a password.
   Password check is performed automatically, when you do not enter a further character in the password field for a few seconds or you click outside the password field.
   If the passwords of all devices are identical, you can enter it in the first **Password** field. Then right-click this field and click **Copy cell to column**.
   In the **Status** column, the successful logons are indicated with 🔓.
   The failed logons are indicated with 🔒.
6. Click **Finish**.
   The device is added to your Bosch VMS.

To add encoders via scan:

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

To add Bosch live only devices via scan:

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

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

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

The failed logons are indicated with 🔒.

5. Click **Finish**.
   The device is added to your Bosch VMS.

To add ONVIF live only devices via scan:

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

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

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

To add local storage encoders via scan:

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

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

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

To add VSG devices via scan:

1. Right-click and click **Scan for Video Streaming Gateways**.
   The **Bosch VMS Scan Wizard** dialog box is displayed.

2. Select the required VSG devices, select the desired VRM pool and click **Assign** to assign them to the VRM pool.
3. Click **Next >>**.
   The **Authenticate Devices** dialog box of the wizard is displayed.
4. Type in the password for each device that is protected by a password.
   Password check is performed automatically, when you do not enter a further character in the password field for a few seconds or you click outside the password field.
   If the passwords of all devices are identical, you can enter it in the first **Password** field. Then right-click this field and click **Copy cell to column**.
   In the **Status** column, the successful logons are indicated with 🔓.
   The failed logons are indicated with 🔒.
5. Click **Finish**.
   The device is added to your Bosch VMS.

To add DVR devices via scan:

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

To add VIDOS NVRs via scan:

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

5. Click **Finish**.
   The device is added to your Bosch VMS.

See also

– *Adding a device manually, page 150*
– *Bosch VMS Scan Wizard, page 261*

6.3 Using Config Wizard

To start Config Wizard**:**

▸ Click **Start** > **All Programs** > **Bosch VMS** > Config Wizard
  The Welcome page is displayed.

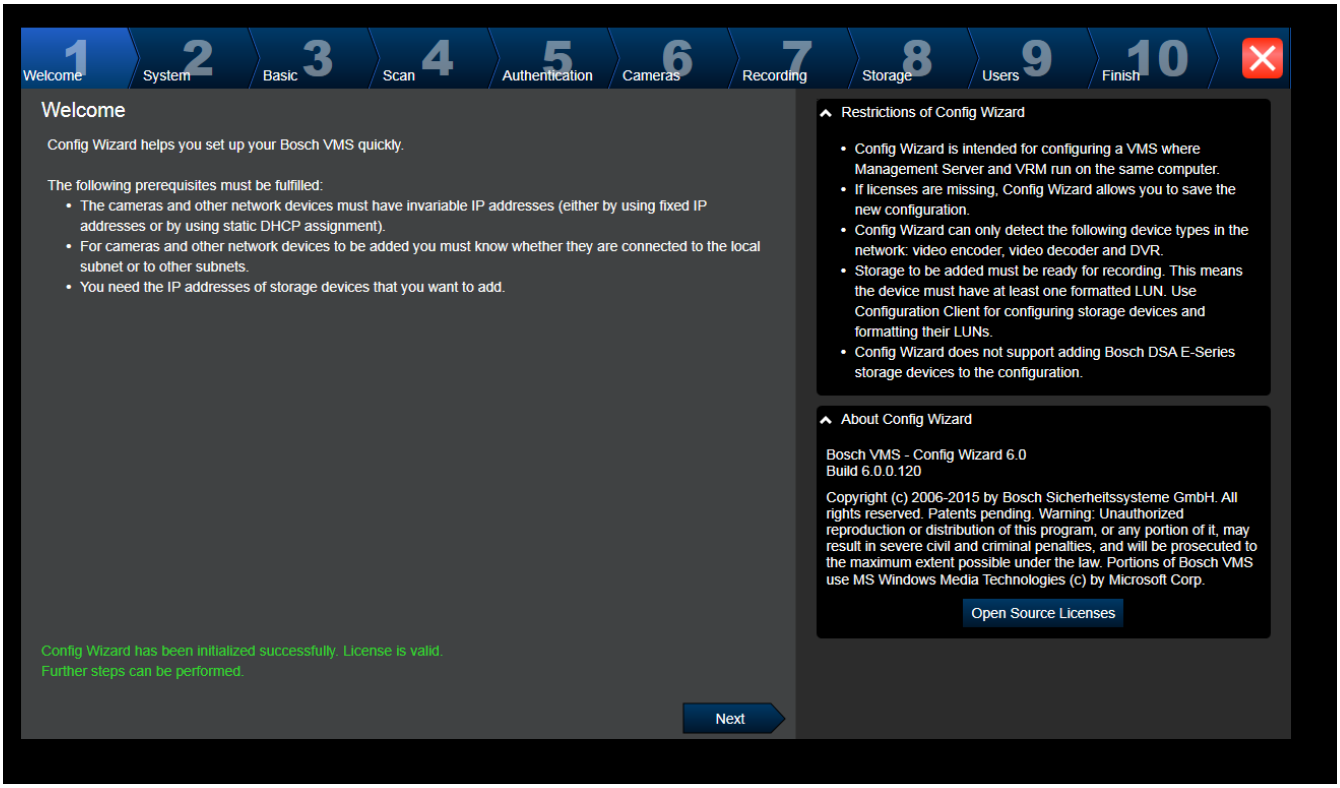
Related Topics

– *Config Wizard, page 26*

Available pages

– *Welcome page, page 86*
– *System page, page 87*
– *Basic page, page 88*
– *Scan page, page 89*
– *Authentication page, page 90*
– *Cameras page, page 91*
– *Recording page, page 92*
– *Storage page, page 93*
– *Users page, page 94*
– *Finish page, page 95*

Welcome page



Welcome

Config Wizard helps you set up your Bosch VMS quickly.

The following prerequisites must be fulfilled:

- The cameras and other network devices must have invariable IP addresses (either by using fixed IP addresses or by using static DHCP assignment).
- For cameras and other network devices to be added you must know whether they are connected to the local subnet or to other subnets.
- You need the IP addresses of storage devices that you want to add.

Config Wizard has been initialized successfully. License is valid.
Further steps can be performed.

Restrictions of Config Wizard

- Config Wizard is intended for configuring a VMS where Management Server and VRM run on the same computer.
- If licenses are missing, Config Wizard allows you to save the new configuration.
- Config Wizard can only detect the following device types in the network: video encoder, video decoder and DVR.
- Storage to be added must be ready for recording. This means the device must have at least one formatted LUN. Use Configuration Client for configuring storage devices and formatting their LUNs.
- Config Wizard does not support adding Bosch DSA E-Series storage devices to the configuration.

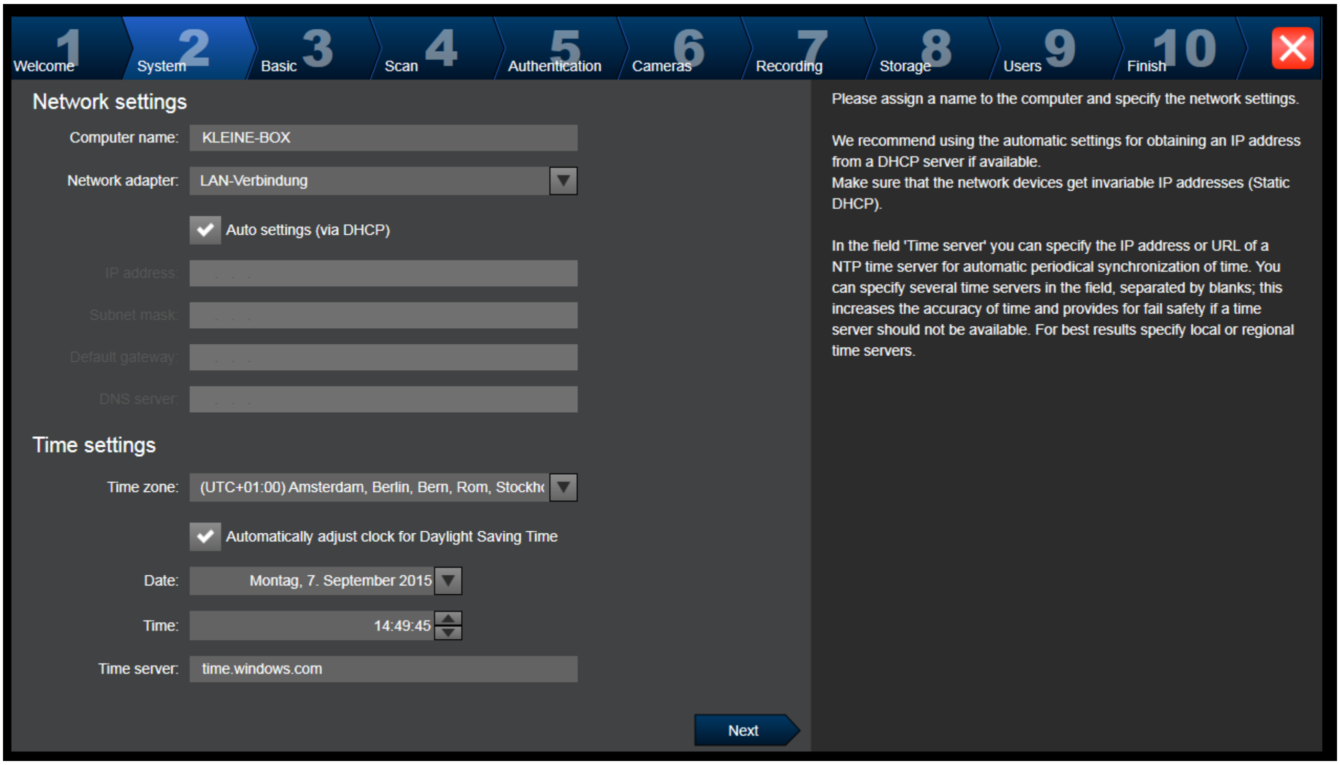
About Config Wizard

Bosch VMS - Config Wizard 6.0
Build 6.0.0.120

Copyright (c) 2006-2015 by Bosch Sicherheitssysteme GmbH. All rights reserved. Patents pending. Warning: Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law. Portions of Bosch VMS use MS Windows Media Technologies (c) by Microsoft Corp.

- Click **Next** button to continue.

System page



Network settings

Computer name: KLEINE-BOX

Network adapter: LAN-Verbindung

☑ Auto settings (via DHCP)

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

DNS server: . . .

Time settings

Time zone: (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockh‹

☑ Automatically adjust clock for Daylight Saving Time

Date: Montag, 7. September 2015

Time: 14:49:45

Time server: time.windows.com

Please assign a name to the computer and specify the network settings.

We recommend using the automatic settings for obtaining an IP address from a DHCP server if available.
Make sure that the network devices get invariable IP addresses (Static DHCP).

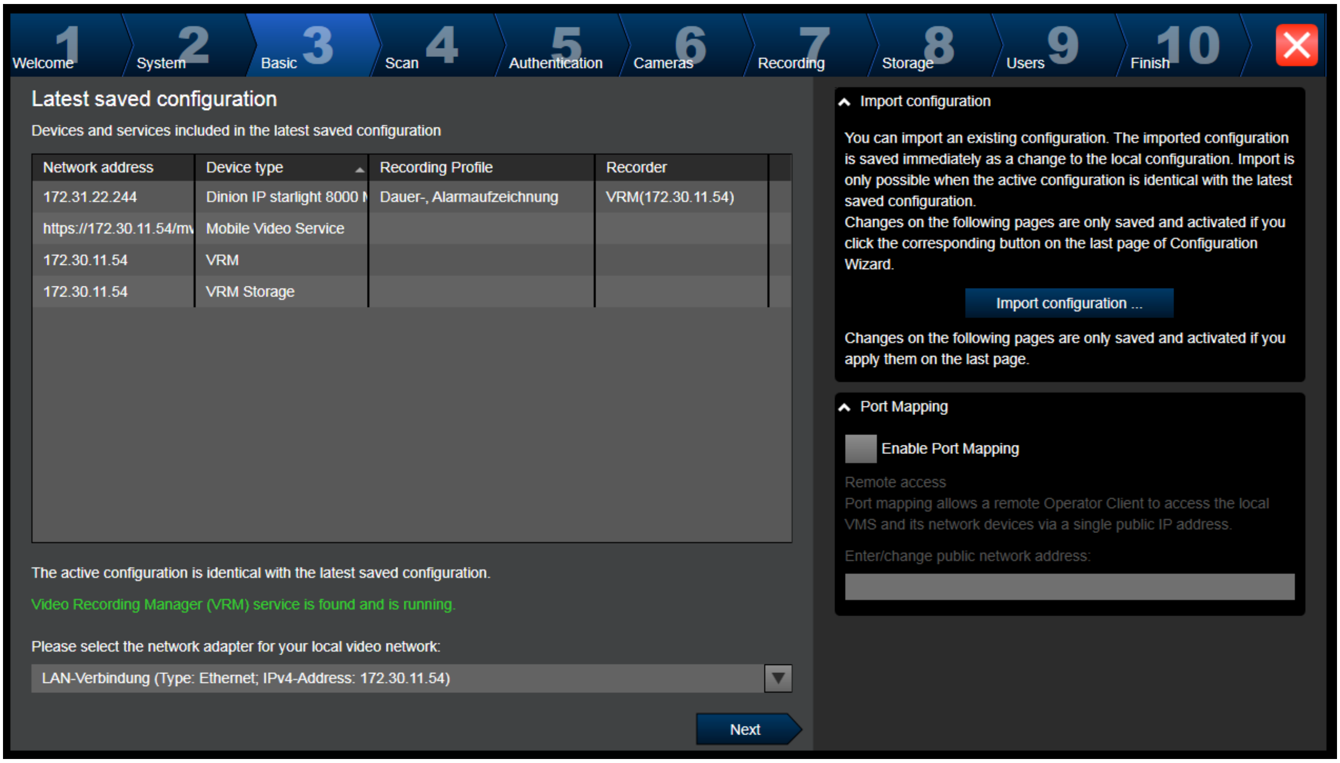
In the field 'Time server' you can specify the IP address or URL of a NTP time server for automatic periodical synchronization of time. You can specify several time servers in the field, separated by blanks; this increases the accuracy of time and provides for fail safety if a time server should not be available. For best results specify local or regional time servers.

Notice!
Only available on DIVAR IP 3000 and DIVAR IP 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** button, the settings are activated.

Basic page



Latest saved configuration

Devices and services included in the latest saved configuration

Network address	Device type	Recording Profile	Recorder
172.31.22.244	Dinion IP starlight 8000 I	Dauer-, Alarmaufzeichnung	VRM(172.30.11.54)
https://172.30.11.54/mv	Mobile Video Service		
172.30.11.54	VRM		
172.30.11.54	VRM Storage		

The active configuration is identical with the latest saved configuration.

Video Recording Manager (VRM) service is found and is running.

Please select the network adapter for your local video network:

LAN-Verbindung (Type: Ethernet; IPv4-Address: 172.30.11.54)

Next

Import configuration

You can import an existing configuration. The imported configuration is saved immediately as a change to the local configuration. Import is only possible when the active configuration is identical with the latest saved configuration.

Changes on the following pages are only saved and activated if you click the corresponding button on the last page of Configuration Wizard.

Import configuration ...

Changes on the following pages are only saved and activated if you apply them on the last page.

Port Mapping

□ Enable Port Mapping

Remote access

Port mapping allows a remote Operator Client to access the local VMS and its network devices via a single public IP address.

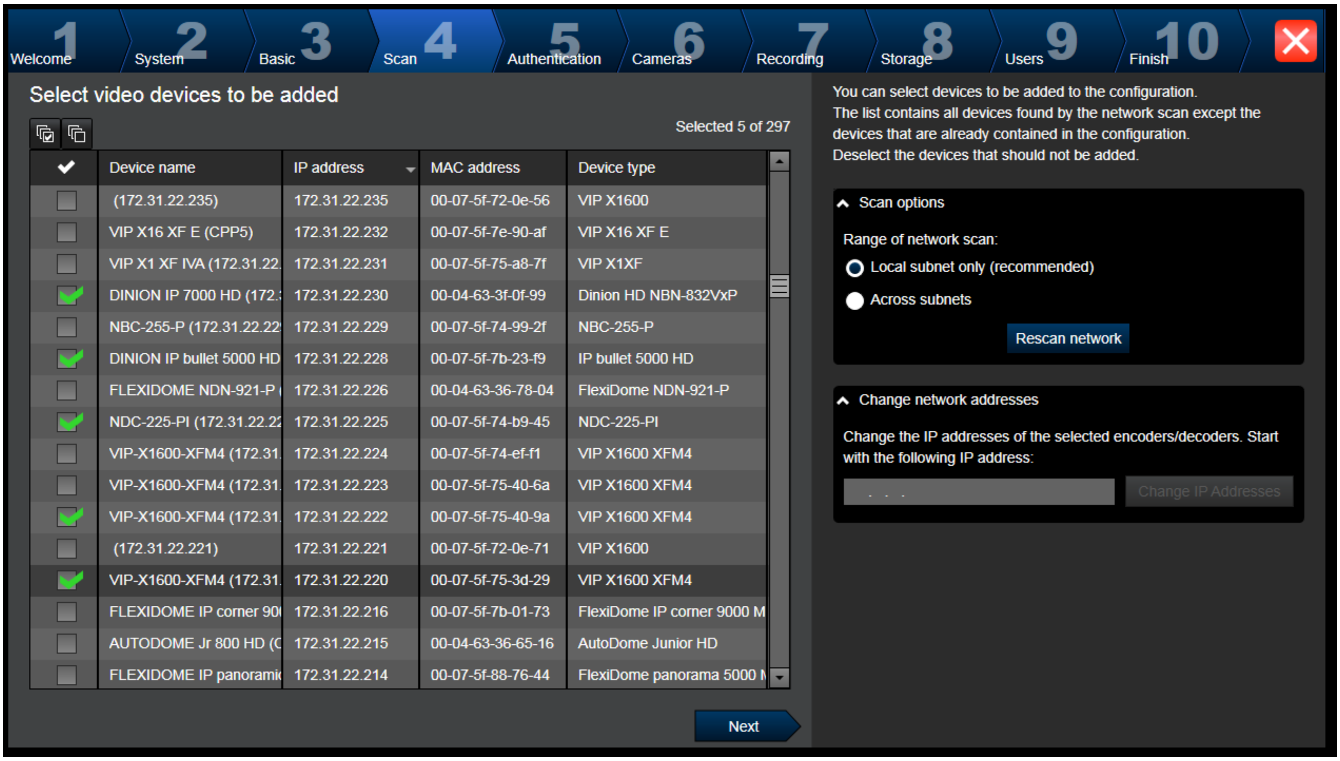
Enter/change public network address:

This page displays the latest saved configuration. You can import a Bosch VMS 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



Select video devices to be added

Selected 5 of 297

✓	Device name	IP address	MAC address	Device type
□	(172.31.22.235)	172.31.22.235	00-07-5f-72-0e-56	VIP X1600
□	VIP X16 XF E (CPP5)	172.31.22.232	00-07-5f-7e-90-af	VIP X16 XF E
□	VIP X1 XF IVA (172.31.22.	172.31.22.231	00-07-5f-75-a8-7f	VIP X1XF
☑	DINION IP 7000 HD (172.3	172.31.22.230	00-04-63-3f-0f-99	Dinion HD NBN-832VxP
□	NBC-255-P (172.31.22.22	172.31.22.229	00-07-5f-74-99-2f	NBC-255-P
☑	DINION IP bullet 5000 HD	172.31.22.228	00-07-5f-7b-23-f9	IP bullet 5000 HD
□	FLEXIDOME NDN-921-P (	172.31.22.226	00-04-63-36-78-04	FlexiDome NDN-921-P
☑	NDC-225-PI (172.31.22.22	172.31.22.225	00-07-5f-74-b9-45	NDC-225-PI
□	VIP-X1600-XFM4 (172.31.	172.31.22.224	00-07-5f-74-ef-f1	VIP X1600 XFM4
□	VIP-X1600-XFM4 (172.31.	172.31.22.223	00-07-5f-75-40-6a	VIP X1600 XFM4
☑	VIP-X1600-XFM4 (172.31.	172.31.22.222	00-07-5f-75-40-9a	VIP X1600 XFM4
□	(172.31.22.221)	172.31.22.221	00-07-5f-72-0e-71	VIP X1600
☑	VIP-X1600-XFM4 (172.31.	172.31.22.220	00-07-5f-75-3d-29	VIP X1600 XFM4
□	FLEXIDOME IP corner 90	172.31.22.216	00-07-5f-7b-01-73	FlexiDome IP corner 9000 M
□	AUTODOME Jr 800 HD (C	172.31.22.215	00-04-63-36-65-16	AutoDome Junior HD
□	FLEXIDOME IP panoramic	172.31.22.214	00-07-5f-88-76-44	FlexiDome panorama 5000 M

Next

You can select devices to be added to the configuration.
The list contains all devices found by the network scan except the devices that are already contained in the configuration.
Deselect the devices that should not be added.

Scan options

Range of network scan:

● Local subnet only (recommended)

○ Across subnets

Rescan network

Change network addresses

Change the IP addresses of the selected encoders/decoders. Start with the following IP address:

. . .

Change IP Addresses

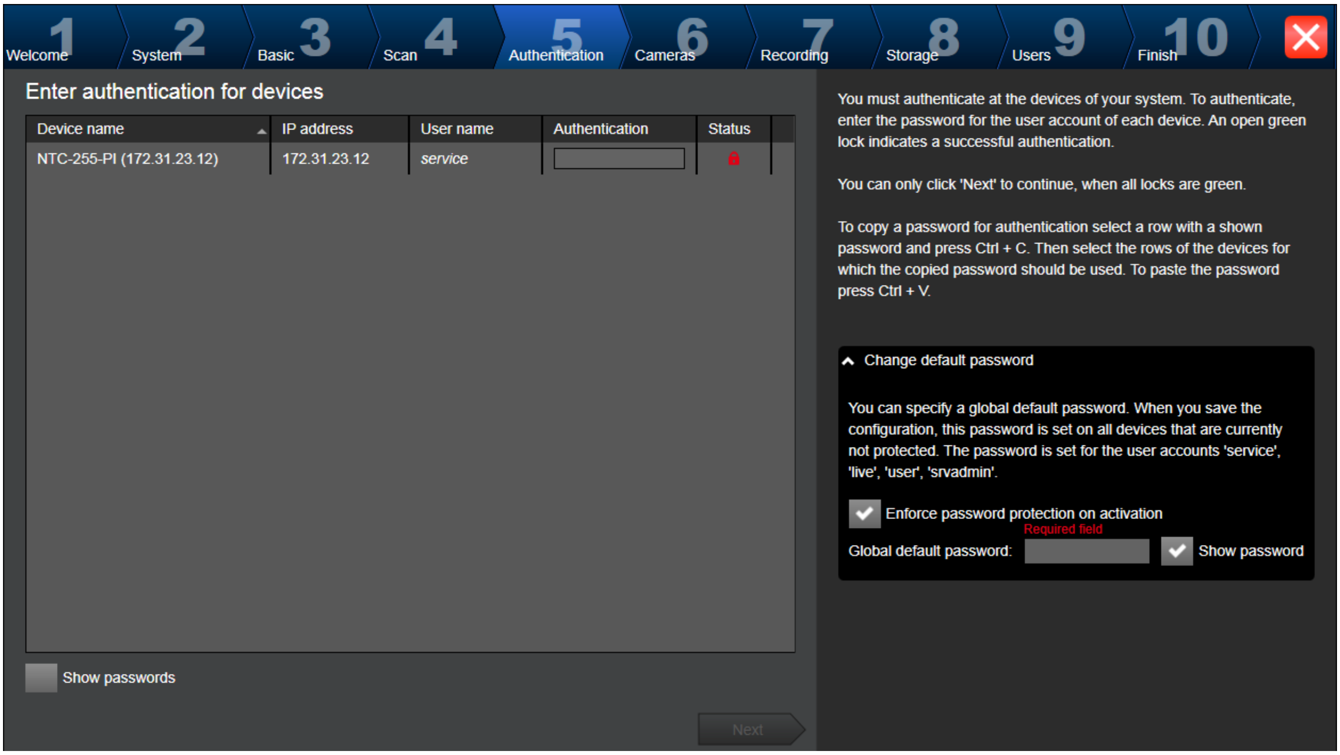
Note:
The scan for devices can take a time. You can cancel the scan. All devices that were already scanned, are displayed in the table.

This page displays all video devices that are not included in the latest saved configuration.

Deselect 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



Enter authentication for devices

Device name	IP address	User name	Authentication	Status
NTC-255-PI (172.31.23.12)	172.31.23.12	*service*		🔒

□ Show passwords

You must authenticate at the devices of your system. To authenticate, enter the password for the user account of each device. An open green lock indicates a successful authentication.

You can only click 'Next' to continue, when all locks are green.

To copy a password for authentication select a row with a shown password and press Ctrl + C. Then select the rows of the devices for which the copied password should be used. To paste the password press Ctrl + V.

Change default password

You can specify a global default password. When you save the configuration, this password is set on all devices that are currently not protected. The password is set for the user accounts 'service', 'live', 'user', 'srvadmin'.

☑ Enforce password protection on activation

Required field

Global default password: ☑ Show password

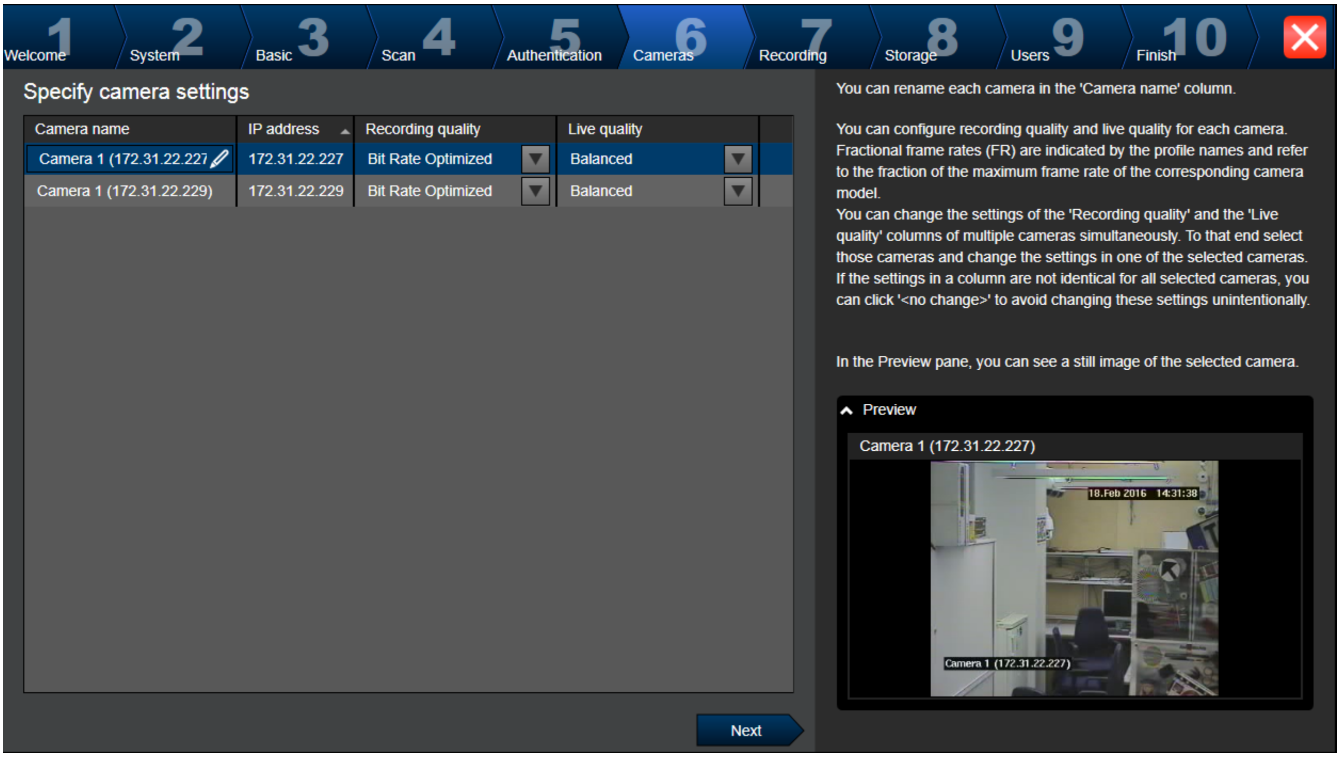
This page is used to authenticate at video devices protected by password. For easy authentication with the same password for multiple devices you can use the clipboard (CTRL +C, CTRL+V):

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 ere currently not protected by a password.

Cameras page



Specify camera settings

Camera name	IP address	Recording quality	Live quality
Camera 1 (172.31.22.227	172.31.22.227	Bit Rate Optimized	Balanced
Camera 1 (172.31.22.229)	172.31.22.229	Bit Rate Optimized	Balanced

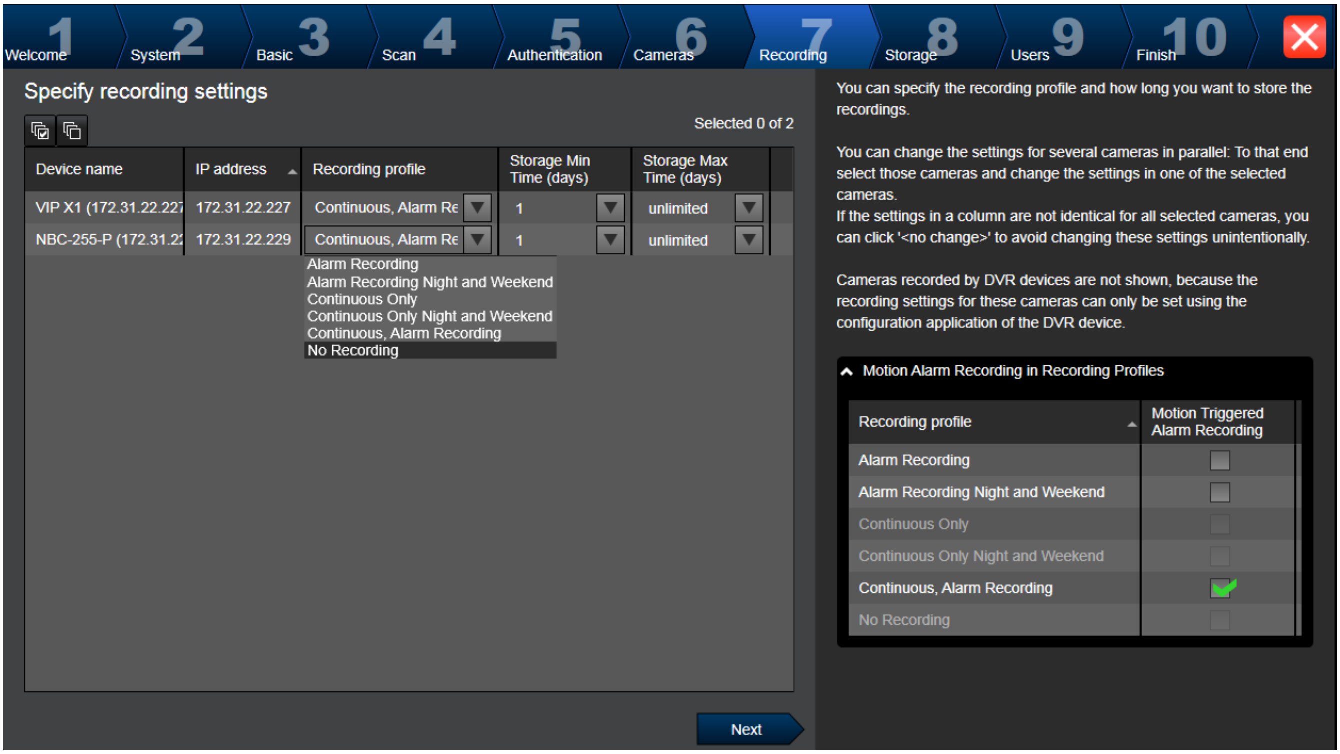
You can rename each camera in the 'Camera name' column.

You can configure recording quality and live quality for each camera. Fractional frame rates (FR) are indicated by the profile names and refer to the fraction of the maximum frame rate of the corresponding camera model.
You can change the settings of the 'Recording quality' and the 'Live quality' columns of multiple cameras simultaneously. To that end select those cameras and change the settings in one of the selected cameras. If the settings in a column are not identical for all selected cameras, you can click '<no change>' to avoid changing these settings unintentionally.

In the Preview pane, you can see a still image of the selected camera.

Use this page to manage the cameras of your system.

Recording page



Specify recording settings

Selected 0 of 2

Device name	IP address	Recording profile	Storage Min Time (days)	Storage Max Time (days)
VIP X1 (172.31.22.227	172.31.22.227	Continuous, Alarm Re	1	unlimited
NBC-255-P (172.31.22	172.31.22.229	Continuous, Alarm Re	1	unlimited

Alarm Recording
Alarm Recording Night and Weekend
Continuous Only
Continuous Only Night and Weekend
Continuous, Alarm Recording
No Recording

You can specify the recording profile and how long you want to store the recordings.

You can change the settings for several cameras in parallel: To that end select those cameras and change the settings in one of the selected cameras.
If the settings in a column are not identical for all selected cameras, you can click '<no change>' to avoid changing these settings unintentionally.

