BOSCH

BVMS

de Konfigurationshandbuch

Inhaltsverzeichnis

1	**Arbeiten mit der Hilfe**	**14**
1.1	Suchen nach Informationen	14
1.2	Drucken der Hilfe	15
2	**Verwendung aktueller Software**	**16**
3	**Einführung**	**17**
3.1	BVMS Versionen	20
3.2	Überblick über die BVMS Lizenzaktivierung	20
4	**Systemüberblick**	**22**
4.1	Hardware-Anforderungen	23
4.2	Software-Anforderungen	23
4.3	Lizenzanforderungen	23
5	**Konzepte**	**24**
5.1	BVMS Designkonzepte	24
5.1.1	System mit einem Management Server	24
5.1.2	Enterprise System	25
5.1.3	Server Lookup	26
5.1.4	Unmanaged Site	28
5.2	Aufzeichnung	29
5.2.1	Automated Network Replenishment (ANR)	29
5.2.2	Duale/Failover-Aufzeichnung	31
5.2.3	VRM-Aufzeichnungsmodi	32
5.2.4	Wiedergabe von VRM-Aufzeichnungsquellen	34
5.2.5	Überblick über speicherbezogene Ereignisse	38
5.3	Alarmbearbeitung	39
5.4	Videoanalyse aktivieren/deaktivieren	40
5.5	ONVIF-Ereigniszuordnung	42
5.6	Abmeldung bei Inaktivität	43
5.7	Version unabhängiger Operator Client	43
5.7.1	Arbeiten im Kompatibilitätsmodus	44
5.8	Anzeigemodi einer Panoramakamera	44
5.8.1	360°-Panoramakamera – Boden- oder Deckenmontage	45
5.8.2	180°-Panoramakamera – Boden- oder Deckenmontage	46
5.8.3	360°-Panoramakamera – Wandmontage	47
5.8.4	180°-Panoramakamera – Wandmontage	48
5.8.5	Zugeschnittene Ansicht bei einer Panoramakamera	49
5.9	SSH-Tunneling	50
5.10	Multipathing	50
5.11	OpenID Connect (OIDC) und Identity Provider (IdP)	51
5.12	Kennzeichenerfassung	51
6	**Unterstützte Hardware**	**52**
6.1	Installieren von Hardware	53
6.2	Installation eines KBD Universal XF Keyboards	53
6.3	Verbinden eines Bosch IntuiKey Keyboards mit BVMS	53
6.3.1	Szenarios für Bosch IntuiKey Keyboard-Anschlüsse	54
6.3.2	Anschluss eines Bosch IntuiKey Keyboards an einen Decoder	56
6.3.3	Aktualisierung der Bosch IntuiKey Keyboard-Firmware	56
6.4	Verbinden einer Bosch Allegiant Kreuzschiene mit BVMS	57
6.4.1	Verbindung mit Bosch Allegiant Systemen – Überblick	57

6.4.2	Konfigurieren des Steuerungskanals	59
6.4.3	Bosch Allegiant Satellitensystem – Konzept	61
6.5	In BVMS unterstützte Allegiant CCL-Befehle	62
7	**Erste Schritte**	**64**
7.1	Installieren der Software-Module	64
7.2	Verwendung von Config Wizard	64
7.3	Starten des Configuration Client	71
7.4	Konfigurieren der Sprache des Configuration Client	72
7.5	Konfigurieren der Sprache des Operator Client	72
7.6	Nach Geräten suchen	73
7.7	Systemzugriff	73
7.8	Mittels Server Lookup	73
7.9	Aktivieren der Softwarelizenzen	74
7.9.1	Dialogfeld „Lizenz-Manager“ (Menü „Werkzeuge“)	75
7.9.2	Dialogfeld „Lizenz hinzufügen“	76
7.9.3	Dialogfeld „License Inspector“ (Menü „Werkzeuge“)	76
7.10	Warten von BVMS	76
7.11	Austausch eines Geräts	77
7.11.1	Austausch eines MS/EMS	78
7.11.2	Austausch eines VRM	79
7.11.3	Austausch eines Encoders oder Decoders	80
7.11.4	Austausch eines Operator Client	82
7.11.5	Abschließende Tests	82
7.11.6	Wiederherstellen von DIVAR IP	83
7.12	Zeitsynchronisation konfigurieren	83
7.13	Speichermedien eines Encoders konfigurieren	83
8	**Erstellung eines Enterprise Systems**	**85**
8.1	Konfigurieren der Serverliste für Enterprise System	85
8.2	Erstellen einer Enterprise User Group	86
8.3	Erstellen eines Enterprise Accounts	86
8.4	Tokenbasierte Authentifizierung	87
9	**Konfigurieren von Kommandoskripten**	**89**
9.1	Verwalten von Kommandoskripten	89
9.2	Konfigurieren eines automatisch startenden Kommandoskripts	90
9.3	Importieren eines Kommandoskripts	90
9.4	Exportieren eines Kommandoskripts	91
9.5	Konfigurieren eines Start-Kommandoskripts (Seite „Einstellungen“)	91
10	**Verwalten von Konfigurationsdaten**	**92**
10.1	Aktivieren der letzten Konfiguration	92
10.2	Aktivieren einer Konfiguration	93
10.3	Exportieren von Konfigurationsdaten	94
10.4	Importieren von Konfigurationsdaten	94
10.5	Exportieren von Konfigurationsdaten auf OPC	95
10.6	Status des Encoders/Decoders überprüfen	95
10.7	SNMP-Überwachung konfigurieren	95
10.8	Berichte erstellen	96
11	**Konfigurationsbeispiele**	**97**
11.1	Hinzufügen einer Bosch ATM/POS-Bridge	97
11.2	Hinzufügen eines Bosch Allegiant Kreuzschienen-Eingangsalarms	98

11.3	Hinzufügen und Konfigurieren von 2 Dinion IP Kameras mit VRM Aufzeichnung	98
12	**Allgemeine Fenster des Configuration Client**	**100**
12.1	Konfigurationsfenster	100
12.2	Menübefehle	101
12.3	Dialogfeld „Aktivierungs-Manager“ (Menü „System“)	103
12.4	Dialogfeld „Konfiguration aktivieren“ (Menü „System“)	104
12.5	Dialogfeld „Initialer Geräte-Scan“ (Menü „Hardware“)	104
12.6	Dialogfeld „Geräte mit globalem Standard-Passwort schützen“ (Menü „Hardware“)	105
12.7	Dialogfeld „iSCSI-Speicher mit CHAP-Passwort schützen“ (Menü „Hardware“)	105
12.8	Dialogfeld „Gerätepasswörter ändern“ (Menü „Hardware“)	106
12.9	Dialogfeld „Geräte-Firmware aktualisieren“ (Menü „Hardware“)	107
12.10	Dialogfeld „Geräte-IP und Netzwerkeinstellungen ändern“ (Menü „Hardware“)	108
12.11	Dialogfeld „Geräte-Monitor“ (Menü „Hardware“)	110
12.12	Dialogfeld Kommandoscript-Editor (Menü „Werkzeuge“)	110
12.13	Dialogfeld Ressourcen-Manager (Menü „Werkzeuge“)	111
12.14	Dialogfeld Kamerasequenzen (Menü „Werkzeuge“)	111
12.15	Dialogfeld „Lizenz-Manager“ (Menü „Werkzeuge“)	111
12.15.1	Dialogfeld „Lizenz hinzufügen“	112
12.16	Dialogfeld „License Inspector“ (Menü „Werkzeuge“)	112
12.17	Dialogfeld Arbeitsstationsüberwachung (Menü „Werkzeuge“)	112
12.18	Dialogfelder „Auswertungen“ (Menü „Auswertungen“)	113
12.18.1	Dialogfeld „Aufzeichnungszeitpläne“	113
12.18.2	Dialogfeld „Geplante Aufzeichnungseinstellungen“	113
12.18.3	Dialogfeld „Aktionszeitpläne“	113
12.18.4	Dialogfeld „Kameras und Aufzeichnungsparameter”	113
12.18.5	Dialogfeld „Stream-Qualität''	113
12.18.6	Dialogfeld „Ereignis-Einstellungen”	113
12.18.7	Dialogfeld „Einstellungen für zusammengesetztes Ereignis”	113
12.18.8	Dialogfeld „Alarmeinstellungen“	114
12.18.9	Dialogfeld „Konfigurierte Benutzer”	114
12.18.10	Das Dialogfeld „Benutzergruppen und Konten”	114
12.18.11	Dialogfeld „Geräteberechtigungen“	114
12.18.12	Dialogfeld „Bedienberechtigungen“	114
12.18.13	Dialogfeld „Konfigurationsberechtigungen“	114
12.18.14	Dialogfeld „Berechtigungen für Benutzergruppen“	114
12.18.15	Dialogfeld „Sicherheitseinstellungen”	115
12.18.16	Dialogfeld Anwendungsberechtigungen	115
12.18.17	Dialogfeld „Umgangene Geräte“	115
12.19	Dialogfeld „Alarmeinstellungen“ (Menü „Einstellungen“)	115
12.20	Dialogfeld „SNMP-Einstellungen“ (Menü „Einstellungen“)	115
12.21	Dialogfeld „LDAP-Server-Einstellungen“ (Menü „Einstellungen“)	116
12.21.1	Zuordnen einer LDAP-Gruppe	118
12.22	Dialogfeld „LDAP-Benutzergruppenreihenfolge definieren“ (Menü „Einstellungen“)	118
12.23	Dialogfeld „Zugriffstoken-Einstellungen“ (Menü Einstellungen)	118
12.24	Dialogfeld Einstellungen für vertrauenswürdige Zertifikate (Menü Einstellungen)	120
12.25	Dialogfeld „Optionen“ (Menü „Einstellungen“)	121
13	**Seite Geräte**	**125**
13.1	Aktualisieren von Gerätestatus und -funktionen	125
13.2	Ändern des Passworts für IP-Geräte	126

13.3	Hinzufügen eines Geräts	126
13.4	Seite „Server-Liste/Adressbuch“	129
13.4.1	Dialogfeld „Server hinzufügen“	130
13.4.2	Konfigurieren von Server Lookup	130
13.4.3	Konfigurieren der Server-Liste	130
13.4.4	Export der Server-Liste	131
13.4.5	Import einer Server-Liste	131
13.5	Seite DVR (Digital-Videorekorder)	132
13.5.1	DVR-Geräte	132
13.5.2	Hinzufügen eines DVR-Geräts per Suchvorgang	133
13.5.3	Dialogfeld „Add DVR“ (DVR hinzufügen)	133
13.5.4	Registerkarte „Einstellungen“	134
13.5.5	Registerkarte „Kameras“	134
13.5.6	Registerkarte „Eingänge“	134
13.5.7	Registerkarte „Relais“	134
13.5.8	Konfigurieren der Integration eines DVR	134
13.6	Seite Kreuzschienen	135
13.6.1	Hinzufügen eines Bosch Allegiant Geräts	135
13.6.2	Konfigurieren eines Bosch Allegiant Geräts	135
13.6.3	Seite Ausgänge	136
13.6.4	Seite Eingänge	137
13.6.5	Seite Verbindung	137
13.6.6	Seite Kameras	137
13.7	Seite Arbeitsstation	137
13.7.1	Manuelles Hinzufügen einer Arbeitsstation	138
13.7.2	Konfigurieren eines Bosch IntuiKey Keyboards (Seite „Einstellungen“) (Arbeitsstation)	138
13.7.3	Konfigurieren eines Start-Kommandoskripts (Seite „Einstellungen“)	139
13.7.4	Seite Einstellungen	139
13.7.5	Ändern der Netzwerkadresse einer Arbeitsstation	141
13.8	Seite "Decoder"	141
13.8.1	Manuelles Hinzufügen eines Encoders	141
13.8.2	Dialogfeld „Encoder/Decoder bearbeiten“	143
13.8.3	Ändern des Passworts für einen Encoder/Decoder (Passwort ändern/Passwort eingeben)	144
13.8.4	Decoderprofil	145
13.8.5	Monitor-Anzeige	146
13.8.6	Konfigurieren eines Bosch IntuiKey Keyboards (Decoder)	146
13.8.7	Konfigurieren eines Decoders für den Einsatz mit einem Bosch IntuiKey Keyboard	146
13.8.8	Löschen des Decoder-Logos	147
13.9	Seite „Monitorgruppen“	147
13.9.1	Manuelles Hinzufügen einer Monitorgruppe	147
13.9.2	Konfigurieren einer Monitorgruppe	148
13.10	Seite Kommunikationsgeräte	149
13.10.1	Hinzufügen eines E-Mail-/SMTP-Servers	149
13.10.2	Seite SMTP-Server	149
13.10.3	Konfigurieren eines Kommunikationsgeräts	150
13.10.4	Dialogfeld Test-E-Mail senden	150
13.11	Seite „ATM/POS“	151
13.11.1	Manuelles Hinzufügen einer Bosch ATM/POS-Bridge	151
13.11.2	Seite Bosch ATM/POS-Bridge	152

13.11.3	Konfigurieren eines Peripheriegeräts	152
13.11.4	Seite „DTP-Einstellungen“	152
13.11.5	Seite „ATM-Einstellungen“	153
13.11.6	Seite Eingänge	153
13.12	Foyer-Kartenleser	153
13.12.1	Dialogfeld „Foyer-Kartenleser hinzufügen“	154
13.12.2	Einstellungen für Foyer-Kartenleser-Seite	154
13.13	Seite Virtuelle Eingänge	154
13.13.1	Manuelles Hinzufügen virtueller Eingänge	155
13.14	Seite SNMP	155
13.14.1	Manuelles Hinzufügen eines SNMP	155
13.14.2	Konfigurieren eines SNMP Trap Receivers (Seite „SNMP Trap Receiver“)	156
13.14.3	Dialogfeld SNMP Trap Logger	157
13.15	Seite „Assign Keyboard“ (Tastatur zuweisen)	157
13.16	Seite Input / Output-Module	158
13.16.1	Manuelles Hinzufügen eines I/O-Moduls	159
13.16.2	Konfigurieren eines I/O-Moduls	159
13.16.3	Seite ADAM-Gerät	159
13.16.4	Seite Eingänge	160
13.16.5	Seite Relais	160
13.17	Seite "Allegiant CCL-Emulation"	160
13.17.1	Manuelles Hinzufügen einer Allegiant CCL-Emulation	161
13.17.2	Allegiant CCL-Befehle	161
13.17.3	Konfigurieren einer Allegiant CCL-Emulation	161
13.18	Seite „Einbruchmeldezentralen”	161
13.18.1	Manuelles Hinzufügen einer Einbruchmeldezentrale	162
13.18.2	Seite "Einstellungen"	162
13.19	Seite „Zutrittskontrollsysteme“	162
13.19.1	Hinzufügen eines Zutrittskontrollsystems	163
13.19.2	Bearbeiten eines Zutrittskontrollsystems	163
13.19.3	Seite „Einstellungen“	164
13.20	Seite „Video Analytics“	164
13.20.1	Seite „Videoanalyse-Einstellungen“	164
13.20.2	Hinzufügen eines Videoanalysegeräts	164
13.20.3	Seite „Person Identification Device“	165
13.20.4	Hinzufügen eines Person Identification Device (PID)	165
13.20.5	Seite „PID“	166
13.20.6	Wiederherstellung des PID-Zugriffs nach Ausfall eines BVMS Management Servers	166
13.20.7	Hinzufügen von Kameras zu einem Person Identification Device (PID)	167
13.20.8	Konfigurieren von Kameraparametern für Person Identification-Alarme	168
13.20.9	Konfigurieren von Personengruppen	168
13.20.10	Hinzufügen eines Tattile LPR-Geräts	169
13.21	Seite VRM-Geräte	170
13.21.1	Hinzufügen eines VRM-Geräts per Suchvorgang	170
13.21.2	Manuelles Hinzufügen eines primären oder sekundären VRMs	172
13.21.3	Bearbeiten eines VRM-Geräts	173
13.21.4	Seite VRM-Einstellungen	174
13.21.5	Seite SNMP	174
13.21.6	Seite „Konten“	174

13.21.7	Seite Erweitert	174
13.21.8	Verschlüsseln der Aufzeichnung für VRM	175
13.21.9	Passwort für ein VRM-Gerät ändern	176
13.21.10	Hinzufügen eines VRM-Pools	176
13.21.11	Manuelles Hinzufügen eines Failover-VRM	177
13.21.12	Manuelles Hinzufügen eines gespiegelten VRM	177
13.21.13	Hinzufügen von Encodern per Suchvorgang	179
13.21.14	Hinzufügen von VSG-Geräten per Suchvorgang	179
13.21.15	Synchronisieren der BVMS Konfiguration	180
13.21.16	Importieren der Konfiguration von VRM	180
13.22	Seite „Pool“	180
13.22.1	Konfigurieren des automatischen Aufzeichnungsmodus auf einem Pool	182
13.22.2	Manuelles Hinzufügen eines Encoders	182
13.22.3	Manuelles Hinzufügen eines iSCSI-Geräts	184
13.22.4	Manuelles Hinzufügen eines Video Streaming Gateway	184
13.22.5	Manuelles Hinzufügen eines iSCSI-Geräts der DSA E-Series	186
13.22.6	Hinzufügen von Encodern per Suchvorgang	188
13.22.7	Hinzufügen von VSG-Geräten per Suchvorgang	189
13.22.8	Duale Aufzeichnung im Gerätebaum konfigurieren	189
13.23	Bosch Encoder-/Decoder-Seite	190
13.24	Seite iSCSI-Gerät	190
13.24.1	iSCSI-Speicherpool	190
13.24.2	Manuelles Hinzufügen eines iSCSI-Geräts	191
13.24.3	Manuelles Hinzufügen eines iSCSI-Geräts der DSA E-Series	192
13.24.4	Konfigurieren eines iSCSI-Geräts	194
13.24.5	Seite „Basic Configuration“ (Grundkonfiguration)	195
13.24.6	Dialogfeld „Lastverteilung“	197
13.24.7	Verschieben eines iSCSI-Systems in einen anderen Pool (Pool ändern)	197
13.24.8	Seite LUNs	197
13.24.9	Hinzufügen einer LUN	198
13.24.10	Formatieren einer LUN	199
13.24.11	Dialogfeld iqn-Mapper	199
13.25	Seite „Video Streaming Gateway-Gerät“	200
13.25.1	Manuelles Hinzufügen eines Video Streaming Gateway	200
13.25.2	Bearbeiten eines Video Streaming Gateway	202
13.25.3	Hinzufügen einer Kamera zu einem VSG	202
13.25.4	Dialogfeld „Bosch Encoder hinzufügen/bearbeiten“	203
13.25.5	Dialogfeld „ONVIF-Encoder hinzufügen/bearbeiten“	204
13.25.6	Dialogfeld „JPEG-Kamera hinzufügen/bearbeiten“	206
13.25.7	Dialogfeld „RTSP-Encoder hinzufügen/bearbeiten“	207
13.25.8	Verschieben eines VSG in einen anderen Pool (Pool ändern)	208
13.25.9	Konfigurieren von Multicast (Registerkarte „Multicast“)	208
13.25.10	Konfigurieren der Protokollierung (Registerkarte „Erweitert“)	209
13.25.11	Starten des ONVIF Camera Event Driver Tool aus dem Configuration Client	209
13.26	Seite Nur Live	210
13.26.1	Hinzufügen von Nur-Live-Geräten per Suchvorgang	210
13.26.2	Manuelles Hinzufügen eines Encoders	211
13.26.3	Angeben des Ziel-Passworts für einen Decoder (Authentifizieren ...)	212
13.27	Seite Lokale Archivierung	212

13.28	Seite „Unmanaged Site“	213
13.28.1	Manuelles Hinzufügen einer Unmanaged Site	214
13.28.2	Importieren von Unmanaged Sites	214
13.28.3	Seite „Unmanaged Site“	214
13.28.4	Hinzufügen eines Unmanaged Netzwerkgeräts	214
13.28.5	Konfiguration der Zeitzone	215
14	**Seite „Bosch Encoder/Decoder/Kamera“**	**217**
14.1	Manuelles Hinzufügen eines Encoders	219
14.2	Hinzufügen eines Encoders zu einem VRM-Pool	220
14.3	Hinzufügen eines Nur-Live-Encoders	220
14.4	Hinzufügen eines Encoders mit lokaler Archivierung	220
14.5	Hinzufügen einer einzelnen Platzhalterkamera	221
14.6	Importieren von Kameras aus einer CSV-Datei	221
14.7	Hinzufügen eines Bosch Encoders mit vorkonfigurierten Geolokalisierungseinstellungen	223
14.8	Bearbeiten eines Encoders	223
14.8.1	Verschlüsseln von Live-Video (Encoder bearbeiten)	223
14.8.2	Aktualisieren der Gerätefunktionen (Encoder bearbeiten)	224
14.8.3	Dialogfeld „Encoder/Decoder bearbeiten“	224
14.9	Verwalten der Authentizitätsprüfung	226
14.9.1	Überprüfung der Authentizität	226
14.9.2	Konfigurieren der Authentifizierung	227
14.9.3	Hochladen eines Zertifikats	228
14.9.4	Download eines Zertifikats	228
14.9.5	Installierung eines Zertifikats auf einer Arbeitsstation	228
14.10	Angeben des Ziel-Passworts für einen Decoder (Authentifizieren ...)	229
14.11	Ändern des Passworts für einen Encoder/Decoder (Passwort ändern/Passwort eingeben)	229
14.12	Verschieben eines Encoders in einen anderen Pool (Pool ändern)	230
14.13	Wiederherstellung von Aufzeichnungen von einem ausgetauschten Encoder (Aufzeichnungen von Vorgänger zuweisen)	231
14.14	Konfigurieren von Encodern/Decodern	232
14.14.1	Speichermedien eines Encoders konfigurieren	232
14.14.2	Konfigurieren mehrerer Encoder/Decoder	232
14.14.3	Konfigurieren des Failover-Aufzeichnungsmodus auf einem Encoder	234
14.14.4	Seite „Recording Management“ (Aufzeichnungsverwaltung)	235
14.14.5	Seite „Aufzeichnungspräferenzen“	235
14.14.6	Konfigurieren von Decodern für das On-Screen-Display (OSD)	235
14.15	Konfigurieren von Multicast	236
15	**ONVIF Seite**	**238**
15.1	Hinzufügen eines Nur-Live-ONVIF-Geräts per Suchvorgang	238
15.2	Seite „ONVIF-Encoder"	238
15.3	Seite "ONVIF-Encoderereignis"	239
15.3.1	Hinzufügen und Entfernen eines ONVIF Profils	241
15.3.2	Exportieren einer ONVIF-Mapping-Tabelle	242
15.3.3	Importieren einer ONVIF Mapping-Tabelle	242
15.3.4	Konfigurieren einer ONVIF-Mapping-Tabelle	243
15.4	Seite „ONVIF Konfiguration“	245
15.4.1	Gerätezugriff	245
15.4.2	Datum/Zeit	246
15.4.3	Benutzerverwaltung	246