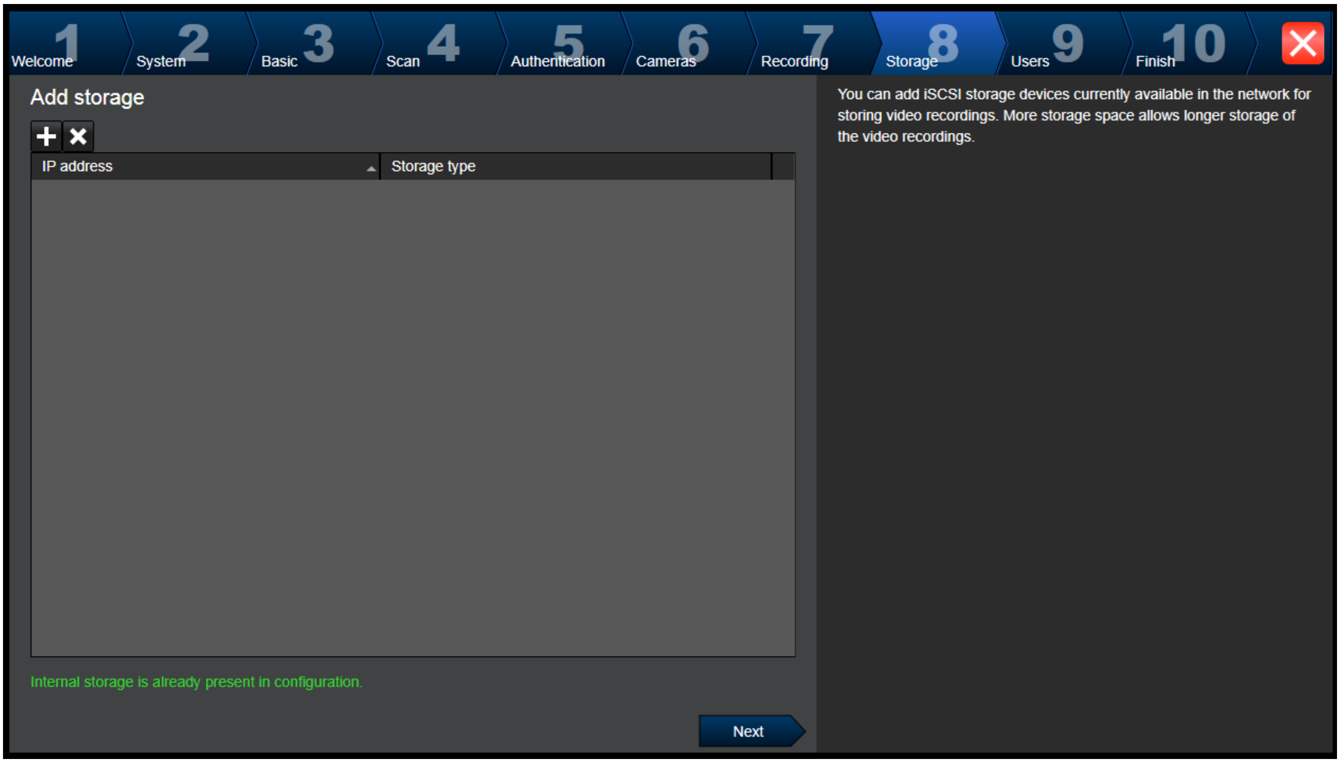
Cameras recorded by DVR devices are not shown, because the recording settings for these cameras can only be set using the configuration application of the DVR device.

Motion Alarm Recording in Recording Profiles

Recording profile	Motion Triggered Alarm Recording
Alarm Recording	☐
Alarm Recording Night and Weekend	☐
Continuous Only	☐
Continuous Only Night and Weekend	☐
Continuous, Alarm Recording	☑
No Recording	☐

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

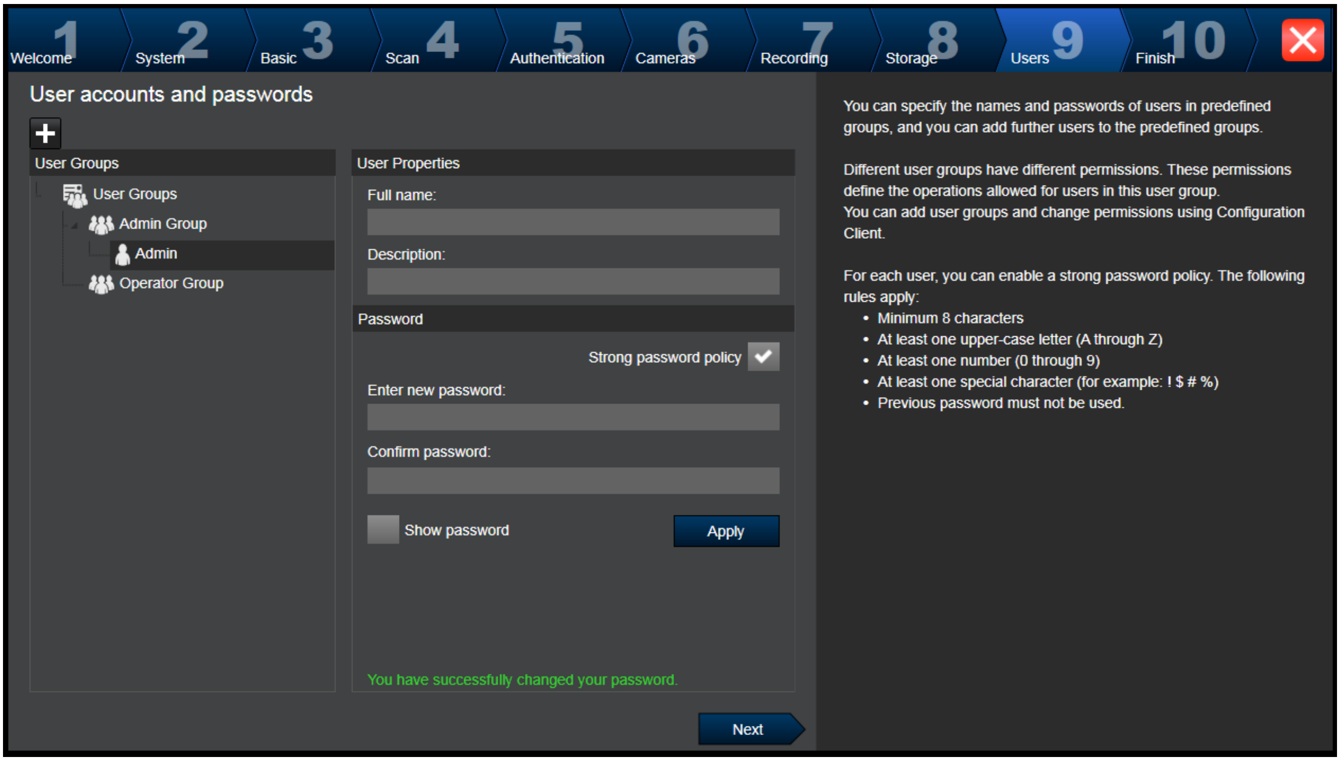


Internal storage is already present in configuration.

You can add iSCSI storage devices currently available in the network for storing video recordings. More storage space allows longer storage of the video recordings.

This page allows the addition of further iSCSI storage devices

Users page



You have successfully changed your password.

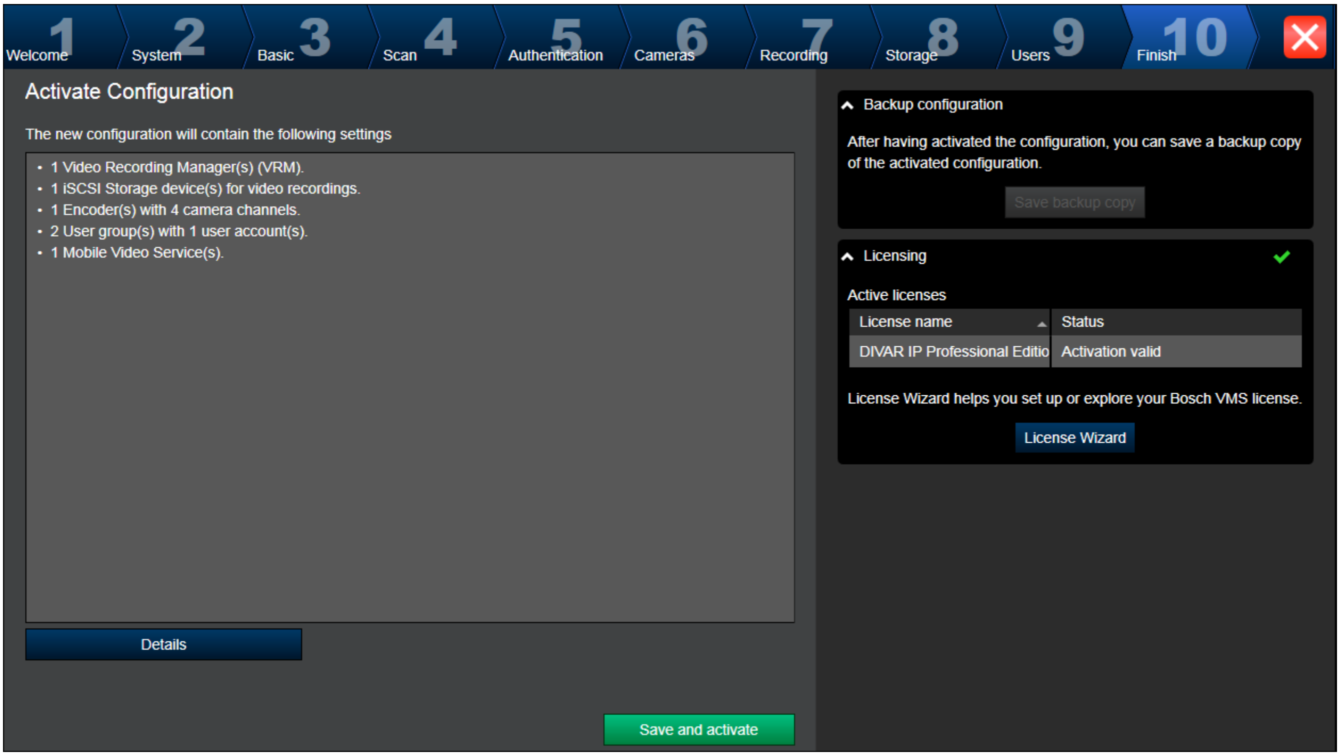
You can specify the names and passwords of users in predefined groups, and you can add further users to the predefined groups.

Different user groups have different permissions. These permissions define the operations allowed for users in this user group.
You can add user groups and change permissions using Configuration Client.

For each user, you can enable a strong password policy. The following rules apply:
- Minimum 8 characters
- At least one upper-case letter (A through Z)
- At least one number (0 through 9)
- At least one special character (for example: ! $ # %)
- Previous password must not be used.

You can add users and passwords and you can activate the strong password policy for each user. Use Configuration Client to add user groups and to change permissions.

Finish page



Activate Configuration

The new configuration will contain the following settings

- 1 Video Recording Manager(s) (VRM).
- 1 iSCSI Storage device(s) for video recordings.
- 1 Encoder(s) with 4 camera channels.
- 2 User group(s) with 1 user account(s).
- 1 Mobile Video Service(s).

Backup configuration

After having activated the configuration, you can save a backup copy of the activated configuration.

Licensing ✓

Active licenses

License name	Status
DIVAR IP Professional Editio	Activation valid

License Wizard helps you set up or explore your Bosch VMS license.

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**.

6.4 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

6.5 Using Server Lookup

A single user of Configuration Client or Operator Client may want to connect to multiple system access points sequentially. This access is called Server Lookup. System access points can be Management Server or Enterprise Management Server.
Server Lookup supports you in locating system access points by their names or descriptions. The user retrieves the list of system access points during logon. He needs to connect to the server hosting the configuration with **Server List / Address Book**.

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.

6.6 Configuring remote access

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

6.6.1 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, page 225*

6.6.2 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 107*
- *Creating a group or account, page 204*
- *Remote Access Settings dialog box, page 225*

6.7 Activating the software licenses

Main window
When you install Bosch VMS 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.
To obtain the Activation Key for a license, you need the Authorization Number. This number is included in your product box.
With a Bundle Information file you can ease the process of activating.

Caution!
The computer signature is used for licensing. This 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.
Switchover of a Stratus server mainboard without teaming settings.

To activate the software:

1. Start 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.
   If you have received a Bundle Information file, click **Import Bundle Info** to import it.
4. Click **Activate**.
   The **License Activation** dialog box is displayed.
5. Write down the computer signature or copy and paste it into a text file.
6. On a computer with Internet access, enter the following URL into your browser:
   https://activation.boschsecurity.com
   If you do not have an account to access the Bosch License Activation Center, either create a new account (recommended) or click the link to activate a new license without logging on. If you create an account and log on before activating, the License Manager keeps track of your activations. You can then review this at any time.
   Follow the instructions to obtain the License Activation Key.
7. Return to the Bosch VMS software. In the **License Activation** dialog box, type the License Activation Key obtained from the License Manager and click **Activate**.
   The software package is activated.

See also

- *License Manager dialog box, page 222*
- *License Activation dialog box, page 223*

6.8 Starting Configuration Client

Only the user called Admin can log on to Configuration Client.

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** > Bosch VMS > Config 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.

6.9 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 **System language**, the language of your Windows installation is used.
3. Click **OK**.
   The language is switched after the next restart of the application.

6.10 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.
2. In the **Language:** list, select the desired language.
3. Click 💾 to save the settings.
4. Click 👆 to activate the configuration.
   Restart Operator Client.

6.11 Adding a new license

Main window
Have the Activation Letter at hand that you received from Bosch.
To add a new license:

1. On the **Tools** menu, click **License Manager...**.
   The **License Manager** dialog box is displayed.
2. Select the software package that you want to activate.

3. Click **Activate**.
   The **License Activation** dialog box is displayed.
4. Type the License Activation Key that you find in the Activation Letter.
5. Click **Activate**.
   The software package is activated.
6. Repeat this procedure for each software package that you want to activate.

Related Topics

- *License Manager dialog box, page 222*
- *License Activation dialog box, page 223*

6.12 Maintaining Bosch VMS

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

- Export Bosch VMS 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 99* 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 99* for the procedure.
- Save VRM configuration file (config.xml)
  - See *To save VRM configuration:, page 100* 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 **Bosch VMS Central Server** on the (Enterprise) Management Server.
2. Copy the file elements.bvms to the desired directory for backup.
3. Start the service **Bosch VMS 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 Bosch VMS configuration. When you change something within these data, it is written to config.xml after activating the Bosch VMS configuration.
The following settings are not stored in the Bosch VMS 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 Bosch VMS 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

6.13 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 Bosch VMS, page 99*

6.13.1 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 **Bosch VMS Central Server** service is stopped.

1. Stop the service **Bosch VMS 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 **Bosch VMS 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\`.

6.13.2 Replacing a VRM

To replace the VRM device from within Bosch VMS:

Prerequisite is an installed OS with correct network settings and the correct version of VRM (for example from the suitable Bosch VMS Setup DVD).

1. Start Bosch VMS 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 > > iSCSI > **Load Balancing**

To replace the VRM device without Bosch VMS:

Prerequisite is an installed OS with correct network settings and the correct version of VRM (e.g. from the suitable Bosch Bosch VMS SetupDVD).

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.

6.13.3 Replacing an encoder or decoder

Caution!

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 Bosch VMS Configuration Client! When deleting the device from VRM, recording is lost.
3. Connect the new device of the same type to the network.

Caution!

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 Bosch VMS (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 Bosch VMS 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 > Right-click > Click **Edit Encoder** > **Edit Encoder** dialog box
or

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

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

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

Main window > **Devices** > Expand > 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 Bosch VMS.

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 ONVIV 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 Bosch VMS

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

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

Stored in the Bosch VMS configuration but not changed on the devices:

- IP address (you can change IP addresses with Bosch VMS IP Device Configuration)
- Relay / input names (difference between names in the device and names configured in Bosch VMS 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.

6.13.4 Replacing an Operator Client

To replace an Operator Client workstation:

1. Replace the computer.
2. Start the Bosch VMS 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.

6.13.5 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.

6.13.6 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.

6.14 Configuring time synchronization

Notice!
Ensure that the time of the all computers of Bosch VMS 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.

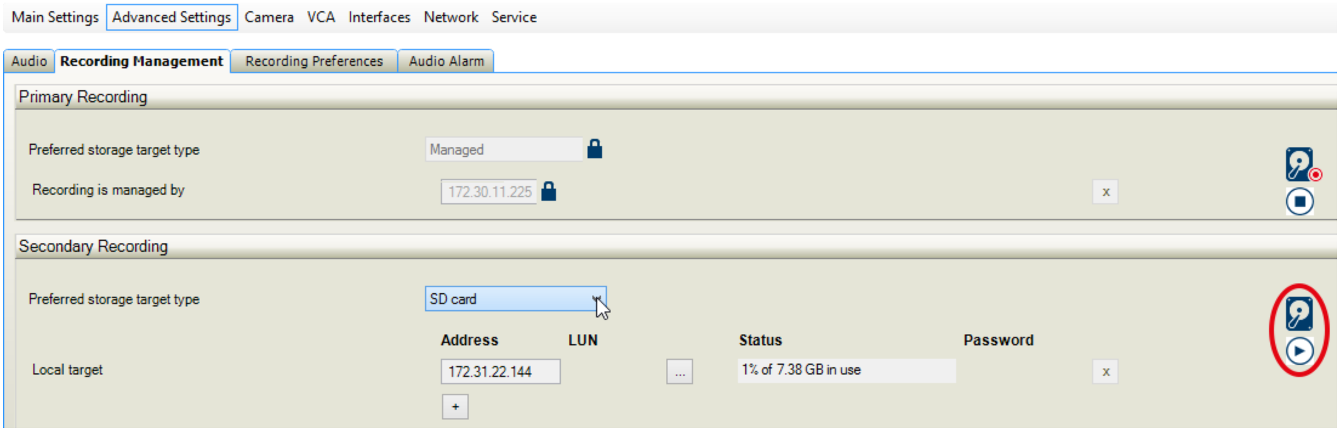
6.15 Configuring the storage media of an encoder

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:



Primary Recording

Preferred storage target type: Managed

Recording is managed by: 172.30.11.225

Secondary Recording

Preferred storage target type: SD card

	Address	LUN	Status	Password
Local target	172.31.22.144		1% of 7.38 GB in use	

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 286*
– *Configuring the ANR function, page 189*

6.16 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 107*
2. *Creating an Enterprise User Group, page 108*
3. *Creating an Enterprise Account, page 109*

This example covers the Scenario 1 described in the *Enterprise System , page 26* chapter:

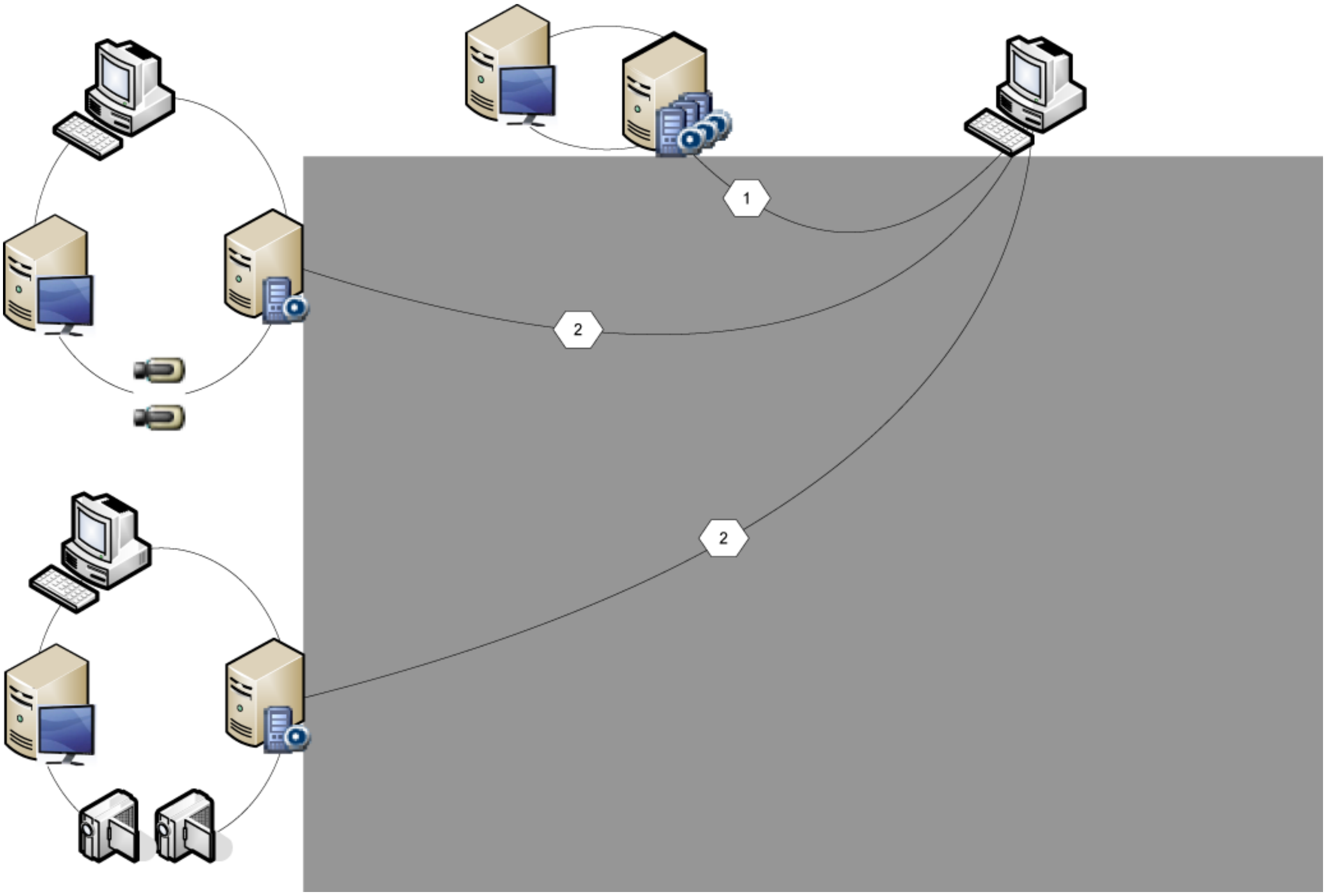


Figure 6.9: Enterprise Scenario 1

You need valid licenses for using an Enterprise System.

6.16.1 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.

1. Click to save the settings.
2. Click to undo the last setting.

3. 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:

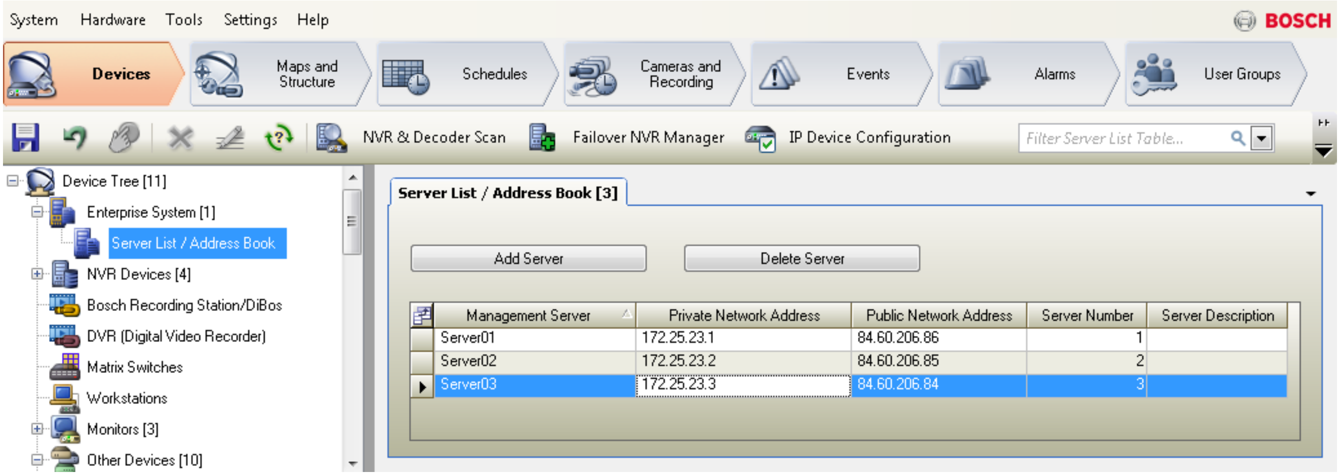
▶ Right-click on the table header and click **Add column**.
You can add up to 10 columns.
To delete a column, right-click the desired column and click **Delete column**.

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

The Management Server computers for your Enterprise System are configured.

Now configure the desired Enterprise User Groups and the Enterprise Access.

The following screenshot shows an example:



Management Server	Private Network Address	Public Network Address	Server Number	Server Description
Server01	172.25.23.1	84.60.206.86	1	
Server02	172.25.23.2	84.60.206.85	2	
Server03	172.25.23.3	84.60.206.84	3	

Related Topics

– *Enterprise System , page 26*
– *Server List / Address Book page, page 229*
– *User Groups page, page 361*
– *Using Server Lookup, page 96*

6.16.2 Creating an Enterprise User Group

Main window > **User Groups**

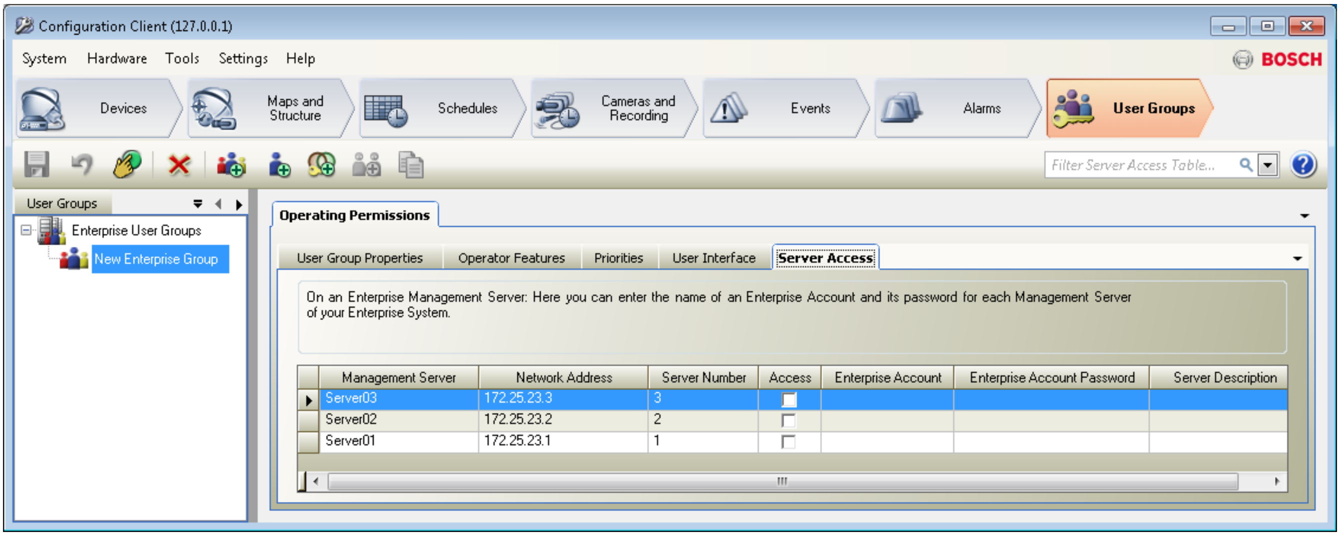
You perform the task of creating an Enterprise User Group for an Enterprise Management system on the Enterprise Management Server.

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 Groups tab.
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. Configure the operating permissions and server access for the configured Management Server computers as required.

The following screenshot shows an example:



On an Enterprise Management Server: Here you can enter the name of an Enterprise Account and its password for each Management Server of your Enterprise System.

Management Server	Network Address	Server Number	Access	Enterprise Account	Enterprise Account Password	Server Description
Server03	172.25.23.3	3	□			
Server02	172.25.23.2	2	□			
Server01	172.25.23.1	1	□			

See also

- *User Group Properties page, page 363*
- *Operator Features page, page 372*
- *Priorities page, page 374*
- *User Interface page, page 375*
- *Server Access page, page 376*

6.16.3 Creating an Enterprise Account

Main window > **User Groups**

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

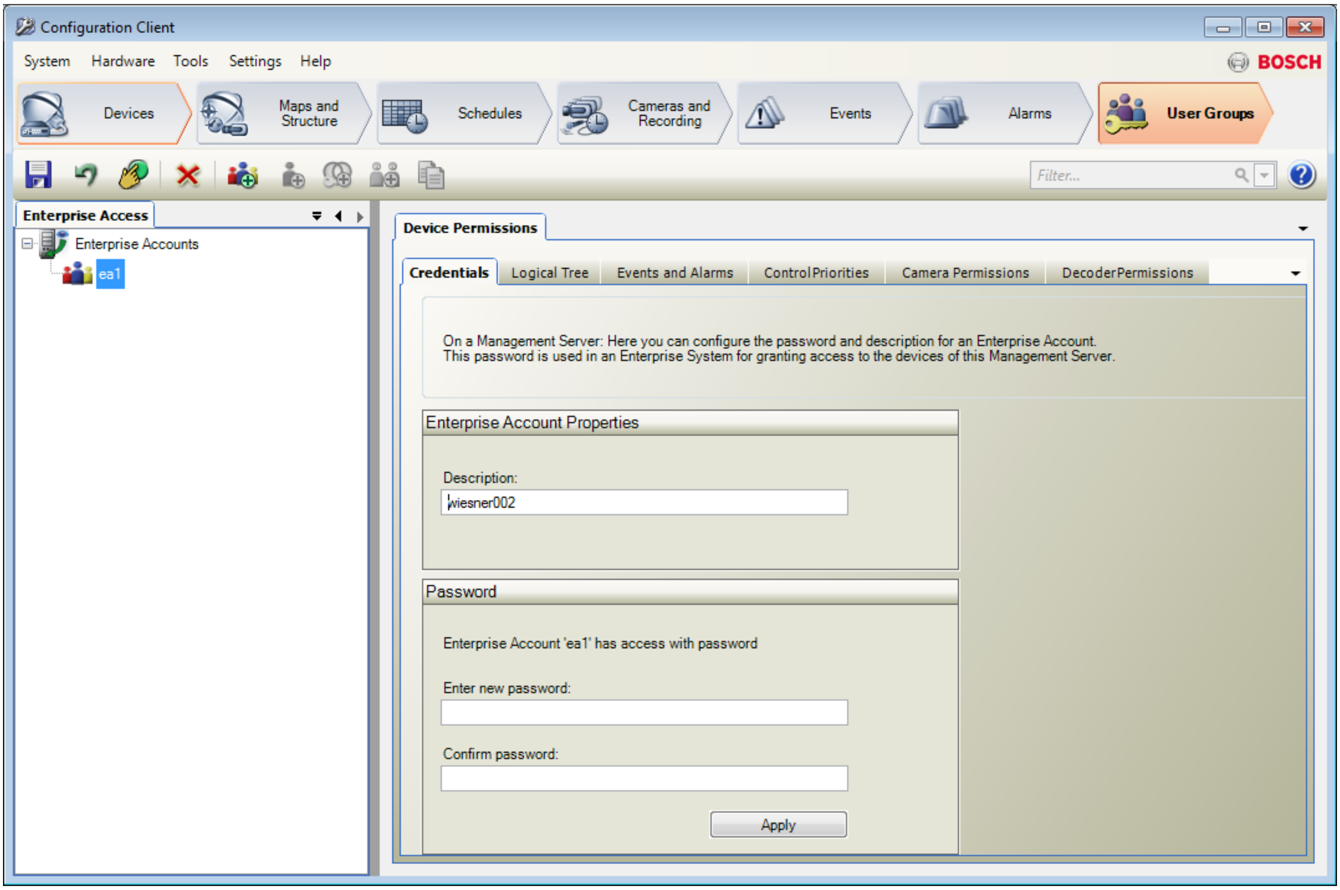
You perform the task of creating an Enterprise Account on a Management Server. Repeat this task on each Management Server that is a member of your Enterprise System.
You create an Enterprise Account to configure the device permissions for an Operator Client using an Enterprise System.

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. Click **OK**.
   The Enterprise Account is added to the corresponding tree.
5. Configure the credentials and the device permissions as required.

The following screenshot shows an example:



On a Management Server: Here you can configure the password and description for an Enterprise Account.
This password is used in an Enterprise System for granting access to the devices of this Management Server.

Description: wiesner002

Enterprise Account 'ea1' has access with password

Enter new password:

Confirm password:

See also

- *Credentials page, page 371*
- *Logical Tree page, page 372*
- *Events and Alarms page, page 369*
- *Control Priorities, page 367*
- *Camera Permissions page, page 366*
- *Decoder Permissions page, page 368*

6.17 Configuring the mounting position of a panoramic camera

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

or

Main window > **Devices** > >
or

Main window > **Devices** > >

To configure:

1. Click **Main Settings** > **Initialization**.
2. In the **Calibration** field, set the mounting position.

See also

– *Viewing modes of a panoramic camera, page 61*

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 112*
2. *Creating an Enterprise User Group, page 114*
3. *Creating an Enterprise Account, page 114*

This example covers the Scenario 1 described in the *Enterprise System , page 26* chapter:

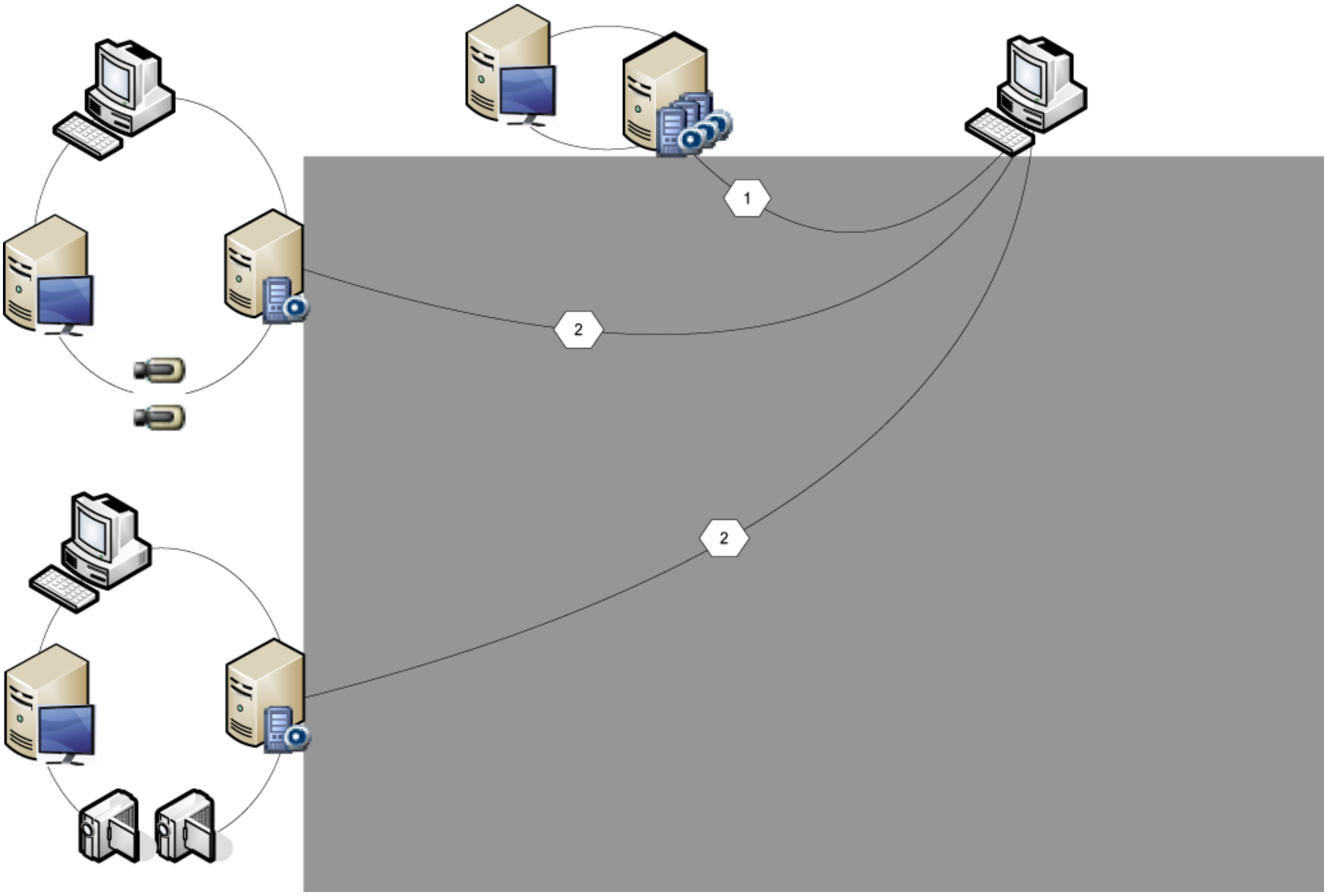


Figure 7.10: Enterprise Scenario 1

You need valid licenses for using an Enterprise System.

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.

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

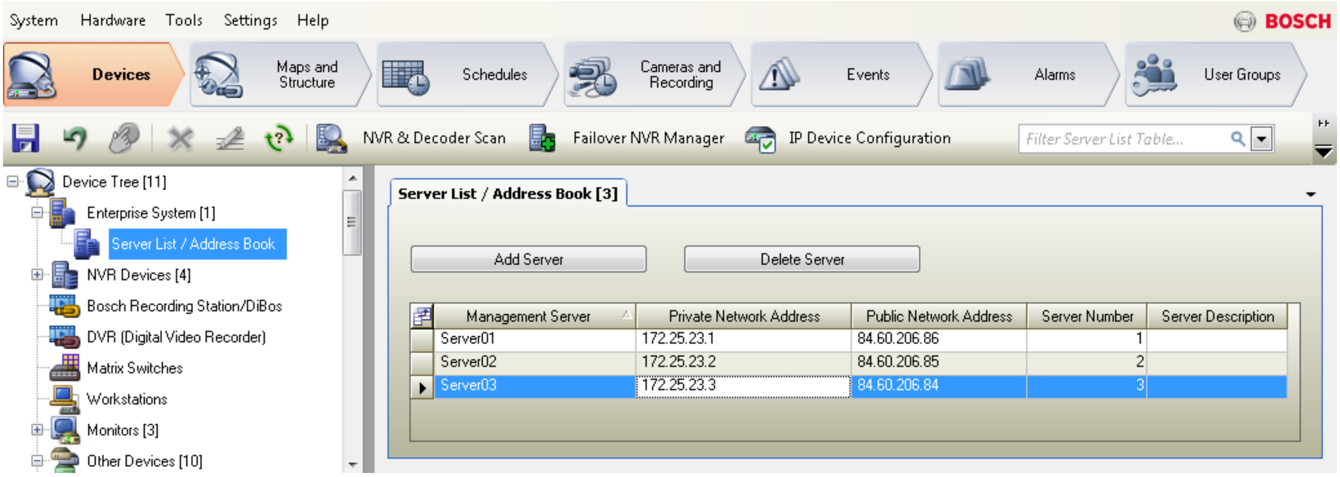
- Right-click on the table header and click **Add column**.
  You can add up to 10 columns.
  To delete a column, right-click the desired column and click **Delete column**.

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

The Management Server computers for your Enterprise System are configured.

Now configure the desired Enterprise User Groups and the Enterprise Access.

The following screenshot shows an example:



Management Server	Private Network Address	Public Network Address	Server Number	Server Description
Server01	172.25.23.1	84.60.206.86	1	
Server02	172.25.23.2	84.60.206.85	2	
Server03	172.25.23.3	84.60.206.84	3	

Related Topics

– *Enterprise System , page 26*
– *Server List / Address Book page, page 229*
– *User Groups page, page 361*
– *Using Server Lookup, page 96*

7.2 Creating an Enterprise User Group

Main window > **User Groups**

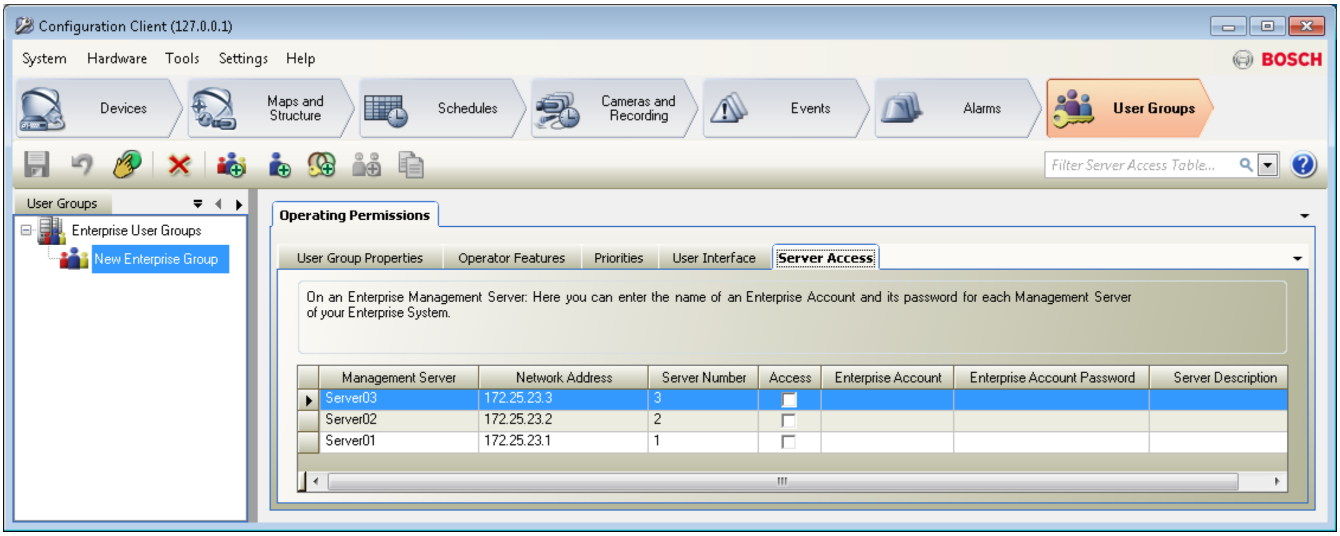
You perform the task of creating an Enterprise User Group for an Enterprise Management system on the Enterprise Management Server.

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 Groups tab.
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. Configure the operating permissions and server access for the configured Management Server computers as required.

The following screenshot shows an example:



On an Enterprise Management Server: Here you can enter the name of an Enterprise Account and its password for each Management Server of your Enterprise System.

Management Server	Network Address	Server Number	Access	Enterprise Account	Enterprise Account Password	Server Description
Server03	172.25.23.3	3	☐			
Server02	172.25.23.2	2	☐			
Server01	172.25.23.1	1	☐			

See also

- *User Group Properties page, page 363*
- *Operator Features page, page 372*
- *Priorities page, page 374*
- *User Interface page, page 375*
- *Server Access page, page 376*

7.3 Creating an Enterprise Account

Main window > **User Groups**

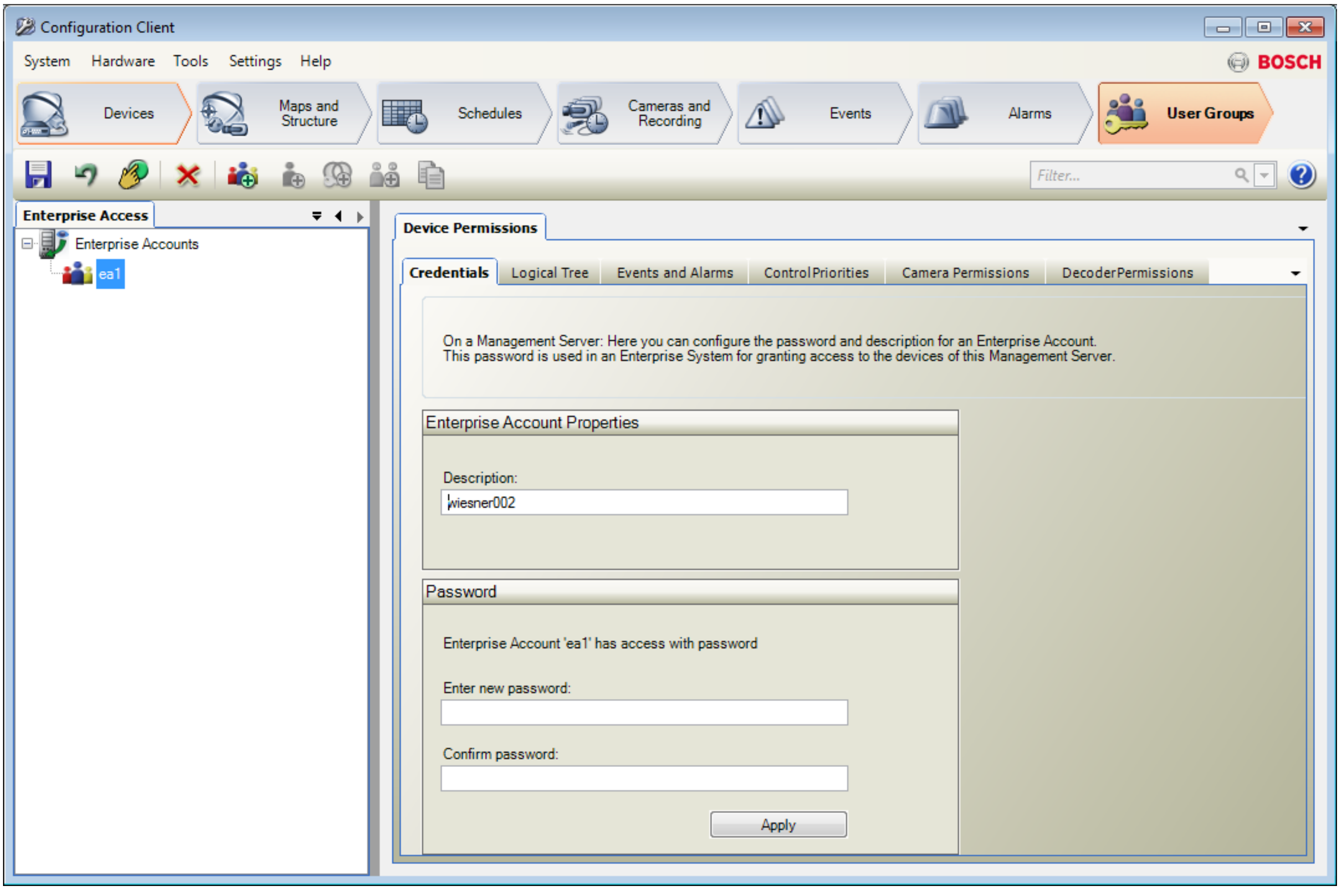
Caution!
At least one device must be configured in the Device Tree before you can add an Enterprise Account.

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. Click **OK**.
   The Enterprise Account is added to the corresponding tree.
5. Configure the credentials and the device permissions as required.

The following screenshot shows an example:



On a Management Server: Here you can configure the password and description for an Enterprise Account.
This password is used in an Enterprise System for granting access to the devices of this Management Server.

Description: wiesner002

Enterprise Account 'ea1' has access with password

Enter new password:

Confirm password:

See also

- *Credentials page, page 371*
- *Logical Tree page, page 372*
- *Events and Alarms page, page 369*
- *Control Priorities, page 367*

- *Camera Permissions page, page 366*
- *Decoder Permissions page, page 368*

8 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.

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

To add servers:

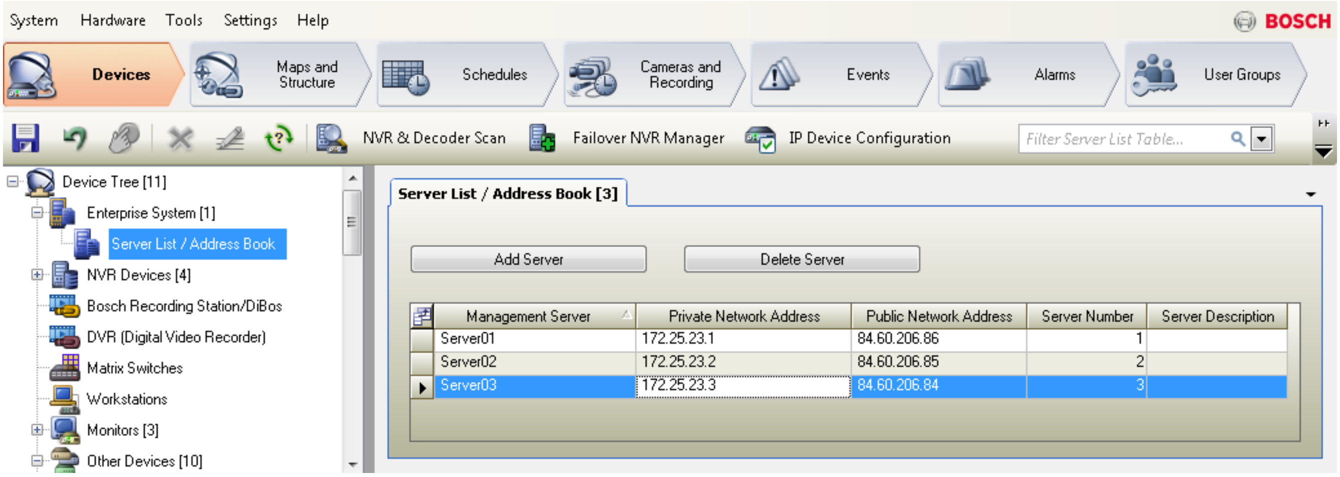
1. Click **Add Server**.
   The **Add Server** dialog box is displayed.
2. Type in a display name for the server and type in the private network address (DNS name or IP address).
3. If required, type in a public network address (DNS name or IP address) for remote access.
4. Click **OK**.
5. Repeat these 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.
Now configure the desired Enterprise User Groups and the Enterprise Access.
The following screenshot shows an example:



Management Server	Private Network Address	Public Network Address	Server Number	Server Description
Server01	172.25.23.1	84.60.206.86	1	
Server02	172.25.23.2	84.60.206.85	2	
Server03	172.25.23.3	84.60.206.84	3	

Related Topics

- *Enterprise System , page 26*
- *Server List / Address Book page, page 229*
- *User Groups page, page 361*
- *Using Server Lookup, page 96*

9 Configuring Server Lookup

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

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.

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

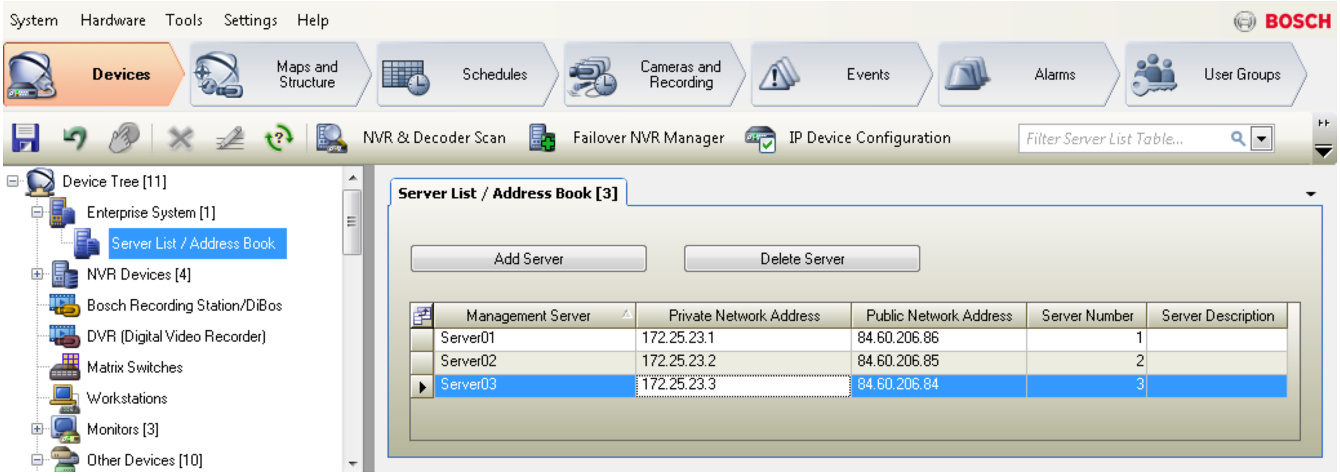
To add colums:

▶ 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 Server Lookup are configured.

The following screenshot shows an example:



Management Server	Private Network Address	Public Network Address	Server Number	Server Description
Server01	172.25.23.1	84.60.206.86	1	
Server02	172.25.23.2	84.60.206.85	2	
Server03	172.25.23.3	84.60.206.84	3	

Related Topics

– *Server Lookup , page 33*
– *Server List / Address Book page, page 229*
– *Using Server Lookup, page 96*

9.1 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, page 35* 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 33*
- *Server List, page 35*
- *Server List / Address Book page, page 229*

9.2 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, page 35* 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 33*
- *Server List, page 35*
- *Server List / Address Book page, page 229*

10 Adding an unmanaged site

Main window > **Devices** >

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

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. Click **OK**.
   A new unmanaged site is added to the system.
4. Right-click this item and then click **Add Unmanaged Network Device**.
   The **Add Unmanaged Network Device** dialog is displayed.
5. Select the desired device type.
6. Type in a valid IP address and credentials for this device.
7. Click **OK**.
   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.

See also

- *Add Unmanaged Network Device dialog box, page 281*
- *Unmanaged Sites page, page 280*
- *Unmanaged site, page 31*

10.1 Importing a configuration of unmanaged sites

Main window > **Devices** >

You can import a CSV file containing a configuration of a DVR or another Bosch VMS that you want to import in your Bosch VMS 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.

See also

- *Structure of CSV file for importing unmanaged sites, page 32*

11 Managing VRM storage

Main window > **Devices** >

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

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

11.1 Synchronizing Bosch VMS configuration

Main window > **Devices** > Expand > Right-click > **Synchronize Bosch VMS Configuration** command

As of Bosch VMS 6.0, VRM 3.50 is supported. If you do not upgrade your VRM version from earlier versions to version 3.50, you cannot change the configuration of the VRM with the earlier version.

If you upgraded your VRM software to version 3.50, you must manually synchronize the Bosch VMS configuration.

11.2 Scanning for VRM devices

Main window > **Devices** >

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

Caution!

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

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

See *Configuring an iSCSI device, page 126* for details.

The system supports you with a scan for devices.

To add VRM devices via scan:

1. Right-click and click **Scan for VRM Devices**.
   The **Bosch VMS Scan Wizard** dialog box is displayed.
2. Select the desired check boxes for the devices that you want to add.
3. In the **Role** list, select the desired role.
   It depends on the current type of the VRM device which new role you can select.
   If you select **Mirrored** or **Failover**, the next configuration step is additionally required.
4. Click **Next >**.
5. In the **Master VRM** list, select the Master VRM for the selected Mirrored or Failover VRM.

6. Click **Next >>**.
   The **Authenticate Devices** dialog box of the wizard is displayed.
7. Type in the password for each device that is protected by a password.
   Password check is performed automatically, when you do not enter a further character in the password field for a few seconds or you click outside the password field.
   If the passwords of all devices are identical, you can enter it in the first **Password** field. Then right-click this field and click **Copy cell to column**.

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

   The failed logons are indicated with 🔒.
8. Click **Finish**.
   The device is added to your Bosch VMS.

See also

- *Bosch VMS Scan Wizard, page 261*
- *VRM Devices page, page 263*
- *Configuring an iSCSI device, page 126*
- *Dual / failover recording, page 40*

11.3 Adding a Primary VRM manually

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

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

To add a Primary VRM device:

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

The VRM device is added.

See also

- *Add VRM dialog box, page 264*
- *Dual / failover recording, page 40*

11.4 Adding a Secondary VRM manually

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

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

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.

See also

– *Add VRM dialog box, page 264*
– *Dual / failover recording, page 40*

11.5 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.

See also

– *Add VRM dialog box, page 264*
– *Dual / failover recording, page 40*

11.6 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 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.

See also

- *Add Failover VRM dialog box, page 264*
- *Dual / failover recording, page 40*

11.7 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 38*

11.8 Adding an iSCSI device

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

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.

11.9 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 136*

11.10 Adding a DSA E-Series iSCSI device

Main window > **Devices** > > Expand > Right-click > **Add DSA E-Series Device** > **Add DSA E-Series Device** dialog box

To add:

1. Type in a displayname, the management IP address and the password.
2. Click **Connect**.
   If connection is established, the fields in the **Controller** group and the **2nd Controller** group are filled.
3. Click **OK**.
   The device is added to the system.

Related Topics

– *Add DSA E-Series Device dialog box, page 271*

11.11 Configuring an iSCSI device

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.

To perform the default configuration of an iSCSI device:

1. Expand the appropriate VRM device and , click the appropriate iSCSI device .
2. Click the **Basic Configuration** tab.
   LUNs are created on the targets of the iSCSI device.
3. Format these LUNs.
   See *Formatting a LUN, page 128*.
4. When the process has finished, click to save the settings.
5. Click to activate the configuration.

To scan the iSCSI device:

1. Expand the appropriate VRM device and , click the appropriate iSCSI device .

2. Right-click iSCSI and click **Scan for iSCSI Device**.
   The process is started.
   Targets and LUNs are detected and added to the Device Tree below the iSCSI node.
3. Click to save the settings.
4. Click to activate the configuration.

To perform IQN mapping:

1. Expand the appropriate VRM device and , click the appropriate iSCSI device iSCSI.
2. Right-click iSCSI 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 272*
– *Load Balancing dialog box, page 272*
– *iqn-Mapper dialog box, page 274*
– *Formatting a LUN, page 128*

11.12 Moving an iSCSI system to another pool

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

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 for** is displayed.
2. In the **New Pool:** list, select the desired pool.
3. Click **OK**.
   The device is moved to the selected pool.

See also

– *Change Pool for dialog box, page 270*

11.13 Adding a LUN

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

To add:

1. Right-click iSCSI and click **Add Target**.
   The **Add Target** dialog box is displayed.
2. Enter the desired target number and click **Ok**.
   The target ID is added.
3. Click the new 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 table row.
   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!

See also

– *LUNs page, page 274*

11.14 Formatting a LUN

Main window > **Devices** > Expand > Expand > Expand > Expand iSCSI > ID >

You format a LUN to prepare it for the first use.

Notice!
All data on the LUN is lost after formatting.

To configure:

1. On the **LUNs** page, 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 274*

11.15 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.
4. Click **OK**.
5. Confirm the next dialog box.

✓ The password is changed immediately on the device.

11.16 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 189*
- *Configuring the ANR function, page 189*
- *Dual / failover recording, page 40*
- *Adding a Secondary VRM manually, page 123*

12 Preparing an ONVIF camera

Perform the steps described in this section to prepare an ONVIF camera so that you can scan it and add it in Bosch VMS.

1. Connect the ONVIF IP camera according the vendors Installation Guide, for example with sufficient Power over Ethernet supply.
   If available, get an appropriate IP Installer Tool from the vendor's Web page and install it.
2. Update the firmware.
   Update the camera to the recommended or latest firmware. Check for the latest compatible firmware certified for Bosch VMS usage in the Bosch IPP portal. Download the firmware from the vendor's homepage. Ensure that the firmware is minimum compliant to ONVIF 1.02.
3. Open the device in your Web browser and execute a reset.
   To avoid issues due to an earlier configuration, reset the device to its factory defaults.
4. Configure the following network settings in your ONVIF camera:
   - Ensure that IP, subnet and default gateway match your network.
   - Disable local loopback IP address if configured on the camera.
5. Synchronize time between camera and system.
   If time is not synchronized, the connection between camera and system can be disconnected.
   If the camera provides SNTP address field, enter your Management Server IP to ensure that the camera is synchronized.
6. Configure an ONVIF user account with administration rights for communication with Bosch VMS.
   Note: The ONVIF user is not identical with the standard user of the camera.
7. Configure camera events.
   Enable the required camera events (input / relay / motion / tamper) according to the installation manual of the device.
8. Check the camera video functionality.
   Open the Web interface of the camera and ensure that a live stream is provided for the different profiles of the camera. Ensure that the connection is stable and video is fluent.
   Note down all available profiles for later configuration in Configuration Client.
9. Verify the camera event functionality.
   Start ONVIF Device Manager (available in the Internet) and wait for the camera shown in the list. Select the camera and the menu item events, log on with the created ONVIF user account.
   Trigger all supported input events. Use the Web interface for virtual and digital inputs or hot-wire alarm inputs according to the circuit diagram for digital inputs and outputs.
   Switch the status of the relay using ONVIF Device Manager. Trigger motion and tamper events, for example by covering the camera lens, pointing a flashlight into the lens or disconnecting the iris control.
   All expected events get listed in ONVIF Device Manager.
   Note down ONVIF source, data, and values for the later ONVIF event configuration in Configuration Client.
   If any of the events does not provide a counter event, please make a note to be mapped in BVMS as ONVIF generic event and not as regular ONVIF event.
10. Check the PTZ function.
    Use ONVIF Device Manager to check the correct operation of pan, tilt, zoom and the selection and setting of preset positions.
    Note down the camera to be enabled later in Configuration Client as a PTZ camera.

Notice!
Some manufacturers declare their ONVIF cameras to be ONVIF compliant, but they actually are not.
Some cameras have limited network connection capabilities. Only a limited number of parallel clients are possibly allowed.
Some cameras have limited CPU performance. Check at high image quality settings and stream bitrates the correct operation of the camera.

For configuring an ONVIF camera, please refer to the following chapter:

- *ONVIF Configuration page, page 319*

13 Managing encoders / decoders

Main window > **Devices**

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

Changing the Device Tree impacts other pages of the Configuration Client:

- **Maps and Structure**
  With the devices of the Device Tree you create a user defined structure called Logical Tree. Hence, if you remove a device from the Device Tree, this device is automatically removed from the Logical Tree. But adding a device to the Device Tree does not add this device to the Logical Tree.
- **Cameras and Recording**
  All cameras of the Device Tree are available in the Camera Table and the Recording Tables. You cannot modify DiBos or Bosch Allegiant cameras.
- **Events**
  All devices of the Device Tree are available in the corresponding Event Tables.
- **User Groups**
  You can reduce the functional range of the devices on several permission pages (per user group or Enterprise Account).

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

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

13.1 Adding an encoder to a VRM pool

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

The system supports you with a scan for devices.

To add encoders via scan:

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

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

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

The failed logons are indicated with 🔒.

5. Click **Finish**.
   The device is added to your Bosch VMS.

See also

– *Bosch VMS Scan Wizard, page 261*

13.2 Moving an encoder to another pool

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

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

To move:

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

See also

– *Change Pool for dialog box, page 270*

13.3 Adding a live only encoder

Main window > **Devices** >

The system supports you with a scan for devices.

To add Bosch live only devices via scan:

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

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

   The failed logons are indicated with 🔒.

5. Click **Finish**.
   The device is added to your Bosch VMS.

To add ONVIF live only devices via scan:

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

See also

– *Bosch VMS Scan Wizard, page 261*
– *Live Only page, page 279*

13.4 Adding a local storage encoder

Main window > **Devices** >

The system supports you with a scan for devices.

To add local storage encoders via scan:

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

See also

– *Bosch VMS Scan Wizard, page 261*
– *Local Storage page, page 280*

13.5 Configuring an encoder / decoder

To configure an encoder:

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

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

Main window > **Devices** > >
or

Main window > **Devices** > >

To configure a decoder:

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

See the Online Help for the pages for details.

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

See also

– *Bosch Encoder / Decoder page, page 282*

13.6 Updating the device capabilities

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

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

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

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 241*

13.7 Configuring failover recording mode on an encoder

Main window > **Devices** > Expand > Expand > >
Prerequisites: On the **Pool** page, in the **Recording preferences mode** list, select **Failover**. If **Automatic** is selected, the settings are performed automatically and cannot be configured.
If you want to use a secondary target for both automatic or failover mode: On the **Pool** page, in the **Secondary target usage** list, select **On**.
It is recommended to configure at least 2 iSCSI devices for failover mode.
To configure:

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

Related Topics

– *Configuring automatic recording mode on a pool, page 125*

13.8 Configuring multiple encoders / decoders

Main window

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

- Display names
- IP addresses
- Firmware versions

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

To configure multiple IP addresses:

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

To configure multiple display names:

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

To update firmware for multiple devices:

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

13.9 Changing the password of an encoder / decoder

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

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

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

Main window > **Devices** > >

Main window > **Devices** > >

Define and change a separate password for each level. Enter the password (19 characters maximum; no special characters) for the selected level.

To change the password:

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

✓ The password is changed immediately on the device.

See also

– *Enter password dialog box, page 243*

13.10 Providing the destination password for a decoder

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

To enable the access of a password protected encoder to a decoder, you must enter the password of the user authorization level of the encoder as the destination password in the decoder.

To provide:

1. In the **Enter user name** list, select destination password.
2. In the **Enter password for user** field, type in the new password.
3. Click **OK**.

✓ The password is changed immediately on the device.

See also

– *Enter password dialog box, page 243*

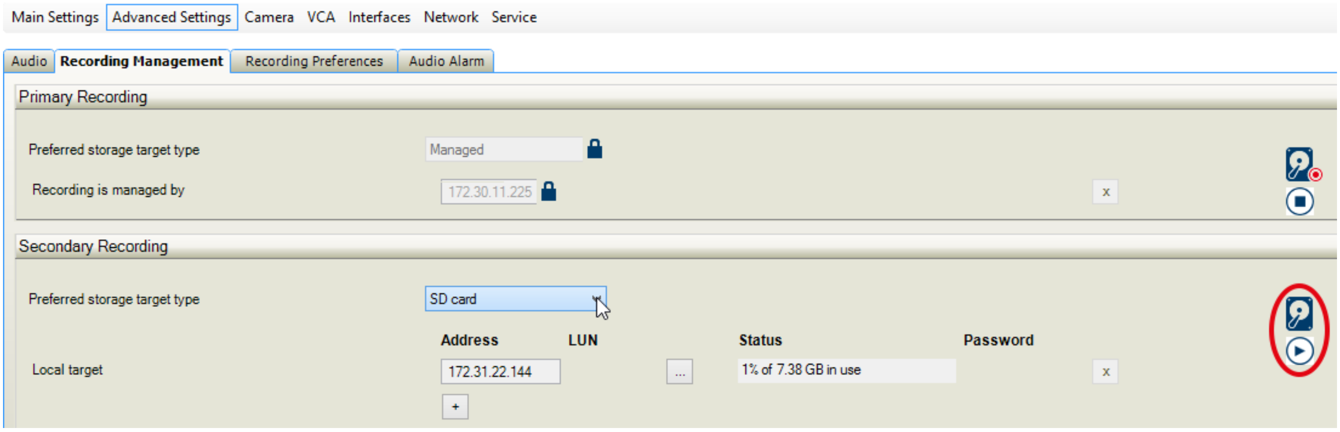
13.11 Configuring the storage media of an encoder

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:



Primary Recording

Preferred storage target type: Managed

Recording is managed by: 172.30.11.225

Secondary Recording

Preferred storage target type: SD card

	Address	LUN		Status	Password
Local target	172.31.22.144		...	1% of 7.38 GB in use	

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 286*
- *Configuring the ANR function, page 189*

13.12 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.

13.13 Configuring ONVIF events

Main window > **Devices** > 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 Bosch VMS 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.

See also

- *Enabling logging for ONVIF events, page 385*
- *ONVIF events, page 60*
- *ONVIF Encoder Events page, page 317*
- *ONVIF Event Source page, page 332*

13.14 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**.