15.4.4	Seite „Videoencoderprofil”	247
15.4.5	Audioencoderprofil	249
15.4.6	Imaging allgemein	250
15.4.7	Gegenlichtkompensation	251
15.4.8	Belichtung	251
15.4.9	Fokus	252
15.4.10	Großer dynamischer Bereich	253
15.4.11	Weißabgleich	253
15.4.12	Netzwerkzugriff	254
15.4.13	Bereiche	256
15.4.14	Relais	257
15.5	Seite "ONVIF-Ereignisquelle"	258
15.6	ONVIF-Profile zuweisen	259
16	**Seite Nummernschild-Erkennung**	**260**
17	**Seite „Karten und Struktur“**	**261**
18	**Konfigurieren von Karten und dem Logischen Baum**	**263**
18.1	Konfigurieren des Logischen Baums	263
18.2	Hinzufügen eines Geräts zum Logischen Baum	264
18.3	Entfernen eines Baumelements	264
18.4	Verwalten von Ressourcen-Dateien	265
18.4.1	Dialogfeld Ressourcen-Manager	266
18.4.2	Dialogfeld Ressource auswählen	267
18.5	Hinzufügen eines Dokuments	267
18.5.1	Dialogfeld URL hinzufügen	267
18.6	Dialogfeld „Link zu externer Anwendung“	268
18.7	Hinzufügen eines Kommandoskripts	268
18.8	Hinzufügen einer Kamerasequenz	269
18.8.1	Dialogfeld Kamerasequenzen	269
18.9	Verwalten von vorkonfigurierten Kamerasequenzen	270
18.9.1	Dialogfeld Kamerasequenz hinzufügen	271
18.9.2	Dialogfeld Sequenzschritt hinzufügen	272
18.10	Hinzufügen eines Ordners	272
18.11	Hinzufügen einer Karte	272
18.12	Hinzufügen eines Links zu einer anderen Karte	273
18.12.1	Dialogfeld Karte für Link auswählen	273
18.13	Zuordnen einer Karte zu einem Ordner	273
18.14	Verwalten von Geräten auf einem Lageplan	273
18.15	Konfigurieren der globalen Karte und der Karten-Anzeigebereiche	274
18.15.1	Konfigurieren der globalen Karte	275
18.15.2	Konfigurieren von Kameras auf der globalen Karte	276
18.15.3	Hinzufügen von Karten auf der globalen Karte	278
18.16	Hinzufügen eines Karten-Anzeigebereichs	279
18.17	Aktivierung des Map-based Tracking Assistant	279
18.18	Ein Störungsrelais hinzufügen	280
18.18.1	Dialogfeld „Störungsrelais“	280
18.19	Konfigurieren der Geräteumgehung	281
19	**Seite Zeitpläne**	**282**
19.1	Seite Aufzeichnungszeitpläne	282
19.2	Seite Aktionszeitpläne	282

20	**Konfigurieren von Zeitplänen**	**284**
20.1	Konfigurieren eines Aufzeichnungszeitplans	284
20.2	Hinzufügen eines Aktionszeitplans	285
20.3	Konfigurieren eines Standard-Aktionszeitplans	285
20.4	Konfigurieren eines wiederkehrenden Aktionszeitplans	285
20.5	Entfernen eines Aktionszeitplans	286
20.6	Hinzufügen von Feiertagen und besonderen Tagen	286
20.7	Entfernen von Feiertagen und besonderen Tagen	287
20.8	Umbenennen eines Zeitplans	287
21	**Seite Kameras und Aufzeichnung**	**289**
21.1	Seite Kameras	290
21.2	Seiten für Aufzeichnungseinstellungen	294
22	**Konfigurieren von Kameras und Aufzeichnungseinstellungen**	**296**
22.1	Kopieren und Einfügen in Tabellen	296
22.2	Kameratabelle exportieren	297
22.3	Konfigurieren von Stream-Qualitätseinstellungen	298
22.3.1	Dialogfeld Stream-Qualitätseinstellungen	298
22.4	Konfigurieren der Kameraeigenschaften	301
22.5	Konfigurieren von Aufzeichnungseinstellungen (nur VRM und Lokale Archivierung)	301
22.6	Dialogfeld Geplante Aufzeichnungseinstellungen (nur VRM und Lokale Archivierung)	302
22.7	Konfigurieren von PTZ Port-Einstellungen	305
22.8	Konfigurieren von voreingestellten Positionen und AUX-Kommandos	305
22.9	Dialogfeld „Voreingestellte Positionen und AUX-Kommandos“	306
22.10	ROI-Funktion konfigurieren	307
22.11	ANR-Funktion konfigurieren	308
22.12	Duale Aufzeichnung in der Kameratabelle konfigurieren	308
22.13	Verwalten von Video-Streaming-Gateways	308
22.13.1	ONVIF-Profile zuweisen	309
23	**Seite Ereignisse**	**310**
23.1	Registerkarte „Entprelleinstellungen“	311
23.2	Registerkarte „Einstellungen” für die erweiterte Anzeige der Karte	311
23.3	Registerkarte „Einstellungen” für die Ereigniskonfiguration	312
23.4	Dialogfeld Kommandoskript-Editor	312
23.5	Zusammengesetztes Ereignis erzeugen / Dialogfeld Zusammengesetztes Ereignis bearbeiten	313
23.6	Dialogfeld Skriptsprache auswählen	314
23.7	Prioritäten des Dialogfelds „Ereignistyp“ bearbeiten	314
23.8	Dialogfeld Geräte auswählen	314
23.9	Dialogfeld „Textatenaufzeichnung“	314
24	**Seite Alarme**	**315**
24.1	Dialogfeld „Alarmeinstellungen“	316
24.2	Dialogfeld Bildfensterinhalt auswählen	317
24.3	Dialogfeld „Bildfensterinhalt auswählen“ (MG)	318
24.4	Dialogfeld Alarmoptionen	318
24.5	Dialogfeld Ressource auswählen	322
25	**Konfigurieren von Ereignissen und Alarmen**	**323**
25.1	Kopieren und Einfügen in Tabellen	324
25.2	Entfernen einer Tabellenzeile	324
25.3	Verwalten von Ressourcen-Dateien	324
25.4	Konfigurieren eines Ereignisses	324

25.5	Duplizieren eines Ereignisses	324
25.6	Protokollieren von Benutzerereignissen	325
25.7	Konfigurieren von Benutzerereignisschaltflächen	325
25.8	Erzeugen eines Zusammengesetzten Ereignisses	326
25.9	Bearbeiten eines Zusammengesetzten Ereignisses	327
25.10	Konfigurieren eines Alarms	327
25.11	Konfigurieren der Einstellungen aller Alarme	328
25.12	Vor- und Nachalarmdauer bei einem Alarm konfigurieren	328
25.13	Alarmaufzeichnung mit Textdaten auslösen	329
25.14	Textdaten einer Daueraufzeichnung hinzufügen	329
25.15	Alarmaufzeichnung schützen	330
25.16	Konfigurieren der blinkenden Hotspots	330
25.17	Ereignisse und Alarme für Zutrittskontrollsysteme	331
25.18	Ereignisse und Alarme zur Person Identification	331
26	**Seite Benutzergruppen**	**333**
26.1	Seite Eigenschaften der Benutzergruppen	335
26.2	Seite Benutzereigenschaften	336
26.3	Seite Eigenschaften des Anmeldungspaares	337
26.4	Seite Kamerafreigaben	338
26.5	Seite „Prioritäten für Steuerungen“	339
26.6	Dialogfeld Freigaben für Benutzergruppen kopieren	340
26.7	Seite Decoder-Freigaben	340
26.8	Seite Ereignisse und Alarme	341
26.9	Seite „Zugangsberechtigungen“	341
26.10	Seite Logischer Baum	342
26.11	Seite mit den Bedienereigenschaften	342
26.12	Seite Prioritäten	346
26.13	Seite Benutzeroberfläche	346
26.14	Seite „Server-Zugriff“	347
26.15	Seite „Konfigurationsberechtigungen“	348
26.16	Seite „Berechtigungen für Benutzergruppen“	350
26.17	Seite „Kontorichtlinien“	350
26.17.1	Offline Operator Client	352
26.18	Berechtigungen für die Anmeldung pro Anwendungstypseite	355
26.19	Seite mit den Einstellungen für das Bedrohungsmanagement	356
27	**Konfigurieren von Benutzern, Berechtigungen und Enterprise Access**	**357**
27.1	Erstellen einer Gruppe oder eines Kontos	358
27.1.1	Erstellen einer Standard-Benutzergruppe	358
27.1.2	Erstellen einer Enterprise User Group	359
27.1.3	Erstellen eines Enterprise Accounts	359
27.2	Erzeugen eines Benutzers	360
27.3	Erzeugen einer 4-Augen-Gruppe	361
27.4	Hinzufügen eines Anmeldungspaars zu einer 4-Augen-Gruppe	361
27.5	Konfigurieren der Admin-Gruppe	362
27.6	Auswählen einer zugeordneten LDAP-Gruppe	363
27.7	Festlegen eines Freigabezeitplans für Benutzeranmeldungen	363
27.8	Konfigurieren von Bedienberechtigungen	364
27.9	Konfigurieren von Geräteberechtigungen	364
27.10	Konfigurieren verschiedener Prioritäten	365

27.11	Kopieren von Freigaben für Benutzergruppen	368
28	**Audit Trail-Seite**	**369**
28.1	Audit Trail-Protokollierungsdetails	370
28.2	Audit Trail-Dialogfeld zum Filtern	370
29	**Konfigurieren der videobasierten Brandmeldeanlage**	**372**
29.1	Konfigurieren einer Branderkennungskamera	372
29.2	Hinzufügen eines Encoders zu einem VRM-Pool	373
29.3	Hinzufügen von Encodern per Suchvorgang	373
29.4	Hinzufügen von Nur-Live-Geräten per Suchvorgang	373
29.5	Hinzufügen von Encodern mit lokaler Archivierung per Suchvorgang	374
29.6	Konfigurieren eines Brandereignisses	374
29.7	Konfigurieren eines Feueralarms	375
30	**Konfigurieren der MIC IP 7000, die mit einem VIDEOJET 7000 connect verbunden ist**	**376**
31	**Problembehandlung**	**377**
31.1	Konfigurieren der gewünschten Sprache in Windows	379
31.2	Wiederherstellen der Verbindung mit einem Bosch IntuiKey Keyboard	379
31.3	Reduzieren der Anzahl der Allegiant Kameras	379
31.4	Verwendete Ports	379
31.5	Ermöglicht die Protokollierung von ONVIF-Ereignissen	385
	Glossar	**387**

1 Arbeiten mit der Hilfe

Hinweis!
In diesem Dokument werden einige Funktionen beschrieben, die nicht für BVMS Viewer verfügbar sind.
Ausführliche Informationen zu den verschiedenen Versionen von BVMS finden Sie unter www.boschsecurity.com und in der BVMS Schnellauswahlhilfe: BVMS Schnellauswahlhilfe.

Um mehr zu einem bestimmten BVMS Thema zu erfahren, greifen Sie auf die Online-Hilfe zu und wenden Sie eine der nachfolgenden Methoden an.

So verwenden Sie Inhalt, Index oder Suche:

- Klicken Sie im Menü **Hilfe** auf **Hilfe anzeigen**. Navigieren Sie mithilfe der Schaltflächen und Links.

So erhalten Sie Hilfe zu einem Fenster oder Dialogfeld:

- Klicken Sie in der Symbolleiste auf ? .

ODER

- Drücken Sie F1, um Hilfe zu einem Programmfenster oder Dialogfeld zu erhalten.

1.1 Suchen nach Informationen

Sie haben mehrere Möglichkeiten, in der Hilfe nach Informationen zu suchen.
So suchen Sie nach Informationen in der Online-Hilfe:

1. Klicken Sie im Menü **Hilfe** auf **Hilfe**.
2. Wenn das linke Fenster nicht sichtbar ist, klicken Sie auf die Schaltfläche **Anzeigen**.
3. Gehen Sie im Hilfefenster wie folgt vor:

Option:	Aktion:
Inhalt	Anzeigen des Inhaltsverzeichnisses der Online-Hilfe. Klicken Sie auf die einzelnen Bücher, um Seiten anzuzeigen, die Links zu Themen enthalten. Klicken Sie auf die einzelnen Seiten, um das entsprechende Thema im rechten Fenster anzuzeigen.
Index	Suchen nach bestimmten Wörtern oder Ausdrücken bzw. Auswahl aus einer Liste mit Indexschlüsselwörtern. Doppelklicken Sie auf das Schlüsselwort, um das entsprechende Thema im rechten Fenster anzuzeigen.
Suche	Suchen nach Wörtern oder Ausdrücken im Textinhalt der ausgewählten Themen. Geben Sie das Wort oder den Ausdruck in das Textfeld ein, drücken Sie die Eingabetaste, und wählen Sie das gewünschte Thema in der Themenliste aus.

Text der Benutzeroberfläche ist **fett** markiert.

- Der Pfeil gibt Ihnen die Möglichkeit, auf den unterstrichenen Text oder auf ein Element in der Anwendung zu klicken.

Verwandte Themen

- Klicken Sie darauf, um ein Thema mit Informationen zum aktuell verwendeten Anwendungsfenster anzuzeigen. Dieses Thema liefert Informationen zu den Bedienelementen des Anwendungsfensters.

Konzepte, Seite 24 bietet Hintergrundinformationen zu ausgewählten Themen.

Hinweis!
Dieses Symbol weist auf ein potenzielles Risiko für Sachschäden oder Datenverlust hin.

1.2 Drucken der Hilfe

In der Online-Hilfe können Sie Themen und Informationen direkt aus dem Browser-Fenster heraus drucken.

So drucken Sie ein Hilfethema:

1. Klicken Sie mit der rechten Maustaste in das rechte Fenster, und wählen Sie **Drucken** aus. Das Dialogfeld **Drucken** wird geöffnet.
2. Klicken Sie auf **Drucken**.

⇨ Das Thema wird auf dem angegebenen Drucker gedruckt.

2 Verwendung aktueller Software

Wir erstellen nur neue Updates für Softwareversionen mit allgemeiner oder eingeschränkter Verfügbarkeit. Weitere Informationen finden Sie unter:
Bosch Building Technologies Software Service und Support.
Unter den folgenden Links finden Sie weitere Informationen:

- Allgemeine Informationen: https://www.boschsecurity.com/xc/en/support/product-security/
- Sicherheitshinweise, d. h. eine Liste identifizierter Schwachstellen und Lösungsvorschläge: https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html

Bosch übernimmt keinerlei Haftung für Schäden, die durch Produkte entstehen, die mit veralteten Softwarekomponenten in Betrieb genommen wurden.

3 Einführung

Auf den Link klicken, um auf die Open Source Software-Lizenz, die von BVMS und der Mobile App verwendet wird, zuzugreifen.
http://www.boschsecurity.com/oss/

HEVCAdvance™
Unterliegt einem oder mehreren Patentansprüchen unter patentlist.hevcadvance.com.

BVMS

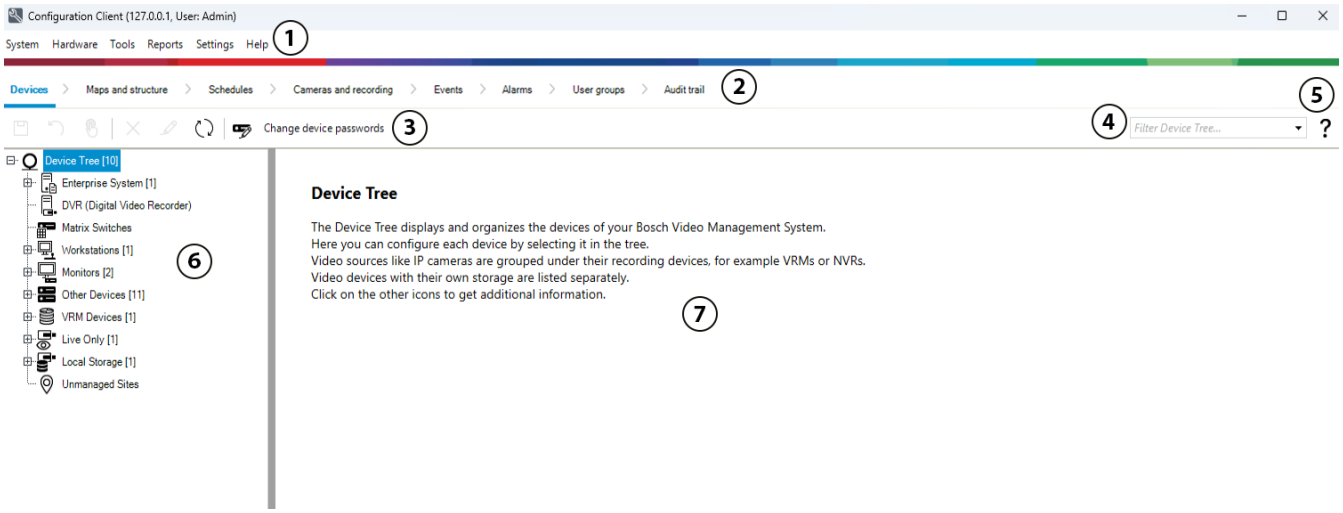
BVMS integriert digitale Video- und Audiosignale sowie Daten innerhalb von IP-Netzwerken.
Das System umfasst die folgenden Softwaremodule:
- Management Server
- VRM-Aufzeichnung (Video Recording Manager)
- Operator Client
- Configuration Client

Gehen Sie wie folgt vor, um das System einzurichten:
- Dienste installieren (Management Server und VRM)
- Operator Client und Configuration Client installieren
- Mit dem Netzwerk verbinden
- Geräte mit dem Netzwerk verbinden
- Grundkonfiguration:
  - Geräte hinzufügen (z. B. durch Geräte-Scan)
  - Logische Struktur erstellen
  - Zeitpläne, Kameras, Ereignisse und Alarme konfigurieren
  - Benutzergruppen konfigurieren

BVMS Configuration Client

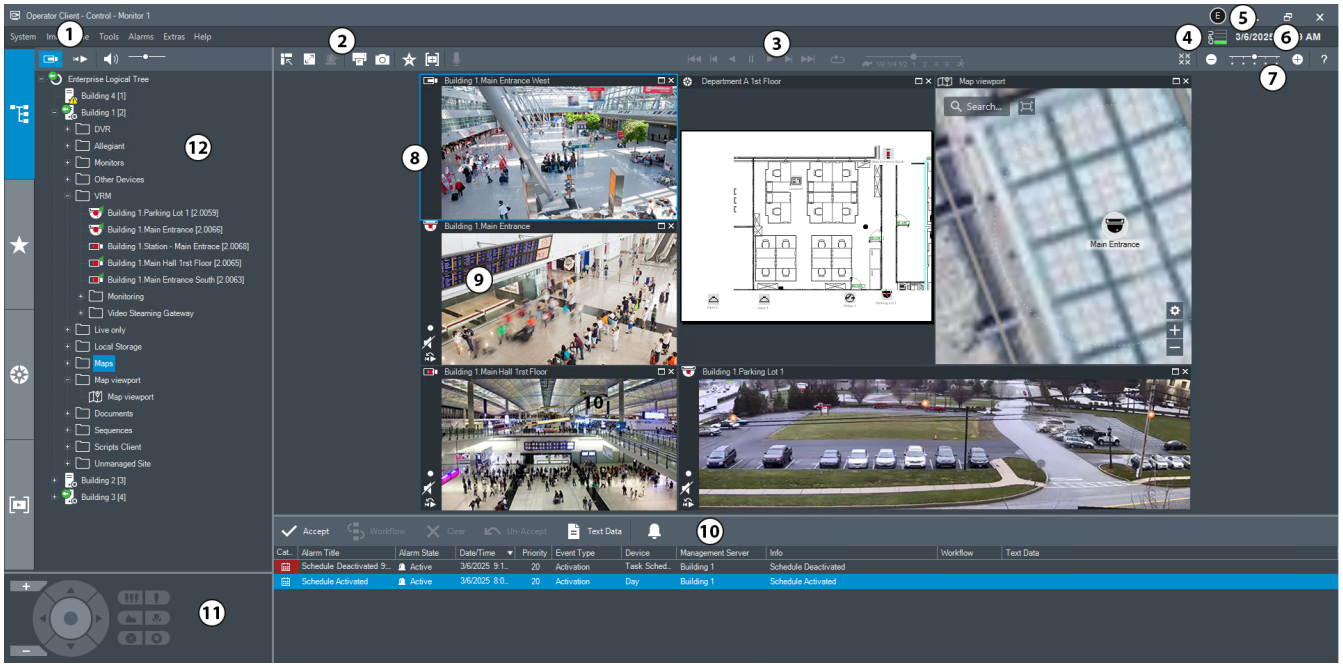
Das Konzept von BVMS Configuration Client besteht darin, dass Sie mit der Konfiguration der Geräte beginnen und dann mit der Konfiguration des logischen Baums fortfahren. Nach diesen zwei Schritten können die Zeitpläne, Aufzeichnungen, Ereignisse und Alarme für die Geräte auf den entsprechenden Seiten konfiguriert werden. Der letzte Schritt ist die Konfiguration der Benutzergruppen auf der Seite „Benutzergruppen“. Nach der Konfiguration aller Seiten von links nach rechts ist alles konfiguriert und der Bediener kann Operator Client starten.
Speichern Sie die Konfiguration nach dem Konfigurieren jeder Seite, indem Sie im Menü „Werkzeuge“ auf klicken.

Klicken Sie auf , um die Änderungen in BVMS Operator Client sichtbar zu machen.



1	Menüleiste	Dient zum Auswählen eines Menübefehls.
2	Seitenleiste	Dient zum Konfigurieren aller notwendigen Schritte von links nach rechts.
3	Werkzeugleiste	Zeigt die verfügbaren Schaltflächen der jeweiligen aktiven Registerkarte an. Bewegen Sie den Mauszeiger über ein Symbol, um die QuickInfo anzuzeigen.
4	Suchleiste	Dient zum Suchen eines bestimmten Geräts und seiner entsprechenden übergeordneten Elemente im Gerätebaum.
5	Hilfesymbol	Zeigt die Online-Hilfe für BVMS Configuration Client an.
6	Auswahlfenster	Hierarchische Liste aller verfügbaren Geräte im System.
7	Konfigurationsfenster	Dient zum Konfigurieren des ausgewählten Geräts.

BVMS Operator Client



1	Menüleiste	Dient zum Auswählen eines Menübefehls.
2	Symbolleiste	Zeigt die verfügbaren Schaltflächen an. Zeigen Sie zum Anzeigen der QuickInfo auf ein Symbol.
3	Wiedergabesteuerung	Dient zum Steuern der zeitversetzten Wiedergabe, einer Kamerasequenz oder einer Alarmsequenz.
4	Performance-Messung	Zeigt die CPU-Auslastung an.
5	Symbol für die Benutzeranmeldung	Zeigt den Anfangsbuchstaben des Benutzernamens des angemeldeten Benutzers an. Bewegen Sie den Mauszeiger über das Symbol, um den Benutzernamen und die entsprechende Benutzergruppe anzuzeigen.. wenn konfiguriert in Configuration Client, werden auch der vollständige Name und die Beschreibung des Benutzers angezeigt (nur verfügbar für Benutzer, die als BVMS Benutzer. Nicht verfügbar für Benutzer, die angemeldet sind als Windows Benutzer, LDAP Nutzer oder über einen externen Identity provider). Bei doppelter Berechtigung wird für jeden angemeldeten Benutzer ein Anmeldesymbol angezeigt, das die Benutzerinformationen und die entsprechende doppelte Berechtigungsgruppe enthält.
6	Zeitzonen-Auswahl	Wählen Sie einen Eintrag für die Zeitzone, die in den meisten entsprechenden Feldern angezeigt werden soll. Nur verfügbar, wenn sich mindestens ein Management Server oder eine unmanaged site im Logischen Baum in einer anderen Zeitzone als Ihr Operator Client befindet.
7	Steuerung für Bildfenster	Dient zum Auswählen der gewünschten Anzahl von Bildfenstern und zum Schließen aller Bildfenster.
8	Bildfensterbereich	Zeigt die Bildfenster an. Dient zum Anordnen der Bildfenster.
9	Bildfenster	Zeigt eine Kamera, eine Karte, ein Bild oder ein Dokument (HTML-Datei) an.
10	Fenster **Alarmliste**	Zeigt sämtliche vom System erzeugten Alarme an. Dient zum Annehmen oder Löschen von Alarmen oder zum Starten eines Workflows, beispielsweise durch Senden einer E-Mail an einen Techniker. Die Alarmliste wird nicht angezeigt, wenn die Verbindung zum Management Server unterbrochen ist.
11	Fenster **PTZ-Bedienfeld**	Dient zum Steuern einer PTZ-Kamera.
12	Fenster **Logischer Baum**	Zeigt die Geräte an, auf die Ihre Benutzergruppe Zugriff hat. Dient zum Auswählen eines Geräts, um es einem Bildfenster zuzuweisen.

	Fenster **Favoritenbaum**	Dient dazu, die Geräte des Logischen Baums Ihren Bedürfnissen entsprechend zu strukturieren.
	Fenster **Lesezeichen**	Dient zum Verwalten von Lesezeichen.
	Fenster **Karte**	Zeigt einen Lageplan an. Dient zum Ziehen der Karte, um einen bestimmten Kartenausschnitt anzuzeigen. Wenn Sie diese Option aktivieren, wird automatisch für jede in einem Bildfenster angezeigte Kamera eine Karte angezeigt. In diesem Fall muss die Kamera auf einer Karte konfiguriert werden.

3.1 BVMS Versionen

Die verschiedenen Versionen von BVMS sind vollständig skalierbar, damit Sie Ihr Videoüberwachungssystem Ihren Anforderungen entsprechend erweitern können.
Die folgenden Versionen von BVMS stehen zur Auswahl:

- BVMS Professional
- BVMS Enterprise
- BVMS Plus
- BVMS Lite
- BVMS Viewer

BVMS Viewer und BVMS Professional sind Software-Only-Produkte. Sie können nicht mit Bosch DIVAR IP Geräten verwendet werden.
Sie können BVMS Lite und BVMS Plus mit Bosch DIVAR IP Geräten oder als Software-Only-Produkte mit jeder anderen Hardware verwenden.
Ausführliche Informationen zu den verschiedenen Versionen von BVMS finden Sie unter www.boschsecurity.com und in der BVMS Schnellauswahlhilfe:
BVMS Schnellauswahlhilfe.

3.2 Überblick über die BVMS Lizenzaktivierung

Dieses Kapitel gibt einen Überblick über die Lizenzaktivierung von BVMS.

Lizenzbestellung

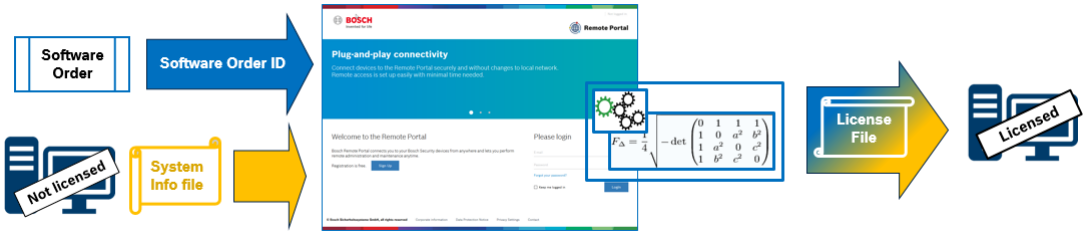
- Bestellen Sie Lizenzen am Bosch Order Desk.
- Die Bestellbestätigung beinhaltet die neue Softwarebestell-ID, die für den späteren Softwareaktivierungsprozess erforderlich ist.
- Ab BVMS 11.0 sind die BVMS Basis- und Erweiterungslizenzen nicht mehr von der Softwareversion abhängig.

Lizenzaktivierung

- Das Bosch Remote Portal (https://www.remote.boschsecurity.com) ersetzt den Bosch **Lizenz-Manager**.
- Für das Bosch Remote Portal ist eine neue Benutzerregistrierung erforderlich.
- Für die Lizenzaktivierung müssen die Systeminformationsdatei und die Softwarebestell-ID bereitgestellt werden.
- Remote Portal gibt die Lizenzdatei und alle Details zur Aktivierung aus. Fügen Sie diese Datei zum installierten BVMS System hinzu.

– Der Aktivierungsprozess legt das Startdatum des Softwareversicherungszeitraums fest. Das Enddatum wird im **Lizenz-Manager** des BVMS Configuration Client angezeigt.

Aktivierungsprozess für die Softwarelizenz



Gehen Sie wie folgt vor, um Ihre Softwarelizenzen zu aktivieren:

1. Bestellen Sie die Softwareprodukte
– Bestellen Sie Ihre Softwareprodukte entsprechend dem üblichen Bosch Bestellvorgang.
– Softwarebestellungen können aus einem oder mehreren Produkten einer oder mehrerer Produktversionen bestehen.
2. Erhalt der Softwarebestell-ID
– Nach der Bestellung erhalten Sie eine Softwarebestellbestätigung, in der die Softwarebestell-ID enthalten ist.
– Mit der Softwarebestell-ID können Sie die installierte Software (auf einem Betriebssystem und Hardware) mit den bestellten Softwareprodukten verbinden.
3. Aktivieren Sie die Lizenz
– Für die Lizenzaktivierung muss die Systeminformationsdatei bereitgestellt werden, die das eindeutige Betriebssystem und die Hardware enthält, auf dem bzw. der die Software installiert wird.
– Bei der Aktivierung wird die Softwarebestell-ID mit der installierten Software verknüpft und die Lizenzdatei wird erstellt.
– Die Aktivierung legt Systemattribute wie Start- und Enddatum der Softwareversicherung fest.
4. Aktivieren Sie die Software
– Zur Aktivierung der Software müssen Sie die Lizenzdatei zur installierten Software hinzufügen.
– Durch Hinzufügen der Lizenzdateien werden die BVMS Funktionen entsprechend der aktivierten Elemente verfügbar gemacht.

Hinweis!
Die Lizenzdatei enthält die folgenden Aktivierungsdetails:
– BVMS Produktversion
– Zulässige BVMS Version
– Ablaufdatum der Softwareversicherung
– Nummer der Erweiterungs-/Funktionslizenz

Siehe
– *Aktivieren der Softwarelizenzen, Seite 74*

4 Systemüberblick

Hinweis!
In diesem Dokument werden einige Funktionen beschrieben, die nicht für BVMS Viewer verfügbar sind.
Ausführliche Informationen zu den verschiedenen Versionen von BVMS finden Sie unter www.boschsecurity.com und in der BVMS Schnellauswahlhilfe: BVMS Schnellauswahlhilfe.

Wenn Sie planen, BVMS zu installieren und zu konfigurieren, empfehlen wir Ihnen eine Systemschulung zu BVMS.
Nähere Informationen zur aktuellen BVMS Version für unterstützte Versionen von Firmware und Hardware sowie weitere wichtige Informationen finden Sie in den Versionshinweisen.
Siehe Datenblätter zu Bosch Arbeitsstationen und Servern für Informationen zu Computern, auf denen BVMS installiert werden kann.
Die BVMS Software-Module können optional auf einem einzelnen PC installiert werden.

Wichtige Komponenten

Komponente	Beschreibung
Management Server (wählbar in Setup)	Stream-Verwaltung, Alarmverwaltung, Prioritätenverwaltung, Management-Logbuch, Benutzerverwaltung, Gerätezustandsverwaltung. Zusätzliche Enterprise System Lizenz: Verwalten von Enterprise User Groups und Enterprise Accounts.
Config Wizard	Einfache und schnelle Einrichtung eines Aufzeichnungssystems.
Configuration Client (wählbar in Setup)	Systemkonfiguration und -verwaltung für Operator Client.
Operator Client (wählbar in Setup)	Live-Überwachung, Abrufen und Wiedergabe von Aufzeichnungen, Alarm und gleichzeitiger Zugriff auf mehrere Management Server-Computer.
Video Recording Manager (wählbar in Setup)	Verteilen von Speicherkapazitäten auf iSCSI-Geräten zu den Encodern bei gleichzeitigem Lastenausgleich zwischen mehreren iSCSI-Geräten. Streaming von aufgezeichneten Video- und Audiodaten von iSCSI zu Operator Clients.
Web Client	Zugriff auf Live- und aufgezeichnete Videos über Webbrowser.
Mobile App	Zugriff auf Live- und aufgezeichnete Videos über die Mobile App auf iPhone oder iPad.
Bosch Video Streaming Gateway (wählbar in Setup)	Bietet die Integration von Drittanbieter-Kameras, z. B. in Netzwerken mit geringer Bandbreite.
Cameo SDK (wählbar in Setup)	Das Cameo SDK dient zum Einbetten von Live- und aufgezeichneten BVMS Bildfenstern in Ihre externe Drittanbieter-Anwendung. Die Bildfenster folgen den BVMS basierten Benutzerfreigaben. Das Cameo SDK stellt eine Teilmenge der Funktionalitäten von BVMS Operator Client dar, mit denen Sie Anwendungen ähnlich dem Operator Client erstellen können.

Komponente	Beschreibung
Client Enterprise SDK	Das Client Enterprise SDK dient zur Steuerung und Überwachung des Verhaltens des Operator Client eines Enterprise System durch externe Anwendungen. Das SDK ermöglicht das Durchsuchen von Geräten, auf die über den laufenden, angeschlossenen Operator Client zugegriffen werden kann, sowie die Steuerung einiger UI-Funktionen.
Client SDK / Server SDK	Das Server SDK dient zur Steuerung und Überwachung des Management Server durch Skripte und externe Anwendungen. Sie können die Schnittstellen mit einem gültigen Administrator-Konto nutzen. Das Client SDK dient zur Steuerung und Überwachung des Operator Client durch externe Anwendungen und Skripte (Teil der zugehörigen Server-Konfiguration).

4.1 Hardware-Anforderungen

Siehe Datenblatt zu BVMS. Datenblätter für Plattform-PCs sind ebenfalls verfügbar.

4.2 Software-Anforderungen

Sie können BVMS Viewer nicht installieren, wo eine andere BVMS-Komponente installiert ist.
Siehe Datenblatt für BVMS.

4.3 Lizenzanforderungen

Weitere Informationen zu den verfügbaren Lizenzen finden Sie im Datenblatt für BVMS.

5 Konzepte

Hinweis!
BVMS Viewer bietet nur Grundfunktionen. Erweiterte Funktionen sind in BVMS Professional enthalten. Ausführliche Informationen zu den verschiedenen Versionen von BVMS finden Sie unter www.boschsecurity.com und in der BVMS Schnellauswahlhilfe: BVMS Schnellauswahlhilfe.

Dieses Kapitel enthält Hintergrundinformationen zu ausgewählten Themen.

5.1 BVMS Designkonzepte

System mit einem Management Server, Seite 24
Ein einzelnes BVMS Management Server-System ermöglicht die Verwaltung, Überwachung und Steuerung von bis zu 2000 Kameras bzw. Encodern.

Enterprise System, Seite 25
Ein Enterprise Management Server bietet den gleichzeitigen Zugriff auf mehrere Management Servers. Das Enterprise System ermöglicht den vollen Zugriff auf Ereignisse und Alarme von mehreren Subsystemen.

Server Lookup, Seite 26
Die Server Lookup-Funktion stellt dem BVMS Operator Client eine Liste der verfügbaren BVMS Management Servers bereit. Der Bediener kann einen Server aus der Liste der verfügbaren Server auswählen. Wenn er mit einem Management Server verbunden ist, hat der Client vollen Zugriff auf den Management Server.

Unmanaged Site, Seite 28
Geräte können unmanaged sites zugeordnet werden. Geräte unter unmanaged sites werden nicht vom Management Server überwacht. Der Management Server stellt dem Operator Client eine Liste der unmanaged sites bereit. Der Bediener kann sich nach Bedarf mit dem Standort verbinden und erhält Zugriff auf Live- und aufgezeichnete Videodaten. Ereignis- und Alarmverarbeitung sind beim unmanaged site-Konzept nicht verfügbar.

5.1.1 System mit einem Management Server

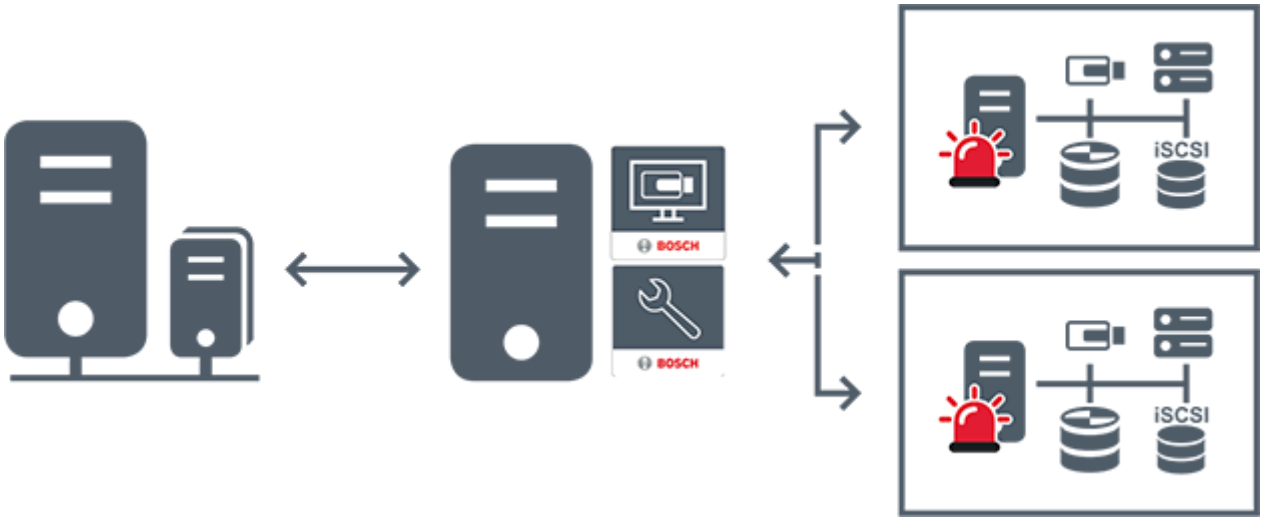
- Ein einzelner BVMS Management Server kann bis zu 2000 Kanäle verwalten.
- Ein BVMS Management Server stellt Funktionen zur Verwaltung, Überwachung und Steuerung des gesamten Systems bereit.
- Der BVMS Operator Client ist mit dem Management Server verbunden und empfängt Ereignisse und Alarme vom BVMS Management Server und zeigt Live- und aufgezeichnete Inhalte an.
- In den meisten Fällen befinden sich alle Geräte in einem Local Area Network mit einer hohen Bandbreite und einer geringen Latenz.