See also

– *Import Mapping Table dialog box, page 319*
– *ONVIF Encoder Events page, page 317*

13.15 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 317*

14 Managing Video Streaming Gateway

Main window > **Devices**

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

Changing the Device Tree impacts other pages of the Configuration Client:

- **Maps and Structure**
  With the devices of the Device Tree you create a user defined structure called Logical Tree. Hence, if you remove a device from the Device Tree, this device is automatically removed from the Logical Tree. But adding a device to the Device Tree does not add this device to the Logical Tree.
- **Cameras and Recording**
  All cameras of the Device Tree are available in the Camera Table and the Recording Tables. You cannot modify DiBos or Bosch Allegiant cameras.
- **Events**
  All devices of the Device Tree are available in the corresponding Event Tables.
- **User Groups**
  You can reduce the functional range of the devices on several permission pages (per user group or Enterprise Account).

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

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

See also

- *Video Streaming Gateway device page , page 274*
- *Add Bosch Encoder dialog box, page 276*
- *Add ONVIF Encoder dialog box, page 277*
- *Add JPEG Camera dialog box, page 278*
- *Add RTSP Encoder dialog box, page 279*

14.1 Adding a Video Streaming Gateway device

Main window > **Devices** > Expand >

To add VSG devices via scan:

1. Right-click and click **Scan for Video Streaming Gateways**.
   The **Bosch VMS Scan Wizard** dialog box is displayed.
2. Select the required VSG devices, select the desired VRM pool and click **Assign** to assign them to the VRM pool.
3. Click **Next >>**.
   The **Authenticate Devices** dialog box of the wizard is displayed.

4. Type in the password for each device that is protected by a password.
   Password check is performed automatically, when you do not enter a further character in the password field for a few seconds or you click outside the password field.
   If the passwords of all devices are identical, you can enter it in the first **Password** field. Then right-click this field and click **Copy cell to column**.

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

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

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.

See also

- *Add Streaming Gateway dialog box, page 270*
- *Add Bosch Encoder dialog box, page 276*
- *Add ONVIF Encoder dialog box, page 277*
- *Add JPEG Camera dialog box, page 278*
- *Add RTSP Encoder dialog box, page 279*

14.2 Moving a VSG to another pool

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

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

To move:

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

See also

- *Change Pool for dialog box, page 270*

14.3 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 276*
- *Add ONVIF Encoder dialog box, page 277*
- *Add JPEG Camera dialog box, page 278*
- *Add RTSP Encoder dialog box, page 279*

14.4 Configuring multicast

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.

See also

- *Multicast tab (Video Streaming Gateway), page 275*

14.5 Configuring logging

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

For each a Video Streaming Gateway device you can configure logging.

To configure logging:

1. Click the **Service** tab, then click **Advanced**.
2. Click to select the desired logging settings.

The log files are usually stored in the following path:

```
C:\Program Files (x86)\Bosch\Video Streaming Gateway\log
```

See also

- *Advanced tab (Video Streaming Gateway) , page 275*

14.6 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.

14.7 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 341*

14.8 Configuring ONVIF events

Main window > **Devices** > 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 Bosch VMS 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.

See also

- *Enabling logging for ONVIF events, page 385*
- *ONVIF events, page 60*
- *ONVIF Encoder Events page, page 317*
- *ONVIF Event Source page, page 332*

14.9 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**.

See also

- *Import Mapping Table dialog box, page 319*
- *ONVIF Encoder Events page, page 317*

14.10 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 317*

15 Managing various devices

Main window > **Devices**

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

Changing the Device Tree impacts other pages of the Configuration Client:

- **Maps and Structure**
  With the devices of the Device Tree you create a user defined structure called Logical Tree. Hence, if you remove a device from the Device Tree, this device is automatically removed from the Logical Tree. But adding a device to the Device Tree does not add this device to the Logical Tree.
- **Cameras and Recording**
  All cameras of the Device Tree are available in the Camera Table and the Recording Tables. You cannot modify DiBos or Bosch Allegiant cameras.
- **Events**
  All devices of the Device Tree are available in the corresponding Event Tables.
- **User Groups**
  You can reduce the functional range of the devices on several permission pages (per user group or Enterprise Account).

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

15.1 Adding a device manually

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.
- Bosch VMS 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
- Analog monitor group
- I/O module
- Allegiant CCL emulation
- Intrusion panel from Bosch

- Server-based analytics device

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

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

Notice:

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

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.

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.

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

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.

To add a Bosch VMS workstation:

1. Right-click and click **Add Workstation**.
   The **Add Workstation** dialog box is displayed.
2. Enter the appropriate value click **OK**.
   The workstation is added to your system.

To add an analog monitor group:

1. Expand , right-click and click **Add Monitor Group**.
   The **Create New Analog Monitor Group** dialog box is displayed.
   If you already have performed a network scan, and decoders have been detected, there is already a default analog monitor group available with all detected decoders assigned.
2. Make the appropriate settings.
3. Click **OK**.
   The analog monitor group is added to your system.

To add a communication device:

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

To add a peripheral device:

1. Expand , right-click and click the required command.
   The appropriate dialog box is displayed.
2. Enter the appropriate settings.
3. Click **OK**.
   The peripheral device is added to your system.

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.

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.

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.

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.
   If you want to skip the currently selected device and jump to the next one, click **Skip**.
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.

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.

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.

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.

See also

- *Add Encoder / Add Decoder dialog box, page 241*
- *Add DiBos System dialog box, page 234*
- *E-mail/SMTP Server dialog box, page 248*
- *Add SMS Device dialog box, page 248*
- *Add Bosch ATM/POS-Bridge dialog box, page 251*
- *DTP Settings page, page 252*
- *Add Virtual Inputs dialog box, page 254*
- *Add SNMP dialog box, page 255*
- *Assign Keyboard page, page 256*
- *I/O Modules page, page 257*
- *Allegiant CCL Emulation page, page 258*
- *Add Intrusion Panel dialog box, page 260*

15.2 Adding a VIDOS NVR

Main window > **Devices** > Expand >

The system supports you with a scan for devices.

To add VIDOS NVRs via scan:

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

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

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

See also

– *Bosch VMS Scan Wizard, page 261*

15.3 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 71*
– *Connecting a Bosch IntuiKey keyboard to a decoder, page 72*
– *Updating Bosch IntuiKey keyboard firmware, page 73*
– *COM1, page 303*

15.4 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 Bosch VMS.

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.

15.5 Configuring the integration of a DVR

Main window > **Devices** > Expand >

Caution!
Add the DVR using the administrator account of the device. Using a DVR user account with restricted permissions can result in features that are not usable in Bosch VMS, 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 Bosch VMS.

To add DVR devices via scan:

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

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

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

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

– *Bosch VMS Scan Wizard, page 261*
– *DVR (Digital Video Recorder) page, page 235*

15.6 Configuring a Bosch Allegiant device

Main window > **Devices** > Expand >

You do not configure the Bosch Allegiant device itself but only the Bosch VMS 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 Bosch VMS, page 71*
- *Connection page, page 236*
- *Cameras page, page 237*
- *Outputs page, page 237*
- *Inputs page, page 238*

15.7 Configuring a startup Command Script

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 200*.

To configure a startup script:

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

See also

- *Workstation page, page 238*

15.8 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.

15.9 Enabling Forensic Search on a workstation

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.

15.10 Assigning an analog monitor group to a workstation

Main window > **Devices** > Expand > > **Analog Monitor Groups** page

You assign an analog monitor group to a Bosch VMS workstation. In the **Options** dialog box, you can configure that all workstations can control analog monitor groups regardless of the setting here.

To assign an analog monitor group:

- In the **Assigned Analog Monitor Groups** column, select the check box.

See also

- *Options dialog box, page 224*
- *Workstation page, page 238*

15.11 Configuring an analog monitor group

Main window > **Devices** > Expand >

Caution!

You cannot control an analog monitor group from within Operator Client when the connection to the Management Server is lost or when Operator Client with Enterprise System is used.

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

To configure an analog monitor group:

1. In the **Name:** field, type a name for the analog monitor group.
2. In the **Columns:** and **Rows:** fields, enter the desired values.
3. Drag each available decoder to an analog monitor image on the right.
   The logical number of the decoder is displayed as a black number on the monitor image and the color of this image changes.
   If no decoder is available, unassign a decoder from another analog monitor group or repeat network scan.
4. Click the **Advanced Configuration** tab.
5. Change the logical numbers of the assigned decoders as required. If you enter an already used number, a message box is displayed.

6. Click **Quad View** to enable quad view for this decoder.
   Note:
   We do not recommend configuring quad view for H.264 cameras.
7. In the **Initial Camera** column, select the desired camera.
8. In the OSD related columns, select the desired options.

15.12 Adding a monitor wall

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

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

To add:

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

See also

– *Add Monitor Wall dialog box, page 247*

15.13 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

– *E-mail/SMTP Server dialog box, page 248*
– *Add SMS Device dialog box, page 248*
– *SMTP Server page, page 248*
– *GSM Settings / SMSC Settings page, page 249*

15.14 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 252*
- *Bosch ATM/POS-Bridge page, page 251*
- *DTP Settings page, page 252*

15.15 Configuring an SNMP trap receiver

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.

See also

- *SNMP Trap Receiver page, page 255*

15.16 Configuring a Bosch IntuiKey keyboard (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 238*

15.17 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 256*
- *Scenarios for Bosch IntuiKey keyboard connections, page 71*
- *Connecting a Bosch IntuiKey keyboard to a decoder, page 72*

15.18 Configuring an I/O module

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

To configure an I/O module:

1. Click the **ADAM** tab.
2. In the **ADAM type:** list, select the appropriate device type.

Caution!
Do not change the device type if not really necessary.
If you for example change the device type to a type with fewer inputs, all configuration data for the removed inputs get lost.

1. Click the **Inputs** tab.
2. In the **Name** column, change the display name of an input if required.
3. Click the **Relays** tab.
4. In the **Relays** column, change the name of a relay if required.

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

See also

- *I/O Modules page, page 257*

15.19 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 Bosch VMS, page 78* 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 258*

15.20 Adding a Mobile Video Service

Main window > **Devices** > Right-click > Click **Add Mobile Video Service**

You can add one or more Mobile Video Service entries to your Bosch VMS.

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.

See also

– *Mobile Video Service page, page 259*

15.21 Adding a video analytics device

Main window > **Devices** > Expand >

When adding a server-based analytics device, you type in the credentials for the new device.

To add:

1. Right-click and click **Add Video Analytics Device**.
   The **Add Video Analytics Device** dialog box is displayed.
2. Type in the required information.

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

See also

– *Add Video Analytics Device dialog box, page 261*

– *Configuring server-based video analytics, page 168*

16 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 163*
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 164*
   - *Adding a live only encoder, page 164*
   - *Adding a local storage encoder, page 165*
3. Configure a fire event for this camera.
   - *Configuring a fire event, page 166*
4. Configure the alarm for the fire event.
   - *Configuring a fire alarm, page 166*

See also

- *Adding an encoder to a VRM pool, page 164*
- *Adding a live only encoder, page 164*
- *Adding a local storage encoder, page 165*
- *Configuring a fire event, page 166*
- *Configuring a fire alarm, page 166*

16.1 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.

16.2 Adding an encoder to a VRM pool

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

The system supports you with a scan for devices.

To add encoders via scan:

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

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

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

See also

– *Bosch VMS Scan Wizard, page 261*

16.3 Adding a live only encoder

Main window > **Devices** >

The system supports you with a scan for devices.

To add Bosch live only devices via scan:

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

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

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

The failed logons are indicated with .

5. Click **Finish**.
   The device is added to your Bosch VMS.

To add ONVIF live only devices via scan:

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

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

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

See also

- *Bosch VMS Scan Wizard, page 261*
- *Live Only page, page 279*

16.4 Adding a local storage encoder

Main window > **Devices** >

The system supports you with a scan for devices.

To add local storage encoders via scan:

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

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

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

The failed logons are indicated with 🔒.

5. Click **Finish**.
   The device is added to your Bosch VMS.

See also

– *Bosch VMS Scan Wizard, page 261*
– *Local Storage page, page 280*

16.5 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.

16.6 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.

17 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 Bosch VMS, 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 Bosch VMS:

1. In the Device Tree, add only the MIC IP 7000 camera.
   You cannot add the VIDEOJET 7000 connect device to Bosch VMS.
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.

18 Configuring server-based video analytics

Perform the following steps to configure video analytics:

1. Install the alarm viewer application of the video analytics on each Bosch VMS workstation to be used for analytics. Take a note containing the path to the alarm viewer application.
   For detailed information on installing the alarm viewer application, see: *Installing the alarm viewer application, page 168*.
2. Add the cameras to the Device Tree that you want to use as analytics cameras.
   These cameras are automatically retrieved when the Bintelan Analytics Platform connects with your Bosch VMS Management Server.
3. Add a video analytics device to the Device Tree of Configuration Client.
   For detailed information on adding a video analytics device, see: *Adding a video analytics device, page 169*.
4. In the video analytics device, configure the path to the alarm viewer application. A default path of the alarm viewer application is pre-configured.
5. Configure the IP address of the Bintelan Analytics Platform.
6. Use the Bintelan Bosch Client application on the Bintelan Analytics Platform for connecting with Bosch VMS Management Server.
   Type in the IP address of this Management Server.
7. Add the video analytics device to the Logical Tree.
8. Configure an alarm for the **External Data** event for the desired video analytics cameras.
9. The user of Operator Client drags the video analytics device to an Image pane.
10. When an alarm occurs, an external data alarm entry is displayed in the Alarm List.
11. The user selects this entry in the Alarm List.
    An image with the matched person or object is displayed in the alarm viewer application.

See also

- *Adding a video analytics device, page 169*
- *Video Analytics Settings page, page 260*
- *Installing the alarm viewer application, page 168*

18.1 Installing the alarm viewer application

For displaying the Ganetec alarm viewer application, the software must be installed in the directory configured in Configuration Client.

For installation, you need the BintelanClient_BoschAlarmViewer.exe from the Ganetec Webpage or from the Bosch Online Product Catalog.

Perform the installation on each Operator Client workstation where you want to use the alarm viewer application.

To install:

1. Double-click the Setup.
2. Follow the instructions on the screen.
   Note: The installation directory for the alarm viewer application must be below `%ProgramFiles(x86)%\VideoAnalysis`.

18.2 Adding a video analytics device

Main window > **Devices** > Expand >

When adding a server-based analytics device, you type in the credentials for the new device.

To add:

1. Right-click and click **Add Video Analytics Device**.
   The **Add Video Analytics Device** dialog box is displayed.
2. Type in the required information.

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

See also

– *Add Video Analytics Device dialog box, page 261*

– *Configuring server-based video analytics, page 168*

19 Configuring the structure

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

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

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

- *Resource Manager dialog box, page 335*
- *Select Resource dialog box, page 335*
- *Sequence Builder dialog box, page 336*
- *Add Sequence dialog box, page 337*
- *Add Sequence Step dialog box, page 337*
- *Add URL dialog box, page 337*
- *Select Map for Link dialog box, page 338*

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

19.1 Configuring the Logical Tree

See also

- *Maps and Structure page, page 334*

19.2 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 334*

19.3 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 334*

19.4 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)
– 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 335*

19.5 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 200* 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 335*

19.6 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.

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

- Click **OK**.
  A new camera sequence is added.

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

1. Select the desired camera sequence.
2. Click **Add Step**.
   The **Add Sequence Step** dialog box is displayed.
3. Make the appropriate settings.
4. Click **OK**.
   A new step is added to the camera sequence.

To remove a step from a camera sequence:

- Right-click the desired camera sequence and click **Remove Step**.
  The step with the highest number is removed.

To delete a camera sequence:

1. Select the desired camera sequence.
2. Click ❌. The selected camera sequence is removed.

See also

- *Sequence Builder dialog box, page 336*
- *Add Sequence dialog box, page 337*
- *Add Sequence Step dialog box, page 337*

19.7 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 336*

19.8 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 334*

19.9 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 171* 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 335*

19.10 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 338*

19.11 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 171* 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 334*
– *Select Resource dialog box, page 335*

19.12 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.

See also

– *Maps and Structure page, page 334*

19.13 Adding a document

Main window > **Maps and Structure**

You can add text files, HTML files (including MHT files) or an URL file (containing an Internet address) 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 171* for details.

To add a map document file:

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 335*

19.14 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 338*

20 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.

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

- *Recording Schedules page, page 339*
- *Task Schedules page, page 340*

▸ Click to save the settings.

▸ Click to undo the last setting.

▸ Click to activate the configuration.

20.1 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 339*

20.2 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 340*

20.3 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 340*

20.4 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 340*

20.5 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 340*

20.6 Adding holidays and exception days

Main window > **Schedules**

Caution!

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 339*
- *Task Schedules page, page 340*

20.7 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 339*
- *Task Schedules page, page 340*

20.8 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 339*
- *Task Schedules page, page 340*

21 Configuring cameras and recording settings

Main window > **Cameras and Recording**

This chapter provides information on how to configure the cameras in your Bosch VMS.

You configure various camera properties and the recording settings.

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

- *Cameras page, page 341*
- *Scheduled Recording Settings dialog box (only VRM and Local Storage), page 344*
- Stream Quality Settings dialog box
- *COM1, page 303*
- *PTZ/ROI Settings dialog box, page 348*
- Copy Recording Settings dialog box (NVR only)

▸ Click to save the settings.

▸ Click to undo the last setting.

▸ Click to activate the configuration.

21.1 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 341*
– *Scheduled Recording Settings dialog box (only VRM and Local Storage), page 344*
– *Events page, page 350*
– *Alarms page, page 355*

21.2 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 Bosch VMS.
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.

21.3 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.

21.4 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 341*

21.5 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 344*

21.6 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 341*

21.7 Configuring PTZ port settings

Main window > **Devices** > Expand > Expand > Expand > > **Interfaces** tab > **Periphery** tab
or

Main window > **Devices** > Expand > Expand > > **Interfaces** tab > **Periphery** tab
or

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.

See also

– *Periphery page, page 303*

21.8 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 hot spot on a map.

To configure the control of a camera:

1. In the Camera Table, select the required encoder.
2. To activate the control of a camera: In the column, select the check box.
3. Click the button.
   The dialog box for configuring PTZ settings is displayed.
4. Remove the prepositions that you do not want to be displayed as context menu items on a map.
5. Make the appropriate settings.
6. Click **OK**.

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

See also

– *PTZ/ROI Settings dialog box, page 348*

– *Configuring PTZ port settings, page 187*

21.9 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 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 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 341*

21.10 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 348*

21.11 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 189*
– *Cameras page, page 341*
– *Configuring the storage media of an encoder, page 139*

21.12 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 129*
- *Configuring the ANR function, page 189*
- *Dual / failover recording, page 40*
- *Cameras page, page 341*

22 Configuring events and alarms

Main window > **Events**

or

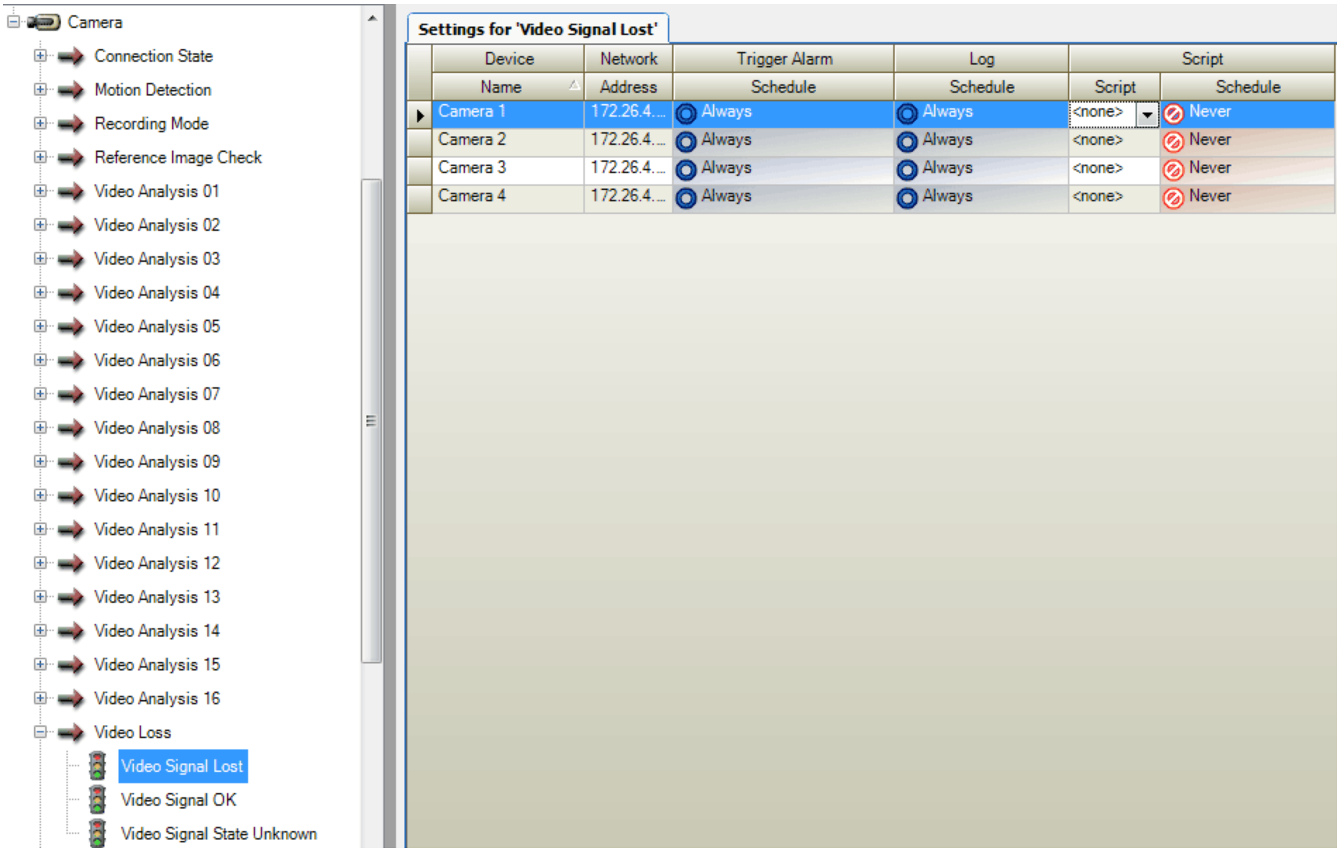
Main window > **Alarms**

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 Bosch VMS triggers an alarm, executes a Command Script, and is logged.

Example (part of an Event Configuration Table):



Device	Network	Trigger Alarm	Log	Script	
Name	Address	Schedule	Schedule	Script	Schedule
Camera 1	172.26.4....	Always	Always	<none>	Never
Camera 2	172.26.4....	Always	Always	<none>	Never
Camera 3	172.26.4....	Always	Always	<none>	Never
Camera 4	172.26.4....	Always	Always	<none>	Never

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.

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

- *Command Script Editor dialog box, page 352*
- *Create Compound Event / Edit Compound Event dialog box, page 353*
- *Select Script Language dialog box, page 353*
- *Alarm Settings dialog box, page 356*
- *Select Image Pane Content dialog box, page 356*

– *Alarm Options dialog box, page 357*

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

22.1 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 183*.

22.2 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 350*

22.3 Managing resource files

For detailed information see:
– *Managing resource files, page 171*.

22.4 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 350*

22.5 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 350*

22.6 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 350*

22.7 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

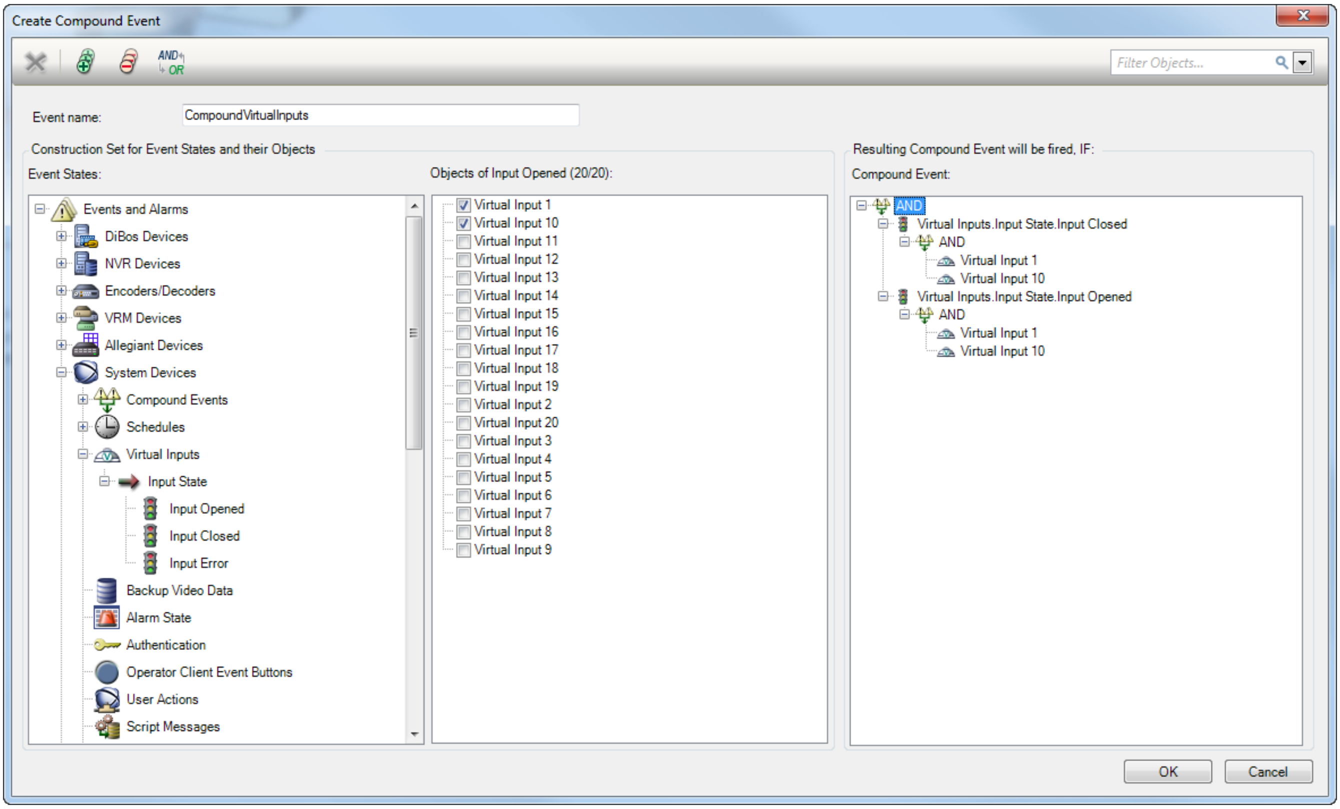
– *Events page, page 350*

22.8 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**.



Event name: CompoundVirtualInputs

Objects of Input Opened (20/20):
☑ Virtual Input 1
☑ Virtual Input 10
□ Virtual Input 11
□ Virtual Input 12
□ Virtual Input 13
□ Virtual Input 14
□ Virtual Input 15
□ Virtual Input 16
□ Virtual Input 17
□ Virtual Input 18
□ Virtual Input 19
□ Virtual Input 2
□ Virtual Input 20
□ Virtual Input 3
□ Virtual Input 4
□ Virtual Input 5
□ Virtual Input 6
□ Virtual Input 7
□ Virtual Input 8
□ Virtual Input 9

Compound Event:

```
AND
  Virtual Inputs.Input State.Input Closed
    AND
      Virtual Input 1
      Virtual Input 10
  Virtual Inputs.Input State.Input Opened
    AND
      Virtual Input 1
      Virtual Input 10
```

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 350*

22.9 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 350*

22.10 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 Bosch VMS, 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 192*
– *Alarms page, page 355*
– *Select Image Pane Content dialog box, page 356*
– *Alarm Options dialog box, page 357*

22.11 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
– Configure the behavior of all analog 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 356*

22.12 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 357*

22.13 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 357*
- *Text Data Recording dialog box, page 354*

22.14 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.

22.15 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.
5. Select the **Protect Recording** checkbox.

See also

- *Alarm Options dialog box, page 357*

22.16 Configuring blinking hot spots

For each 🚦 event, you can configure the background color and the behavior (blinking or not blinking) for hot spots. For example you can configure for a 🚦 event 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 hot spots. This is required when different events occur for the same device. (1 = highest priority)
The configured color is valid for all hot spots with the same display priority. You can change color, behavior and priority at any 🚦 event: The changed color and behavior is used for all hot spots of all other 🚦 events 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 in the **Options** dialog box.

To configure:

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**.

See also

- *Events page, page 350*
- *Options dialog box, page 224*

23 Configuring Command Scripts

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

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.

23.1 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 352*

23.2 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 357*

23.3 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 352*

23.4 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 352*

23.5 Configuring a startup Command Script

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 200*.
To configure a startup script:

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

See also

– *Workstation page, page 238*

24 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 make all settings per user group and not per user. A user can only be the member of one user group or Enterprise User Group.

You cannot change the settings of a default user group.

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

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

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

- *User Properties page, page 364*
- *New User Group/Enterprise Account dialog box, page 362*
- *User Group Properties page, page 363*
- *Add New Dual Authorization Group dialog box, page 365*
- *LDAP Server Settings dialog box, page 369*
- *Copy User Group Permissions dialog box, page 368*
- *Select User Groups dialog box, page 366*
- *Logical Tree page, page 372*
- *Events and Alarms page, page 369*
- *Operator Features page, page 372*
- *Priorities page, page 374*
- *Camera Permissions page, page 366*
- *Decoder Permissions page, page 368*
- *User Interface page, page 375*

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

24.1 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 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 .
   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, enter the user name and the password.

See also

– *User Groups page, page 361*

24.2 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.
You perform the task of creating an Enterprise User Group for an Enterprise Management 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.
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 a group or account:

1. Click the desired tab for the group or account that you want to add:
   - **User Groups**
   - **Enterprise User Group**
   - **Enterprise Access**
2. Click .
   The appropriate dialog box is displayed.
3. Type in the name and a description.
4. For an Enterprise Account enter a password and confirm this password.
5. Click **OK**.
   A new group or account is added to the corresponding tree.

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

See also

– *Enterprise System , page 26*
– *Creating an Enterprise System, page 112*
– *User Group Properties page, page 363*
– *Credentials page, page 371*
– *Server Access page, page 376*

- *New User Group/Enterprise Account dialog box, page 362*
- *Add New Dual Authorization Group dialog box, page 365*

24.3 Creating a dual authorization group

Main window > **User Groups** > **User Groups** tab > > **New Dual Authorization Group** dialog box
or

Main window > **User Groups** > **Enterprise User Group** tab > > **New Enterprise Dual Authorization Group** dialog box
You select two groups. The members of these groups are the members of the new dual authorization group.
You can configure dual authorization for user groups and for Enterprise User Groups.

To create:

1. Type in a name and description.
2. Click .
   The appropriate dialog box is displayed.
3. Select a group in each list.
   It is possible to select the same group in the second list.
4. 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.

Related Topics

- *Logon Pair Properties page, page 365*
- *Add New Dual Authorization Group dialog box, page 365*
- *Select User Groups dialog box, page 366*

24.4 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

Caution!
Do not assign an LDAP group to different Bosch VMS 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.

24.5 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 Bosch VMS 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.

24.6 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.

24.7 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.

To configure operating permissions:

1. Click the **Operating Permissions** tab.
2. Select or clear the check boxes as appropriate.

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

See also

- *User Group Properties page, page 363*
- *User Interface page, page 375*
- *Operator Features page, page 372*
- *Server Access page, page 376*
- *Priorities page, page 374*

24.8 Configuring user interface settings

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 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.
You configure operating permissions in standard user groups or Enterprise User Groups.

To configure user interface settings:

1. Click the **User Interface** tab.

2. In the 4 monitor list, select the required entries.
   If you click **Restore Default**, all list entries are reset to their default settings.
3. If required, select the **Save settings when shutting down** check box to enable the user to save his individual settings when shutting down the Operator Client.

24.9 Configuring permissions for Logical Tree

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

To configure permissions:

1. In the User Groups tree, select a user group or account.
2. Click the **Logical Tree** tab.
3. 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.

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

24.10 Configuring permissions for events and alarms

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

Main window > **User Groups** > **Enterprise Access** tab > **Device Permissions** tab

You configure which events the user group or account is authorized to process.
You cannot change these settings for a default user group.
You configure permissions for events and alarms in standard user groups or Enterprise Accounts.

To configure permission for events and alarms:

1. In the User Groups tree, select a user group or account.
2. Click the **Events and Alarms** tab.
3. Select the check box to enable all available events and alarms.
   Or:
   Select the required check boxes to enable the appropriate events and alarms.

See also

– *Events and Alarms page, page 369*

24.11 Configuring camera permissions

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

or

Main window > **User Groups** > **Enterprise Access** tab > **Device Permissions** tab

You can configure various permissions for cameras, e.g. PTZ control.

You cannot change these settings for a default user group.

You configure camera permissions in standard user groups or Enterprise Accounts.

To configure camera permissions:

1. In the User Groups tree, select a user group or account.
2. Click the **Camera Permissions** tab.
3. Select or clear the check boxes as appropriate.

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

24.12 Configuring decoder permissions

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

or

Main window > **User Groups** > **Enterprise Access** tab > **Device Permissions** tab

You can configure permissions for decoders.

You cannot change these settings for a default group.

You configure decoder permissions in standard user groups or Enterprise Accounts.

To configure decoder permissions:

1. In the User Groups tree, select a user group or account.
2. Click the **Decoder Permissions** tab.
3. Select or clear the check boxes as appropriate.

See also

– *Decoder Permissions page, page 368*

24.13 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.

24.14 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.

25 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.

25.1 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, page 222*
- *Activate Configuration dialog box, page 221*

25.2 Activating a configuration

Main window

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

To activate a configuration:

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

See also

- *Activate Configuration dialog box, page 221*
- *Activation Manager dialog box, page 220*

25.3 Exporting configuration data

Main window

You can export the device configuration data of Bosch VMS 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 213*

25.4 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 Bosch VMS 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 212*

25.5 Exporting configuration data to OPC

Main window

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

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

Caution!