Zuständigkeiten:
- Konfigurieren von Daten
- Ereignisprotokoll (Logbuch)
- Benutzerprofile
- Benutzerprioritäten
- Lizenzierung
- Ereignis- und Alarmmanagement

	Live, Wiedergabe, Ereignisse, Alarme
	Management Server
	Operator Client / Configuration Client
	Kameras
	VRM
iSCSI	iSCSI
	Andere Geräte

5.1.2 Enterprise System

- Das Ziel eines BVMS Enterprise System besteht darin, einem Benutzer des Operator Client zu ermöglichen, gleichzeitig auf mehrere Management Servers (Subsysteme) zuzugreifen.
- Mit einem Enterprise-Server verbundene Clients haben vollen Zugriff auf alle Kameras und Aufzeichnungen der Subsysteme.
- Mit einem Enterprise-Server verbundene Clients werden in Echtzeit umfassend über Ereignisse und Alarme aller Subsysteme informiert.
- Typische Anwendungsbereiche:
  - U-Bahnen
  - Flughäfen



	Live, Wiedergabe, Ereignisse, Alarme
	BVMS Enterprise Management Server
	BVMS Operator Client / Configuration Client
	BVMS Subsystem

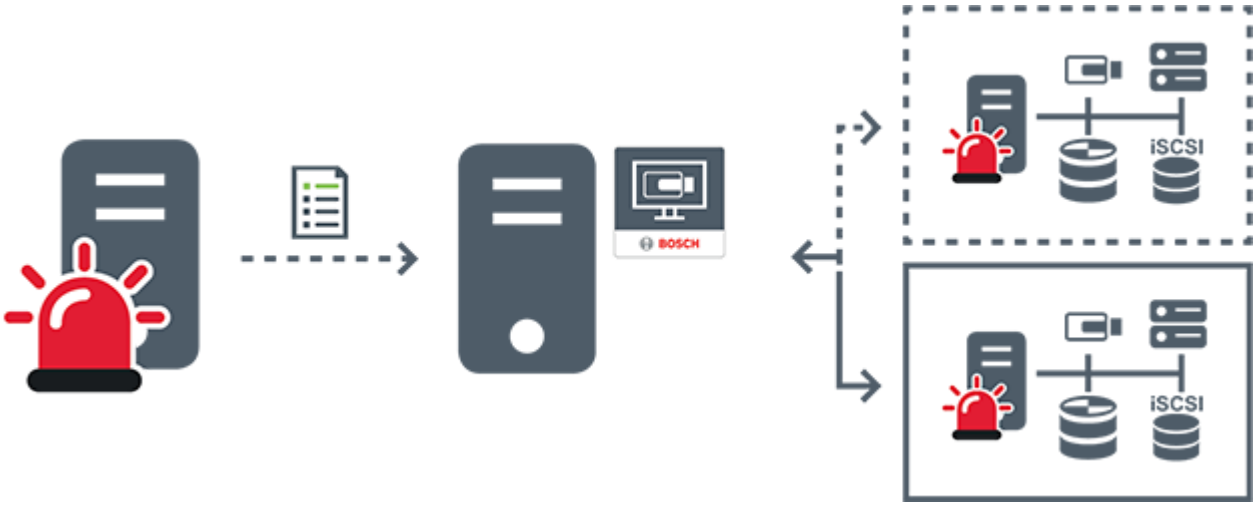
Siehe

- *Erstellung eines Enterprise Systems, Seite 85*
- *Konfigurieren der Serverliste für Enterprise System, Seite 85*
- *Konfigurieren von Benutzern, Berechtigungen und Enterprise Access, Seite 357*
- *Systemzugriff, Seite 73*

5.1.3 Server Lookup

- Mit der BVMS Server Lookup-Funktion können Benutzer eine Verbindung mit einem BVMS Management Server aus einer bereitgestellten Server-Liste herstellen.
- Ein einzelner Benutzer von Configuration Client oder Operator Client kann nacheinander zu mehreren System-Access Points eine Verbindung herstellen.
- System-Access Points können entweder Management Server oder Enterprise Management Server sein.
- Server Lookup verwendet dedizierte Management Server zum Hosten der Server-Liste.
- Server Lookup und Management Server oder Enterprise Management Server können funktional auf einem Computer ausgeführt werden.
- Server Lookup unterstützt Sie bei der Suche von System-Access Points durch ihren Namen oder Beschreibungen.

– Sobald der Operator Client mit dem Management Server verbunden ist, empfängt er Ereignisse und Alarme vom BVMS Management Server und zeigt Live- und aufgezeichnete Inhalte an.



	Live auf Abruf, Wiedergabe, Ereignisse, Alarme – verbunden
	Live auf Abruf, Wiedergabe, Ereignisse, Alarme – nicht verbunden
	Management Server
	Server-Liste
	Operator Client
	Verbundenes BVMS aus Server-Liste
	Nicht verbundenes BVMS aus Server-Liste

Siehe

- *Konfigurieren von Server Lookup, Seite 130*
- *Seite „Server-Liste/Adressbuch“, Seite 129*
- *Mittels Server Lookup, Seite 73*
- *Export der Server-Liste, Seite 131*
- *Import einer Server-Liste, Seite 131*

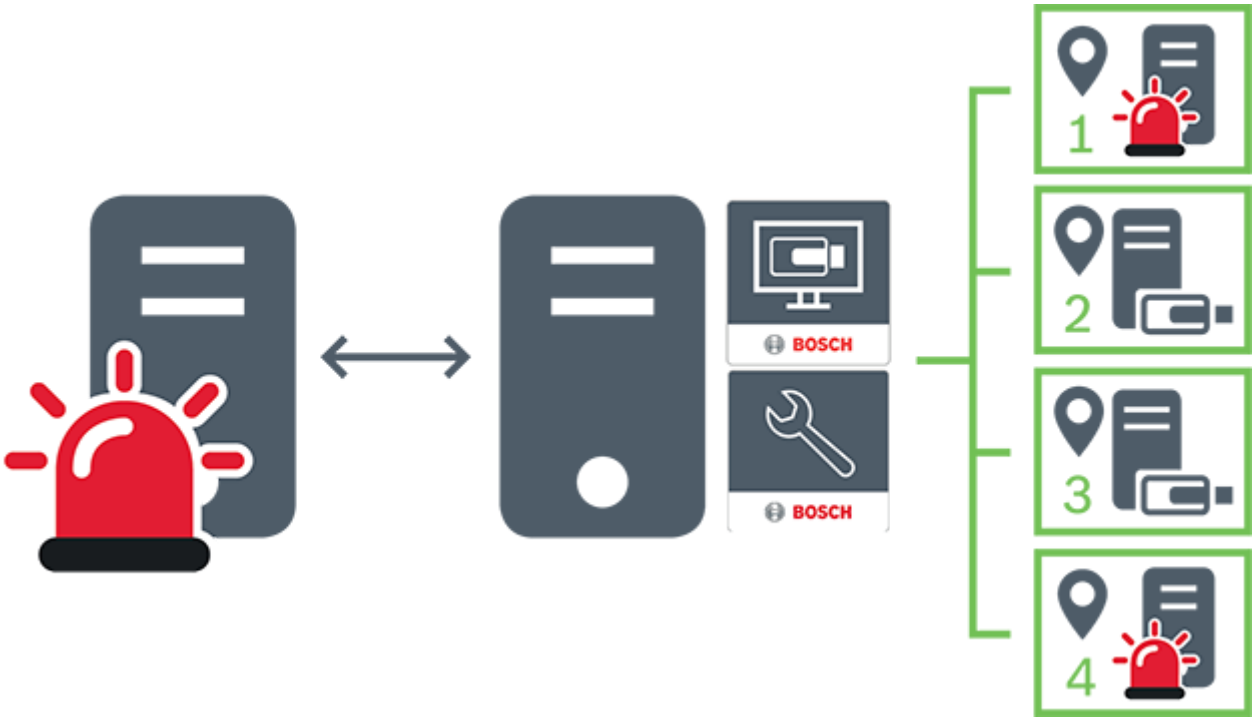
5.1.4 Unmanaged Site

- Eine Systemdesignoption im BVMS mit einer großen Anzahl kleiner Subsysteme.
- Es ermöglicht die Konfiguration von bis zu 9999 Standorten auf einem BVMS Management Server.
- Bediener können auf Live- und aufgezeichnete Videodaten von bis zu 20 sites gleichzeitig zugreifen.
- sites können für eine einfache Navigation in Ordnern gruppiert oder auf Karten platziert werden. Vordefinierte Benutzernamen und Passwörter ermöglichen Bedienern die schnelle Verbindung mit einer site.

Das unmanaged site-Konzept unterstützt IP-basierte BVMS Systeme sowie analoge DVR-Lösungen:

- Bosch DIVAR AN 3000/5000 analoge Rekorder
- DIVAR hybrid Rekorder
- DIVAR network Rekorder
- DIP 3000/7000 Geräte mit IP-basierter Aufzeichnung
- System mit einem BVMS Management Server

Das Hinzufügen einer site für die zentrale Überwachung erfordert nur eine Lizenz pro site und ist nicht von der Anzahl der Kanäle am site abhängig.



⟷	Live, Wiedergabe, Ereignisse, Alarme
▬	Datenverkehr durch Live-Videos auf Abruf und Wiedergabe
	Management Server

	Operator Client / Configuration Client
	site
	DVR

Siehe

– *Manuelles Hinzufügen einer Unmanaged Site, Seite 214*

5.2 Aufzeichnung

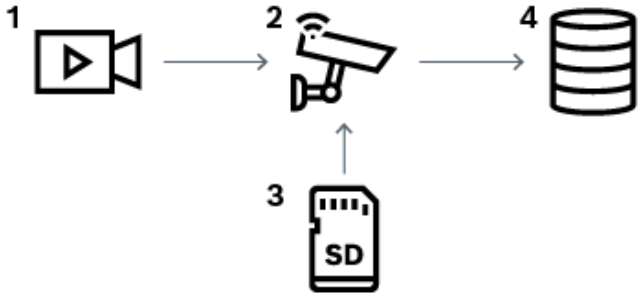
In diesem Kapitel werden die verschiedenen Aufzeichnungs- und Wiedergabefunktionen im System erläutert.

5.2.1 Automated Network Replenishment (ANR)

Hinweis!
BVMS Viewer bietet nur Grundfunktionen. Erweiterte Funktionen sind in BVMS Professional enthalten. Ausführliche Informationen zu den verschiedenen Versionen von BVMS finden Sie unter www.boschsecurity.com und in der BVMS Schnellauswahlhilfe: BVMS Schnellauswahlhilfe.

Vorgesehene Verwendung

Tritt ein Netzwerkfehler oder Fehler bei der zentralen Speicherung auf, wird über die ANR-Funktion sichergestellt, dass der Encoder die lokal zwischengespeicherte Aufzeichnung des fehlenden Zeitraums an die zentrale Speicherung überträgt, nachdem der Fehler behoben wurde.
Die nachfolgende Grafik zeigt die Übertragung von Videodaten, nachdem ein Netzwerk- oder Speicherfehler behoben wurde.



1	Video
2	Encoder, IP-Netzwerk
3	SD-Karte (Ringspeicher)

4	iSCSI-Ziel (zentrale Speicherung)

Beispiel: Behebung eines Netzwerkfehlers
Fällt das Netzwerk unerwartet aus, wird dank dieser ANR-Funktion die zentrale Speicherung mit der lokal zwischengespeicherten Aufzeichnung ergänzt, sobald das Netzwerk wieder zur Verfügung steht.

Beispiel: Speicherung von Videodaten, wenn das Netzwerk nicht zur Verfügung steht
Sobald sich eine U-Bahn zwischen zwei Stationen befindet, steht keine Netzwerkverbindung mit der zentralen Speicherung zur Verfügung. Nur an den Haltestellen kann die zwischengespeicherte Aufzeichnung an die zentrale Speicherung übertragen werden.
Stellen Sie sicher, dass die Zeitspanne, die für die Übertragung der zwischengespeicherten Aufzeichnung erforderlich ist, nicht die Verweildauer der Bahn an der Haltestelle übersteigt.

Beispiel: ANR für die Alarmaufzeichnung
Die Voralarmaufzeichnung wird lokal gespeichert. Nur im Falle eines Alarms wird die Voralarmaufzeichnung an die zentrale Speicherung übertragen. Tritt kein Alarm auf, wird die alte Voralarmaufzeichnung nicht an die zentrale Speicherung übertragen und somit das Netzwerk nicht belastet.

Beschränkungen

Hinweis!
Sind am Encoder für die Berechtigungsstufen „User“ und „Live“ Passwörter eingerichtet, können Sie die Wiedergabe aus den lokalen Speichermedien nicht nutzen. Entfernen Sie gegebenenfalls das Passwort.

Die ANR-Funktion ist nur zusammen mit der VRM-Aufzeichnung möglich.
Die ANR Funktion funktioniert nicht mit einem Encoder, bei dem eine sichere Verbindung zur Live-Anzeige konfiguriert ist.
Um die ANR-Funktion nutzen zu können, müssen Sie die Speichermedien des Encoders entsprechend konfigurieren.
Der Encoder, bei dem Sie die ANR-Funktion konfigurieren möchten, muss die Firmware-Version 5.90 oder höher besitzen. Nicht alle Encoder-Typen unterstützen die ANR-Funktion.
Bei einer dualen Aufzeichnung können Sie die ANR-Funktion nicht nutzen.
Das iSCSI-Speichersystem muss ordnungsgemäß konfiguriert sein.
In der nachfolgenden Liste sind mögliche Gründe aufgeführt, warum die ANR-Funktion nicht konfiguriert werden kann.

- Der Encoder ist nicht erreichbar (falsche IP-Adresse, Netzwerkfehler usw.).
- Die Speichermedien des Encoders sind nicht verfügbar oder schreibgeschützt.
- Falsche Firmware-Version
- Der Encoder-Typ unterstützt die ANR-Funktion nicht.
- Es läuft eine duale Aufzeichnung.

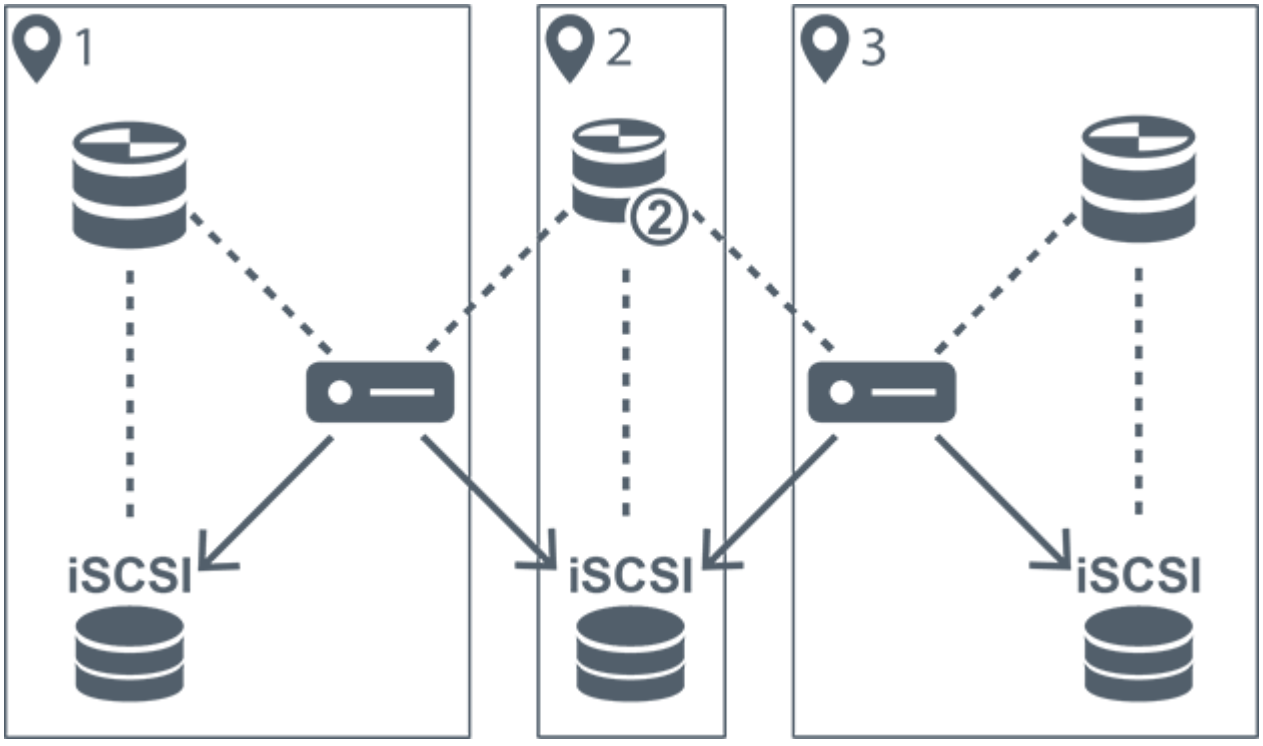
Siehe

- *Konfigurieren eines iSCSI-Geräts, Seite 194*
- *Speichermedien eines Encoders konfigurieren, Seite 83*
- *ANR-Funktion konfigurieren, Seite 308*

5.2.2 Duale/Failover-Aufzeichnung

Vorgesehene Verwendung

Ein primärer VRM verwaltet die normale Aufzeichnung der Kameras Ihres Systems. Für eine duale Aufzeichnung der Kameras verwenden Sie einen Sekundären VRM.
Die duale Aufzeichnung dient zum Speichern von Videodaten von derselben Kamera an unterschiedlichen Orten.
Die duale Aufzeichnung wird gewöhnlich mit unterschiedlichen Stream-Einstellungen und Aufzeichnungsmodi durchgeführt. Als Sonderfall der dualen Aufzeichnung kann die gespiegelte Aufzeichnung konfiguriert werden: Dabei wird dasselbe Videosignal zweimal an unterschiedlichen Orten aufgezeichnet.
Die duale Aufzeichnung erfolgt über die Verwendung von 2 VRM Servern, die mehrere, sich an unterschiedlichen Orten befindende iSCSI-Geräte verwalten.
Ein Sekundärer VRM kann die sekundäre Aufzeichnung für mehrere Primäre VRMs verwalten.
Der Benutzer kann zwischen den Aufzeichnungen, die vom Primären VRM und vom Sekundären VRM verwaltet werden, wählen. Bei einer einzelnen Kamera kann der Benutzer zwischen den Aufzeichnungen des Sekundären bzw. Primären VRM wechseln. Darüber hinaus kann sich der Benutzer die vom Primären VRM und Sekundären VRM verwalteten Aufzeichnungen der gleichen Kamera gleichzeitig anzeigen lassen.
Für eine duale Aufzeichnung muss bei der Einrichtung ein Sekundärer VRM installiert werden.
Ein Failover-VRM wird für die Fortsetzung der Aufzeichnung eines ausgefallenen Primären oder Sekundären VRM-Computers verwendet.
In der folgenden Grafik ist ein Beispiel für ein duales Aufzeichnungsszenario dargestellt:



1	Standort 1		Encoder
2	Zentraler Standort	iSCSI	iSCSI-Speichergerät

3	Standort 2	-------	Steuerungsverbindung
	Primärer VRM	⟶	Video-Stream
	Sekundärer VRM		

Beschränkungen

Sie können die duale Aufzeichnung nicht zusammen mit der ANR-Funktion nutzen.

Das Cameo SDK unterstützt nur die Wiedergabe der primären Aufzeichnung.

Siehe

- *Duale Aufzeichnung in der Kameratabelle konfigurieren, Seite 308*
- *Manuelles Hinzufügen eines gespiegelten VRM, Seite 177*
- *Manuelles Hinzufügen eines Failover-VRM, Seite 177*
- *Seite Kameras, Seite 290*

5.2.3 VRM-Aufzeichnungsmodi

Dieses Kapitel enthält Grafiken, um mögliche VRM-Aufzeichnungsmodi zu veranschaulichen.

Liste möglicher VRM-Aufzeichnungsmodi:

- Primärer-VRM-Aufzeichnung
- Gespiegelte VRM-Aufzeichnung
- Sekundärer-VRM-Aufzeichnung
- Failover-VRM-Aufzeichnung

Für eine ANR-Aufzeichnung siehe Kapitel *Automated Network Replenishment (ANR), Seite 29*.

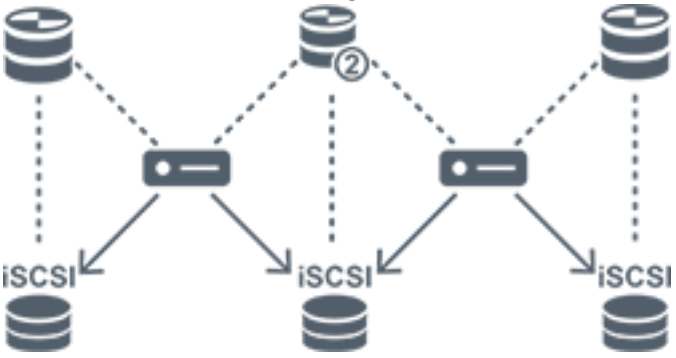
Primär-VRM-Aufzeichnung

	Primärer VRM	-------	Steuerungsverbindung
iSCSI	iSCSI-Speichergerät	⟶	Video-Stream
	Encoder		

Gespiegelte VRM-Aufzeichnung

	Primärer VRM		Sekundärer VRM
	iSCSI-Speichergerät		Steuerungsverbindung
	Encoder		Video-Stream

Sekundärer-VRM-Aufzeichnung



	Primärer VRM		Sekundärer VRM
	iSCSI-Speichergerät		Steuerungsverbindung
	Encoder		Video-Stream

Failover-VRM-Aufzeichnung

	Primärer VRM		Primärer Failover-VRM
	iSCSI-Speichergerät		Encoder
	Steuerungsverbindung		Video-Stream

5.2.4 Wiedergabe von VRM-Aufzeichnungsquellen

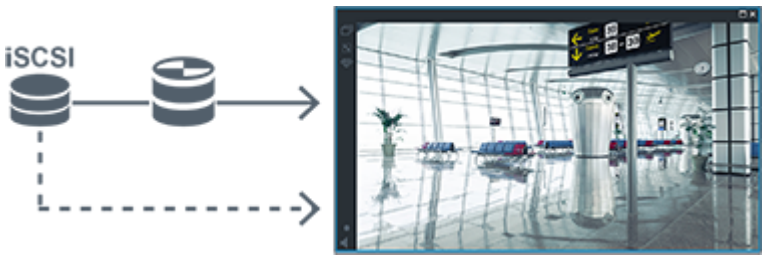
Die nachfolgenden Grafiken zeigen Bildfenster, in denen die Wiedergabe aller möglichen VRM-Aufzeichnungsquellen dargestellt ist. Als ein Beispiel für die Wiedergabe ist in jeder Grafik das Speichergerät, die VRM-Instanz (sofern verfügbar) und ein Ausschnitt eines Bildfensters zu sehen. Gegebenenfalls wird die Aufzeichnungsquelle durch ein entsprechendes Symbol in der Bildfensterleiste gekennzeichnet.

- *Wiedergabe einer einzelnen Aufzeichnung, Seite 34*
- *Wiedergabe einer dualen VRM-Aufzeichnung, Seite 35*
- *Wiedergabe einer Primärer VRM-Aufzeichnung mit optionalem Failover-VRM, Seite 35*
- *Wiedergabe einer Sekundär-VRM-Aufzeichnung mit optionalem Failover-VRM, Seite 36*
- *Automatic Network Replenishment, Seite 37*

Wiedergabe einer einzelnen Aufzeichnung

Dieses Bildfenster wird angezeigt, wenn nur ein Primärer VRM konfiguriert wurde. Sie können keine andere Aufzeichnungsquelle auswählen.

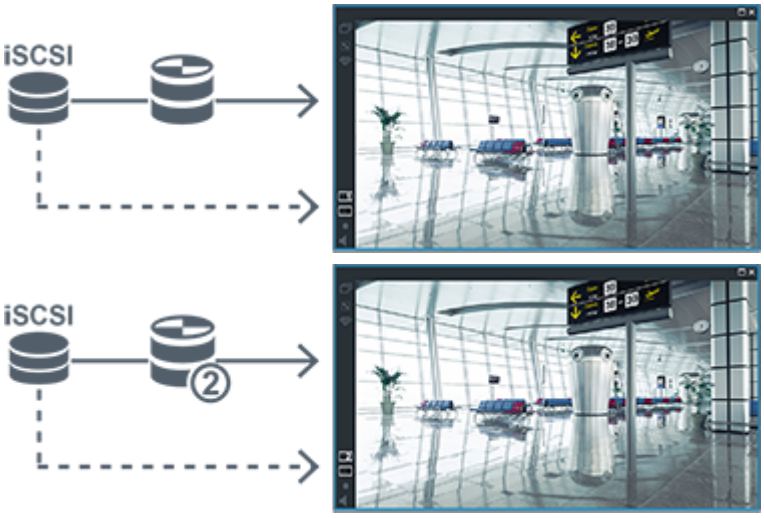
: Falls die Wiedergabe für diese Arbeitsstation konfiguriert ist, erfolgt sie direkt durch das iSCSI-Speichergerät.



	iSCSI-Speichergerät
	Primärer VRM

Wiedergabe einer dualen VRM-Aufzeichnung

Es sind ein Primärer VRM und ein Sekundärer VRM konfiguriert. Klicken Sie auf das Aufzeichnungsquellensymbol, um sich eine primäre oder sekundäre Wiedergabe anzeigen zu lassen. Falls die Wiedergabe für diese Arbeitsstation konfiguriert ist, erfolgt sie direkt durch das iSCSI-Speichergerät.



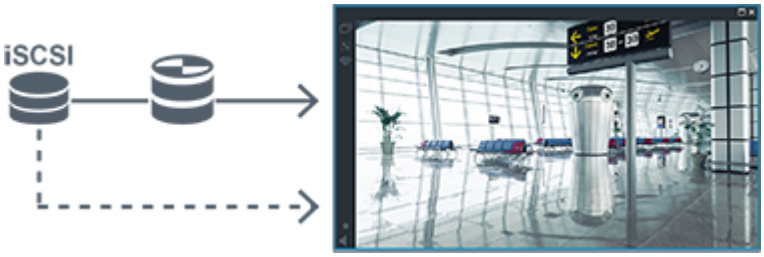
	iSCSI-Speichergerät
	Primärer VRM
	Sekundärer VRM

Wiedergabe einer Primärer VRM-Aufzeichnung mit optionalem Failover-VRM

Eine Wiedergabe ist möglich, während der Primäre VRM in Betrieb ist. Der Failover-VRM befindet sich im Ruhezustand.

Falls die Wiedergabe für diese Arbeitsstation konfiguriert ist, erfolgt sie direkt durch das iSCSI-Speichergerät.

Wurde eine Sekundär-VRM- oder ANR-Aufzeichnung konfiguriert, können Sie die Aufzeichnungsquelle umschalten.



Ist der Primäre VRM nicht angeschlossen, ist eine Wiedergabe über den konfigurierten Failover-VRM möglich. Schließen Sie das Bildfenster und lassen Sie sich die Kamera erneut in einem Bildfenster anzeigen:

Sind sowohl der Primäre VRM als auch der optionale Primäre Failover-VRM nicht angeschlossen, ist eine Wiedergabe über den Encoder möglich. Schließen Sie das Bildfenster und lassen Sie sich die Kamera erneut in einem Bildfenster anzeigen:

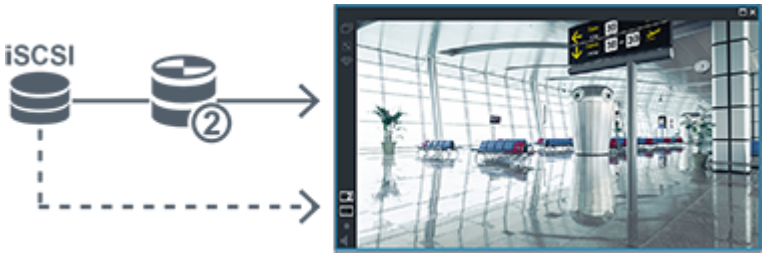
	iSCSI-Speichergerät
	Primärer VRM
	Primärer Failover-VRM
	Encoder

Die Encoder-Wiedergabe ist nur für einen begrenzten Aufzeichnungszeitraum möglich.

Wiedergabe einer Sekundär-VRM-Aufzeichnung mit optionalem Failover-VRM

Eine Wiedergabe ist möglich, während der Sekundäre VRM in Betrieb ist. Der Failover-VRM befindet sich im Ruhezustand.

Falls die Wiedergabe für diese Arbeitsstation konfiguriert ist, erfolgt sie direkt durch das iSCSI-Speichergerät.



Ist der Sekundäre VRM nicht angeschlossen, ist eine Wiedergabe über den konfigurierten Failover-VRM möglich. Schließen Sie das Bildfenster und lassen Sie sich die Kamera erneut in einem Bildfenster anzeigen:

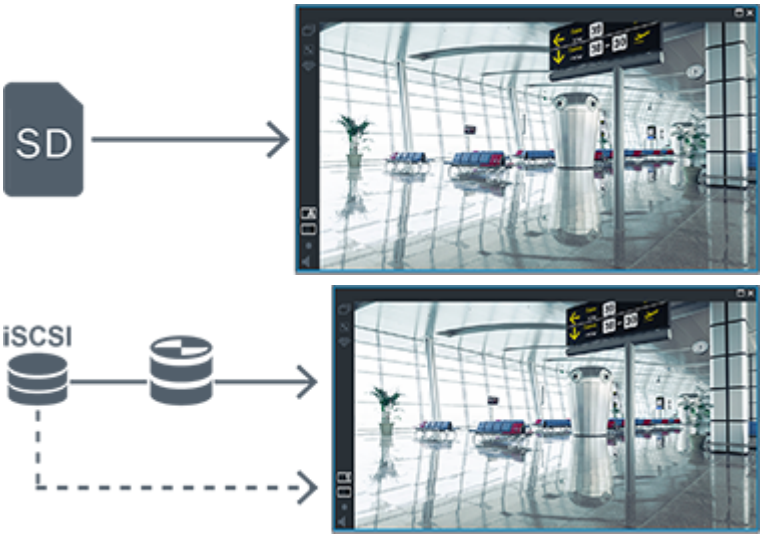
Sind sowohl der Sekundäre VRM als auch der optionale Sekundäre Failover-VRM nicht angeschlossen, ist eine Wiedergabe über den Encoder möglich. Schließen Sie das Bildfenster und ziehen Sie die Kamera erneut zu einem Bildfenster:

iSCSI	iSCSI-Speichergerät
	Primärer VRM
	Sekundärer Failover-VRM
	Encoder

Die Encoder-Wiedergabe ist nur für einen begrenzten Aufzeichnungszeitraum möglich.

Automatic Network Replenishment

ANR ist konfiguriert. Klicken Sie auf das Aufzeichnungsquellensymbol, um sich die primäre (primäre Failover-Wiedergabe, primäre Encoder-Wiedergabe) oder die ANR-Wiedergabe anzeigen zu lassen. Falls die Wiedergabe für diese Arbeitsstation konfiguriert ist, erfolgt sie direkt durch das iSCSI-Speichergerät.



	iSCSI-Speichergerät
	Primärer VRM
	SD-Karte

5.2.5 Überblick über speicherbezogene Ereignisse

In diesem Kapitel werden die verschiedenen speicherbezogenen Ereignisse beschrieben.

Status lokales Speichermedium

Tritt ein Netzwerkfehler oder Fehler bei der zentralen Speicherung auf, wird über die ANR-Funktion sichergestellt, dass der Encoder die lokal zwischengespeicherte Aufzeichnung des fehlenden Zeitraums an die zentrale Speicherung überträgt, nachdem der Fehler behoben wurde.
Die Zwischenspeicherzustände sind:

- **Speicherstatus Unbekannt**
- **Speicherstatus OK**
- **Speicherstatus kritischer Füllstand lokales Speichermedium**
- **Speicherstatus Ausfall**

Überlauf lokales Speichermedium

Dieses Ereignis gibt an, dass der Zwischenspeicher bereits voll ist und die Aufzeichnung nicht mehr in den Zentralspeicher übertragen wird.

Speicherstatus / Status Sekundärer Speicher

Der **Speicherstatus** zeigt den Verbindungsstatus zwischen einer Kamera und dem Zentralspeicher an. Das Ereignis **Speicherstatus Ausfall** wird ausgelöst, wenn die Kamera die Verbindung zum Zentralspeicher verliert. Wenn die Verbindung nur für einen kurzen Moment getrennt ist, weist dieses Ereignis nicht zwingend darauf hin, dass Videodaten verloren gegangen sind.
Die Speicherzustände sind:

- **Speicherstatus Unbekannt**
- **Speicherstatus OK**
- **Speicherstatus Ausfall**

Status Überwachung Aufzeichnung / Status Überwachung Sekundäre Aufzeichnung

Dieses Ereignis weist auf eine Aufzeichnungsüberwachung hin. Solange die Kamera die Aufzeichnung im Arbeitsspeicher zwischenspeichern kann, wird kein Alarm ausgelöst. Das Ereignis **Status Überwachung der Aufzeichnung Aufzeichnungsverlust** wird nur ausgelöst, wenn innerhalb der letzten zwei Minuten keine Videodaten mehr im Arbeitsspeicher gespeichert werden konnten und verloren gegangen sind. Das Ereignis gibt außerdem den Zeitraum an, in dem Videodaten verloren gegangen sind.
Die Aufzeichnungsüberwachungszustände sind:

- **Status Überwachung der Aufzeichnung unbekannt**
- **Status Überwachung der Aufzeichnung OK**
- **Status Überwachung der Aufzeichnung Aufzeichnungsverlust**

Siehe

- *Automated Network Replenishment (ANR), Seite 29*
- *Konfigurieren von Ereignissen und Alarmen, Seite 323*

5.3 Alarmbearbeitung

Alarme können einzeln konfiguriert werden, um von einer oder mehreren Benutzergruppen bearbeitet zu werden. Wenn ein Alarm auftritt, wird er in der Alarmliste aller Benutzer angezeigt, die sich in den Benutzergruppen befinden, die für den Empfang dieses Alarms konfiguriert sind. Wenn einer dieser Benutzer mit der Bearbeitung des Alarms beginnt, wird der Alarm aus der Alarmliste der anderen Benutzer entfernt.
Alarme werden auf dem Monitor der Arbeitsstation angezeigt. Dieses Verhalten wird in den folgenden Abschnitten beschrieben.

Alarmfluss

1. Im System tritt ein Alarm auf.
2. In der Alarmliste aller für diesen Alarm konfigurierten Benutzer wird eine Alarmbenachrichtigung angezeigt. Das Alarmvideo wird sofort auf den konfigurierten Monitoren angezeigt. Wenn es sich um einen automatisch angezeigten Alarm (automatischen Popup-Alarm) handelt, wird das Alarmvideo ebenfalls automatisch auf den Alarmmonitoren der Operator Client Arbeitsstation angezeigt.
   Wenn ein Alarm als Auto-Löschen-Alarm konfiguriert ist, wird der Alarm nach der festgelegten Zeit für Auto-Löschen (konfiguriert im Configuration Client) aus der Alarmliste entfernt.
   Bei Monitoren werden Vierfachteilungen von VIP XDs vorübergehend durch Vollbildschirmanzeigen ersetzt.
3. Einer der Benutzer nimmt den Alarm an. Das Alarmvideo wird daraufhin auf der Arbeitsstation dieses Benutzers angezeigt (sofern es nicht bereits durch die automatische Popup-Funktion angezeigt wird). Der Alarm wird aus allen anderen Alarmlisten und Alarmvideoanzeigen entfernt.
4. Der Benutzer, der den Alarm angenommen hat, ruft einen Workflow auf, der das Lesen eines Aktionsplans und das Eingeben von Kommentaren beinhalten kann. Dieser Schritt ist optional. Die Anforderungen für den Workflow können vom Administrator konfiguriert werden.
5. Als letzten Schritt löscht der Benutzer den Alarm. Dadurch wird der Alarm aus seiner Alarmliste und der Alarmanzeige entfernt.
   Bei einer Monitorgruppe zeigen die Monitore wieder die Kameras an, die vor dem Alarm angezeigt wurden.

Alarmfensterbereich

1. Zur Anzeige eines Alarmvideos ersetzt der Alarmfensterbereich den Live- oder Wiedergabe-Bildfensterbereich auf dem für die Alarmanzeige konfigurierten Monitor.
2. Jedem Alarm wird eine Bildfensterreihe mit bis zu 5 Bildfenstern zugeordnet. In diesen Bildfenstern können Live-Videos, aufgezeichnete Videos oder Karten angezeigt werden.
   In einer Monitorgruppe wird ein Alarm in einer Reihe von Monitoren angezeigt. Die Anzahl der Kameras in der Reihe ist auf die Spaltenzahl in der Monitorgruppe begrenzt. Die nicht für die Alarmvideoanzeige verwendeten Monitore der Monitorreihe können so konfiguriert werden, dass die aktuelle Anzeige weiterläuft oder ein leerer Bildschirm angezeigt wird.
3. Sowohl bei Monitorreihen als auch bei Alarmreihen der Operator Client-Arbeitsstationsanzeige werden Alarme mit höherer Priorität über Alarmen mit niedrigerer Priorität angezeigt.
4. Wenn der Alarmfensterbereich keine Bildfensterreihen mehr aufnehmen kann, aber ein weiterer Alarm angezeigt werden muss, werden die Alarme mit der niedrigsten Priorität in der untersten Reihe des Alarmfensterbereichs „gestapelt“. Mit Hilfe der Bedienelemente links neben der Alarmreihe können Sie durch die gestapelten Alarme blättern.
   Bei Monitorgruppen erfolgt das Blättern durch einen Alarmstapel mithilfe der Bedienelemente im Fenster **Monitore** der Arbeitsstationsanzeige des Operator Client. Monitore mit aktueller Alarmanzeige werden durch ein rotes Symbol mit blinkender „LED“ gekennzeichnet.

Titel, Uhrzeit und Datum des Alarms können optional auf allen Monitoren oder nur auf dem ersten Monitor einer Alarmreihe angezeigt werden.

5. Für Alarme mit gleicher Priorität kann der Administrator die Reihenfolge konfigurieren:
   – LIFO-Modus (Last-in-First-out): Bei dieser Konfiguration werden neue Alarme *über* älteren Alarmen der gleichen Priorität eingefügt.
   – FIFO-Modus (First-in-First-out): Bei dieser Konfiguration werden neue Alarme *unter* älteren Alarmen der gleichen Priorität eingefügt.
6. Die Anzeige der Fensterreihe eines Alarms im Alarmfensterbereich erfolgt:
   – Bei der Alarmerzeugung (automatischer Popup-Alarm). Dies geschieht, wenn die Alarmpriorität höher als die Anzeigepriorität ist.
   – Bei Annahme des Alarms. Dies geschieht, wenn die Alarmpriorität niedriger als die Anzeigepriorität ist.

Automatische Popup-Alarme

Alarme können so konfiguriert werden, dass sie je nach Alarmpriorität automatisch im Alarmfensterbereich angezeigt werden (Popup). Der Live- und Wiedergabeanzeige der einzelnen Benutzergruppen wird ebenfalls eine Priorität zugeordnet. Wenn Alarme mit einer höheren Priorität als die der Benutzeranzeige eingehen, wird die Alarmreihe des Alarms automatisch im Alarmfensterbereich angezeigt. Wird der Alarmfensterbereich zurzeit nicht angezeigt, ersetzt er bei einem für den Alarm aktivierten Monitor automatisch den Live- oder Wiedergabe-Bildfensterbereich. Automatische Popup-Alarme werden zwar im Alarmfensterbereich angezeigt, sie werden jedoch nicht automatisch angenommen. Sie können auf den Anzeigen mehrerer Benutzer gleichzeitig angezeigt werden. Wenn ein Benutzer einen automatischen Popup-Alarm annimmt, wird der Alarm aus den Alarmlisten und Alarmanzeigen der anderen Benutzer entfernt.

Alarmverarbeitung bei einer Abschaltung

Beim Abschalten eines Servers werden alle anstehenden Alarme gespeichert. Die Alarme werden wiederhergestellt und werden nach dem Neustart des Systems wieder im Fenster **Alarmliste** angezeigt.

Alarme mit dem Status **Angenommen** oder **Workflow** werden beim Neustart des Systems automatisch in den Status **Aktiv** zurückgesetzt. Kommentare, die für Alarme im Status **Workflow** eingegeben wurden, werden gespeichert.

Hinweis!

Die Alarmdaten werden einmal pro Minute automatisch gespeichert, damit der maximale Datenverlust nur die innerhalb der letzten Minute aufgezeichneten Daten betrifft.

Siehe

– *Vor- und Nachalarmdauer bei einem Alarm konfigurieren, Seite 328*

5.4 Videoanalyse aktivieren/deaktivieren

Benutzer einer Benutzergruppe mit entsprechender Berechtigung können die Videoanalyse für bestimmte Kameras vorübergehend aktivieren bzw. deaktivieren.

So konfigurieren Sie die Berechtigung in Configuration Client:

– Hauptfenster > **Benutzergruppen** > Registerkarte **Benutzergruppen** > > Registerkarte **Bedienberechtigungen** > Registerkarte **Bediener Funktionen** > **Video Analysis aktivieren/ deaktivieren**

oder

– Hauptfenster > **Benutzergruppen** > Registerkarte **Enterprise User Groups** > > Registerkarte **Bedienberechtigungen** > Registerkarte **Bediener Funktionen** > **Video Analysis aktivieren/deaktivieren**

In Operator Client ist die Videoanalyse für alle Kameras standardmäßig aktiviert. Sie können die Funktion für eine einzelne Kamera oder für mehrere Kameras deaktivieren.

So deaktivieren Sie die Videoanalyse für eine einzelne Kamera:

1. Navigieren Sie in Operator Client im logischen Baum, im Favoritenbaum, in einem Bildfenster oder auf einem Lageplan zur gewünschten Kamera.
2. Klicken Sie mit der rechten Maustaste auf die Kamera und dann auf **Videoanalyse deaktivieren**.

   Die Videoanalyse ist deaktiviert, und das Symbol wird auf der Kamera angezeigt.

So deaktivieren Sie die Videoanalyse für mehrere Kameras:

1. Navigieren Sie in Operator Client zum Ordner im logischen Baum oder im Favoritenbaum, in dem die gewünschten Kameras enthalten sind.
2. Klicken Sie mit der rechten Maustaste auf den Ordner und anschließend auf **Videoanalyse deaktivieren**.

   Die Videoanalyse ist für alle Kameras in diesem Ordner deaktiviert, und das Symbol wird auf allen Kameras im Ordner angezeigt.

So aktivieren Sie die Videoanalyse für eine einzelne Kamera mit dem Status Videoanalyse: Deaktiviert:

1. Navigieren Sie in Operator Client im logischen Baum, im Favoritenbaum, in einem Bildfenster oder auf einem Lageplan zur gewünschten Kamera.
2. Klicken Sie mit der rechten Maustaste auf die Kamera und anschließend auf **Videoanalyse aktivieren**.

   Die Videoanalyse ist aktiviert, und das Symbol auf der Kamera wird nicht mehr angezeigt.

So aktivieren Sie die Videoanalyse für mehrere Kameras mit dem Status Videoanalyse: Deaktiviert:

1. Navigieren Sie in Operator Client zum Ordner im logischen Baum oder im Favoritenbaum, in dem die gewünschten Kameras enthalten sind.
2. Klicken Sie mit der rechten Maustaste auf den Ordner und anschließend auf **Videoanalyse aktivieren**.

   Die Videoanalyse ist für alle Kameras in diesem Ordner aktiviert, und das Symbol auf den Kameras wird nicht mehr angezeigt.

Hinweis!
Die Aktivierung/Deaktivierung der Videoanalyse in Operator Client ist nur möglich, wenn Operator Client mit dem Central Server verbunden ist.

Hinweis!
Die Aktivierung/Deaktivierung der Videoanalyse ist für ONVIF Profile G-Encoder nicht verfügbar.

Hinweis!
Nach dem Neustart von Operator Client oder Central Server wird die letzte Einstellung beibehalten.

5.5 ONVIF-Ereigniszuordnung

Hinweis!
Hinweis: Diese Funktion wird bald eingestellt.
Verwenden Sie das ONVIF Camera Event Driver Tool zur einfachen ONVIF-Ereigniszuordnung.
Siehe *Starten des ONVIF Camera Event Driver Tool aus dem Configuration Client, Seite 209*.