Install OPC server and Bosch VMS 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.

25.6 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, page 226*

25.7 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.
  Bosch VMS no longer listens to SNMP GetRequest.

See also

- *SNMP Settings dialog box, page 227*

25.8 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 223*
- *Task Schedules dialog box, page 223*
- *Cameras and Recording Parameters dialog box, page 223*
- *Stream Quality Settings dialog box, page 223*
- *Event Settings dialog box, page 224*
- *Compound Event Settings dialog box, page 224*
- *Alarm Settings dialog box, page 224*
- *Configured Users dialog box, page 224*
- *User Groups and Accounts dialog box, page 224*
- *Operating Permissions dialog box, page 224*

26 Configuration examples

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

26.1 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 Bosch VMS

1. Connect the device to your Bosch VMS 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.

26.2 Adding a Bosch Allegiant input alarm

After a Bosch Allegiant device is added to Bosch VMS, 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.

26.3 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.

Performing a Forensic Search

Operator Client VRM main window > > **Timeline** tab

Perform the Forensic Search on the workstation where you have enabled Forensic Search.

To perform a Forensic Search:

1. Using the Hairline, select the time period on the Timeline and select the corresponding Image pane.
2. Click .
   The **Forensic Search** dialog box is displayed.
   The selected time period is copied to the **Start:** and **End:** fields.
   If required, change the values. Click .
3. In the **Algorithm:** list, select an IVA entry.
4. In the **Surveillance Tasks** field, configure your Forensic Search.
   You can find information on this in the relevant documents on the product CD supplied.
5. Click **Search** to start the Forensic Search.

   The window with the matching entries is displayed.

27 Global Configuration Client windows

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

27.1 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.

27.2 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.
	IP Device Configuration...	Displays the **IP Device Configuration** dialog box.
	Device Monitor...	Displays the **Device Monitor** dialog box.
	Failover NVR Manager...	Displays a dialog box for re-assigning cameras to a fixed NVR.

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.

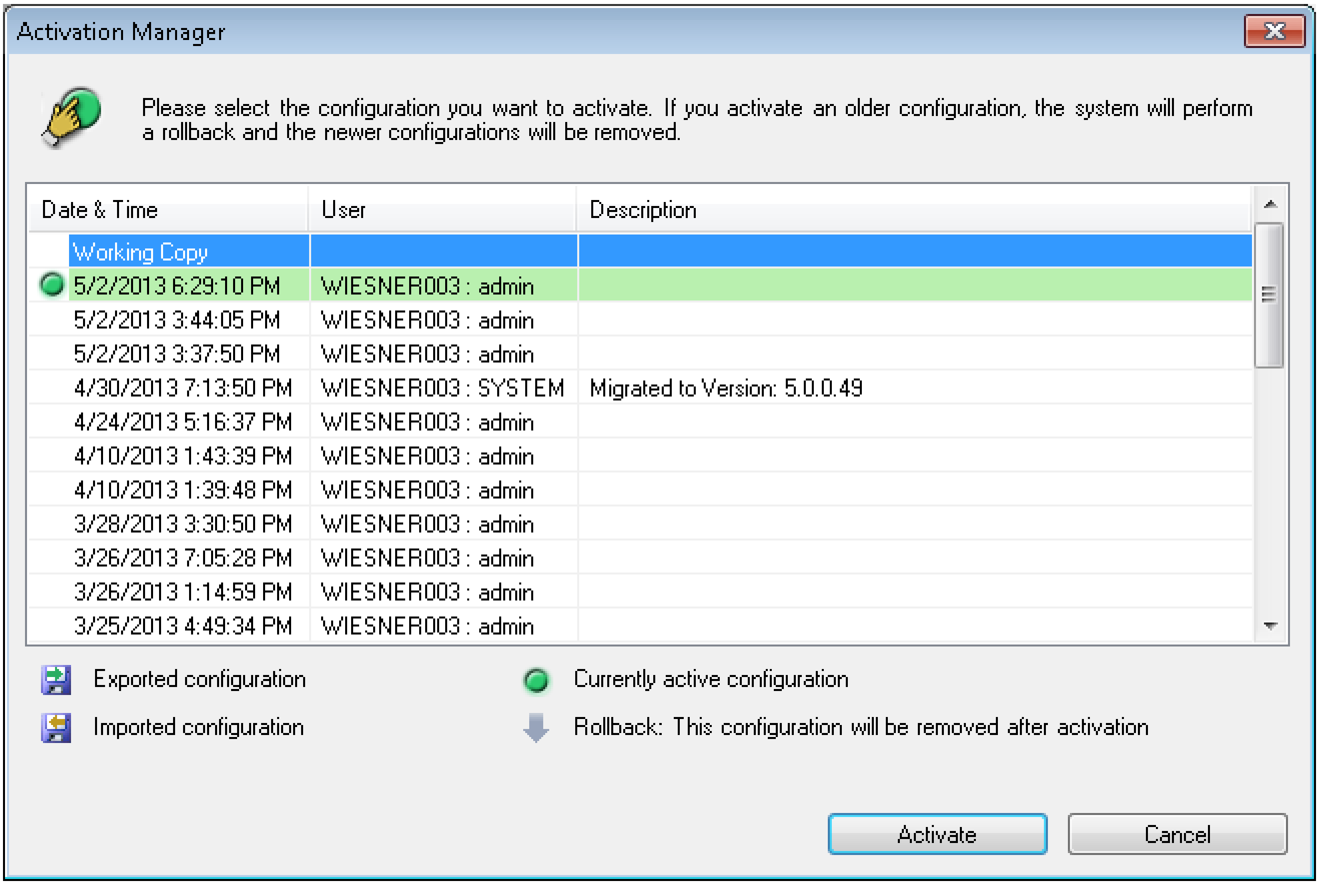
Reports menu commands		
	Recording Schedules...	Displays the **Recording Schedules** report dialog box.
	Task Schedules...	Displays the **Task Schedules** report dialog box.
	Cameras and Recording Parameters...	Displays the **Cameras and Recording Parameters** report dialog box.
	Stream Quality Settings...	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.
	Operating Permissions...	Displays the **Operating Permissions** 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 Bosch VMS Application Help.
	Help	Displays a dialog box containing information on the installed system, e.g., the version number.

27.3 Activation Manager dialog box

Main window > **System** menu > **Activation Manager...** command
Allows you to activate the current configuration or to rollback to a previous configuration.



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

	Date & Time	User	Description
	Working Copy		
●	5/2/2013 6:29:10 PM	WIESNER003 : admin	
	5/2/2013 3:44:05 PM	WIESNER003 : admin	
	5/2/2013 3:37:50 PM	WIESNER003 : admin	
	4/30/2013 7:13:50 PM	WIESNER003 : SYSTEM	Migrated to Version: 5.0.0.49
	4/24/2013 5:16:37 PM	WIESNER003 : admin	
	4/10/2013 1:43:39 PM	WIESNER003 : admin	
	4/10/2013 1:39:48 PM	WIESNER003 : admin	
	3/28/2013 3:30:50 PM	WIESNER003 : admin	
	3/26/2013 7:05:28 PM	WIESNER003 : admin	
	3/26/2013 1:14:59 PM	WIESNER003 : admin	
	3/25/2013 4:49:34 PM	WIESNER003 : admin	

Exported configuration

Imported configuration

● Currently active configuration

⬇ Rollback: This configuration will be removed after activation

Activate

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

See also

– *Activating the working configuration, page 211*
– *Activating a configuration, page 212*

27.4 Activate Configuration dialog box

Main window >

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

Set Delayed Activation time

Click to select a delayed activation time.

Force activation for all Operator Clients

If checked, each Operator Client workstation is automatically restarted to activate the new configuration. The user cannot refuse the new configuration.

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

Configure RRAS service before Activation

Only available if you have enabled the **Enable Port Mapping** option in the **Remote Access Settings** dialog box.

If checked, the **RRAS Configuration** dialog box is displayed before activation is performed.

See also

– *Activating the working configuration, page 211*

27.5 Protect Devices with Global Default Password dialog box

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 211*

27.6 License Manager dialog box

Main window > **Tools** menu > **License Manager...** command
Allows you to license the Bosch VMS 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 97*

27.7 License Activation dialog box

Main window > **Tools** menu > **License Manager...** command > **License Manager** dialog box > **Activate** button

Allows you to license the Bosch VMS packages that you have ordered and to upgrade with additional packages.

For obtaining the License Activation Key you must contact the Bosch Activation Center and specify the desired package and the computer signature of the Management Server.

Additionally you need the Authorization Number. This number is included in your software box.

License Activation Key:

Allows you to type the License Activation Key received from the Bosch Activation Center.

See also

– *Activating the software licenses, page 97*

27.8 Reports dialog boxes

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

See also

– *Creating a report, page 214*

27.8.1 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.

27.8.2 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.

27.8.3 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.

27.8.4 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.

27.8.5 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.

27.8.6 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.

27.8.7 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.

27.8.8 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.

27.8.9 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.

27.8.10 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.

27.8.11 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.

27.9 Alarm Settings dialog box

See *Alarm Settings dialog box, page 356* for details.

27.10 Options dialog box

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

Language

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

Analog Monitor Group (AMG) Settings

Allows you to configure that the users can control all analog monitor groups with each Bosch VMS 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. 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.
This setting is enabled after activating the configuration.

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

Enforce automatic logoff of Configuration Client after this time of inactivity
This setting is enabled after activating the configuration.

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

See also

- *Assigning an analog monitor group to a workstation, page 158*

27.11 Remote Access Settings dialog box

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. Bosch VMS 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 35*

27.11.1 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 Bosch VMS. You can copy the table into the clipboard and you can add entries that are not managed by Bosch VMS.

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.

27.12 Device Monitor dialog box

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 Bosch VMS.

Display Name
Device name that was configured in Bosch VMS.

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 214*

27.13 SNMP Settings dialog box

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 Bosch VMS.

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 Bosch VMS supports SNMP GetRequest. When an SNMP manager software (for example iReasoning MIB Browser) sends an SNMP GetRequest to the Bosch VMS 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 Bosch VMS Management Server listens for SNMP GetRequest.

Note: Bosch VMS 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 Bosch VMS Management Server is installed on.

The default value is `12544`.

System contact

Type in contact data for your Bosch VMS. 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 Bosch VMS. 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 Bosch VMS. 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 Bosch VMS 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 214*

27.14 License Investigator dialog box

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

28 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:

Video data from encoders that are assigned to an NVR, is always encoded with MPEG-4.

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.

Scans the network for NVRs, decoders, and encoders. When the scan process is finished, a dialog box for assigning the detected encoders to NVRs is displayed.

Failover NVR Manager

Click to display the **Failover NVR Manager** dialog box.

IP Device Configuration

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

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

To cancel filtering, click ✕.

- Click a tree item to display the corresponding page.

28.1 Server List / Address Book page

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

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

You can add multiple Management Server computers for simultaneous access in Bosch VMS 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 117*
- *Configuring Server Lookup , page 119*
- *Exporting the Server List, page 120*
- *Importing a Server List, page 120*

28.1.1 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.

28.2 Initial Device Scan dialog box

Main window > **Hardware** menu > **Initial Device Scan...** command
Displays the devices which have duplicate IP addresses or a default IP address (192.168.0.1).
Allows you to change such IP addresses and subnet masks.
You must enter the correct subnet mask before changing an IP address.

28.3 NVR & Decoder Scan dialog box

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

Main window > **Devices** > **NVR & Decoder Scan**
Displays detected encoders, NVRs, and decoders.
Allows you to assign detected encoders to an NVR. This is required to store the video data of the encoder on an NVR and to manage events of their assigned devices.
Unassigned devices do not appear in the Device Tree.

Notice!
Only devices in the local subnet are detected automatically. If a device is located in another subnet, add it manually to the Device Tree. To perform this, right-click the required node (for example an NVR), click **Add Encoder**, type the IP address of the device, click the **Network** tab and enter the subnet mask of the device.

Unassigned Encoders
Displays the unassigned encoders that were detected.

Assigned Encoders and NVRs
Displays assigned encoders and NVRs. NVRs are automatically assigned when they are detected. For assigning encoders you must drag them from the **Unassigned Encoders** list to an NVR.

Decoders
Displays the detected decoders.

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

Next >
Click to display the next page of this dialog box. If the device names differ from their names in Bosch VMS, a dialog box is displayed for changing the names as required.

Finish
Click to confirm the scan results and the assignments of encoders and close the dialog box.

28.4 IP Device Configuration dialog box

Main window > **Devices** >
Displays the following properties of the available IP devices:

- Device name and type
- Connection type (BVIP or ONVIF)
- IP address
- Subnet mask
- System password

- Firmware version
- Gateway IP address

Allows you to set the following properties of the available IP devices:

- Display name
- IP address
- Firmware version

You can configure display names, IP addresses and firmware versions for multiple devices at once.

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.

Update Firmware
Click to update the firmware version of the selected device.

Show passwords
Click to clear 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 ✕.

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

See also

- *Configuring multiple encoders / decoders, page 137*

28.5 Set IP Addresses dialog box

Main window > **Devices** > > **IP Device Configuration** dialog box > Right-click two or more entries > Click **Set IP Addresses...**
Allows you to set the IP addresses for multiple IP devices.

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.

See also

- *Configuring multiple encoders / decoders, page 137*

28.6 Set Display Names dialog box

Main window > **Devices** > > **IP Device Configuration** dialog box > Right-click two or more entries > Click **Set Display Names...**
Allows you to set the display names for multiple IP devices.

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.

See also
- *Configuring multiple encoders / decoders, page 137*

28.7 NVRs / Failover NVRs / Redundant NVRs page

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

28.8 Vidos NVRs page

Main window > **Devices** > Expand > Expand >
Allows you to add and configure VIDOS NVRs.
You cannot configure VIDOS systems from within Bosch VMS.

Network Address:
Type the DNS name or the IP address of your VIDOS NVR.

User Name:
Type the user name for logging on to the VIDOS NVR.

Password:
Type the password for logging on to the VIDOS NVR.

See also
- *Scanning for devices, page 81*

28.9 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 Bosch VMS related properties.

- Click a tab to display the corresponding property page.

See also

– *Adding a device manually, page 150*
– *Configuring the integration of a DiBos system, page 155*

28.9.1 Add DiBos System dialog box

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

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.

See also

– *Adding a device manually, page 150*

28.9.2 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 155*

28.9.3 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 155*

28.9.4 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 155*

28.9.5 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 155*

28.10 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 Bosch VMS.

Caution!

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

See also

– *DVR devices, page 52*

– *Configuring the integration of a DVR, page 156*

28.10.1 Add DVR dialog box

Main window > **Devices** > Expand > > **Add DVR Recorder**

Allows you to manually add a DVR device.

Network address:

Type the DNS name or the IP address of your DVR.

User name:

Type the user name for connecting to the DVR.

Password:

Type the password for connecting to the DVR.

Click below to get step-by-step instructions:

– *Adding a device manually, page 150*

28.10.2 Settings tab

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

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

28.10.3 Cameras tab

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

Displays all video channels of the DVR as cameras. Allows you to remove cameras.
A video input that is disabled in a DVR device is displayed as an active camera in Bosch VMS because earlier recordings could exist for this input.

28.10.4 Inputs tab

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

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

28.10.5 Relays tab

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

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

28.11 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 Bosch VMS related properties. For connecting an Allegiant device with Bosch VMS, 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

– *Adding a device manually, page 150*
– *Configuring a Bosch Allegiant device, page 157*
– *Connecting Bosch Allegiant Matrix to Bosch Video Management System, page 74*

28.11.1 Connection page

Main window > **Devices** > Expand > > **Connection** tab

Displays the name of the Bosch Allegiant configuration file.
Bosch VMS 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 157*

28.11.2 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 157*

28.11.3 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 Bosch VMS, 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.

Bosch VMS Logical No.

Allows you to change the logical number of the output within Bosch VMS. 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 157*

28.11.4 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 157*

28.12 Workstation page

Main window > **Devices** > Expand >

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 data stream for live display.
- Enable Forensic Search.
- Assign analog monitor groups to a workstation.

A workstation must have the Operator Client software installed.

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

To assign an analog monitor group, configure such a group in > > .

See also

- *Adding a device manually, page 150*
- *Configuring a startup Command Script, page 202*
- *Configuring an analog monitor group, page 158*

28.12.1 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.

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 Bosch VMS, 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.

Retrieve Live video from 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.

28.12.2 Assigned Analog Monitor Groups page

Main window > **Devices** > Expand > > **Assigned Analog Monitor Groups** tab
Allows you to assign an analog monitor group to this workstation. Beforehand you must have added an analog monitor group in > > .

Assigned Analog Monitor Groups
Select the check box to assign the analog monitor group to this workstation. In the **Options** dialog box, you can configure that all other workstations can also control analog monitor groups.

Analog Monitor Group
Displays the name of each analog monitor group.

See also

- *Assigning an analog monitor group to a workstation, page 158*

28.13 Decoders page

Main window > **Devices** > Expand >
Allows you to add and configure decoders.
See *Bosch Encoder / Decoder page, page 282* for details.

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

See also

- *Scanning for devices, page 81*

28.13.1 Add Encoder / Add Decoder dialog box

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

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

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

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

Main window > **Devices** > Expand > Right-click > Click **Add Decoder** > **Add Decoder** dialog box
Allows you to add an encoder or decoder manually. This is especially useful when you want to add any Video IP device from Bosch (only for VRM).

IP address:
Type in a valid IP address.

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

See also
- *Adding a device manually, page 150*

28.13.2 Edit Encoder / Edit Decoder dialog box

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

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

or

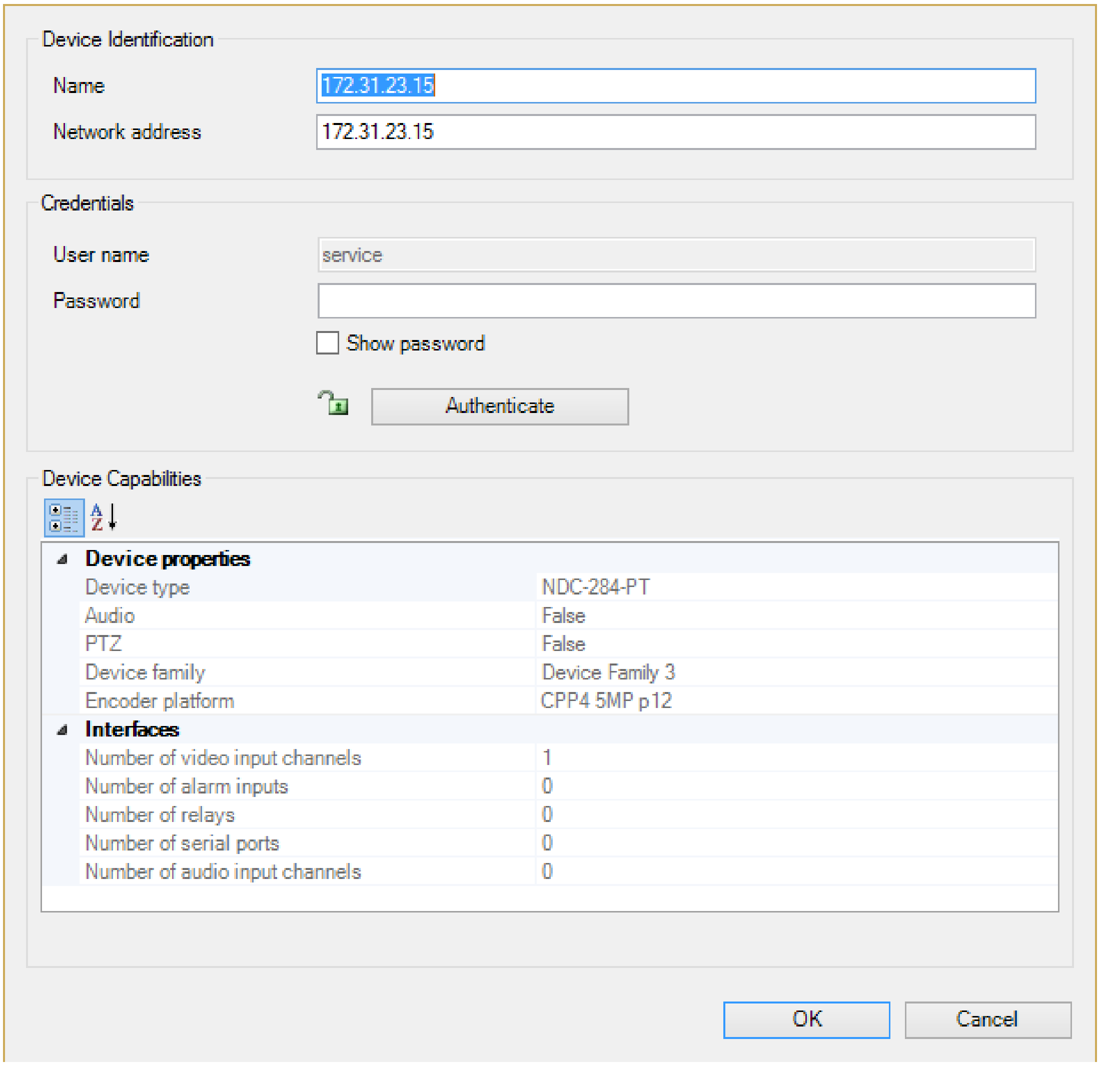
Main window > **Devices** > Right-click > Click **Edit Encoder** > **Edit Encoder** dialog box

or

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

or

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



Device Identification

Name: 172.31.23.15

Network address: 172.31.23.15

Credentials

User name: service

Password:

☐ Show password

Device Capabilities

Device properties	
Device type	NDC-284-PT
Audio	False
PTZ	False
Device family	Device Family 3
Encoder platform	CPP4 5MP p12
Interfaces	
Number of video input channels	1
Number of alarm inputs	0
Number of relays	0
Number of serial ports	0
Number of audio input channels	0

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 Bosch VMS.

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

Type in the network address of the device.

User name

Displays the user name used for authenticating at the device.

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.

Authenticate

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

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

– *Updating the device capabilities, page 135*

28.13.3 Enter password dialog box

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

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

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

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

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

A password prevents unauthorized access to the device. You can use different authorization levels to limit access.
Proper password protection is only guaranteed when all higher authorization levels are also protected with a password. Therefore, you always have to start from the highest authorization level when assigning passwords.

You can define and change a password for each authorization level if you are logged in as service or if the unit is not password protected.
Enter the password for the appropriate authorization level here. The maximum password text length is 19 characters and no special characters are allowed.
The device has three authorization levels: service, user, and live.

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

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

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

See also

- *Changing the password of an encoder / decoder, page 137*
- *Providing the destination password for a decoder, page 138*

28.14 Analog Monitor Groups page

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

Caution!
You cannot control an analog monitor group from within Operator Client when the connection to the Management Server is lost or when Operator Client with Enterprise System is used.

See also

- *Adding a device manually, page 150*
- *Configuring an analog monitor group, page 158*

28.14.1 Settings page

Main window > **Devices** > Expand > > **Settings** tab
Allows you to perform the following tasks:

- Configure an analog monitor group
- Assign decoders to an analog monitor group
- Enable quad view for decoders that support quad view

Name:
Type the name of the analog monitor group.

Columns:
Enter the number of columns for the analog monitor group. The result is displayed.

Rows:
Enter the number of rows for the analog monitor group. The result is displayed.

Unassigned Decoder Channels
Drag a decoder to an available analog monitor.

Monitor image
The white number, if present, displays the logical number of the initial camera. The black number displays the logical number of the decoder.
Right-click an analog monitor image to toggle between single view and quad view. On the **Advanced Configuration** page, the **Quad View** column displays the corresponding setting.
To un-assign a decoder, right-click the analog monitor image and click **Clear Monitor**.

See also
- *Configuring an analog monitor group, page 158*

28.14.2 Advanced Configuration page

Main window > **Devices** > Expand > > **Advanced Configuration** tab
Allows you to perform the following tasks:
- Configure the logical number of a decoder or decoder channel.
- Enable quad view for decoders that support quad view
- Configure the OSD.

Notice!
We do not recommend configuring quad view for H.264 cameras.

Note the following hints on switching the decoder between quad view and single view in the Operator Client:
- The user can manually switch the decoder back to single view when it is configured as quad view.
- When the decoder is switched to single view or to quad view and a sequence is just running, only the last video stream remains visible.
- When the user switches to quad view, the last cameras that have been displayed on Image pane 2-4 are reconnected.
- This is also valid for trunk lines. There is only one limitation: If the matrix camera cannot be reconnected, this is ignored without an error message. A black Image pane is visible.
- When switching to single view, all trunk lines that are displayed on Image pane 2-4 are disconnected. Only the camera number is stored for a later switch to quad view.

Decoder Name
Displays the display name of the decoder.

Network Address
Displays the IP address of the decoder.

Logical Number
Enter the logical number of the decoder. If you enter an already used number, a message is displayed.

Quad
Displays the position of the decoder on the quad view. 1 is left upper corner, 4 is right lower corner.

Quad View
Select the check box to enable quad view for this decoder. On the **Settings** page, the corresponding analog monitor image displays the quad view. Logical numbers are created automatically. If you want the Operator Client user to be able to switch between quad view and single view, then check **Quad View**. If you clear **Quad View**, the Operator Client user cannot switch.

AMG
Displays the analog monitor group that the decoder in this row is assigned to.

Initial Camera
Click to select the camera that is displayed initially on the monitor after having started the Operator Client. The logical number of the initial camera is displayed as the white number on the monitor image in the **Settings** page.

OSD Camera Name
Check to display the camera name as OSD.

OSD Camera No.
Check to display the logical number of the camera as OSD.

OSD Position
To set the location of an OSD, select the desired entry.

See also

- *Configuring an analog monitor group, page 158*

28.15 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 336*
- *Adding a monitor wall, page 159*
- *Adding a monitor wall, page 159*

28.15.1 Add Monitor Wall dialog box

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

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

Name

Type in a display name for your monitor wall.

Monitor

Select a monitor that is connected to a decoder.

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

Maximum number of cameras to connect

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

Enable thumbnails

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

Initial sequence

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

See also

- *Adding a monitor wall, page 159*

28.16 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

- *Adding a device manually, page 150*
- *Configuring a communication device, page 159*

28.16.1 E-mail/SMTP Server dialog box

Main window > **Devices** > Expand > Right-click > **Add E-mail/SMTP Device** command

Allows you to add an e-mail server to your Bosch VMS.

Name:

Type the display name of the e-mail server.

See also

- *Adding a device manually, page 150*

28.16.2 Add SMS Device dialog box

Main window > **Devices** > Expand > Right-click > **Add SMS Device** command

Allows you to add an SMS device to your system.

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.

See also

- *Adding a device manually, page 150*

28.16.3 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 Bosch VMS.

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.

Username:

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 159*

28.16.4 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 159*

28.16.5 GSM Settings / SMSC Settings page

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

Allows you to configure the SMS settings of your Bosch VMS. 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 159*

28.17 POS + ATM 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 device manually, page 150*
- *Adding a Bosch ATM/POS bridge, page 215*

– *Configuring a peripheral device, page 159*

28.17.1 Add Bosch ATM/POS-Bridge dialog box

Main window > **Devices** > Expand > Right-click > **Add Bosch ATM/POS-Bridge** command

Allows you to add a Bosch ATM/POS Bridge.

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 Bosch VMS Management Server.

Caution!

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 device manually, page 150*
– *Adding a Bosch ATM/POS bridge, page 215*

28.17.2 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 Bosch VMS Management Server.

Caution!

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 159*
– *Adding a Bosch ATM/POS bridge, page 215*

28.17.3 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 159*
- *Adding a Bosch ATM/POS bridge, page 215*

28.17.4 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 252*
- *Configuring a peripheral device, page 159*

28.17.5 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, Bosch VMS 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 159*

28.18 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 Bosch VMS 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.

28.18.1 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.

28.18.2 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 Bosch VMS 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, Bosch VMS 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**

28.19 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.

See also
- *Adding a device manually, page 150*

28.19.1 Add Virtual Inputs dialog box

Main window > **Devices** > Expand > **Add Inputs** button
Allows you to add new virtual inputs.

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.

See also
- *Adding a device manually, page 150*

28.20 SNMP page

Main window > **Devices** > Expand >
Allows you to add or configure an SNMP measurement for maintaining the network quality.

See also

- *Adding a device manually, page 150*
- *Configuring an SNMP trap receiver, page 160*

28.20.1 Add SNMP dialog box

Main window > **Devices** > Expand > Right-click > **Add SNMP** command
Allows you to add a network monitoring system to your Bosch VMS.

Name:
Type a name for the network monitoring device.

See also

- *Configuring an SNMP trap receiver, page 160*

28.20.2 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.

See also

- *Configuring an SNMP trap receiver, page 160*

28.20.3 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, page 160*

28.21 Assign Keyboard page

Main window > **Devices** > Expand >

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

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**
  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

- *Adding a device manually, page 150*
- *Configuring a decoder for use with a Bosch IntuiKey keyboard, page 155*
- *Configuring a Bosch IntuiKey keyboard (workstation), page 160*
- *Configuring a Bosch IntuiKey keyboard (decoder), page 160*

28.22 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

- *Adding a device manually, page 150*
- *Configuring an I/O module, page 161*

28.22.1 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.

See also

- *Adding a device manually, page 150*

28.22.2 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.

See also
- *Adding a device manually, page 150*

28.22.3 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.

See also
- *Adding a device manually, page 150*

28.23 Allegiant CCL Emulation page

Main window > **Devices** > Expand >
Allows you to activate the Allegiant CCL emulation.
Allegiant CCL commands supported in Bosch VMS, page 78 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 161*

28.24 Mobile Video Service page

Main window > **Devices** >
Allows you to add one or more transcoding service entries to your Bosch VMS. This transcoding service adapts the video stream from a camera configured in Bosch VMS 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, page 162*

28.24.1 Add Mobile Video Service dialog box

Main window > **Devices** > Right-click > Click **Add Mobile Video Service**

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.

See also
- *Adding a Mobile Video Service, page 162*

28.25 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 Bosch VMS.

Notice!
All alarm events that can occur at a point, are automatically configured as a Bosch VMS alarm.
Example: Fire alarm

Warning!
If a door is not assigned to a point in the configuration of an intrusion panel that is added to your Bosch VMS, an alarm from this door does not trigger a Bosch VMS event and hence no Bosch VMS alarm.

See also

– *Adding a device manually, page 150*

28.25.1 Add Intrusion Panel dialog box

Main window > **Devices** > Expand > Right-click > **Add Panel** command
Allows you to add an intrusion panel from Bosch.

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.

28.25.2 Settings page

Main window > **Devices** > Expand > Expand > > **Settings** tab
Allows you to change the connection settings of the intrusion panel.

28.26 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. Use the same user name that Bintelan Bosch Client is using for connection with Bosch VMS.

Password
Type in the password as configured in the server-based analytics device. Use the same password that Bintelan Bosch Client is using for connection with Bosch VMS.

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
```

See also

– *Configuring server-based video analytics, page 168*

28.26.1 Add Video Analytics Device dialog box

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.

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. Use the same user name that Bintelan Bosch Client is using for connection with Bosch VMS.

Password

Type in the password as configured in the server-based analytics device. Use the same password that Bintelan Bosch Client is using for connection with Bosch VMS.

See also

– *Adding a video analytics device, page 169*

28.27 Bosch VMS Scan Wizard

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

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

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

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

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

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

Use

Click to select a device for adding to the system.

Type (not available for VSG devices)

Displays the type of the device.

Display Name

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

Network Address

Displays the IP address of the device.

User Name

Displays the user name that is configured on the device.

Password

Type in the password for authenticating with this device.

Status

Displays the status of authentication.

🔓 : Succeeded

🔒 : Failed

Main window > **Devices** > Right-click > Click **Scan for VRM Devices**> Bosch VMS 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

- *Scanning for VRM devices, page 122*
- *Adding an encoder to a VRM pool, page 164*
- *Adding a live only encoder, page 164*
- *Adding a local storage encoder, page 165*
- *Scanning for devices, page 81*

28.28 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 Bosch VMS, you must add the IQN of each encoder to this iSCSI device (valid for some iSCSI device types).
See *Configuring an iSCSI device, page 126* 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.

As of Bosch VMS 6.0, VRM 3.50 is supported. If you do not upgrade your VRM version from earlier versions to version 3.50, you cannot change the configuration of the VRM with the earlier version.
If you upgraded your VRM software to version 3.50, you must manually synchronize the Bosch VMS configuration.

See also

- *Synchronizing Bosch VMS configuration, page 122*
- *VRM Settings page, page 265*
- *Pool page, page 266*
- *iSCSI device page, page 271*
- *Changing the password of a VRM device, page 129*

28.28.1 Add VRM dialog box

Main window > **Devices** > Right-click > Click **Add VRM** > **Add VRM** dialog box
Allows you to add a VRM device. You can select the type of the device and enter the credentials.
You can effectively assign a Failover VRM to a Master VRM only when both are online and are successfully authenticated. The passwords are then synchronized.

Name
Type in a display name for the device.

Network Address / Port:
Type in the IP address of your device.

Type:
Select the desired device type.

User Name:
Type in the user name for authentication.

Password:
Type in the password for authentication.

Show password
Click to enable that the password is visible.

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

Properties
If required, change the port numbers for the HTTP port and for the HTTPS port. This is only possible when you add or edit a VRM that is not connected. If the VRM is connected, the values are retrieved and you cannot change them.
The **Master VRM** table row shows the selected device if applicable.

See also
- *Adding a Primary VRM manually, page 123*
- *Adding a Secondary VRM manually, page 123*
- *Adding a Mirrored VRM manually, page 124*
- *Adding a Failover VRM manually, page 124*

28.28.2 Add Failover VRM dialog box

Main window > **Devices** > Expand > Right-click > Click **Add Failover VRM** > **Add Failover VRM** dialog box
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 Failover VRM device. You can either add it manually or you can select a device from a list of scanned VRM devices.

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.

28.29 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.

28.29.1 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.

28.29.2 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.

28.29.3 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.

Caution!

Extensive logging requires considerable CPU power and HDD capacity.
Do not use extensive logging in continuous operation.

28.30 Pool page

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

Allows you to configure recording settings valid for all devices that are collected in this storage pool.

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.

See also

– *Adding a VRM pool, page 125*

28.30.1 Add Encoder / Add Decoder dialog box

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

or

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

or

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

or

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

or

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

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

IP address:

Type in a valid IP address.

Encoder type: / Decoder type:

For a device with known device type, select the appropriate entry. It is not necessary that the device is available in the network.

If you want to add any Video IP device from Bosch, select **<Auto Detect>**. The device must be available in the network.

See also

– *Adding a device manually, page 150*

28.30.2 Edit Encoder / Edit Decoder dialog box

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

or

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

or

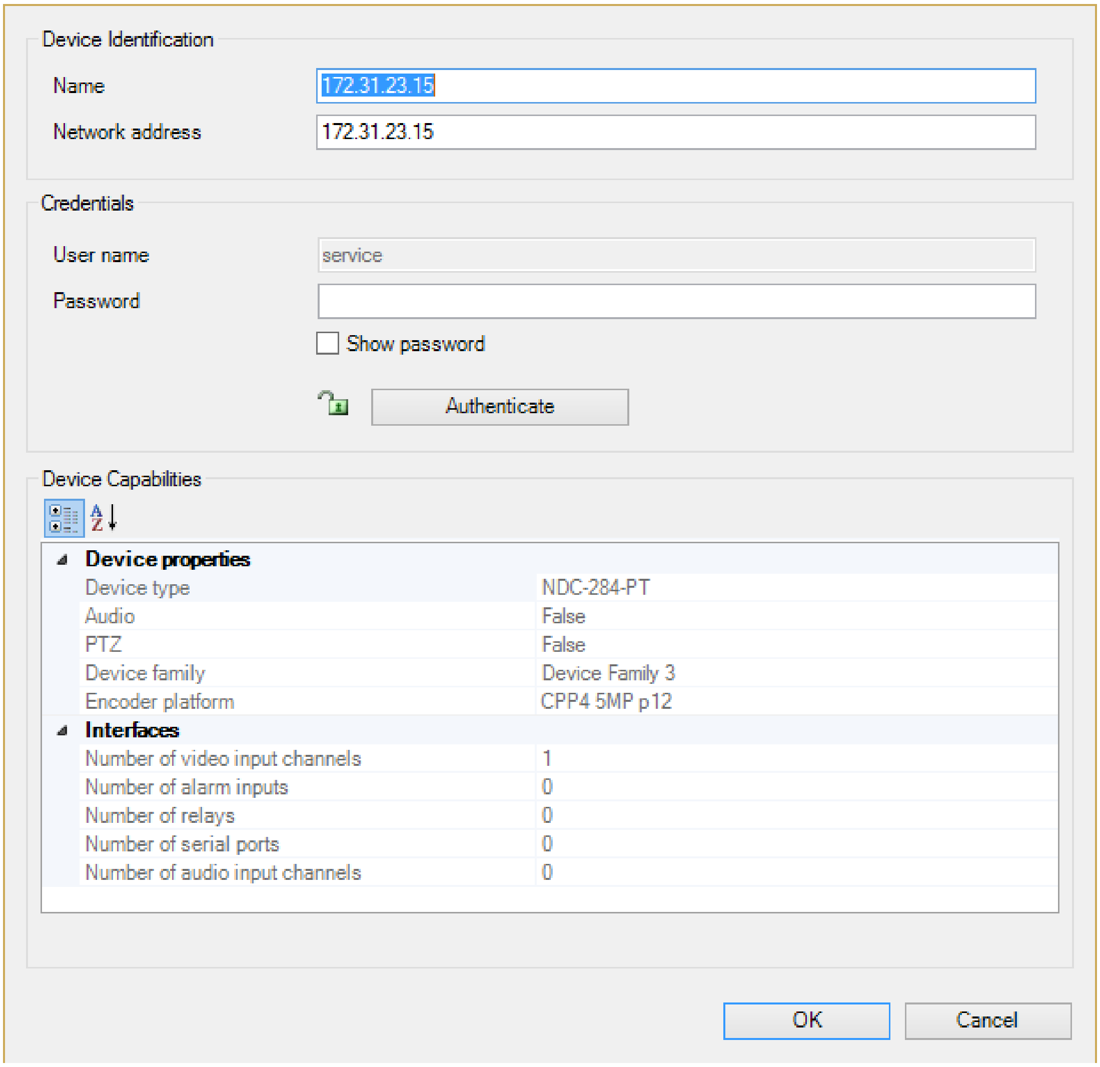
Main window > **Devices** > Right-click > Click **Edit Encoder** > **Edit Encoder** dialog box

or

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

or

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



Device Identification

Name: 172.31.23.15

Network address: 172.31.23.15

Credentials

User name: service

Password:

□ Show password

Device Capabilities

Device properties	
Device type	NDC-284-PT
Audio	False
PTZ	False
Device family	Device Family 3
Encoder platform	CPP4 5MP p12
Interfaces	
Number of video input channels	1
Number of alarm inputs	0
Number of relays	0
Number of serial ports	0
Number of audio input channels	0

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 Bosch VMS.

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

Type in the network address of the device.

User name

Displays the user name used for authenticating at the device.

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.

Authenticate

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

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

– *Updating the device capabilities, page 135*

28.30.3 Change Pool for dialog box

Main window > **Devices** > Expand > Expand > > Right-click > **Change Pool ...** command > **Change Pool for** dialog box
or

Main window > **Devices** > Expand > Expand > > Right-click iSCSI > **Change Pool ...** command > **Change Pool for** dialog box
or

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

See also

– *Moving an encoder to another pool, page 133*
– *Moving an iSCSI system to another pool, page 127*
– *Moving a VSG to another pool, page 144*

28.30.4 Add Streaming Gateway dialog box

Right-click > **Add Video Streaming Gateway** > **Add Video Streaming Gateway** dialog box
You can add VSG devices to a VRM pool.

Name:
Type in the desired display name for the device.

Network address
Type in the network address of the device.

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.

See also

– *Video Streaming Gateway device page , page 274*

28.31 iSCSI device page

You can either add a E-Series iSCSI device or any other supported iSCSI device.

See also

– *Adding an iSCSI device, page 125*
– *Adding a DSA E-Series iSCSI device, page 126*
– *Configuring an iSCSI device, page 126*
– *Adding a LUN, page 128*
– *Formatting a LUN, page 128*

28.31.1 Add iSCSI Device dialog box

Main window > **Devices** > > Expand > Right-click > **Add iSCSI Device** > **Add iSCSI Device** dialog box

Allows you to add an iSCSI devices to a VRM.

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

– *Scanning for VRM devices, page 122*

28.31.2 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 3

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 3

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.

Related Topics

– *Adding a DSA E-Series iSCSI device, page 126*

28.31.3 Load Balancing dialog box

Main window > **Devices** > Expand > Expand > Expand > Right-click iSCSI > **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.

28.31.4 Basic Configuration page

Main window > **Devices** > Expand > Expand > Expand > Click iSCSI > **Basic Configuration** tab

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.
The displayed options can differ depending on the used type of iSCSI storage system.

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.

Clear
Clears the configuration, i.e. deleting all LUNs.

Defaults
Sets the storage system back to its factory default. Additionally to clear the storage system name and all iSCSI IP addresses are deleted. Only management addresses and the configuration password are retained.

Serial number
The serial number needed for support cases. It is only correct if the controller is not moved to a different shelf.

Delete all LUNs
As already stated above the user should wait some hours before he creates new LUNs.

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.

28.31.5 iqn-Mapper dialog box

Main window > **Devices** > Expand > Expand > Expand > Right-click iSCSI > **Map IQNs**

Allows you to start the IQN mapping process.

See also

- *Scanning for VRM devices, page 122*
- *Configuring an iSCSI device, page 126*

28.31.6 LUNs page

Main window > **Devices** > Expand > Expand > Expand > Expand iSCSI > ID

Allows you to add, remove, or format LUNs.

Add

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

Remove

Click to remove the selected LUNs. A message box is displayed.

Format LUN

Click to format the selected LUN. A message box is displayed.

Note:

In the **Format LUN** column, click the check box for the desired LUN.

See also

- *Scanning for VRM devices, page 122*

28.31.7 Add LUN dialog box

Main window > **Devices** > Expand > Expand > Expand > Expand iSCSI > ID > Click **Add**

Allows you to add a LUN.

Id

Enter the ID of the desired LUN.

See also

- *Scanning for VRM devices, page 122*

28.32 Video Streaming Gateway device page

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

Allows you to add and configure the following encoder types:

- Bosch encoders
- ONVIF encoders
- JPEG encoders
- RTSP encoders

See also

- *ONVIF page, page 316*
- *Adding a Video Streaming Gateway device, page 143*

28.32.1 Multicast tab (Video Streaming Gateway)

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.

See also

- *Configuring multicast, page 145*

28.32.2 Advanced tab (Video Streaming Gateway)

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
```

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.

Caution!

Extensive logging requires considerable CPU power and HDD capacity.

Do not use extensive logging in continuous operation.

See also

– *Configuring logging, page 145*

28.32.3 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 144*

28.32.4 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.

Name:
Type in the desired display name for the device.

Network address
Type in the network address of the device.

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

Device type	Displays the retrieved device type.
Manufacturer	Displays the retrieved manufacturer name.

Model	Displays the retrieved model name.
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.

See also

– *Adding a camera to a VSG, page 144*

28.32.5 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?jpegCam0<channel_no.>
```

For an RTSP camera from Bosch, type in the following string:

```
rcpp://<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 144*

28.32.6 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?jpegCam0<channel_no.>
```

For an RTSP camera from Bosch, type in the following string:

```
rcpp://<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 144*

28.33 Live Only page

Main window > **Devices** > Expand >

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

See also

- *Adding a live only encoder, page 164*
- *Scanning for devices, page 81*
- *Bosch Encoder / Decoder page, page 282*
- *ONVIF page, page 316*

28.34 Local Storage page

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

See also

- *Adding a local storage encoder, page 165*
- *Bosch Encoder / Decoder page, page 282*
- *Scanning for devices, page 81*

28.35 Unmanaged Sites page

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

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

Description:
Type in a description for this site.

See also

- *Unmanaged site, page 31*
- *Adding an unmanaged site, page 121*
- *Importing a configuration of unmanaged sites, page 121*

28.35.1 Unmanaged Network Device page

Main window > **Devices** > Expand >

Device type:
Select the entry that is applicable for this device.
Available entries:

- **DIVAR AN / DVR**
- **DIVAR IP 3000/7000 / Bosch VMS**

IP address:
Type in an IP address.

User name:
Type in the valid user name for this network device if available. See *Unmanaged site, page 31* for details.

Password:
Type in the valid password if available. See *Unmanaged site, page 31* for details on user credentials.

28.35.2 Add Unmanaged Network Device dialog box

Main window > **Devices** > Right-click > **Add Unmanaged Network Device** command > **Add Unmanaged Network Device** dialog box

Device type:
Select the entry that is applicable for this device.
Available entries:

- **DIVAR AN / DVR**
- **DIVAR IP 3000/7000 / Bosch VMS**

IP address:
Type in an IP address.

User name:
Type in the valid user name for this network device if available. See *Unmanaged site, page 31* for details.

Password:
Type in the valid password if available. See *Unmanaged site, page 31* for details on user credentials.

See also

- *Adding an unmanaged site, page 121*
- *Unmanaged site, page 31*

29 Bosch Encoder / Decoder page

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

To configure an encoder / decoder:

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

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

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

Main window > **Devices** > Expand >

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

Most of the settings on the encoder / decoder pages are active immediately after you click . If you click another tab without clicking and changes have occurred, two corresponding message boxes are displayed. Confirm them both if you want to save.

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

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

Note:

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

- Click a tab to display the corresponding property page.

See also

- *Scanning for devices, page 81*
- *Configuring an encoder / decoder, page 135*

29.1 Enter password dialog box

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

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

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

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

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

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

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

You can define and change a password for each authorization level if you are logged in as service or if the unit is not password protected.

Enter the password for the appropriate authorization level here. The maximum password text length is 19 characters and no special characters are allowed.

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

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

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

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

See also

- *Changing the password of an encoder / decoder, page 137*
- *Providing the destination password for a decoder, page 138*

29.2 Unit Access page

29.2.1 Identification / Camera identification

Device name

Type the name of the device.

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

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

Click 💾 to update the name in the Device Tree.
Each device should be assigned a unique identifier that can be entered here as an additional means of identification.

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

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

29.2.2 Camera name

Camera
Type the name of the camera. Ensure that Camera 1 is allocated to Video Input 1, Camera 2 to Video Input 2, etc.
The camera name facilitates the identification of the remote camera location, for example in case of an alarm. Use a name that makes it as easy as possible to identify the location.
Do not use any special characters in the name. Special characters are not supported and may cause problems, for example the play back of recordings. The settings on this page apply to all camera inputs.
Click 💾 to update the name in the Device Tree.

29.2.3 Version information

Hardware version
Displays the version of the hardware.

Firmware version
Displays the version of the firmware.

29.3 Date/Time page

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

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

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

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

Time server IP address

Set by Bosch VMS Management Server.

Time server type

Set by Bosch VMS Management Server. Default setting is SNTP.

29.4 Installer / Initialization menu

29.4.1 Application variant

The camera has a choice of application variants that set up the camera for optimum performance in a specific environment. Select the application variant best suited to your installation.

The application variant must be selected before any other changes are made, as the camera reboots automatically and resets the factory defaults when the application variant is changed.

29.4.2 Base frame rate

Select the base frame rate for the camera.

Note:

Shutter times and frame rates, and the analog output (if present) are affected by this value.

29.4.3 Camera LED

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

29.4.4 Mirror image

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

29.4.5 Flip image

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

29.4.6 Menu button

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

29.4.7 Heater

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

29.4.8 Reboot device

Click **Reboot** to restart the camera.

29.4.9 Factory defaults

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

29.4.10 Lens Wizard

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

29.5 Privacy Masks page

Privacy masking is used to block a specific area of a scene from being viewed. Four privacy mask areas can be defined. The activated masked areas are filled with the selected pattern in live view.

1. Select the pattern to be used for all masks.

2. Check the box of the mask you wish to activate.
3. Use the mouse to define the area for each of the masks.

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

Active masks
To activate a mask, select the appropriate check box.

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

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

Pattern
Pattern of the privacy mask.

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

29.6 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 139*

29.7 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 266*

29.8 Video Input page

75 Ohm termination input %s

Select **Off** if the video signal is to be looped through.

Source type input %s

To allow the connection of VCRs as a video source, you can change the video source characteristics from the default **Camera** to **VCR**. VCRs require a more tolerant setting for the internal PLL as a result of jitter effects caused by the mechanical components of a VCR.

Notice!
In some cases, selecting the **VCR** option can lead to an improvement in the video image even with a camera connected.

Camera name stamping

This field sets the position of the camera name overlay. It can be displayed at the **Top**, at the **Bottom** or at a position of your choice that you can then specify using the **Custom** option. Or it can be set to **Off** for no overlay information.

1. Select the desired option from the list.
2. If you select the **Custom** option, additional fields are displayed where you can specify the exact position (**Position (XY)**).
3. In the **Position (XY)** fields, enter the values for the desired position.

Logo

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

Logo position

Select the position for the logo on the OSD: Left or Right.
Select Off (the default value) to disable logo positioning.

Time stamping

This field sets the position of the time overlay. It can be displayed at the **Top**, at the **Bottom** or at a position of your choice that you can then specify using the **Custom** option. Or it can be set to **Off** for no overlay information.

1. Select the desired option from the list.

2. If you select the **Custom** option, additional fields are displayed where you can specify the exact position (**Position (XY)**).
3. In the **Position (XY)** fields, enter the values for the desired position.

Display milliseconds

If necessary, you can also display milliseconds. This information can be useful for recorded video images; however, it does increase the processor's computing time. Select **Off** if you do not need to display milliseconds.

Alarm mode stamping

Select **On** to display a text message overlay in the image in the event of an alarm. It can be displayed at a position of your choice that you can then specify using the **Custom** option. Or it can be set to **Off** for no overlay information.

1. Select the desired option from the list.
2. If you select the **Custom** option, additional fields are displayed where you can specify the exact position (**Position (XY)**).
3. In the **Position (XY)** fields, enter the values for the desired position.

Alarm message

Enter the message to be displayed in the image in the event of an alarm. The maximum text length is 31 characters.
Check this box to make the stamp on the image transparent.
Various overlays or “stamps” in the video image provide important supplementary information. These overlays can be enabled individually and are arranged on the image in a clear manner.

Camera OSD

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

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

Title OSD

Select **On** to continuously display sector or shot title overlays in the image. Select **Momentary** to display sector or shot title overlays for a few seconds. OSD titles can be displayed at a position of your choice, or it can be set to **Off** for no overlay information.

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

After you set all necessary parameters, click the **View Control** link to see how the stamping appears on the **LIVE** page.
Select a method for verifying the integrity of the video in the **Video authentication** drop-down box.
If you select **Watermarking** all images are marked with an icon. The icon indicates if the sequence (live or saved) has been manipulated.
If you want to add a digital signature to the transmitted video images to ensure their integrity, select one of the cryptographic algorithms for this signature.
Enter the interval (in seconds) between insertions of the digital signature.

Signature intervals

Select the interval (in seconds) for the signature.

29.9 Picture settings - Scene mode

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

29.9.1 Current mode

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

29.9.2 Mode ID

The name of the selected mode is displayed.

29.9.3 Copy mode to

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

29.9.4 Restore Mode Defaults

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

29.9.5 Scene mode factory defaults

Outdoor

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

Motion

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

Low light

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

BLC

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

Indoor

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

Vibrant

This mode has enhanced contrast, sharpness and saturation.

29.9.6 Scene mode factory defaults

Outdoor

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

Motion

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

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

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

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

Vibrant
This mode has enhanced contrast, sharpness and saturation.

29.9.7 Scene mode factory defaults

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

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

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

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

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

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

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

Vibrant
This mode has enhanced contrast, sharpness and saturation.

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

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

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

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

29.10 Picture settings - Color

Contrast (0...255)

Adjust the contrast with the slider from 0 to 255.

Saturation (0...255)

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

Brightness (0...255)

Adjust the brightness with the slider from 0 to 255.

29.10.1 White balance

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

Hold

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

R-gain

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

G-gain

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

B-gain

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

Note:

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

Default

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

29.10.2 White balance

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

Hold

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

R-gain

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

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

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

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

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

29.10.3 White balance

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

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

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

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

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

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

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

29.10.4 White balance

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

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

RGB-weighted white balance

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

R-gain

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

G-gain

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

B-gain

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

Note:

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

Default

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

29.11 Picture settings - ALC

29.11.1 ALC mode

Select the mode for automatic light-level control:

- Fluorescent 50 Hz
- Fluorescent 60 Hz
- Outdoor

29.11.2 ALC level

Adjust the video output level (-15 to 0 to +15).
Select the range within which the ALC will operate. A positive value is more useful for low-light conditions; a negative value is more useful for very bright conditions.

29.11.3 Saturation (av-pk)

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

29.11.4 Exposure/frame rate

Automatic exposure

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

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

Fixed exposure

Select to set a fixed shutter speed.

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

Default shutter

The default shutter improves the motion performance in auto exposure mode.

- Select a default shutter speed.

29.11.5 Day/night

Auto - the camera switches the IR cut-off filter on and off depending on the scene illumination level.
Monochrome - the IR cut-off filter is removed, giving full IR sensitivity.
Color - the camera always produces a color signal regardless of light levels.

Switch level
Set the video level at which the camera in **Auto** mode switches to monochrome operation (-15 to 0 to +15).
A low (negative) value means that the camera switches to monochrome at a lower light level. A high (positive) value means that the camera switches to monochrome at a higher light level.

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

Switch level
Set the video level at which the camera in **Auto** mode switches to monochrome operation (-15 to 0 to +15).
A low (negative) value means that the camera switches to monochrome at a lower light level. A high (positive) value means that the camera switches to monochrome at a higher light level.

IR function
(only for cameras with built-in IR illuminators)
Select the control setting for IR illumination:

- **Auto**: the camera automatically switches the IR illumination.
- **On**: the IR illumination is always on.
- **Off**: the IR illumination is always off.

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

Day-to-night switchover
Adjust the slider to set the video level at which the camera in **Auto** mode switches from color to monochrome operation (-15 to +15).
A low (negative) value means that the camera switches to monochrome at a lower light level. A high (positive) value means that the camera switches to monochrome at a higher light level.

Night-to-day switchover
Adjust the slider to set the video level at which the camera in **Auto** mode switches from monochrome to color operation (-15 to +15).
A low (negative) value means that the camera switches to color at a lower light level. A high (positive) value means that the camera switches to color at a higher light level.
(The actual switch-over point might change automatically to avoid instable switching.)

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

29.12 Encoder Regions page

1. Select one of the eight available regions from the drop-down box.
2. Use the mouse to define the area for that region by dragging the center or sides of the shaded window.

3. Select the encoder quality to be used for the defined area.
   (Object and background quality levels are defined on the **Expert Settings** section of the **Encoder Profile** page.)
4. If required, select another region and repeat steps 2 and 3.
5. Click **Set** to apply the region settings.

Preview

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

29.13 Camera page

AE-response speed

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

Backlight compensation

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

Blue Gain

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

Color hue

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

Fixed Gain

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

Gain control

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

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

High Sensitivity

Adjusts the level of intensity or lux within the image (HD only). Select from Off or On.

Maximum Gain Level

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

- **Normal**
- **Medium**
- **High** (default)

Night mode

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

- **Monochrome**: Forces the camera to stay in Nigh Mode and transmit monochrome images.

- **Color**: The camera does not switch to Night Mode regardless of ambient light conditions.
- **Auto** (default): The camera switches out of Night Mode after the ambient light level reaches a pre-defined threshold.

Night mode threshold

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

Noise Reduction

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

Noise Reduction Level

Adjusts the noise level to the appropriate level for shooting conditions. Select a value between 1 and 5.

Red Gain

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

Saturation

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

Sharpness

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

Current mode

Shutter

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

Shutter Mode

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

Stabilization

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

White Balance

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

29.13.1 ALC

ALC mode

Select the mode for automatic light-level control:

- Fluorescent 50 Hz
- Fluorescent 60 Hz
- Outdoor

ALC level

Adjust the video output level (-15 to 0 to +15).
Select the range within which the ALC will operate. A positive value is more useful for low-light conditions; a negative value is more useful for very bright conditions.
The saturation (av-pk) slider configures the ALC level so that it controls mainly on scene average level (slider position -15) or on scene peak level (slider position +15). Scene peak level is useful for capturing images that contain car headlights.

Exposure

Automatic exposure

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

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

Fixed exposure

Select to set a fixed shutter speed.

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

Default shutter

The default shutter improves the motion performance in auto exposure mode.

- Select a default shutter speed.

Day/night

Auto - the camera switches the IR cut-off filter on and off depending on the scene illumination level.
Monochrome - the IR cut-off filter is removed, giving full IR sensitivity.
Color - the camera always produces a color signal regardless of light levels.

Note:

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

Night-to-day switchover

Adjust the slider to set the video level at which the camera in **Auto** mode switches from monochrome to color operation (-15 to +15).
A low (negative) value means that the camera switches to color at a lower light level. A high (positive) value means that the camera switches to color at a higher light level.
(The actual switch-over point might change automatically to avoid instable switching.)

Day-to-night switchover

Adjust the slider to set the video level at which the camera in **Auto** mode switches from color to monochrome operation (-15 to +15).
A low (negative) value means that the camera switches to monochrome at a lower light level. A high (positive) value means that the camera switches to monochrome at a higher light level.

IR function

(only for cameras with built-in IR illuminators)
Select the control setting for IR illumination:

- **Auto**: the camera automatically switches the IR illumination.
- **On**: the IR illumination is always on.

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

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

29.13.2 Scene mode

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

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

Mode ID
The name of the selected mode is displayed.

29.13.3 Scene Mode Scheduler

The scene mode scheduler is used to determine which scene mode should be used during the day and which scene mode should be used during the night.

1. Select the mode you wish to use during the day from **Day mode** drop-down box.
2. Select the mode you wish to use during the night from **Night mode** drop-down box.
3. Use the two slider buttons to set the **Day time range**.

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

Vibrant
This mode has enhanced contrast, sharpness and saturation.

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

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

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

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

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

29.13.4 WDR

Select **Auto** for automatic Wide Dynamic Range (WDR); select **Off** to disable WDR.

Note:
WDR can only be active if Auto exposure is selected, and there is a match between the base frame rate selected in the installer menu and the ALC fluorescent mode frequency. If there is a conflict, a pop-up window will suggest a solution and adjust the appropriate settings.

29.13.5 Sharpness level

The slider adjusts the sharpness level between -15 and +15. Zero position of the slider corresponds to the factory default level.
A low (negative) value makes the picture less sharp. Increasing sharpness brings out more detail. Extra sharpness can enhance the details of license plates, facial features and the edges of certain surfaces but can increase bandwidth requirements.

29.13.6 Backlight Compensation

Select **Off** to switch off backlight compensation.
Select **On** to capture details in high-contrast and extremely bright-dark conditions.
Select **Intelligent AE** to capture object detail in scenes with people moving in front of a bright background

29.13.7 Contrast enhancement

Select **On** to increase the contrast in low contrast conditions.

29.13.8 Intelligent DNR

Select **On** to activate intelligent Dynamic Noise Reduction (DNR) which reduces noise based on motion and light levels.

Temporal noise filtering

Adjusts the **Temporal noise filtering** level between -15 and +15. The higher the value, the more noise filtering.

Spatial noise filtering

Adjusts the **Spatial noise filtering** level between -15 and +15. The higher the value, the more noise filtering.

29.13.9 Intelligent defog

Select **Intelligent defog** to activate the automatic intelligent defog feature. This feature continuously adjusts image parameters to provide the best picture possible under foggy or misty conditions.

29.14 Lens page

29.14.1 Focus

Autofocus

Continuously adjusts the lens automatically to the correct focus for the sharpest picture.

- **One push** (default): Activates the Auto Focus feature after the camera stops moving. Once focused, Auto Focus is inactive until the camera is moved again.
- **Auto focus**: Auto Focus is always active.
- **Manual**: Auto Focus is inactive.

Focus polarity

- **Normal** (default): Focus controls operate normally.
- **Reverse**: Focus controls are reversed.

Focus speed

Controls how fast the Auto focus will readjust when the focus becomes blurred.

29.14.2 Iris

Auto iris

Automatically adjusts the lens to allow the correct illumination of the camera sensor. This type of lens is recommended for use when there are low light or changing light conditions.

- **Constant** (default): Camera constantly adjusts to varying light conditions.
  If you select this option, for example the AutoDome Junior HD makes the following changes automatically:
  - **Gain control**: switches to AGC
  - **Shutter mode**: switches to Normal
- **Manual**: Camera must be manually adjusted to compensate for varying light conditions.

Iris polarity

Capability to reverse the operation of the iris button on the controller.

- **Normal** (default): Iris controls operate normally.
- **Reverse**: Iris controls are reversed.

Auto iris level

Increases or decreases brightness according to the amount of light. Type a value between 1 and 15, inclusive. The default setting is 8.

Iris speed

Controls how fast the Iris will adjust the opening according to the illumination of the scene. Type a value between 1 and 10, inclusive. The default setting is 5.

29.14.3 Zoom

Maximum zoom speed

Controls the zoom speed. Default setting: **Fast**

Zoom polarity

Capability to reverse the operation of the zoom button on the controller.

- **Normal** (default): Zoom controls operate normally.
- **Reverse**: Zoom controls are reversed.

Digital zoom

Digital zoom is a method of decreasing (narrowing) the apparent angle of view of a digital video image. It is accomplished electronically, without any adjustment of the camera's optics, and no optical resolution is gained in the process.

- **Off** (default): Enables the Digital Zoom feature.
- **On**: Disables the Digital Zoom feature.

29.15 PTZ page

Auto pan speed

Continuously pans the camera at a speed between right and left limit settings. Type a value between 1 and 60 (expressed in degrees), inclusive. The default setting is 30.

Inactivity

Selects the time period the dome must be not controlled until the inactivity event will be executed.

- **Off** (default): Camera remains on a current scene indefinitely.
- **Scene 1**: Camera returns to Preset 1.
- **Previous Aux**: Camera returns to the previous activity.

Inactivity period

Determines the behavior of the dome when the control for dome is inactive. Select a time period from the pull-down list (3 sec. - 10 min.). The default setting is 2 minutes.

Auto pivot
The Auto Pivot tilts the camera through the vertical position as the camera is rotated to maintain the correct orientation of the image.
Set the Auto Pivot to **On** (default) to automatically rotate the camera 180º when following a subject traveling directly beneath the camera. To disable this feature, click **Off**.

Freeze frame
Select **On** (default) to freeze the image while the camera moves to a predetermined scene position.

Tilt up limit
Click **Set**, to set the upper tilt limit of the camera.

Tilt limits
Click **Reset** to clear the upper tilt limit.

29.16 Prepositions and Tours page

Allows you to define the individual scenes and a preposition tour comprised of the defined scenes.

To add scenes:
Click ✚.

To delete scenes:
Select the scene, then click ✕.

To overwrite (save) scenes:
Click 💾.

To view scenes:
Select the scene, then click 👁.

Include in standard tour (marked with *)
Select the check box if the scene should be part of the preposition tour. The asterisk (*) on the left of the scene name indicates this.

29.17 Sectors page

Sector
The pan capability (for example for the AutoDome Junior HD camera) is 360° and is divided into eight equal sectors. This allows you to apply a title for each sector and to designate any sectors as a Blanked Sector.
To define a title for sectors:

1. Place the pointer in the input box to the right of the sector number.
2. Type a title for the sector, up to 20 characters long.
3. To blank the sector, click the check box to the right of the sector title.

29.18 Misc page

Address
Allows the appropriate device to be operated via the numerical address in the control system.
Type a number between 0000 and 9999, inclusive, to identify the camera.

29.19 Logs page

This page allows you to display and to save log files.

Download
Click to obtain the log file information. The log files are displayed in the overview.

Save
Click to save the log files.

29.20 Audio page

This function allows you to set the gain of the audio signals to suit your specific requirements. The current video image is shown in the small window next to the slide controls to help you check the selected audio source and improve assignments. Your changes are effective immediately.
The numbering of the audio inputs follows the labeling on the device and the assignment to the respective video inputs. The assignment cannot be changed for Web browser connections.

Audio
The audio signals are sent in a separate data stream parallel to the video data, and so increase the network load. The audio data are encoded according to G.711 and require an additional bandwidth of approximately 80 kbps for each connection.

- **On**: Transmits audio data.
- **Off**: No transmission of audio data.

Line In 1 - Line In 4

Enter the value of the gain of the audio signal. Make sure that the display of the slider remains green.

Line Out

Enter the value of the gain. Make sure that the display of the slider remains green.

Microphone (MIC)
Enter the value of the gain for the microphone.

Line Out/Speaker (SPK)
Enter the value of the gain of the line and the loudspeaker.

Recording format
Select a format for audio recording.
G.711: default value.
L16: Select L16 if you want better audio quality with higher sampling rates. This requires approximately eight times the G.711 bandwidth.

29.21 Relay page

This function allows you to configure the switching behavior of the relay outputs.
You can configure the switching behavior of the relay outputs. For each relay, you can specify an open switch relay (normally closed contact) or a closed switch relay (normally open contact).
You can also specify whether an output should operate as a bistable or monostable relay. In bistable mode, the triggered state of the relay is maintained. In monostable mode, you can set the time after which the relay returns to the idle state.
You can select different events that automatically activate an output. It is possible, for example, to turn on a floodlight by triggering a motion alarm and then turning the light off again when the alarm has stopped.

Idle state
Select **Open** if you want the relay to operate as an NO contact, or select **Closed** if the relay is to operate as an NC contact.

Operating mode
Select an operating mode for the relay.

For example, if you want an alarm-activated lamp to stay on after the alarm ends, select the **Bistable** entry. If you wish an alarm-activated siren to sound for ten seconds, select the 10 s entry.

Relay follows
If required, select a specific event that will trigger the relay. The following events are possible triggers:
Off: Relay is not triggered by events
Connection: Trigger whenever a connection is made
Video alarm: Trigger by interruption of the video signal at the corresponding input
Motion alarm: Trigger by motion alarm at the corresponding input, as configured on the VCA page.
Local input: Trigger by the corresponding external alarm input
Remote input: Trigger by remote station's corresponding switching contact (only if a connection exists)

Note:
The numbers in the lists of selectable events relate to the corresponding connections on the device, Video alarm 1, for example to the Video In 1 connection.

Trigger output
Click the relay button to trigger the relay manually (for example, for testing purposes or to activate a door opener).
The relay button displays the state of each relay.
Red: Relay is activated.
Blue: Relay is not activated.

29.22 Periphery page

29.22.1 COM1

This function allows you to configure the serial interface parameters according to your requirements.
If the device is working in multicast mode, the first remote location to establish a video connection to the device is also assigned the transparent data connection. However, after about 15 seconds of inactivity the data connection is automatically terminated and another remote location can exchange transparent data with the device.

Serial port function
Select a controllable device from the list. Select Transparent data to transmit transparent data via the serial port. Select Terminal to operate the device from a terminal.
After selecting a device, the remaining parameters in the window are set automatically and should not be changed.

Baud rate (bps)
Select the value for the transmission rate.

Stop bits
Select the number of stop bits per character.

Parity check
Select the type of parity check.