Vorgesehene Verwendung
Die vorgesehene Verwendung ist die Zuordnung von ONVIF Ereignissen zu BVMS Ereignissen. ONVIF Ereignisse können dann BVMS Alarme und Aufzeichnungen auslösen.
Sie können standardmäßig Ereignisaufzeichnungen definieren, die für ein spezifisches ONVIF Gerät, für alle ONVIF Geräte desselben Herstellers und desselben Modells oder für alle ONVIF Geräte desselben Herstellers gelten. Standard-Ereignisaufzeichnungen werden automatisch allen betroffenen ONVIF Encodern zugewiesen, die mittels BVMS Scan-Assistent oder manuell hinzugefügt werden.
Wenn Sie einen ONVIF Encoder der BVMS Konfiguration ohne eine Verbindung zu diesem ONVIF Encoder hinzufügen, wird keine Ereignisaufzeichnung zugewiesen. Sie können einen solchen ONVIF Encoder mit Ereignisaufzeichnungen von einem ONVIF Encoder desselben Herstellers und/oder Modells hinzufügen, das Sie bereits hinzugefügt haben.
Sie definieren Ereignisaufzeichnungen spezifisch für jede der nachfolgenden Quellen:
- ONVIF Encoder
- Kameras von diesem ONVIF Encoder
- Relais von diesem ONVIF Encoder
- Eingänge von diesem ONVIF Encoder

Beispiel
In einer ONVIF Kamera erfolgt ein Ereignis aufgrund einer Bewegungserkennung. Dieses Ereignis kann ein **Bewegung erkannt** Ereignis in BVMS auslösen.
Um dies zu erreichen, konfigurieren Sie für diese ONVIF Kamera:
- ONVIF Thema (`MotionDetection`)
- ONVIF Datensegment (`motion`)
- ONVIF Datentyp (`boolean`)
- ONVIF Datenwert (`true`)

Hinweis: Es reicht nicht, nur das **Bewegung erkannt** Ereignis zu konfigurieren. Konfigurieren Sie auch das Ereignis **Bewegung beendet**. Sie müssen immer ein Ereignispaar konfigurieren.

Importieren oder exportieren Sie eine Ereignistabelle
Sie können eine Mapping-Tabelle von einem Computer, auf dem Sie sie erstellt haben exportieren und diese Mapping-Tabelle auf einem anderen Computer importieren, auf dem die erforderliche Mapping-Tabelle nicht zur Verfügung steht.

Problembehandlung
Zur Problemlösung können Sie Protokolldateien erstellen.

Siehe
- *Konfigurieren einer ONVIF-Mapping-Tabelle, Seite 243*
- *Ermöglicht die Protokollierung von ONVIF-Ereignissen, Seite 385*
- *Seite "ONVIF-Encoderereignis", Seite 239*

5.6 Abmeldung bei Inaktivität

Vorgesehene Verwendung
Eine Abmeldung bei Inaktivität dient dem Schutz des Operator Client oder Configuration Client während der Abwesenheit des Bedieners oder Administrators.
Sie können die Konfiguration pro Benutzergruppe so einstellen, dass der Operator Client automatisch nach einem festgelegten Zeitbereich ohne Aktivität abgemeldet wird.
Für Configuration Client sind keine Benutzergruppen verfügbar. Die Abmeldeeinstellungen bei Inaktivität gelten nur für den **Admin**-Benutzer.
Sämtliche Vorgänge über die Tastatur, Maus und das CCTV-Keyboard haben Auswirkung auf den für die Abmeldung bei Inaktivität festgelegten Zeitraum. Automatische Aktivitäten von Operator Client haben keine Auswirkung auf den Zeitraum. Automatische Aktivitäten von Configuration Client wie Firmware-Upload oder iSCSI-Einstellungen verhindern eine Abmeldung bei Inaktivität.
Sie können die Abmeldung bei Inaktivität auch für einen BVMS Web Client konfigurieren.
Kurz bevor eine Abmeldung bei Inaktivität erfolgt, erinnert ein Dialogfeld den Benutzer daran, dieser aktiv entgegenzuwirken.
Das Logbuch zeichnet eine stattgefundene Abmeldung bei Inaktivität auf.

Beispiel
Befindet sich eine Arbeitsstation in einem öffentlichen Bereich, minimiert eine Abmeldung bei Inaktivität das Risiko, dass eine unbefugte Person auf einen Operator Client einer unbeaufsichtigten Arbeitsstation zugreifen kann.
Ein Mitglied einer Administratorengruppe sollte nach einer Zeit der Inaktivität automatisch abgemeldet werden, doch ein Sachbearbeiter (Bedienergruppe) möchte vielleicht nur ein Video ansehen, ohne das System zu bedienen, und wünscht keine Abmeldung bei Inaktivität.

Beschränkungen
Eine Aktivität des Client SDK unterstützt nicht die Abmeldung bei Inaktivität, was bedeutet, dass die Aktivität des Client SDK keine Auswirkungen auf den festgelegten Zeitraum hat.

Siehe
- *Dialogfeld „Optionen“ (Menü „Einstellungen“), Seite 121*
- *Seite mit den Bedienereigenschaften, Seite 342*

5.7 Version unabhängiger Operator Client

Für den Kompatibilitätsmodus müssen sowohl Operator Client als auch Management Server Version 5.5 oder neuer haben.
Ein Benutzer von Operator Client kann sich erfolgreich bei einem Management Server anmelden, auf dem eine frühere Softwareversion läuft.

Falls der Server eine neuere Konfiguration als die auf der Operator Client Workstation vorhandene zur Verfügung stellt, wird diese Konfiguration automatisch auf die Operator Client kopiert. Der Benutzer kann entscheiden, ober er die neue Konfiguration herunterladen will.
Operator Client stellte weniger Funktionen zur Verfügung und ist mit diesem Management Server verbunden.
Die nachfolgenden auf den Management Server bezogenen Funktionen sind nach der Anmeldung bei einem Management Server mit einer früheren Version möglich:

- Benutzereinstellungen
- Manuelle Aufzeichnung starten
- Anzeige der Gerätestatus
- Wechsel zwischen Relaisstatus
- Logbuch durchsuchen
  Die Suche nach Ereignissen ist nicht möglich.
- Server Lookup
- Remote-Export

5.7.1 Arbeiten im Kompatibilitätsmodus

: Dieser Operator Client Status wird im Falle eines Kompatibilitätsmodus angezeigt.
In der Version später als 5.5 arbeitet Operator Client im Kompatibilitätsmodus, falls die Version des Management Server niedriger ist als die Version des Operator Client.
In der Version später als 10.0 arbeitet Operator Client im Kompatibilitätsmodus, falls Folgendes möglich ist:

- Es konnten nicht alle Kommunikationsdienste verbunden durch den Operator Client verbunden werden.
- Beispiel: Der Management Server läuft, aber WebServiceHost ist „down“.
- Es gibt Änderungen innerhalb der Kommunikationsschnittstelle zwischen Operator Client und Management Server

Nur semantische Schnittstellenänderungen oder ein teilweise Rückgang der Services kann dazu führen, dass einige Funktionalitäten im Operator Client fehlen.

5.8 Anzeigemodi einer Panoramakamera

In diesem Kapitel werden die Anzeigemodi einer Panoramakamera beschrieben, die in BVMS verfügbar sind.
Die folgenden Anzeigemodi stehen zur Verfügung:

- Kreisansicht
- Panorama-Ansicht
- Zugeschnittene Ansicht

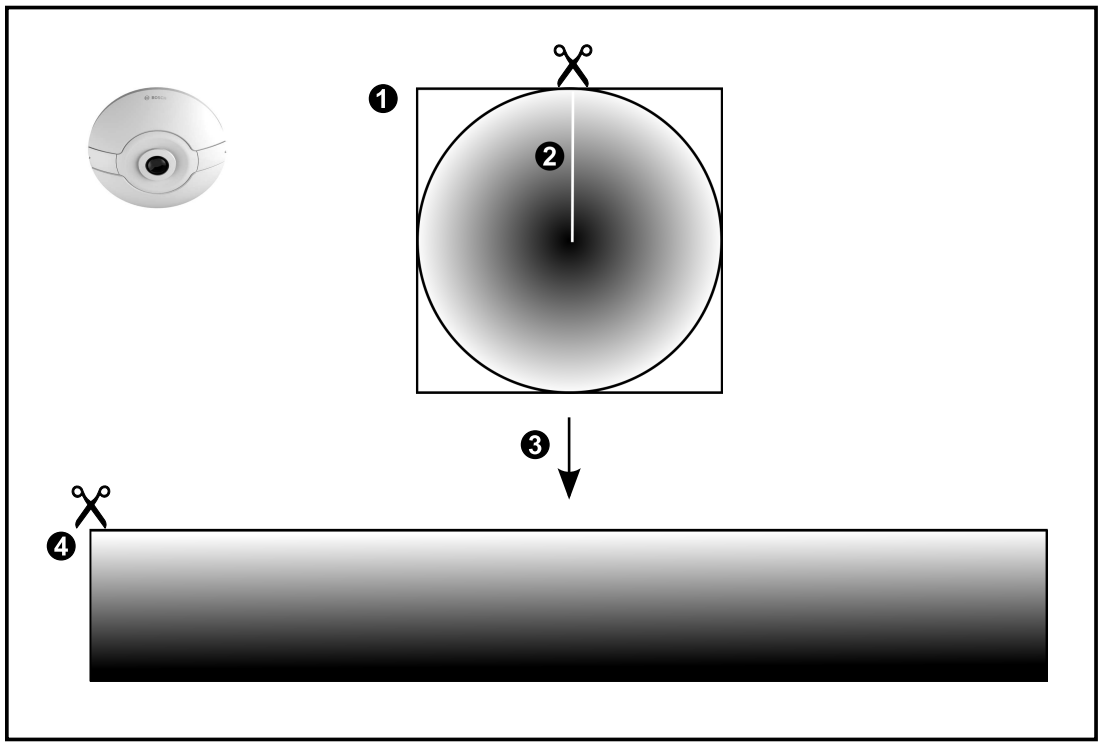
Panorama- und zugeschnittene Ansichtsmodi werden vom Entzerren-Prozess in BVMS erstellt. Entzerren in der Kamera wird nicht verwendet.
Der Administrator muss die Montageposition einer Panoramakamera im Configuration Client konfigurieren.
Sie können die Größe des Bildfensters einer Kamera bei Bedarf ändern. Das Bildfenster-Verhältnis ist nicht auf das Seitenverhältnis 4:3 oder 16:9 beschränkt.

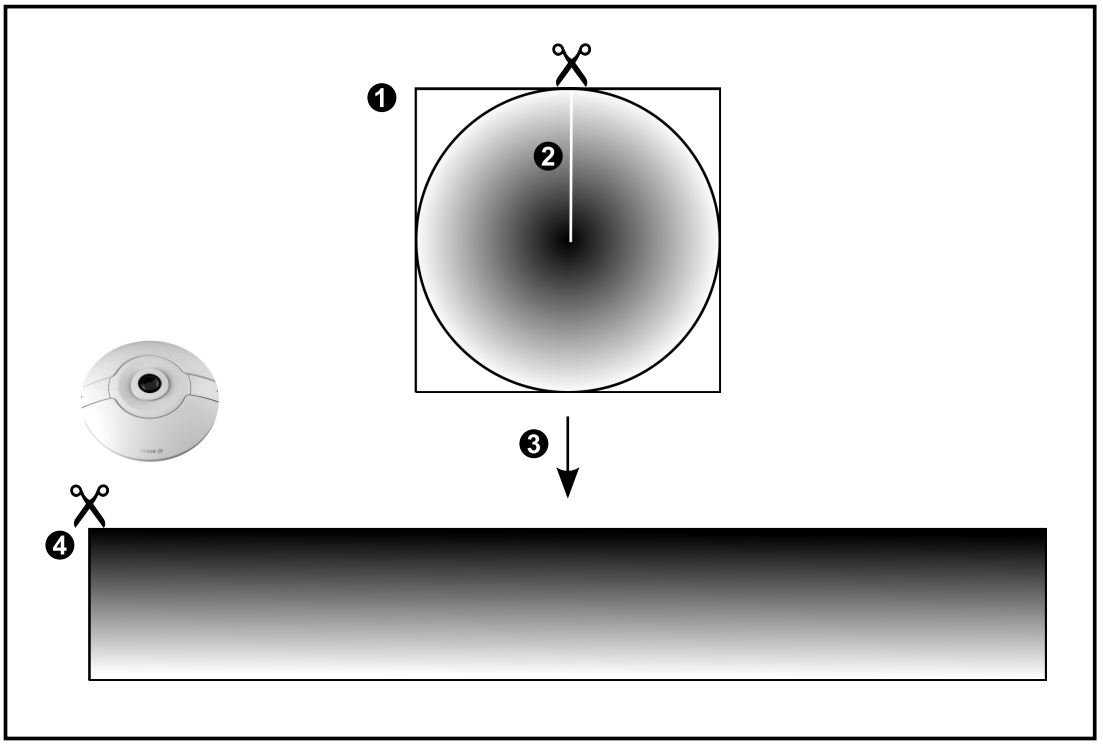
Siehe

- *Konfigurieren von voreingestellten Positionen und AUX-Kommandos, Seite 305*

5.8.1 360°-Panoramakamera – Boden- oder Deckenmontage

Die folgende Abbildung zeigt das Entzerren bei einer 360°-Kamera, die an Boden oder Decke montiert ist.

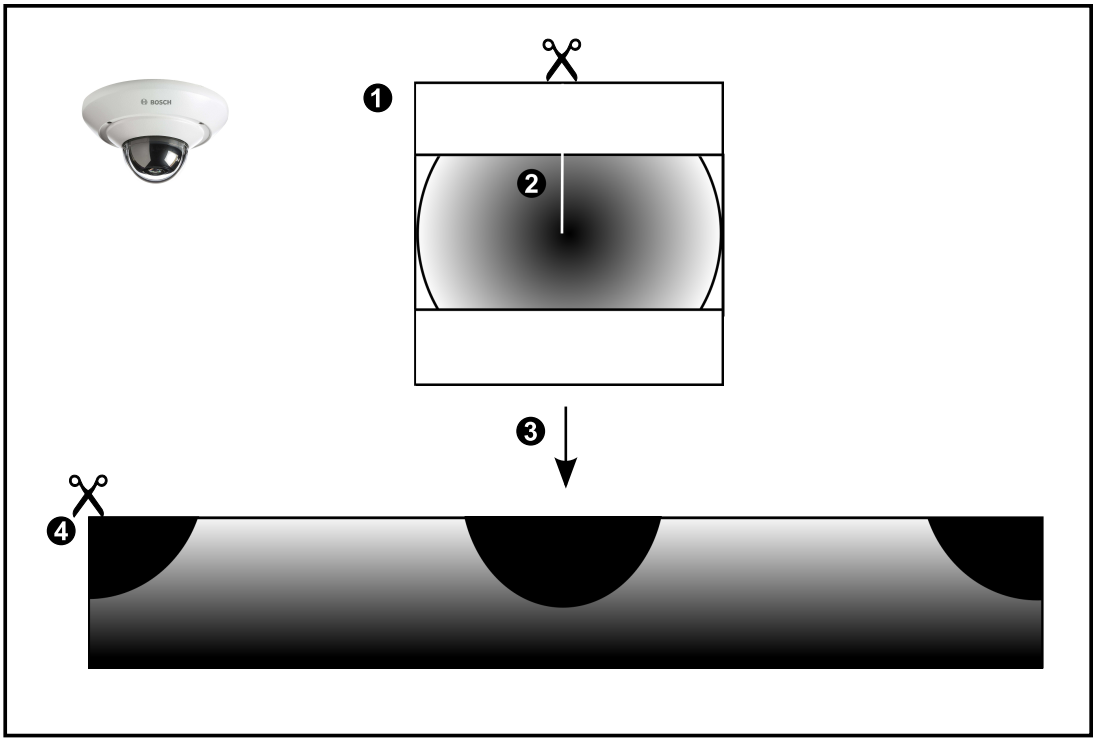


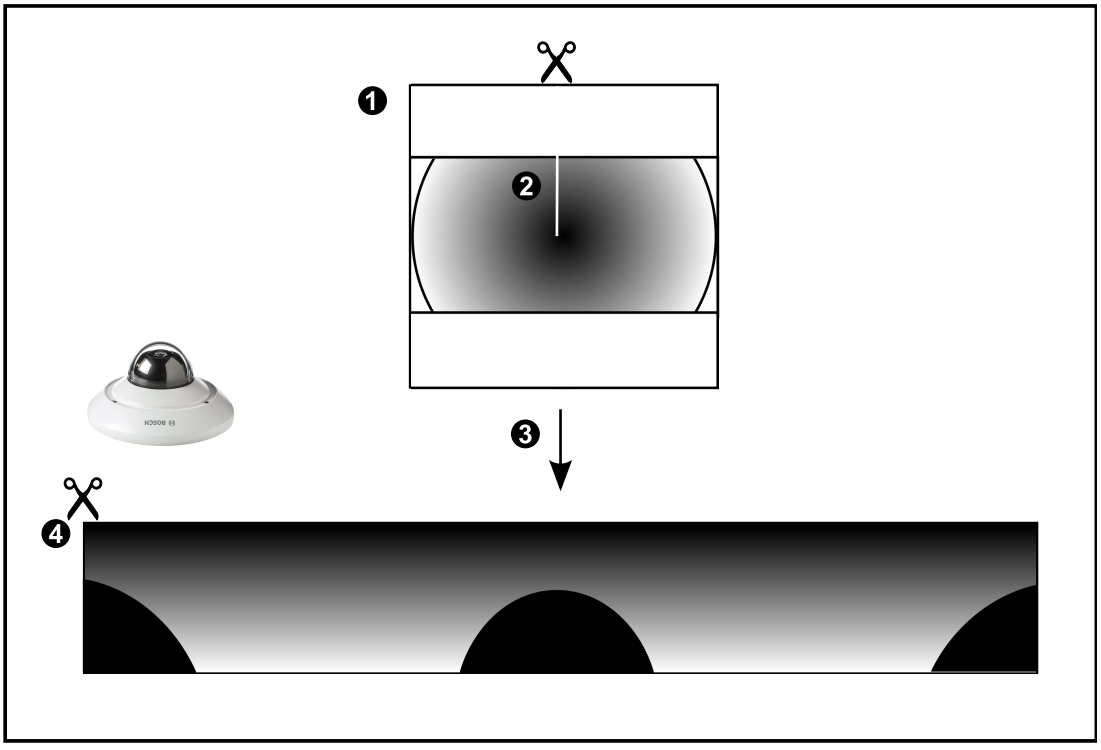


1	Ganzes Kreisbild	3	Entzerren
2	Schnittlinie (Position kann vom Bediener bei Ansicht ohne Zoom geändert werden)	4	Panorama-Ansicht

5.8.2 180°-Panoramakamera – Boden- oder Deckenmontage

Die folgende Abbildung zeigt das Entzerren bei einer 180°-Kamera, die an Boden oder Decke montiert ist.

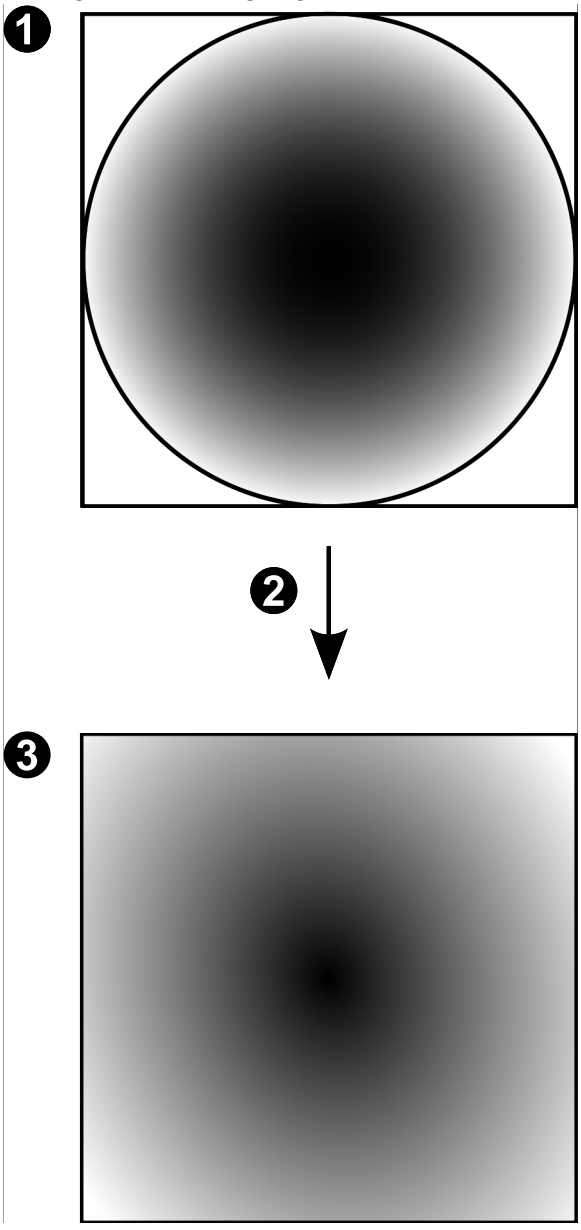




1	Ganzes Kreisbild	3	Entzerren
2	Schnittlinie (Position kann vom Bediener bei Ansicht ohne Zoom geändert werden)	4	Panorama-Ansicht

5.8.3 360°-Panoramakamera – Wandmontage

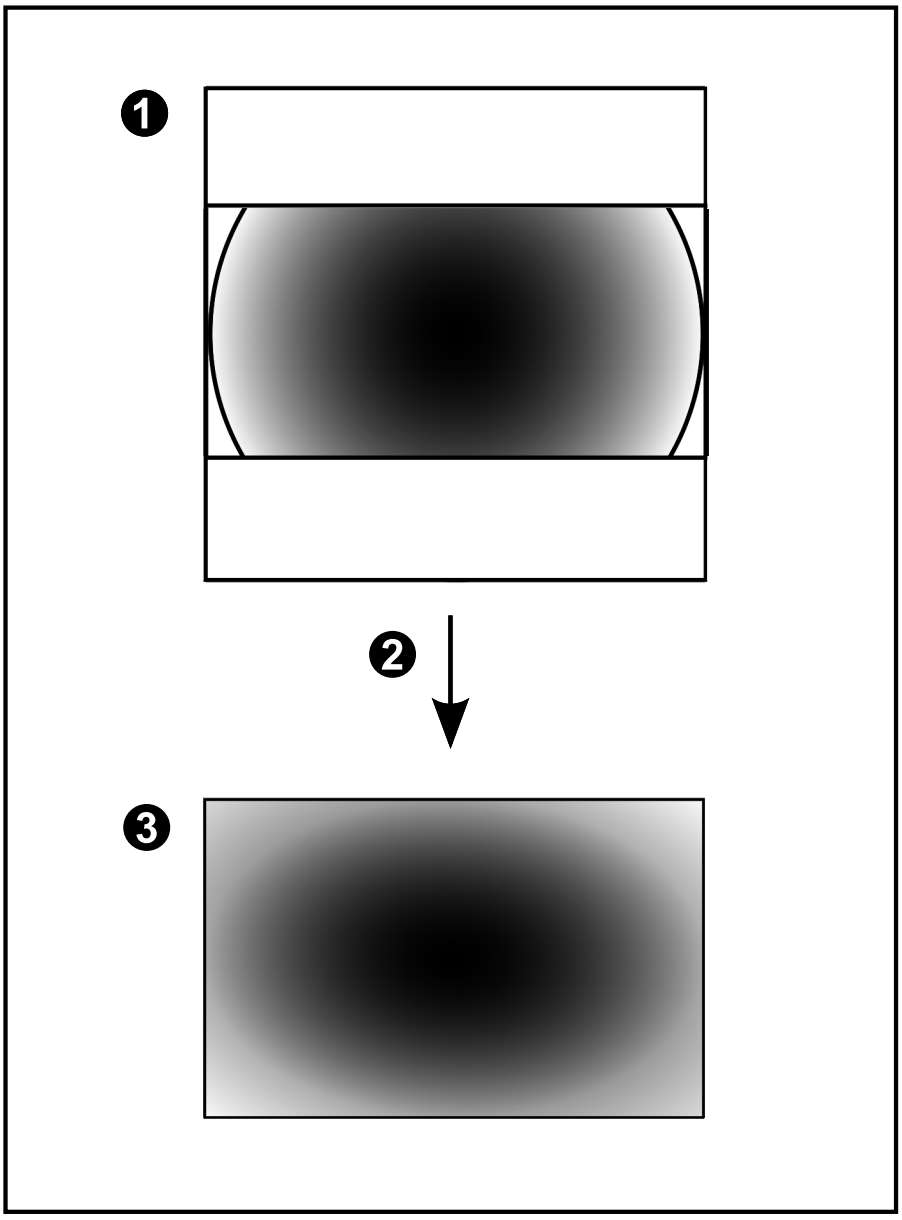
Die folgende Abbildung zeigt das Entzerren bei einer 360°-Kamera, die an einer Wand montiert ist.



1	Ganzes Kreisbild	3	Panorama-Ansicht
2	Entzerren		

5.8.4 180°-Panoramakamera – Wandmontage

Die folgende Abbildung zeigt das Entzerren bei einer 180°-Kamera, die an einer Wand montiert ist.

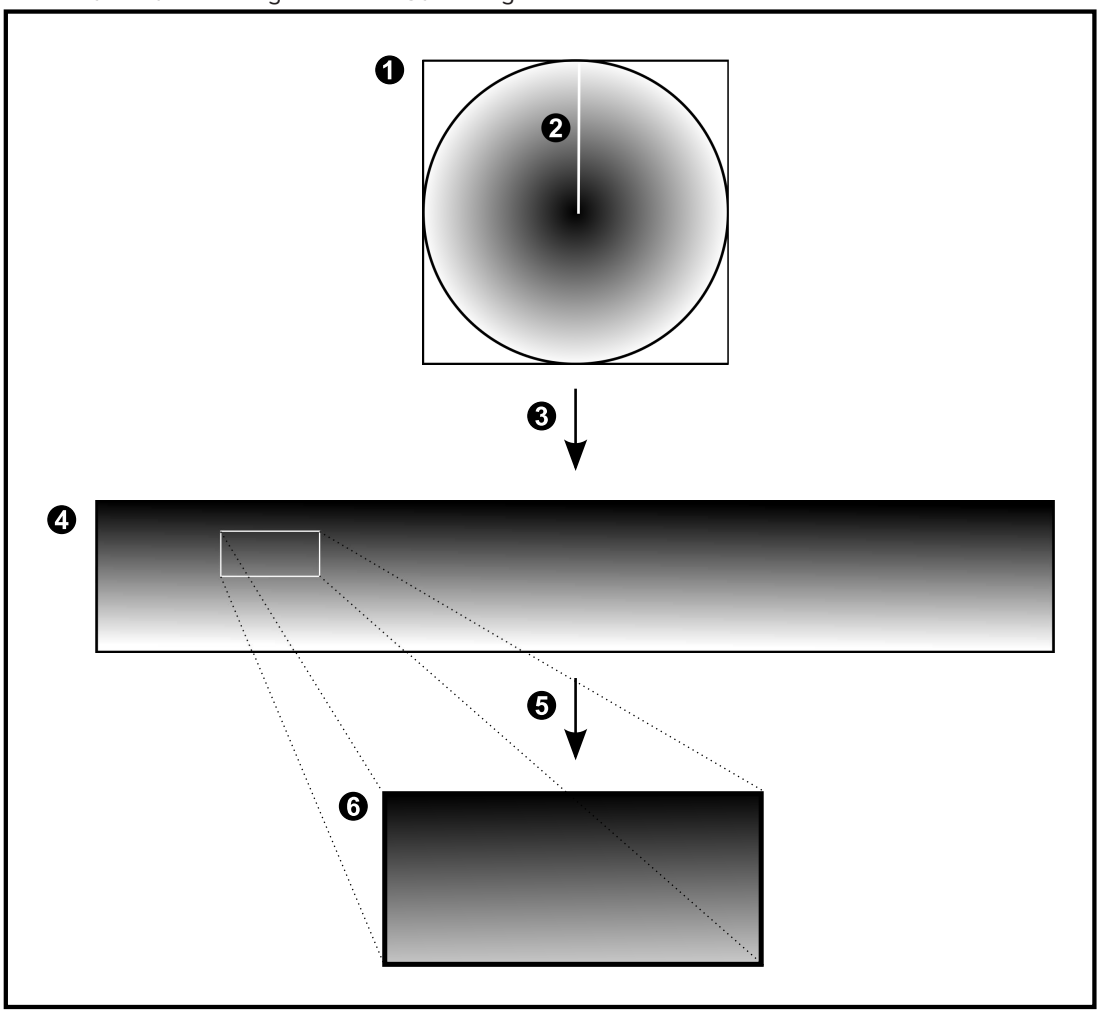


1	Ganzes Kreisbild	3	Panorama-Ansicht
2	Entzerren		

5.8.5 Zugeschnittene Ansicht bei einer Panoramakamera

Die folgende Beispielabbildung zeigt das Zuschneiden bei einer 360°-Kamera, die an Boden oder Decke montiert ist.

Der rechteckige, zuzuschneidende Bereich ist festgelegt. Sie können den Bereich im zugeschnittenen Bildfenster mit den verfügbaren PTZ-Steuerungen ändern.



1	Ganzes Kreisbild	4	Panorama-Ansicht
2	Schnittlinie (Position kann vom Bediener bei Ansicht ohne Zoom geändert werden)	5	Zuschneiden
3	Entzerren	6	Zugeschnittenes Bildfenster

5.9 SSH-Tunneling

BVMS ermöglicht eine Remote-Verbindung durch den Einsatz von SSH-Tunneling (Secure Shell). Beim SSH-Tunneling wird ein verschlüsselter Tunnel über eine SSH-Protokoll/Socket-Verbindung aufgebaut. Dieser verschlüsselte Tunnel ermöglicht verschlüsselten und unverschlüsselten Datenverkehr. Die Bosch SSH-Implementierung nutzt außerdem das Omni-Path-Protokoll, ein von Intel entwickeltes, hochleistungsfähiges Kommunikationsprotokoll mit niedriger Latenz.

Technische Aspekte und Einschränkungen

- SSH-Tunneling nutzt Port 5322. Dieser Port kann nicht geändert werden.
- Der SSH-Dienst muss auf demselben Server wie der BVMS Management Server installiert sein.
- (Enterprise) Benutzerkonten müssen mit einem Passwort geschützt sein. (Enterprise) Benutzerkonten ohne Passwort können sich nicht mit einer SSH-Verbindung anmelden.
- Kameras mit lokaler Aufzeichnung unterstützen keine SSH-Verbindung.
- Configuration Client kann keine Fernverbindung über SSH herstellen. Die Verbindung von Configuration Client muss über Port Mapping erfolgen.
- Operator Client prüft die Verbindung mit dem SSH-Dienst alle 15 Sekunden. Wenn die Verbindung unterbrochen wird, prüft Operator Client die Verbindung einmal pro Minute.

Port Mapping

- Konfigurieren Sie eine Portweiterleitung, damit der BVMS Management Server den Port 5322 für interne und externe Verbindungen nutzt.
  Dies ist der einzige Eintrag, der beim Port Mapping für das gesamte System erforderlich ist. BVMS Port Mapping ist nicht erforderlich.

Verschlüsselte Kommunikation

Nachdem die Verbindung über einen SSH-Tunnel hergestellt wurde, ist die gesamte Kommunikation zwischen dem BVMS Management Server und einem Remote-Client verschlüsselt.

5.10 Multipathing

BVMS bietet Multipathing für Dual-Controller-Systeme. Multipathing ist eine Fehlertoleranz-Technologie, die durch redundante Netzwerkverbindungen mehr als einen physischen Pfad zwischen der Kamera und ihren iSCSI-Speichergeräten definiert. Bei der Verwendung von Multipathing ist die Aufzeichnung und Wiedergabe von Videodaten selbst bei Ausfall eines iSCSI-Controllers möglich.

Voraussetzungen und Einschränkungen

- Ein NetApp E2800 Dual-Controller iSCSI-Gerät ist installiert.
- Firmware 6.43 ermöglicht Geräten, die auf E2800 aufzeichnen, alternative Pfade zu verwenden.
- VRM 3.71 kann Geräte mit Multipathing überwachen und protokollieren.
- Zwei physische iSCSI-Ports sind pro Controller konfiguriert: entweder 2 x 2 RJ-45 oder 2 x 2 optisch.
- Die Verbindungsgeschwindigkeit muss 10 Gbit/s betragen, damit die volle Leistung erzielt werden kann.
- Der Dual-Simplex-Modus von E2700 wird nicht mehr unterstützt.

Weitere Informationen zur Installation von DSA E2800 Vollduplex finden Sie im DSA E-Series E2800 Installationshandbuch.

5.11 OpenID Connect (OIDC) und Identity Provider (IdP)

BVMS unterstützt die Authentifizierung über einen externen Berechtigungsanbieter-Dienst. Bei der Verwendung von Open ID Connect (OIDC) wird die Authentifizierung über eine vorkonfigurierte Identity provider (IdP), while BVMS focuses on the authorization task.
Dies ist hilfreich für große Unternehmensgruppen, die nicht einzelne Benutzer verwalten möchten. Durch Zuordnung von Benutzergruppen zu IdP-Gruppen erhalten Benutzer gemäß ihren Anforderungen Zugriff.

Siehe
- *Dialogfeld „Optionen“ (Menü „Einstellungen“), Seite 121*
- *Seite Benutzergruppen, Seite 333*

5.12 Kennzeichenerfassung

Die neuesten Bosch-Kameras mit Intelligent Video Analytics (IVA) Pro unterstützen die Nummernschilderkennung.
Um die Kennzeichenerkennungsfunktion zu nutzen, müssen Sie eine spezielle Lizenz auf der Kamera installieren. Es ist keine Lizenzaktivierung in BVMS erforderlich.
Je nach installierter Lizenz liefert die Kamera nur Daten über das Kennzeichen und den Ländercode oder auch Daten über den Fahrzeugtyp, den Fahrzeughersteller und das Fahrzeugmodell.

Sie müssen die LPR-Einstellungen auf der Webseite der Kamera konfigurieren.
Im BVMS Configuration Client können Sie entsprechende Ereignisse und Alarme für erkannte Nummernschilder konfigurieren und im Logbuch nach erkannten Nummernschildern suchen.

Hinweis!
Bei einem LPR-Ereignis können Sie der Aufzeichnung keine Textdaten hinzufügen.

Hinweis!
Wenn ein Fahrzeug vorbeifährt, braucht die Kamera bis zu 3 Sekunden, um das Nummernschild zu erkennen. Anschließend erstellt BVMS das LPR-Ereignis mit dem jeweiligen Zeitstempel.
Achten Sie aufgrund dieser Erkennungsverzögerung bei der Konfiguration der Aufzeichnungseinstellungen für die Kamera darauf, einen Voralarm von mindestens 5 Sekunden zu konfigurieren.

Siehe
- *Seite Nummernschild-Erkennung, Seite 260*
- *Seite Ereignisse, Seite 310*

6 Unterstützte Hardware

Hinweis!
Verbinden Sie ein Gerät nur mit einem einzigen BVMS! Anderenfalls kann es zu Aufzeichnungslücken und anderen unerwünschten Effekten kommen.

Sie können die folgenden Geräte an das BVMS anschließen:

- Mobile Video-Clients wie iPhone oder iPad über DynDNS
- Verschiedene IP-Kameras, Encoder und ONVIF-Kameras (nur live oder über Video Streaming Gateway)
  Angeschlossen über das Netzwerk
- Nur-Live-Encoder mit lokaler Archivierung
  Angeschlossen über das Netzwerk
- iSCSI-Speichergeräte
  Angeschlossen über das Netzwerk
- Analogkameras
  Angeschlossen an Encoder
- Decoder
  Angeschlossen über das Netzwerk
- Monitore
  Angeschlossen an einen Decoder, eine Bosch Allegiant Kreuzschiene, eine BVMS Client-Arbeitsstation
- Bosch Allegiant Kreuzschiene (Firmware-Version: 8.75 oder höher, MCS-Version: 2.80 oder höher)
  Angeschlossen an einen COM-Port des Management Server oder an einen entfernten Computer und einen IP-Encoder im Netzwerk
- KBD-Universal XF Keyboard
  Angeschlossen an einen USB-Port einer BVMS Arbeitsstation.
- Bosch IntuiKey Keyboard
  Angeschlossen an den COM-Port einer BVMS Arbeitsstation (Firmware-Version: 1.82 oder höher) oder an einen Hardware-Decoder (VIP XD)
  Wenn das Keyboard an eine Arbeitsstation angeschlossen wird, kann der Benutzer das gesamte System mit dem Keyboard steuern. Wenn das Keyboard an einen VIP XD Decoder angeschlossen wird, kann der Benutzer nur die Monitore mit dem Keyboard steuern.
- SMTP-E-Mail-Server
  Angeschlossen über das Netzwerk
- POS
  Angeschlossen über das Netzwerk
- ATM
  Angeschlossen über das Netzwerk
- Netzwerküberwachungsgerät
  Angeschlossen über das Netzwerk
- I/O-Module
  Angeschlossen über das Netzwerk
  Nur ADAM-Geräte werden unterstützt.

Alle über das Netzwerk angeschlossenen Geräte sind an einen Switch angeschlossen. Die Computer des BVMS sind ebenfalls an dieses Gerät angeschlossen.

6.1 Installieren von Hardware

BVMS unterstützt folgende Hardware-Komponenten:

- KBD-Universal XF Keyboard
- Bosch IntuiKey Keyboard
- Bosch Allegiant Kreuzschiene mit Kameras und Monitor: Angeschlossen an den COM-Port eines Netzwerk-Computers sowie an in das Netzwerk eingebundene IP-Encoder
- Encoder mit Analogkameras
- Encoder mit lokaler Archivierung
- IP-Kameras und IP AutoDomes
- Monitore, angeschlossen an einen Decoder (Monitorgruppen für Alarmverarbeitung möglich)
- DVR-Systeme mit Kameras
- ATM/POS-Geräte
- I/O-Module
  Nur ADAM-Geräte werden unterstützt.

6.2 Installation eines KBD Universal XF Keyboards

Hinweis!
Weitere Informationen finden Sie im Handbuch, das mit Ihrer KBD-Universal XF Tastatur im Online-Produktkatalog zur Verfügung steht.

Weitere Informationen
(IdP), während sich das BVMS auf die Autorisierungsaufgabe konzentriert www.boschsecurity.com und die entsprechende Produktseite.
Sie können die folgenden Geräte an das BVMS anschließen:

- Mobile Video-Clients wie iPhone oder iPad über DynDNS
- Verschiedene IP-Kameras, Encoder und ONVIF-Kameras (nur live oder über Video Streaming Gateway)
  Angeschlossen über das Netzwerk
- Nur-Live-Encoder mit lokaler Archivierung
  Angeschlossen über das Netzwerk
- iSCSI-Speichergeräte
  Angeschlossen über das Netzwerk
- Analogkameras
  Angeschlossen an Encoder
- Decoder
  Angeschlossen über das Netzwerk
- Monitore
  Angeschlossen an einen Decoder, eine Bosch Allegiant Kreuzschiene, eine BVMS Client-Arbeitsstation
- Bosch Allegiant Kreuzschiene (Firmware-Version: 8.75 oder höher, MCS-Version: 2.80 oder höher)
  Angeschlossen an einen COM-Port des Management Server oder an einen entfernten Computer und einen IP-Encoder im Netzwerk

6.3 Verbinden eines Bosch IntuiKey Keyboards mit BVMS

Dieses Kapitel enthält Hintergrundinformationen zur Konfiguration eines Bosch IntuiKey-Keyboards

6.3.1 Szenarios für Bosch IntuiKey Keyboard-Anschlüsse

Sie können ein Bosch IntuiKey Keyboard an den COM-Port einer BVMS Arbeitsstation (Szenario 1) oder an einen Hardware-Decoder (z. B. VIP XD, Szenario 2) anschließen.
Wenn Sie das Keyboard an eine BVMS Arbeitsstation anschließen, können Sie das gesamte System steuern. Wenn Sie das Keyboard an einen Decoder anschließen, können Sie nur die analogen Monitore des Systems steuern.
Wenn Sie das Keyboard mit einem Enterprise Operator Client verbinden, können Sie die Kameras eines bestimmten Management Server kontrollieren, indem Sie zuerst die Server-Taste drücken, um die Nummer dieses Servers einzugeben und dann die Kameranummer eingeben.

Hinweis!
Verwenden Sie zum Anschließen des Bosch IntuiKey Keyboards an eine BVMS Arbeitsstation das angegebene Bosch Kabel.
Zum Anschließen des Bosch IntuiKey Keyboards an einen VIP XD Decoder benötigen Sie ein Kabel, das den seriellen COM-Port des Keyboards mit der seriellen Schnittstelle des Decoders verbindet. Informationen zu den Anschlüssen finden Sie unter Anschließen eines CCTV-Keyboards an einen Decoder.