Interface mode
Select the protocol for the serial interface.

29.23 VCA page

The device contains an integrated Video Content Analysis (VCA), which can detect and analyze changes in the signal using image processing algorithms. Such changes are triggered by motion in the camera's field of view.

If there is not enough computing power, priority is given to live images and recordings. This can lead to impairment of the VCA system. Observe the processor load and optimize the settings of the device or the VCA settings, if necessary.

You can configure profiles with different VCA configurations. You can save profiles on your computer's hard drive and load saved profiles from there. This can be useful if you want to test a number of different configurations. Save a functioning configuration and test new settings. You can use the saved configuration to restore the original settings at any time.

- Select a VCA profile and change the settings if necessary.

To rename the VCA profile:

- Click ✎. The **Edit** dialog box is displayed. Type the new name, and then click **OK**.

Alarm status

Displays the current alarm state to check the effects of your settings immediately.

Aggregation time [s]

Set an aggregation time of between 0 and 20 seconds. The aggregation time always starts when an alarm event occurs. It extends the alarm event by the value set. This prevents alarm events that occur in quick succession from triggering several alarms and successive events in a rapid sequence. No further alarm is triggered during the aggregation time.

The post-alarm time set for alarm recordings only starts once the aggregation time has expired.

Analysis type

Select the required analysis algorithm. Motion+ offers a motion detector and essential recognition of tampering.

Metadata is always created for a video content analysis, unless this is explicitly excluded. Depending on the analysis type selected and the relevant configuration, additional information overlays the video image in the preview window next to the parameter settings. With the Motion+ analysis type, for example, the sensor fields in which motion is recorded are marked with rectangles.

Note:

For suitable devices, additional analysis algorithms with comprehensive functions, such as IVMD and IVA, are also available. Refer to the IVA documentation for more information on using these.

Motion detector

See *Motion detector (MOTION+ only), page 305*.

Motion detection is available for the Motion+ analysis type. For the detector to function, the following conditions must be met:

- Analysis must be activated.
- At least one sensor field must be activated.
- The individual parameters must be configured to suit the operating environment and the desired responses.
- The sensitivity must be set to a value greater than zero.

Note:
Reflections of light (from glass surfaces, etc.), lights switching on and off, or changes in the light level caused by cloud movement on a sunny day can trigger unintended responses from the motion detector and generate false alarms. Run a series of tests at different times of the day and night to ensure that the video sensor is operating as intended. For indoor surveillance, ensure constant lighting of the areas during the day and at night.

Tamper detection
See *Tamper detection, page 306*

Load...
Click to load a saved profile. The **Open** dialog box is displayed. Select the filename of the profile you want to load, and then click **OK**.

Save...
Click to save the profile settings to another file. The **Save** dialog box is displayed. Type the filename, select the folder where to save the file, and then click **OK**.

Default
Click to return all settings to their default values.

29.23.1 Motion detector (MOTION+ only)

Motion detector
For the detector to function, the following conditions must be met:

- Analysis must be activated.
- At least one sensor field must be activated.
- The individual parameters must be configured to suit the operating environment and the desired responses.
- The sensitivity must be set to a value greater than zero.

Caution!
Reflections of light (off glass surfaces, etc.), switching lights on or off or changes in the light level caused by cloud movement on a sunny day can trigger unintended responses from the motion detector and generate false alarms. Run a series of tests at different times of the day and night to ensure that the video sensor is operating as intended.
For indoor surveillance, ensure constant lighting of the areas during the day and at night.

Debounce time 1 s
The debounce time prevents very brief alarm events from triggering individual alarms. If the **Debounce time 1 s** option is activated, an alarm event must last at least 1 second to trigger an alarm.

Selecting the area
Select the areas of the image to be monitored by the motion detector. The video image is subdivided into square sensor fields. Activate or deactivate each of these fields individually. To exclude particular regions of the camera's field of view from monitoring due to continuous movement (by a tree in the wind, for example), the relevant fields can be deactivated.

1. Click **Mask...** to configure the sensor fields. A new window opens.
2. If necessary, click **Clear All** first to clear the current selection (fields marked red).
3. Left-click the fields to be activated. Activated fields are marked red.
4. If necessary, click **Select All** to select the entire video- frame for monitoring.
5. Right-click any fields to deactivate.
6. Click **OK** to save the configuration.

7. Click the close button (**X**) in the window title bar to close the window without saving the changes.

Sensitivity

Sensitivity is available for the Motion+ analysis type. The basic sensitivity of the motion detector can be adjusted for the environmental conditions to which the camera is subject. The sensor reacts to variations in the brightness of the video image. The darker the observation area, the higher the value that must be selected.

Minimum object size

Specify the number of sensor fields that a moving object must cover to generate an alarm. This setting prevents objects that are too small from triggering an alarm. A minimum value of 4 is recommended. This value corresponds to four sensor fields.

29.23.2 Select Area dialog box

This dialog box displays the camera image. Within this window you can activate the areas of the image to be monitored.

To activate an area:

In the camera image, drag over the area you want to activate. Activated areas are marked yellow.

To deactivate an area:

In the camera image, press the SHIFT key and click the area you want to deactivate.

To obtain commands in the window:

To see the commands for activating or deactivating the areas, right-click anywhere in the window. The following commands are available:

- **Undo**
  Undoes the last command.
- **Set All**
  Activates the entire camera image.
- **Clear All**
  Deactivates the entire camera image.
- **Tool**
  Defines the shape of the mouse pointer.
- **Settings**
  Displays the Editor Settings dialog box. In this dialog box you can change the sensitivity and the minimum object size.

29.23.3 Tamper detection

You can detect tampering of cameras and video cables by means of various options. Run a series of tests at different times of the day and night to ensure that the video sensor is operating as intended.

The options for tamper detection can only be set for fixed cameras. Dome cameras or other motorized cameras cannot be protected in this manner as the movement of the camera itself causes changes in the video image that are too great.

Scene too bright

Activate this function if tampering associated with exposure to extreme light (for instance, shining a flashlight directly on the objective) should trigger an alarm. The average brightness of the scene provides a basis for recognition.

Global change (slider)

Set how large the global change in the video image must be for an alarm to be triggered. This setting is independent of the sensor fields selected under **Mask...**. Set a high value if fewer sensor fields need to change to trigger an alarm. With a low value, it is necessary for changes to occur simultaneously in a large number of sensor fields to trigger an alarm. This option allows detection, independently of motion alarms, manipulation of the orientation or location of a camera resulting from turning the camera mount bracket, for example.

Scene too dark

Activate this function if tampering associated with covering the objective (for instance, by spraying paint on it) should trigger an alarm. The average brightness of the scene provides a basis for recognition.

Scene too noisy

Activate this function if tampering associated with EMC interference (noisy scene as the result of a strong interference signal in the vicinity of the video lines) should trigger an alarm.

Reference check

Save a reference image that can be continuously compared with the current video image. If the current video image in the marked areas differs from the reference image, an alarm is triggered. This detects tampering that would otherwise not be detected, for example, if the camera is turned.

1. Click **Reference** to save the currently visible video- image as a reference.
2. Click **Mask...** and select the areas in the reference image that are to be monitored.
3. Check the box **Reference check** to activate the on-going check. The stored reference image is displayed in black and white below the current video image, and the selected areas are marked in yellow.
4. Select the **Disappearing edges** or **Appearing edges** option to specify the reference check once again.

Trigger delay [s]

Set delayed alarm triggering here. The alarm is only triggered after a set time interval in seconds has elapsed and then only if the triggering condition still exists. If the original condition has been restored before this time interval elapses, the alarm is not triggered. This avoids false alarms triggered by short-term changes, for example, cleaning activities in the direct field of vision of the camera.

Sensitivity

The basic sensitivity of the tamper detection can be adjusted for the environmental conditions to which the camera is subject. The algorithm reacts to the differences between the reference image and the current video image. The darker the observation area, the higher the value that must be selected.

Appearing edges

Select this option if the selected area of the reference image includes a largely homogenous surface. If structures appear in this area, then an alarm is triggered.

Disappearing edges

The area selected in the reference image should contain a prominent structure. If this structure is concealed or moved, the reference check triggers an alarm. If the selected area is too homogenous, so that concealing and moving the structure would not trigger an alarm, then an alarm is triggered immediately to indicate the inadequate reference image.

See also

– *Select Area dialog box, page 306*

29.24 Network Access page

The settings on this page are used to integrate the device into an existing network.

Note:
After changing the Subnet mask and/or the Gateway address, restart the computer.

DHCP
If the network has a DHCP server for the dynamic assignment of IP addresses, select **On** to automatically accept the DHCP-assigned IP address.
For certain applications, the DHCP server must support the fixed assignment between IP address and MAC address, and must be appropriately set up so that, once an IP address is assigned, it is retained each time the system is rebooted.

Subnet mask
Enter the appropriate subnet mask for the set IP address.

Gateway address
For the device to establish a connection to a remote location in a different subnet, enter the IP address of the gateway here. Otherwise, this field can remain empty (0.0.0.0).

IP address
Enter the desired IP address for the camera. The IP address must be valid for the network.

Prefix length
Enter the appropriate prefix length for the set IP address.
The device is easier to access if it is listed on a DNS server. For example, to establish an Internet connection to the camera, it is sufficient to enter the name given to the device on the DNS server as a URL in the browser. Enter the DNS server's IP address. Servers are supported for secure and dynamic DNS.

Video transmission
Select TCP as protocol for units used behind firewalls. Select UDP for units used in a local network.
Note:

- UDP supports multicast. TCP does not. The Maximum Transmission Unit (MTU) value in UDP mode is 1514 bytes.
- Bosch VMS NVR only supports UDP.

HTTP browser port
Select the HTTP browser port from the list. The default port is 80. To limit connection to HTTPS, deactivate the HTTP port. To do this, select **Off**.

HTTPS browser port
To limit browser access to encrypted connections, choose an HTTPS port from the list. The standard HTTPS port is 443. Select the **Off** option to deactivate HTTPS ports and limit connections to unencrypted ports.
The camera uses the TLS 1.0 protocol. Ensure that the browser has been configured to support this protocol. Also ensure that Java application support is activated (in the Java Plug-in Control Panel of the Windows Control Panel).
To limit connections to SSL encryption, set the **Off** option in the HTTP browser port, the RCP+ port, and Telnet support. This deactivates all unencrypted connections allowing connections on the HTTPS port only.
Configure and activate encryption for media data (video, audio, metadata) on the **Encryption** page.

RCP+ port 1756

Select **On** to allow unencrypted connections on this port. Select **Off** to allow only encrypted connections (not supported).

Telnet support

Select **On** to allow unencrypted connections on this port. Select **Off** to allow only encrypted connections (not supported).

Interface mode ETH 1 / Interface mode ETH 2

If necessary select the value for the interface, for example 100 Mbps HD. This value is device dependent and must be set individually.

Network MSS [Byte]

Enter the maximum segment size (MSS) for the IP packet's user data.
This setting allows you to adjust the size of the data packets to the network environment and to optimize data transmission. Observe the MTU value of 1514 bytes in UDP mode.

iSCSI MSS [Byte]

Enter the Maximum Segment Size (MSS) for a connection to the iSCSI system.
The maximum segment size for a connection to the iSCSI system can be higher than for the other data traffic via the network. The size depends on the network structure. A higher value is only useful if the iSCSI system is located in the same subnet as the device.

MAC address

Displays the MAC address.

29.24.1 JPEG posting

This function allows you to save individual JPEG images on an FTP server at specific intervals. Then, retrieve these images at a later date to reconstruct alarm events, if required.

Image size

Select the resolution for the JPEG images.

File name

Select how file names are created for the individual images that are transmitted.

- **Overwrite**
  The same file name is always used. An existing file is overwritten by the current file.
- **Increment**
  A number from 000 to 255 is added to the file name and automatically incremented by 1. When the number reaches 255, the number starts again from 000.
- **Date/time suffix**
  The date and time are automatically added to the file name. Ensure that the date and time of the device are always set correctly. For example, the file snap011008_114530.jpg was stored on October 1, 2008 at 11.45 and 30 seconds.

Posting interval (s; 0 = Off)

Enter the interval in seconds at which the images is sent to an FTP server. Enter zero for no images to be sent.

29.24.2 FTP server

FTP server IP address

Type the IP address of the FTP server on which to save the JPEG images.

FTP server login

Type your login name for the FTP server.

FTP server password

Type the password for the FTP server.

Path on FTP server

Type the exact path where to save the images on the FTP server.

Post JPEG from camera

Select the check box to activate the camera input for the JPEG image. The numbering follows the labeling of the video inputs on the device.

Max. bit rate

You can limit the bit rate for FTP posting.

29.25 DynDNS

29.25.1 Enable DynDNS

A dynamic Domain Name Service (DNS) allows you to select the unit via the Internet using a host name, without having to know the current IP address of the unit. You can enable this service here. To do this, you must have an account with one of the dynamic DNS providers and you must register the required host name for the unit on that site.

Note:

For information about the service, registration process and available host names refer to the provider.

29.25.2 Provider

Select your dynamic DNS Provider from the drop-down list.

29.25.3 Host name

Enter the host name registered for the unit.

29.25.4 User name

Enter the user name you registered.

29.25.5 Password

Enter the password you registered.

29.25.6 Force registration now

Force the registration by transferring the IP address to the DynDNS server. Entries that change frequently are not provided in the Domain Name System. It is a good idea to force the registration when setting up the device for the first time. Only use this function when necessary and no more than once a day, to avoid the possibility of being blocked by the service provider. To transfer the IP address of the device, click the **Register** button.

29.25.7 Status

The status of the DynDNS function is displayed here for information purposes; these settings cannot be changed.

29.26 Network Management

29.26.1 SNMP

The camera supports the SNMP V1 (Simple Network Management Protocol) for managing and monitoring network components, and can send SNMP messages (traps) to IP addresses. It supports SNMP MIB II in the unified code.

If **On** is selected for the SNMP parameter and a SNMP host address is not entered, the device does not send the traps automatically and will only reply to SNMP requests. If one or two SNMP host addresses are entered, SNMP traps are sent automatically. Select **Off** to deactivate the SNMP function.

SNMP host addresses
To send SNMP traps automatically, enter the IP address of one or two target devices here.

SNMP traps
To choose which traps are sent:

1. Click **Select**. A dialog box appears.
2. Click the check boxes of the appropriate traps.
3. Click **Set** to close the window and send all of the checked traps.

29.26.2 UPnP

Select **On** to activate UPnP communication. Select **Off** to deactivate it.
When the Universal Plug-and-Play (UPnP) function is activated, the unit responds to requests from the network and is automatically registered on the requesting computers as a new network device. This function should not be used in large installations due to the large number of registration notifications.

Note:
To use the UPnP function on a Windows computer, both the Universal Plug-and-Play Device Host and the SSDP Discovery Service must be activated.

29.26.3 Quality of Service

The priority of the different data channels can be set by defining the DiffServ Code Point (DSCP). Enter a number between 0 and 252 as a multiple of four. For alarm video you can set a higher priority than for regular video and you can define a Post Alarm Time over which this priority is maintained.

29.27 Advanced page

29.27.1 SNMP

The device supports the SNMP V2 (Simple Network Management Protocol) for managing and monitoring network components, and can send SNMP messages (traps) to IP addresses. The device supports SNMP MIB II in the unified code.

SNMP
Select **On** to activate the SNMP function.

1. SNMP host address / 2. SNMP host address
Type the IP addresses of one or two target units. The device (for example encoder, camera) sends SNMP traps automatically to the target units.
If you do not enter IP addresses, the device only replies to SNMP requests and does not send SNMP traps to the target units.

SNMP traps
Allows you to select which traps the device sends to the target units. To do this, click **Select**. The **SNMP traps** dialog box is displayed.

SNMP traps dialog box
Select the check boxes of the appropriate traps, and then click **OK**.

29.27.2 802.1x

IEEE 802.1x allows you to communicate with the device if a RADIUS server is used in a network.

Authentication
Select **On** to activate 802.1x.

Identity
Type the user name that the RADIUS server uses for identifying the device.

Password
Type the password that the RADIUS server uses for identifying the device.

29.27.3 RTSP

RTSP port
If necessary, select a different port for the exchange of the RTSP data. The default port is 554. **Off** disables the RTSP function.

29.27.4 UPnP

You can activate the universal plug and play function (UPnP). When activated the camera reacts on requests from the network and will be registered automatically as a new network device on the inquiring computers. The access to the camera is then possible using the Windows file explorer, and without knowledge of the camera's IP address.

Note:
In order to use the UPnP function on a computer with Windows XP or Windows Vista, the Universal Plug and Play Device Host and the SSDP Discovery services must be activated.

29.27.5 TCP metadata input

This feature allows a device to receive data from an external TCP sender, for example an ATM or POS device, and store it as metadata.

TCP port
Select the port for TCP communication. Select **Off** to deactivate the TCP metadata function.

Sender IP address
Type the IP address of the TCP metadata sender here.

29.28 Multicast page

In addition to a 1:1 connection between an encoder and a single receiver (unicast), the device enables multiple receivers to receive the video signal from an encoder simultaneously.
The device either duplicates the data stream itself and then distributes it to multiple receivers (Multi-unicast) or it sends a single data stream to the network, where the data stream is simultaneously distributed to multiple receivers in a defined group (Multicast). You can enter a dedicated multicast address and port for each stream.
The prerequisite for multicast operation is a multicast-capable network that uses the UDP and IGMP protocols. Other group management protocols are not supported. The TCP protocol does not support multicast connections.
A special IP address (class D address) must be configured for multicast operation in a multicast-enabled network. The network must support group IP addresses and the Internet Group Management Protocol (IGMP V2). The address range is from 225.0.0.0 to 239.255.255.255. The multicast address can be the same for multiple streams. However, it is then necessary to use a different port in each case so that multiple data streams are not sent simultaneously using the same port and the same multicast address.

Note: The settings must be done for each encoder (video input) and for each stream individually. The numbering follows the labeling of the video inputs on the device.

Enable
To enable simultaneous data reception on several receivers you need to activate the multicast function. To do this, select the check box. Then enter the multicast address.

Multicast Address
Enter a valid multicast address for each stream from the relevant encoder (video input) to be operated in multicast mode (duplication of the data streams in the network).
With the setting 0.0.0.0 the encoder for the relevant stream operates in multi-unicast mode (copying of data streams in the device). The device supports multi-unicast connections for up to five simultaneously connected receivers.
Note: Duplication of data places a heavy demand on the device and can lead to impairment of the image quality under certain circumstances.

Port
Assign a different port to each data stream if there are simultaneous data streams at the same multicast address.
Enter the port address of the required stream here.

Streaming
Select the check box to activate multicast streaming mode for the relevant stream. The device even streams multicast data if no connection is active.
For normal multicast operation, streaming is typically not required.

Packet TTL (only for Dinion IP, Gen4 and FlexiDome)
Enter a value to specify how long the multicast data packets are active on the network. If multicast is to be run via a router, the value must be greater than 1.

29.29 Accounts

Four separate accounts can be defined for posting and recording export.

Type
Select either FTP or Dropbox for the account type.
Before using a Dropbox account ensure that the time settings of the device have been correctly synchronized.

Account name
Enter an account name to be shown as the target name.

FTP server IP address
For an FTP server, enter the IP address.

FTP server login
Enter your login name for the account server.

FTP server password
Enter the password that gives access to the account server. Click Check to confirm that it is correct.

Path on FTP server
Enter an exact path to post the images on the account server. Click Browse... to browse to the required path.

Maximum bit rate
Enter the maximum bit rate in kbps that will be allowed when communicating with the account.

29.30 IP v4 Filter

To restrict the range of IP addresses within which you can actively connect to the device, fill-in an IP address and mask. Two ranges can be defined.

- Click **Set** and confirm to restrict access.

If either of these ranges are set, no IP V6 addresses are allowed to actively connect to the device.

The device itself may initiate a connection (for example, to send an alarm) outside the defined ranges if it is configured to do so.

29.31 Licenses page

You can enter the activation key to release additional functions or software modules.

Notice!
The activation key cannot be deactivated again and is not transferable to other units.

29.32 Decoder page

29.32.1 Decoder profile

Allows you to set the various options for the display of video images on an analog monitor or VGA monitor.

Monitor name
Type the name of the monitor. The monitor name facilitates the identification of the remote monitor location. Use a name that makes it as easy as possible to identify the location.

Click 💾 to update the name in the Device Tree.

Standard
Select the video output signal of the monitor you are using. Eight pre-configured settings for the VGA monitors are available in addition to the PAL and NTSC options for analog video monitors.

Caution!
Selecting a VGA setting with values outside the technical specification of the monitor can result in severe damage to the monitor. Refer to the technical documentation of the monitor you are using.

Window layout
Select the default image layout for the monitor.

VGA screen size
Type the aspect ratio of the screen (for example 4 x 3) or the physical size of the screen in millimeters. The device uses this information to accurately scale the video image for distortion-free display.

29.32.2 Monitor display

The device recognizes transmission interruptions and displays a warning on the monitor.

Display transmission disturbance

Select **On** to display a warning in case of transmission interruption.

Disturbance sensitivity

Move the slider to adjust the level of the interruption that triggers the warning.

Disturbance notification text

Type the text of the warning the monitor displays when connection is lost. The maximum text length is 31 characters.

Delete decoder logo

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

30 ONVIF page

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

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

See also

– *Video Streaming Gateway device page , page 274*
– *Live Only page, page 279*

30.1 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 Bosch VMS.

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 317*
– *Adding a live only encoder, page 164*

- *Configuring ONVIF events, page 147*

30.2 ONVIF Encoder Events page

Main window > **Devices** > Expand > Expand > Expand > Expand > > **ONVIF Encoder Events** tab

or

Main window > **Devices** > Expand > > **ONVIF Encoder Events** tab

You can map ONVIF events to Bosch VMS events. This ensures that you later can configure ONVIF events as Bosch VMS alarms.

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 Bosch VMS event for mapping with an ONVIF event.

The following ⚠ events are available:

- **Onvif Generic Data 01**
- **Onvif Generic Data 02**
- **Onvif Generic Data 03**

The following 🚦 events are available:

- **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 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**

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.

See also

- *ONVIF events, page 60*
- *Configuring ONVIF events, page 147*

30.2.1 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.

30.2.2 Import Mapping Table dialog box

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**.

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 Bosch VMS.

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 Bosch VMS versions.

See also

- *Importing an ONVIF Mapping Table file, page 148*

30.3 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.

30.3.1 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 Bosch VMS 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 Bosch VMS, the ONVIF version 2.0 is required.

30.3.2 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.

30.3.3 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.

30.3.4 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.

- H.264 MP: This setting represents the H.264 Main Profile and offers the maximum configuration options for the H.264 code algorithm. This setting also enables the best image quality and the lowest band width.
- H.264 BP+: This profile setting represents the H.264 Baseline Profile plus, a function from the Main Profile toolset that supports interlace video.

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. 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.

30.3.5 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]**
  Note: Not supported by Bosch VMS. Please select another codec.

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.

30.3.6 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.

30.3.7 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.

30.3.8 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.

30.3.9 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].

30.3.10 Wide Dynamic Range

Main window > **Devices** > 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.

30.3.11 White balance

Main window > **Devices** > 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).

30.3.12 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.
Bosch VMS 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 Bosch VMS.

HTTPS ports

Note: Not supported by Bosch VMS.
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.

30.3.13 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 Bosch VMS.
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.

Category	Defined values	Description
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 influence how the device appears in the device tree and the ONVIF Encoder Identification and Main Settings.

30.3.14 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 Bosch VMS 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.

30.4 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 events, page 60*
- *Configuring ONVIF events, page 147*

31 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 Bosch VMS. Your structure is displayed in the Logical Tree.

Allows you to perform the following tasks:

- Configuring the Full Logical Tree
- Managing resource files, assigning them to nodes
- Creating hot spots on a map
- Creating a malfunction relay

Resource files can be:

- Site map files
- Document files
- Web files
- Audio files
- Command Scripts
- Camera sequence files

Hot spots can be:

- Cameras
- Inputs
- Relays
- Command Scripts
- Sequences
- Links to other maps

Displays a dialog box for managing resource files.

Displays a dialog box for adding a Command Script to the Logical Tree.

Displays a dialog box for adding a camera sequence file.

Displays a dialog box for adding a node.

Displays a dialog box for adding map resource files.

Displays a dialog box for adding an HTML file.

Displays a dialog box for adding a malfunction relay.

✓: Device was added to the Logical Tree.

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

To cancel filtering, click ✖ .

31.1 Resource Manager dialog box

Main window > **Maps and Structure** > ⇄
or
Main window > **Maps and Structure** > > **Manage...**
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)
- MHT files (Web archives)
- WAV (audio file)

✚ Click to display a dialog box for importing a resource file.

URL Click to display the **Add URL** 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 171*

31.2 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 174*
- *Assigning a map to a folder, page 175*
- *Adding a document, page 176*

31.3 Sequence Builder dialog box

Main window > **Maps and Structure** >

Allows you to manage camera sequences.

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

Click to rename a camera sequence.

Click to remove the selected camera sequence.

Notice!

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

Add Step

Click to display the **Add Sequence Step** dialog box.

Remove Step

Click to remove selected steps.

Step

Displays the number of the step. All cameras of a particular step have the same dwell time.

Dwell

Allows you to change the dwell time (seconds).

Camera Number

Click a cell to select a camera via its logical number.

Camera

Click a cell to select a camera via its name.

Camera Function

Click a cell to change the function of the camera in this row.

Data

Type the time for the duration of the selected camera function. To configure this, you must have selected an entry in the **Camera** column and an entry in the **Camera Function** column.

Data Unit

Select the unit for the selected time, for example seconds. To configure this, you must have selected an entry in the **Camera** column and an entry in the **Camera Function** column.

Add to Logical Tree

Click to add the selected camera sequence to the Logical Tree and to close the dialog box.

See also

- *Monitor Wall page, page 246*
- *Managing pre-configured camera sequences, page 172*

31.4 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 172*

31.5 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 172*

31.6 Add URL dialog box

Main window > **Maps and Structure** > >

Allows you to add an Internet address (URL) to your system. You can add this Internet address to the Logical Tree as a document. The user can display an Internet page in his Operator Client.

Name:

Type a display name for the URL.

URL:
Type the URL.

See also

- *Adding a document, page 176*

31.7 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 175*

31.8 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 177*
- *Malfunction relay, page 55*

32 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 178*

32.1 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 178*
– *Adding holidays and exception days, page 180*
– *Removing holidays and exception days, page 181*
– *Renaming a schedule, page 181*

32.2 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 179*
- *Configuring a standard Task Schedule, page 179*
- *Configuring a recurring Task Schedule, page 179*
- *Removing a Task Schedule, page 180*
- *Adding holidays and exception days, page 180*
- *Removing holidays and exception days, page 181*
- *Renaming a schedule, page 181*

33 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.

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 Bosch VMS.

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 ✖.

33.1 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 Bosch VMS.
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 - Platform
Displays the platform name of this encoder.

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.

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 item is selected for stream 2 and stream 2 is assigned to Live Video.
Note: If stream 1 is used for Live for a specific workstation then the Operator Client running on this workstation cannot enable ROI for this camera.

is automatically enabled in the table.

Recording - Setting
Click a cell to select the required recording setting. You configure the available recording settings in the **Scheduled Recording Settings** dialog box.

Recording - Profile (only available for ONVIF cameras)
Click a cell to browse for the available recording profile tokens of this ONVIF camera. Select the desired entry.

Recording - ANR

Select a check box to enable the ANR function. You can only enable this function, if the encoder has an appropriate firmware version and an appropriate device type.

Recording - Max Pre-Alarm Duration

Displays the calculated maximum pre-alarm duration for this camera. This value can help you in calculating the required storage capacity of the local storage medium.

Notice!

If a Mirrored VRM is already configured for an encoder, you cannot change any settings for this encoder in the **Secondary Recording** columns.

Secondary Recording - Setting (only available if a Secondary VRM is configured)

Click a cell to assign a scheduled recording setting to the dual recording of this encoder. Depending on your configuration it can happen that the configured stream quality for secondary recording is not valid. The stream quality configured for primary recording is then used instead.

Secondary Recording - Profile (only available for ONVIF cameras)

Click a cell to browse for available recording profile tokens of this ONVIF camera.

(Only visible when you click **All**)

Select a check box to activate PTZ control.

Note:

For port settings refer to *COM1, page 303*.

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 189*
- *Configuring PTZ camera settings, page 188*
- *Configuring PTZ port settings, page 187*
- *Configuring stream quality settings, page 184*

- *Copying and pasting in tables, page 183*
- *Configuring the ANR function, page 189*
- *Exporting the Camera Table, page 184*
- *Assigning an ONVIF profile, page 146*
- *Configuring the ROI function, page 188*

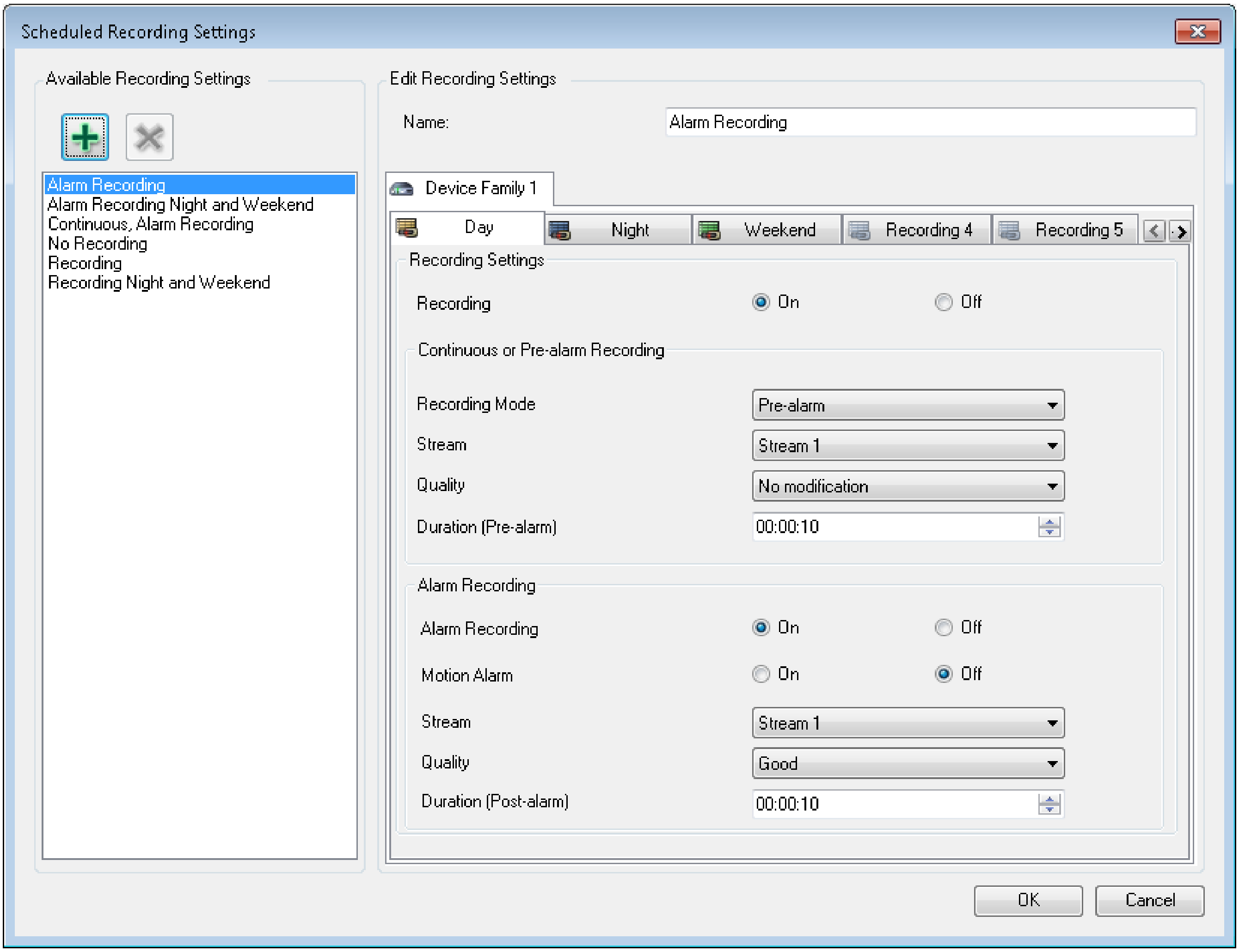
33.2 Scheduled Recording Settings dialog box (only VRM and Local Storage)

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.



Scheduled Recording Settings

Available Recording Settings

- Alarm Recording
- Alarm Recording Night and Weekend
- Continuous, Alarm Recording
- No Recording
- Recording
- Recording Night and Weekend

Edit Recording Settings

Name: Alarm Recording

Device Family 1

Day | Night | Weekend | Recording 4 | Recording 5

Recording Settings

Recording ● On ○ Off

Continuous or Pre-alarm Recording

Recording Mode: Pre-alarm

Stream: Stream 1

Quality: No modification

Duration (Pre-alarm): 00:00:10

Alarm Recording

Alarm Recording ● On ○ Off

Motion Alarm ○ On ● Off

Stream: Stream 1

Quality: Good

Duration (Post-alarm): 00:00:10

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 183*
- *Configuring recording settings (only VRM and Local Storage), page 185*

33.3 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 183*
- *Configuring recording settings (NVR only), page 186*

33.4 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.

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.

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 184*

33.5 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.

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.

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 187*
- *Configuring PTZ camera settings, page 188*

34 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 191*
- *Configuring Command Scripts, page 200*
- *Options dialog box, page 224*

- *Configuring blinking hot spots, page 199*

34.1 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.

34.2 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 in the **Options** dialog box.

For each 🚦 event, you can configure the background color and the behavior (blinking or not blinking) for hot spots. For example you can configure for a 🚦 event 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 hot spots. This is required when different events occur for the same device. (1 = highest priority)
The configured color is valid for all hot spots with the same display priority. You can change color, behavior and priority at any 🚦 event: The changed color and behavior is used for all hot spots of all other 🚦 events which have the same priority.

Enable color states on maps
Click to enable that the hot spots 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 hot spots of the devices belonging to this event.

Background color on map:
Click the color field to select the background color used for the hot spots 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 hot spots of the devices belonging to this event.

34.3 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**

34.4 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.

C# VB 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 Bosch VMS Script API.

Click to display the Online Help for Bosch VMS.

Click to close the **Command Script Editor** dialog box.

See also

- *Configuring Command Scripts, page 200*

34.5 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 194*
- *Editing a Compound Event, page 195*

34.6 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 200*

34.7 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.

34.8 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.

34.9 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 197*

35 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.

Alarm Identity

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 Bosch VMS, 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 Image Panes

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 50*

35.1 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.

Manual alarm recording time:
Only valid for NVR recordings.
Enter the number of minutes for the duration of alarm recording that a user can start manually in the Operator Client.
The user can stop the manual recording before this time is elapsed.

Analog 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 196*

35.2 Select Image Pane Content dialog box

Main window > 🚨 **Alarms** > 🚦 or ⚠ > **Alarm Image Panes** 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 instant playback is configured in the **Alarm Settings** dialog box, see *Alarm Settings dialog box, page 356*.

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.

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
- *Configuring an alarm, page 196*

35.3 Select Resource dialog box

Main window > 🚨 **Alarms** > 🚦 or ⚠ > **Alarm Image Panes** 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 196*
- *Managing resource files, page 192*

35.4 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 analog 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.

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.

Analog 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 analog monitor groups.

Alarm title
Select the check box to configure that the title of the alarm is displayed on the analog monitors as an on-screen display.

Alarm time
Select the check box to configure that the time of the alarm is displayed on the analog monitors as an on-screen display.

Alarm date
Select the check box to configure that the date of the alarm is displayed on the analog 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 analog 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 analog 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 analog 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 197*
– *Configuring an alarm, page 196*
– *Configuring the pre- and post-alarm duration for an alarm, page 197*

36 User Groups page

Main window > **User Groups**

The following user group is available by default:

- Admin Group (user name: Admin)

Allows you to configure user groups, Enterprise User Groups and Enterprise Access.

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.

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.

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 ✕.

36.1 New User Group/Enterprise Account dialog box

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

or

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

or

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

Allows you to create a standard user group, an Enterprise User Group or an Enterprise Account.

The Enterprise User Groups 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**.

Name:
Type in a name for the group or account.

Description:
Type in a description for the group or account.

For Enterprise Accounts:

Password:
Type in a password.

Confirm Password:
Enter the new password again.

See also

- *Creating a group or account, page 204*

36.2 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 Bosch VMS user group is removed.

See also
- *Configuring LDAP settings, page 205*
- *Associating an LDAP group, page 206*
- *Scheduling user logon permission, page 206*

36.3 User Properties page

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

Main window > **User Groups** > **Enterprise User Group** tab > >
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.
Allows you to configure a new user in a standard user group or in an Enterprise User Group.

Full name:
Type the full name of the user.

Description:
Type an informative description for the user.

Strong password policy
Select the check box to enable the system to check for a secure password.
The following rules apply:
- Minimum 8 characters
- At least one upper-case letter (A through Z)
- At least one number (0 through 9)
- At least one special character (for example: ! $ # %)
- Previous password must not be used.

Enter new password:
Type the password for the new user.

Confirm password:
Type the new password again.

Apply

Click to apply the settings.

36.4 Add New Dual Authorization Group dialog box

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

or

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

Allows to create a dual authorization for a standard user group or for an Enterprise User Group.

For Enterprise Access, a dual authorization is not available.

Name:

Type in a name for the group.

Description:

Type in description for the group.

See also

– *Creating a dual authorization group, page 205*

36.5 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

– *Creating a dual authorization group, page 205*

36.6 Select User Groups dialog box

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 add 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
– *Creating a dual authorization group, page 205*

36.7 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.

See also
– *Configuring camera permissions, page 209*

36.8 Control Priorities

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 209*

36.9 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 210*

36.10 Decoder 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 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.

See also

- *Configuring decoder permissions, page 209*

36.11 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, i.e. you set the events the user group is authorized or not authorized to use.
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.

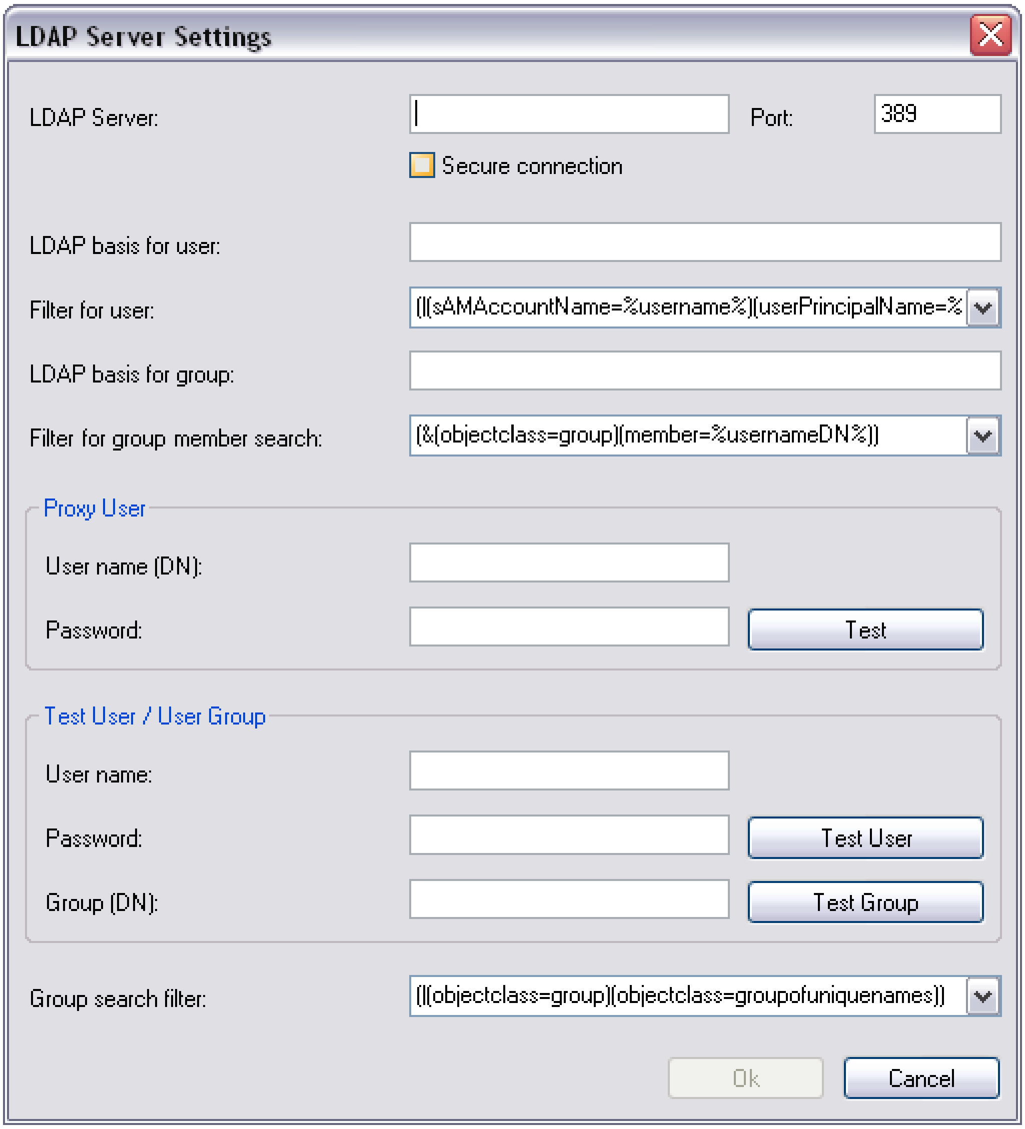
See also

- *Configuring permissions for events and alarms, page 208*

36.12 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 Bosch VMS. 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.



Port: 389

☐ Secure connection

Filter for user: (|(sAMAccountName=%username%)(userPrincipalName=%

Filter for group member search: (&(objectclass=group)(member=%usernameDN%))

Group search filter: (|(objectclass=group)(objectclass=groupofuniquenames))

LDAP Server Settings

LDAP Server:

Type the name of the LDAP server.

Port:

Type the port number of the LDAP server (default unencrypted: 389, encrypted: 636)

Secure connection

Select the check box to activate encrypted data transmission.

LDAP basis for user:

Type the unique name (DN = distinguished name) of the LDAP path in which you can search for a user. Example for a DN of the LDAP basis:CN=Users,DC=Security,DC=MyCompany,DC=com

Filter for user:

Select a filter used to search for a unique user name. Examples are predefined. Replace %username% with the actual user name.

LDAP basis for group:

Type the unique name of the LDAP path in which you can search for groups.
Example for a DN of the LDAP basis: CN=Users,DC=Security,DC=MyCompany,DC=com

Filter for group member search:
Select a filter used to search for a group member.
Examples are predefined. Replace %usernameDN% with the actual user name and his DN.

Proxy User

User name (DN):
Type the unique name of the proxy user. This user is required to allow the users of this Bosch VMS user group to access the LDAP server.

Password:
Type the proxy user password.

Test
Click to test whether the proxy user has access to the LDAP server.

Test User / User Group
The entries in this group box are not saved after clicking **OK**. They only serve for testing.

User name:
Type the name of a test user. Omit the DN.

Password:
Type the test user password.

Test User
Click to test whether the combination of user name and password is correct.

Group (DN):
Type the unique group name with which the user is associated.

Test Group
Click to test the association of the user with the group.

Group search filter:
Do not leave this field empty. If there is no entry, you cannot assign an LDAP group to a Bosch VMS user group.
Select a filter to find a user group.
Examples are predefined.

See also

– *Configuring LDAP settings, page 205*

36.13 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.

Rename the item as desired. This is the name of the Enterprise Account.

Description:
Type in a description for this Enterprise Account.

Enter new password: / Confirm password:
Type in and confirm the password for this Management Server.

See also

- *New User Group/Enterprise Account dialog box, page 362*

36.14 Logical Tree page

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

Main window > **User Groups** > **Enterprise Access** tab > > **Device Permissions** tab > **Camera** tab
Allows you to configure the Logical Tree for each user group.

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.

See also

- *Configuring permissions for Logical Tree, page 208*

36.15 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 video data
Select the check box to allow printing and saving video data.

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 files
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 data
Select the check box to allow protecting video data.

Delete video
Select the check box to allow deleting video data.

Access to video data that has been recorded in periods when the user group has not been allowed to logon
Select the check box to allow accessing the described video data.

Logbook access
Select the check box to allow accessing the Logbook.

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 Bosch VMS 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 Bosch VMS 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 Bosch VMS 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 Bosch VMS 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.

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 the Operator Client.

Instant playback rewind time:
Enter the number of seconds for the duration of 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 55*
- *Configuring operating permissions, page 207*

36.16 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 209*

36.17 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.

Control Monitor

Select the control monitor which displays Live Mode only.

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, select the required entry.

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.

Load Custom Layout

Click to import an XML file with user interface settings.

Unload Custom Layout
Click to display a dialog box for unloading imported interface settings.

See also

– *Configuring user interface settings, page 207*

36.18 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.

Management Server
Displays the name of the Management Server that has been added to the Server List (Main window > **Devices** > **Enterprise System** > **Server List / Address Book**).

Private Network Address
Displays the private IP address or DNS name of the Management Server.

Public Network Address
Displays the public IP address or DNS name of the Management Server.

Server Number
Displays the number of the Management Server. This number is used by an 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 in 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 in 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 204*
– *Creating an Enterprise System, page 112*
– *Configuring the Server List for Enterprise System, page 117*

37 Troubleshooting

This chapter contains information on how to handle known problems using Bosch VMS 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 Bosch VMS 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 379*
Setup stops with a message that OPC Server cannot be installed.	OPC Server files cannot be overwritten.	Uninstall OPC Core Components Redistributable and restart Bosch VMS Setup.
The software cannot be uninstalled by executing Setup.		Start Control Panel > Add/ Remove Programs and uninstall Bosch VMS.

Problems immediately after starting the application

Issue	Cause	Solution
Bosch VMS displays the wrong language.	Windows is not switched to the desired language.	*Configuring the language of Configuration Client, page 98* or *Configuring the language of Operator Client, page 98*
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 379*

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 Bosch VMS 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 379*

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 379*.

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.

37.1 Configuring the desired language in Windows

If you want to change the display language for the setup of Bosch VMS, 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.

37.2 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 Bosch VMS.

37.3 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 (see *Adding a device manually, page 150*).

37.4 Used ports

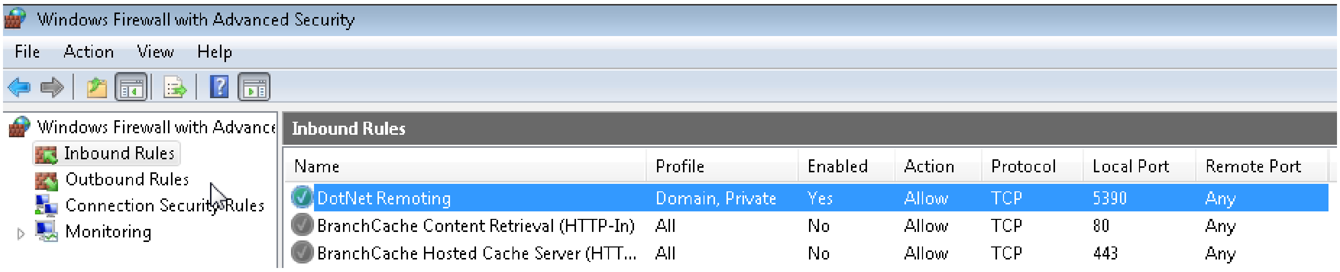
This section lists for all components of Bosch VMS the ports that must be open within a LAN. Do not open these ports to the Internet! For operation via Internet use secure connections like VPN or Remote Access.

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 7 Firewall, configure an Inbound Rule for each open port.

Allow all outgoing connections for all Bosch VMS software applications.

Example for a simple Inbound Rule in Windows 7 Firewall


Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advance
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules

Name	Profile	Enabled	Action	Protocol	Local Port	Remote Port
DotNet Remoting	Domain, Private	Yes	Allow	TCP	5390	Any
BranchCache Content Retrieval (HTTP-In)	All	No	Allow	TCP	80	Any
BranchCache Hosted Cache Server (HTT...	All	No	Allow	TCP	443	Any

Management Server / Enterprise Management Server ports

Server (Listener)	Protocol	Inbound ports	Client (Requester)	Remark
Management Server	TCP	5390	Operator Client, Configuration Client, Bosch VMS SDK Application	.NET Remoting
Management Server	TCP	5392	Operator Client, Configuration Client, Mobile Video Service	WCF, gateway.push.apple.com
Management Server	TCP	5395	Configuration Client, Operator Client	User preferences, File transfer

Video Recording Manager ports

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
VRM	UDP	1800	Management Server, Operator Client	Multicast Network Scan Target
VRM	TCP	80	Operator Client	VRM playback via http
VRM	TCP	443	Operator Client	VRM playback via https
VRM	TCP	5364, 5365	Operator Client	VRM eXport Wizard (project version)

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 Bosch VMS provider	TCP	5383	Operator Client	Media stream
Mobile Video Service mobile provider	TCP	5384	HTML Client, Mobile Apps	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	
Bosch Video Streaming Gateway	TCP	1756	VRM Configuration Client	via RCP+

Server (Listener)	Protocol	Inbound ports	Client (Requester)	Remark
Bosch Video Streaming Gateway	TCP	1757	VRM Configuration Client	Scan Target
Bosch Video Streaming Gateway	TCP	1758	VRM Configuration Client	Scan Response
Bosch Video Streaming Gateway	TCP	1800	VRM Configuration Client	Multicast Network Scan Target
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
ONVIF camera	RTSP	554	Management Server, VSG, Configuration Client, Operator Client	

Bosch VMS Operator Client / Cameo SDK ports

Server (Listener)	Protocol	Inbound ports	Client (Requester)	Remark
Operator Client	TCP	5394	Bosch VMS SDK Application, BIS	.NET Remoting
Operator Client	UDP	1024-65535	Encoder, VRM	

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, Bosch VMS SDK Application	via RCP+
Encoder	UDP	1757	Decoder, Management Server, Operator Client	Scan Target
Encoder	UDP	1758	Decoder, Management Server, Operator Client	Scan Response

Server (Listener)	Protocol	Inbound ports	Client (Requester)	Remark
Encoder	UDP	1800	Decoder, Management Server, Operator Client	Multicast Network Scan Target
Encoder	TCP	80	Operator Client, Bosch VMS SDK Application, VSG	Access via http
Encoder	TCP	443	Operator Client, Bosch VMS SDK Application, VSG	Access via https

Bosch VMS 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, Bosch VMS 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	

NVR / Redundant NVR / Failover NVR ports

Server (Listener)	Protocol	Inbound ports	Client (Requester)	Remark
NVR	TCP	5391	Operator Client, Management Server, Failover NVR, Configuration Client	.NET Remoting
Redundant NVR	TCP	5391	Operator Client, Management Server, Failover NVR, Configuration Client	.NET Remoting
Failover NVR	TCP	5391	Operator Client, Management Server, NVR, Redundant NVR, Configuration Client	.NET Remoting
NVR	UDP	1024-65535	Encoder	
Redundant NVR	UDP	1024-65535	Encoder	
Failover NVR	UDP	1024-65535	Encoder	

DiBos/BRS 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:				
DiBos / BRS	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
DiBos / BRS	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		80	, ,	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, Bosch VMS 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

VIDOS

Server (Listener)	Protocol	Inbound ports	Client (Requester)	Remark
VIDOS	TCP	1756	Encoder, Configuration Client	via RCP+
VIDOS	TCP	1757	Encoder	Scan Target
VIDOS	TCP	1758	Encoder	Scan Response
VIDOS	TCP	1800	Encoder	Multicast Network Scan Target

37.5 Enabling logging for ONVIF events

You can enable logging for ONVIF events for example when you encounter problems with receiving Bosch VMS 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 ONVIF events, page 147*
- *ONVIF events, page 60*

Glossary

802.1x

The IEEE 802.1x standard provides a general method for authentication and authorization in IEEE-802 networks. Authentication is carried out via the authenticator, which checks the transmitted authentication information using an authentication server (see RADIUS server) and approves or denies access to the offered services (LAN, VLAN or WLAN) accordingly.

Activation Key

Number that the user must enter 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.

Alarm viewer

External application that is used for displaying video analytics alarms in Operator Client.

Allegiant

Bosch family of analog matrix switching systems.

analog monitor group

A set of analog monitors connected to decoders. The analog monitor group can be used for alarm processing in a given physical area. For example, an installation with three physically separated control rooms might have three monitor groups. The monitors in an analog monitor group are logically configured into rows and columns and can be set to full-screen or quad view.

analytics viewer

External application that is used for displaying video analytics alarms in Operator Client.

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 find in the Authorization Letter. You must enter the Authorization Number in the Bosch Security System Software License manager to obtain the Activation Key. Additionally you must enter the computer signature.

B-frame

Bidirectional frame. Part of a video compression method.

BIS

Building Integration System

bookmark

Used for storing a time period of live or recorded video. This allows for tagging particular scenes for later investigation. Additionally you can share your investigation results with other users by exporting a bookmark.

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.

CCL emulation

Emulation of the Command Console Language used for controlling an Allegiant matrix. You can use this set of commands to switch a Bosch VMS IP camera / encoder to a Bosch VMS 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, e.g., to display digital video on a analog monitor.

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 Bosch VMS. 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 Bosch VMS 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 Bosch VMS 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.

face detection

Face detection is a software process that detects a face in a video image.

face recognition

Face recognition is a software process that compares a video image of a face with the faces stored in database. In case of a match, a message is issued.

Failover VRM

Software in the Bosch VMS 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.

Hot spot

Mouse sensitive icon on a map. Hot spots are configured in Configuration Client. Hot spots can be for example cameras, relays, inputs. The operator uses it for localizing and selecting a device in a building. If configured, hot spots can display a blinking background color when a specific state event 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 Video Analytics

Algorithm that detects specific properties and the behavior of objects in a scene monitored by a video camera and from this generates alarm events that, in turn, can be processed in a CCTV system. Recording with Intelligent Video Analytics settings activated is a precondition to be able to selectively and quickly search through video material later. Intelligent Video Analytics makes it possible to capture and evaluate directional movement of objects in such a way that false alarms are prevented to a large extent. Intelligent Video Analytics adapts automatically to changing environmental conditions and is therefore largely non-sensitive to perturbing influences such as rain and tree movement. Especially when used for forensic search, Intelligent Video Analytics allows for filtering moving objects by their color specifications. With the aid of Intelligent Video Analytics algorithm extensive video material can be searched selectively for objects with specific color properties.

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

Bosch VMS 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 Bosch VMS 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.

MOV

File extension of the default video format used by QuickTime Player from Apple.

MPEG-4

Motion Picture Expert Group. Standard for encoding (compressing) digital audio and video for multimedia applications.

MSS

Maximum Segment Size. The largest amount of data, specified in bytes, that a computer or communications device can handle in a single, unfragmented piece.

MTU

Maximum Transmission Unit. Describes the maximum amount of data (in bytes) that can be transferred without being fragmented.

Multicast

Communication between a single transceiver and multiple receivers on a network by distribution of a single data stream on the network to a number of receivers in a defined group. Requirement for multicast operation is a multicast compliant network with implementation of the UDP protocol and the IGMP protocol.

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.

number plate detection

Number plate detection is a software process that detects a number plate in a video image. This is for example used to count cars on a highway.

number plate recognition

Number plate recognition is a software process that compares a video image of a number plate with a list of number plates stored in a database. In case of a match, message is issued.

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.

OSD

On-screen Display: Menus are shown on the display monitor.

Panoramic camera

Camera with a 360° or 180° view angle.

P-frame

Predicted frame. Part of a video compression method.

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.

PTZ camera

Camera with pan, tilt, and zoom function.

RADIUS server

Remote Authentication Dial-In User Service: a client/server protocol for the authentication, authorization and accounting of users with dial-up connections on a computer network. RADIUS is the de-facto standard for central authentication of dial-up connections via Modem, ISDN, VPN, Wireless LAN (see 802.1x) and DSL.

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 in the past 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.

Secondary VRM

Software in the Bosch VMS 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).

SNTP

Simple Network Time Protocol is a simplified version of NTP (see NTP). SNTP can be used when the ultimate performance of the full NTP implementation described in RFC 1305 is not needed or justified. SNTP version 4 is described in RFC 2030 (see RFC).

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.

Timeline

Part of the Bosch Video Management System user interface. Displays lines as graphical representations of the recordings of the selected cameras. The Timeline allows you to navigate through recorded videos.

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 connection less protocol used to exchange data over an IP network. UDP is more efficient than TCP for video transmission because of lower overhead.

Unmanaged site

Item of the Device Tree in Bosch VMS 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 IVA (intelligent video analysis)

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 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++ and H.264) 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 Bosch VMS 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 denied
  Allegiant CCL emulation 258
accessing the Help 15
acquire PTZ control 210
activate 211
  Bosch Video Management System 97
  previous configuration 212
activation 98, 214
  configuration 211
  delayed 211, 221
Activation Key 223, 314
add Bosch Allegiant input alarm 216
add Bosch ATM/POS bridge 215
add BVIP decoder 151
add BVIP encoder 53, 151, 241, 242, 267, 269
add encoder 82, 132, 164
add pool
  VRM 125
add text data to continuous recording 354
add unmanaged site 121, 280
add video analytics device 162, 169, 261
add VRM 81, 122
additional data
  text data 56
AE-response speed 295
alarm 288
alarm map 356
alarm message 288
alarm priority 210
alarm recording 197, 198, 356
alarm recording mode 185, 344
alarm recording time (NVR) 356
alarm sequence 197, 356
alarm viewer 168
alarms
  sort order 356
Allegiant
  CCL emulation 150, 161
  control channel 76, 78
  firmware version 69, 70
  Network Host program 77
  PTZ camera 343
  Satellite System 78
  too many cameras 379
Allegiant CCL commands 78
Allegiant CCL emulation 57
  access denied 258
Allegiant CCL Emulation page 258
Allegiant file 379
Allegiant matrix 150, 157, 236
all-in-one system 26
analog matrix 236
analog monitor group 18, 150, 152, 158, 224, 240, 244, 356, 359
  add 152
  controlled by workstations 158
  default 152
  initial camera 158
  OSD 158
  quad view 158
  single view 158
  startup camera 158
analytics viewer 68
ANR 105, 139, 343
ANSI 35
ASF 373
aspect ratio 16/9 207
ATM POS device 150
Audio Intercom functionality 373
Authorization Number 223
automatic alarm popup behavior 51
automatic display of alarms 51
automatic logoff 225
automatic recording mode 266
automatic relogon 211
automatic restart 211

B

backlight compensation 295
basic configuration 126
blinking device icons 199, 351
Bosch IntuiKey Keyboard 69, 70, 71, 73, 150, 155, 238, 256
Bosch Script API help 200
Bosch Video Management System 18
  activate 97
  GUI language 378
  licensing 97
  Online Help 15
  overview 18
  update 377
BVIP decoder 103, 136
  add 151
BVIP device
  password 138, 282
  Web page 282

BVIP encoder 103, 136
    add 53, 151, 241, 267
BVIP encoder:add 242, 269
bypass
    point 374

C

CABAC 348
camera round 334
camera round 172, 337
camera sequence 334
camera sequence 172, 337
CCL emulation 161
CCTV keyboard 153
    connection loss 378
change IP address 137, 157, 231, 232
change network address 137, 157
change password 129, 138, 282, 364
change pool 270
Changes in light level 305
CHAP password 265
character encoding 35
chattering sensors 196
Client Command Script
    alarm accepted 359
    executed on startup 157, 201, 202
CLL commands 57
codecs 185
Command Script 334
    Bosch Script API help 200
    export 201
    import 201
Command Script 172
Commercial Type Number 222
Compatibility Mode 60
Compound Events 194, 350
configuration data
    export 212
configuration data to OPC
    export 213
Configuration Wizard
    Mobile Video Service 26
configure VRM recording 216
connecting
    Allegiant matrix and Bosch VMS 74
    Bosch IntuiKey keyboard and Bosch VMS 71
connection string 225
control of a camera 185, 217
copy and paste 183
crash
    Configuration Client 379
    Operator Client 379
create
    Command Script 200
customized events 194, 350

D

data sheet 20
DCZ keyboard 153, 256
decoder
    Bosch IntuiKey keyboard 155
decoder:destination password 138
decoupled 57
default analog monitor group 152
default configuration 126
default IP address 231
default password 211, 222
delayed activation 211, 221
delete user 364
destination password 138
device capabilities
    update 103, 136
device identification 283
device monitor 214
device name 283
device replacement 99, 100
Device Tree 229, 334
Devices pane 334
devices without password protection 211
DiBos
    version 69, 70
DiBos device 150
digital keyboard 153
digital video recorder 150
disable enforced password protection 222
disconnected 57
display stamping 288
dome camera 188, 348
DSA E-Series 126, 271
DTP3N 252
dual authorization 365, 366
dual recording 40, 129, 189
dual streaming 239
duplicate IP addresses 231
duplicating an event 193
DVR device 52
DynDNS 35

E

E-mail device 150
empty password 211
encoder
  add 82, 132, 164
  Web page 282
encoder:failover recording mode 136
encoding on NVRs 229
enforced password protection 222
Enterprise Management Server 376
Enterprise System 26, 107, 112, 117
examples 215
  add Bosch Allegiant input alarm 216
  add Bosch ATM/POS bridge 215
  configure VRM recording 216
exception days 180
export
  ASF 373
  Camera Table 184
  Command Script 201
  configuration data 212
  configuration data to OPC 213
export Server List 35

F

face detection 67
face recognition 67
failover recording mode 266
  encoder 136
Failover VRM 40, 124, 262
False alarms 305
filtering 229, 232, 335, 341, 350, 353, 355, 362
finding
  devices 229, 232, 335, 341, 350, 353, 355, 362
  information in the Help 15
fire detection camera 163
Firewall 277
firmware upgrade
  Bosch IntuiKey keyboard 73
Forensic Search 158, 217, 238, 239

G

gain control 295
Ganetec
  alarm viewer 168
  analytics viewer 68
global alarm settings 196
global default password 95, 211, 222
GUI language 378

H

H.264 348
H.264 deblocking filter 348
HD cameras 207
help 15
holidays 180
hot spots 334
HTML files 334

I

I/O modules 150
identification 283
import
  Command Script 201
  resource files 171
inactivity 225
Independent Operator Client 57
initial camera 245
Initiator extension 284
Initiator name 284
Intercom functionality 373
interface settings
  VIP XD 155
intrusion panel 259, 260
IntuiKey keyboard 153
IP address
  change 137, 157, 231, 232
  duplicates 231
iPad 162, 259
iPhone 162, 259
IQN mapping 126
iSCSI device 126
iSCSI password 265
iSCSI storage pool 38, 263
iSCSI storage system 38

K

KBD Universal XF keyboard 69, 70, 150, 238

L

language 378
  Configuration Client 224
  Operator Client 363
license 98
Licenses 314
licensing
  Bosch Video Management System 97
  Config Wizard 95
  Stratus server 97
link to map 175
log file information 301
Logbook database 225
  connection string 225
logging 193, 196, 266

logging ONVIF events 385
Logical Tree 170, 359

M

malfunction relay 55
Management Server 20, 26, 57
manual recording 60, 197, 356
manual recording time (NVR) 356
map
  blinking hot spots 199, 351
map link 175
maps 334
menu commands 219
MIC IP 7000 167
milliseconds 288
Mobile Video Service 26, 53
move device 127, 133, 144
multi monitor mode 207
multicast 277
multi-select 170

N

network address
  change 137, 157
network monitoring device 150
network scan 231
new DiBos devices 155, 156, 235
night mode 295
no password 211
noise reduction 296
number plate detection 67
number plate recognition 67
NVR 20

O

offline 57, 364
Offline Mode 57
online application Help 15
ONVIF camera
  prepare 130
ONVIF logging 385
ONVIF Media profile 342
OPC Server 377
Operator Client 18, 170

P

panoramic camera
  viewing modes 61
password 138, 282
password change 129, 138, 282, 364
password missing 211
peripheral device 150
permissions 170, 334
point
  bypass 374
pool
  change 270
  move device 127, 133, 144
  VRM 125, 270
pooling 38, 263
port forwarding 35
port mapping 35, 225
post-alarm time 344
post-event time 185, 344
post-event time 346
pre-alarm time 344
pre-event time 185, 344
pre-event time 346
prepare an ONVIF camera 130
previous configuration 212
Primary Failover VRM 124
Primary VRM 40, 123, 262
printing the Help 15
profile 347
protect alarm recording 198
PTZ blocking 210, 368, 375
PTZ camera 188, 348
  Allegiant 343
PTZ control
  blocking 210, 368, 375
push-to-talk 373

Q

quad view 158, 245

R

RAM recording 344
recording mode
  automatic 266
  failover 266
Recording preferences 287
recording quality 347
recording settings 23
Recording Table 341
redundant recording 40
Redundant VRM 40, 124, 262
Reflections of light 305
refresh states 219, 232
Region of Interest 54, 188, 342, 367
relay
  malfunction 55
Release Notes 20
remote access 35, 108, 113, 117, 119, 225

Remote export 60
remove prepositions 188
remove user 364
replace content 171
resource files
    import 171
resource files 171
ROI 54, 188, 342, 367
routed access 230

S

scan
    across subnets 224
    encoders 262
    in subnets 224
    live only encoders 262
    local storage encoders 262
    VRM 262
scan for conflicting IP addresses 231
scan network 231
scheduled recording settings 23
Secondary Failover VRM 124
secondary recording 129, 189
Secondary VRM 40, 123, 262
sequence 337
Server ID 100
Server initiator name 265
Server List
    add columns 108, 113, 117, 119
    csv export 35
    delete columns 108, 113, 117, 119
Server Lookup 119
Server Network 121, 280, 281
sharpness 296
shutter 296
silence bells 374
SMS device 150
SNMP settings 227
SNMP traps
    get 227
    send 227
software package 98
software update 377
sort order
    alarms 356
Source type 287
states 219, 232
status 214
Stratus server
    licensing 97
stream 345
switch off alarm sirens 374
synchronization 105
synchronize
    VRM configuration 122, 263
system access 22
system requirements 20
system structures 21

T

Target data rate 347
time 287
time server 105
time synchronization 105
time zone 17
too many Allegiant cameras 379
transcoding service 162, 259
trigger text data recording 198

U

unreliable network 259
update 377
    device capabilities 103, 136
user
    delete 364
    remove 364
user event button 193, 194
UTF-8 35

V

VCA 304
VCR 287
video analytics 67, 168, 260
Video Streaming Gateway 150
VIDEOJET 7000 connect 167
VIDOS NVR 84, 154
viewing modes of panoramic camera 61
VIP X1600 XFM4 348
VIP XD 69
    half-duplex mode 155
    interface settings 155
    quad view 158
virtual input 150

VPN 35
VRM
  add 81, 122
  add pool 125
  Failover 40, 124, 262
  pool 125, 270
  Primary 40, 123, 262
  Primary Failover 124
  Redundant 40, 124, 262
  Secondary 40, 123, 262
  Secondary Failover 124
VRM 3.50 122, 263
VRM storage pool 38, 263

W

WAN 35, 225
Web client 162
WLAN 162, 259
workstation 158, 224

Bosch Sicherheitssysteme GmbH
Robert-Bosch-Ring 5
85630 Grasbrunn
Germany
www.boschsecurity.com