Bosch IntuiKey Keyboard, an eine BVMS Arbeitsstation angeschlossen

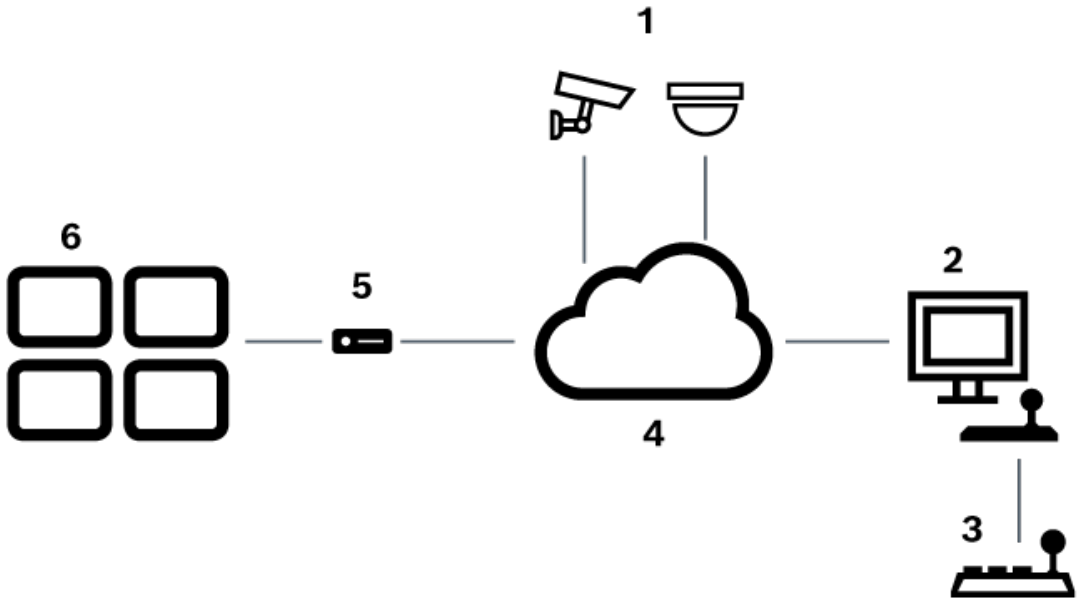


Abbildung 6.1: Szenario 1: An eine Bosch Video Management System Arbeitsstation angeschlossenes Bosch IntuiKey Keyboard

1	Verschiedene über Encoder an das Netzwerk angeschlossene Kameras
2	BVMS Arbeitsstation
3	Bosch IntuiKey Keyboard
4	BVMS Netzwerk
5	Decoder

6	Monitore

An einen Decoder angeschlossenes Bosch IntuiKey Keyboard

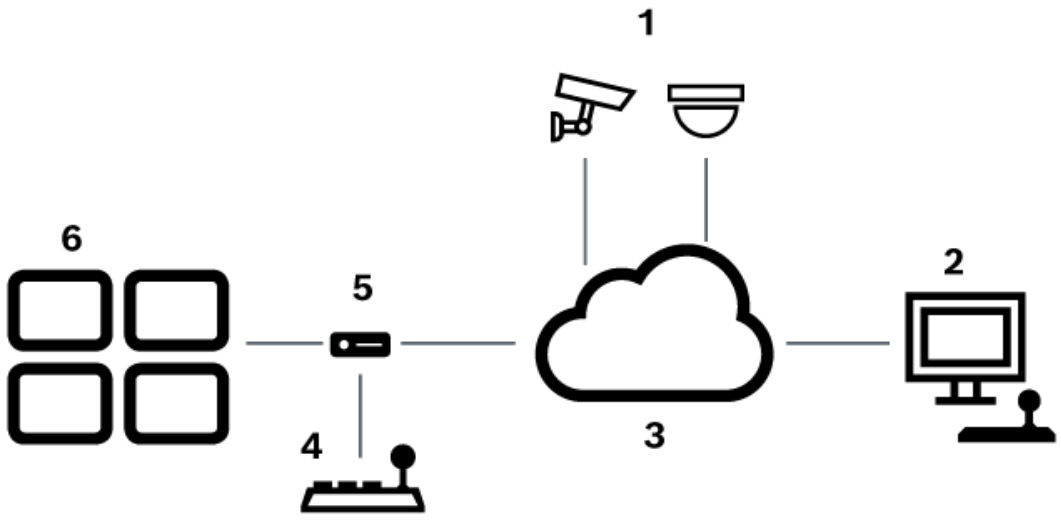


Abbildung 6.2: Szenario 2: An einen Decoder angeschlossenes Bosch IntuiKey Keyboard

1	Verschiedene über Encoder an das Netzwerk angeschlossene Kameras
2	BVMS Arbeitsstation
3	BVMS Netzwerk
4	Bosch IntuiKey Keyboard
5	Decoder
6	Monitore

Ausführliche Informationen zu den verfügbaren Fenstern finden Sie in den folgenden Abschnitten:
– *Seite „Assign Keyboard“ (Tastatur zuweisen), Seite 157*

Ausführliche Informationen zu den verfügbaren schrittweisen Anweisungen finden Sie in den folgenden Abschnitten:
– *Konfigurieren eines Bosch IntuiKey Keyboards (Seite „Einstellungen“) (Arbeitsstation), Seite 138*
– *Konfigurieren eines Bosch IntuiKey Keyboards (Decoder), Seite 146*
– *Konfigurieren eines Decoders für den Einsatz mit einem Bosch IntuiKey Keyboard, Seite 146*

Siehe
– *Seite „Assign Keyboard“ (Tastatur zuweisen), Seite 157*

6.3.2 Anschluss eines Bosch IntuiKey Keyboards an einen Decoder

Konfigurieren des Decoders

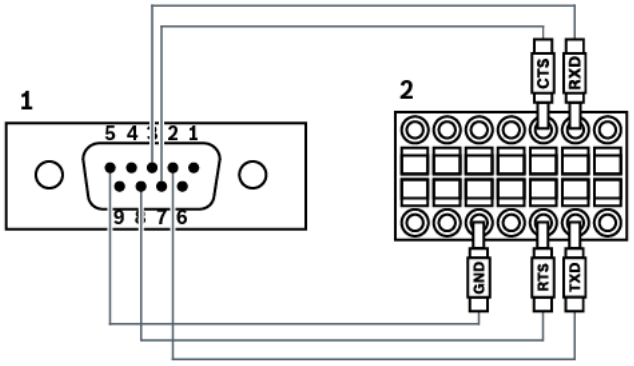
Siehe *Konfigurieren eines Decoders für den Einsatz mit einem Bosch IntuiKey Keyboard, Seite 146* .

Anschlüsse zwischen COM-Port und VIP XD Decoder

In der folgenden Tabelle werden die Anschlüsse zwischen einem RS232-Adapter und der seriellen Schnittstelle eines VIP XD Decoders aufgeführt:

RS232-Adapter	Serielle Schnittstelle eines VIP XD Decoders
1	
2	TX
3	RX
4	
5	Masse
6	
7	CTS
8	RTS
9	

In der folgenden Abbildung ist die Pinbelegung eines RS232-Standardadapters (1) und des seriellen Decoder-Adapters (2) dargestellt:



6.3.3 Aktualisierung der Bosch IntuiKey Keyboard-Firmware

1. Installieren Sie den IntuiKey Downloader auf einem beliebigen PC.
2. Starten Sie das Dienstprogramm zum Aktualisieren der IntuiKey Firmware (IntuiKey Firmware Upgrade Utility).
3. Schließen Sie das Keyboard mit einem zulässigen seriellen Kabel an diesen PC an. (Wenden Sie sich an den Bosch Kundendienst, falls solch ein Kabel nicht verfügbar ist.)
4. Drücken Sie auf dem Keyboard den Softkey Keyboard Control und anschließend Firmware Upgrade.
5. Geben Sie das Passwort: 0 und 1 gleichzeitig ein.
   Das Keyboard befindet sich im Bootloader-Modus.
6. Klicken Sie auf dem PC auf Browse, um die Firmware-Datei auszuwählen, z. B. kbd.s20.
7. Legen Sie den COM-Port fest.

8. Klicken Sie auf die Schaltfläche Download, um die Firmware herunterzuladen.
   Auf der Keyboard-Anzeige wird Programming angezeigt.
   Sie dürfen die Taste Clr jetzt noch nicht drücken. Anderenfalls ist das Keyboard nach dem Neustart nicht funktionsfähig (siehe Hinweis unten).
9. Klicken Sie auf Browse, um die Sprache auszuwählen, z. B. 8900_EN_..82.s20
   . Auf der Keyboard-Anzeige wird Programming angezeigt.
10. Schließen Sie das Dienstprogramm zum Aktualisieren der IntuiKey Firmware (IntuiKey Firmware Upgrade Utility).
11. Drücken Sie auf dem Keyboard zum Beenden die Taste Clr.
    Das Keyboard wird neu gestartet. Warten Sie einige Sekunden, bis das Menü zum Auswählen der Keyboard-Sprache angezeigt wird.
12. Wählen Sie mit einem Softkey die gewünschte Sprache aus.
    Die standardmäßige Startanzeige wird angezeigt.

Hinweis!
Um den Bootloader-Modus direkt zu starten, trennen Sie das Keyboard von der Stromversorgung, drücken Sie gleichzeitig 0 und 1, schließen Sie das Keyboard wieder an die Stromversorgung an und lassen Sie 0 und 1 wieder los.

6.4 Verbinden einer Bosch Allegiant Kreuzschiene mit BVMS

Die BVMS Allegiant Kreuzschienen-Schnittstelle bietet einen nahtlosen Zugang zu analogen Kreuzschienen-Kameras über die Operator Client-Schnittstelle. Die Darstellung von Allegiant Kameras und IP-Kameras ist nahezu identisch. Der einzige Unterschied besteht in einem kleinen Gitternetzsymbol auf der Kamera, das eine Allegiant Kamera kennzeichnet. Für die Anzeige der Kameras können die gleichen Aufgaben durchgeführt werden wie für IP-Kameras. Sie sind sowohl im Logischen Baum als auch in den Lageplänen enthalten, und Benutzer können sie ihren Favoritenbäumen hinzufügen. Die Steuerung im Videofenster für PTZ-Kameras, die an Allegiant Kreuzschienen angeschlossen sind, wird unterstützt. Sie können Allegiant Kameras auch problemlos auf Monitoren anzeigen, die an IP-Decodern angeschlossen sind.
Das BVMS bietet über die Allegiant Master Control Software (MCS) eine Schnittstelle zur Kreuzschiene. Die MCS wird in diesem Fall unsichtbar im Hintergrund ausgeführt. Diese Software bietet eine effiziente, ereignisgesteuerte Schnittstelle zur Allegiant Kreuzschiene. Sie ermöglicht schnelle Echtzeitreaktionen auf Ereignisse von der Allegiant Kreuzschiene zum BVMS. Falls beispielsweise ein defektes Koaxialkabel zu einem Videosignalverlust in der Allegiant Kreuzschiene führt, wird sofort eine Benachrichtigung an das BVMS gesendet. Ferner können Sie das BVMS so programmieren, dass es auf Allegiant Alarme reagiert.

6.4.1 Verbindung mit Bosch Allegiant Systemen – Überblick

Um eine Verbindung zwischen dem BVMS und einem Allegiant Kreuzschienensystem herzustellen, wird ein Steuerungskanal zwischen dem BVMS und der Allegiant Kreuzschiene konfiguriert.
Es gibt zwei mögliche Szenarios:

- Lokale Verbindung
  Der Management Server steuert die Allegiant Kreuzschiene.
- Entfernte Verbindung
  Ein mit dem Netzwerk verbundener dedizierter Bosch Allegiant PC steuert die Allegiant Kreuzschiene.

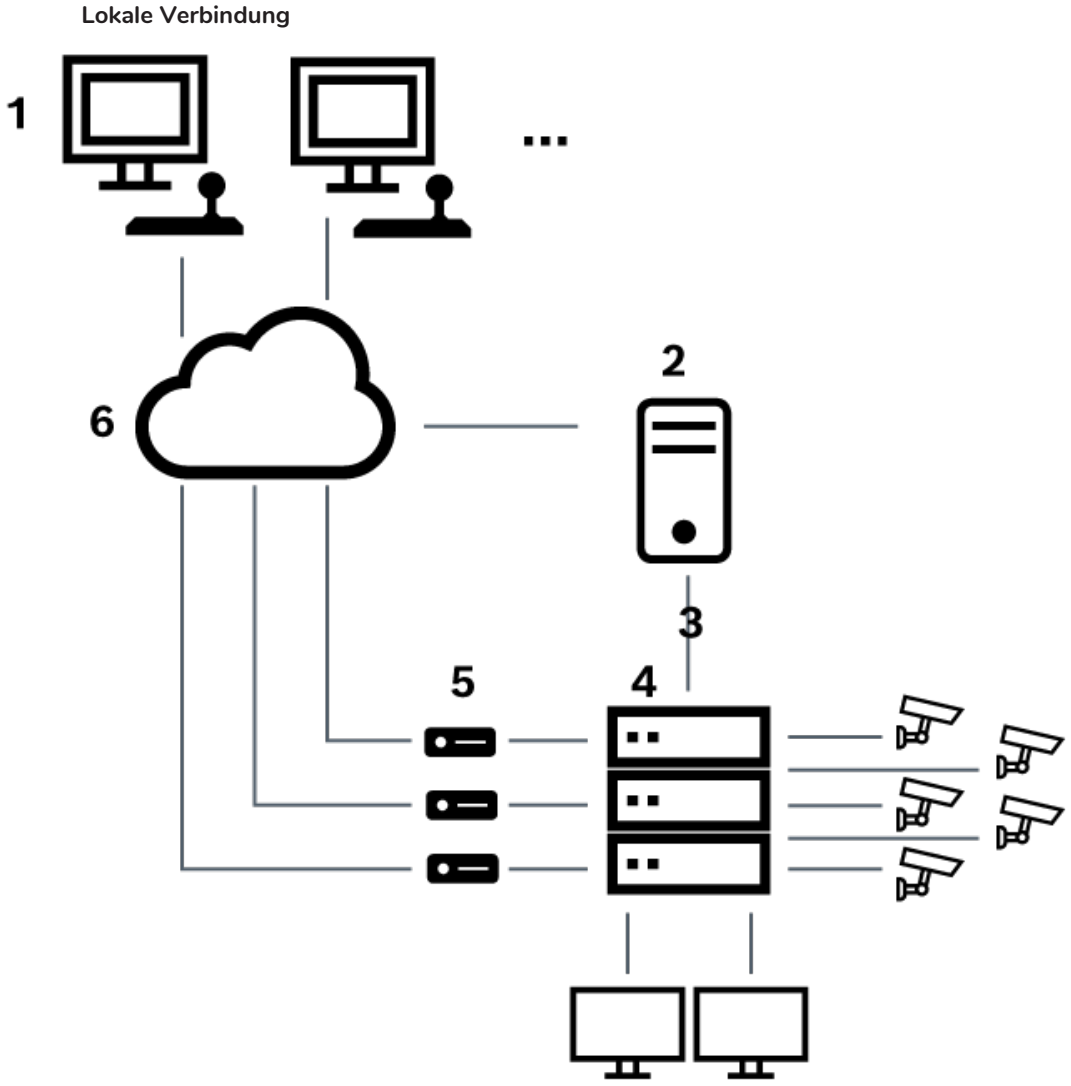


Abbildung 6.3: Lokale Verbindung des Bosch Video Management System mit einem Bosch Allegiant-Matrix-Switch

1	BVMS Client-Arbeitsstationen
2	Management Server mit Master Control Software
3	RS-232-Verbindung
4	Allegiant Kreuzschiene
5	Encoder
6	Netzwerk

Entfernte Verbindung

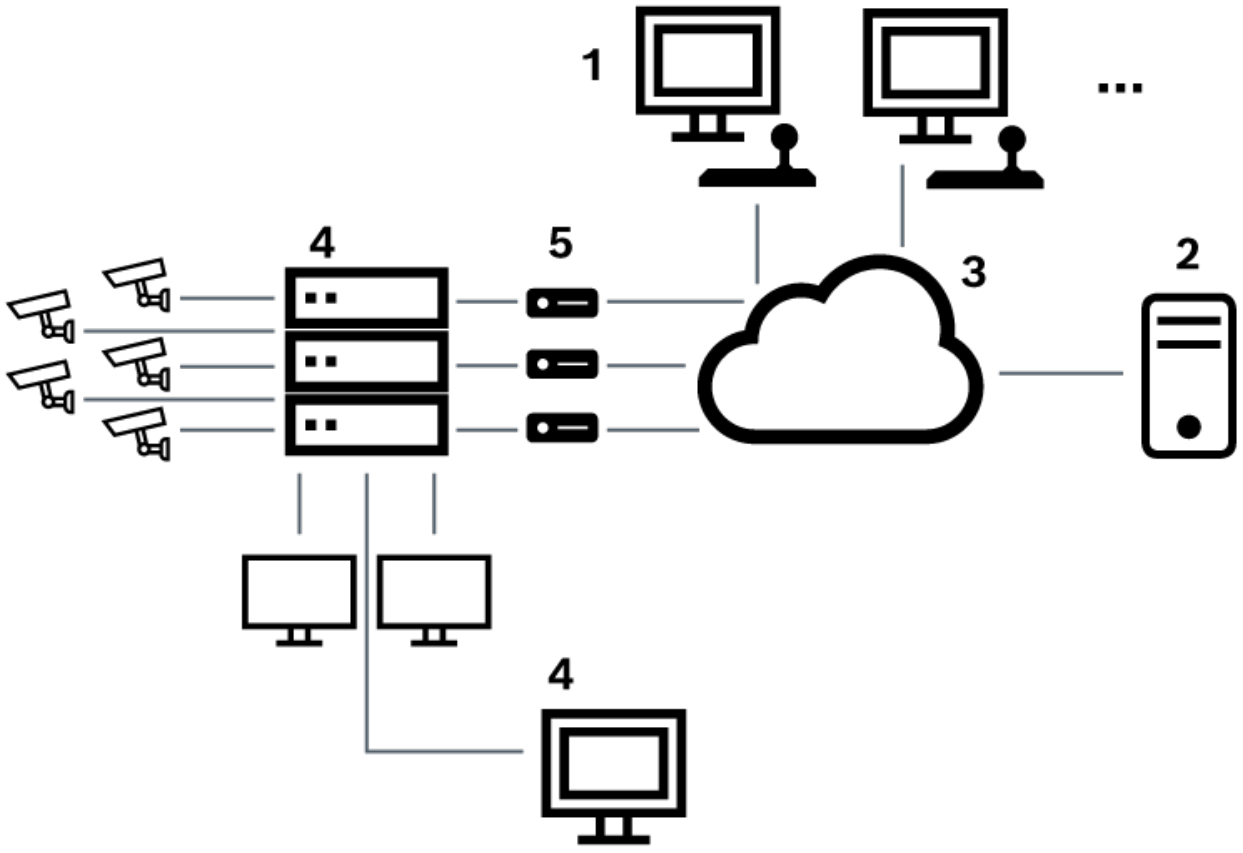


Abbildung 6.4: Entfernte Verbindung des Bosch Video Management System mit einem Bosch Allegiant-Matrix-Switch

1	BVMS Client-Arbeitsstationen
2	Management Server mit Master Control Software
3	Netzwerk
4	Allegiant PC mit Master Control Software
5	RS-232-Verbindung
6	Encoder
7	Allegiant Kreuzschiene

6.4.2 Konfigurieren des Steuerungskanals

Führen Sie die folgenden Aufgaben zur Konfiguration des Steuerungskanals durch:

- Verkabelung
- Installieren der Software
- Erzeugen einer Allegiant Konfigurationsdatei
- Hinzufügen der Allegiant Kreuzschiene zum BVMS

– Konfigurieren von Benutzernamen

Verkabelung

Um den Steuerungskanal zwischen BVMS und der Allegiant-Matrix zu konfigurieren, schließen Sie einen PC über einen seriellen RS-232-Port an den Allegiant-Konsolenport an. (Verwenden Sie dazu das angegebene Bosch Kabel.) Bei dem PC kann es sich um den BVMS Management Server oder einen beliebigen anderen PC im Netzwerk handeln.

Installieren der Allegiant Master Control Software

1. Stoppen Sie den Management Server Dienst, falls er ausgeführt wird (**Start** > **Systemsteuerung** > **Dienste** > Kontextmenü von BVMS Management Server > **Beenden**).
2. Installieren Sie die Allegiant Master Control Software auf dem Management Server und auf dem Allegiant PC (sofern vorhanden).
3. Konfigurieren Sie die Software auf einem entfernten Allegiant PC so, dass das Allegiant Netzwerk-Host-Programm (ld_alghw.exe) beim Systemstart mit gestartet wird. Auf diese Weise werden die erforderlichen Allegiant Dienste gestartet, mit Hilfe derer die anderen PCs im Netzwerk auf die Allegiant Kreuzschiene zugreifen können. Die Software wird unsichtbar ausgeführt. Es muss kein Dongle an diesen Computer angeschlossen sein.
   Damit der Dienst beim Starten des Computers automatisch gestartet wird, kopieren Sie eine Verknüpfung zu ld_alghw.exe den Ordner „Autostart“ Ihres Computers.

Erzeugen einer Bosch Allegiant Konfigurationsdatei

1. Erzeugen Sie mit Hilfe der Allegiant Master Control Software eine Allegiant Konfigurationsdatei, die den an die Allegiant Kreuzschiene angeschlossenen Computer angibt. Für diese Aufgabe ist der Master Control Software-Dongle erforderlich.
2. Klicken Sie im Menü Transfer auf Communication Setup. Geben Sie in der Liste Current Host den DNS-Namen des an die Allegiant Kreuzschiene angeschlossenen Computers ein. Geben Sie außerdem die Parameter (COM-Port-Nummer, Baudrate usw.) des seriellen Ports zur Allegiant Kreuzschiene ein. Dies ermöglicht die Kommunikation zwischen der Master Control Software auf dem Management Server oder PC und dem Allegiant System. Ist eine Kommunikation nicht möglich, stellen Sie sicher, dass die Master Control Software oder das Allegiant Netzwerk-Host-Programm auf dem an die Allegiant Kreuzschiene angeschlossenen Computer ausgeführt wird und dass die Konfiguration der Netzwerksicherheit den Fernzugriff auf diesen Computer zulässt.
3. Klicken Sie im Menü Transfer auf Upload. Wählen Sie alle Tabellen aus, und klicken Sie auf Upload. Wählen Sie zum Speichern der Konfigurationsdatei ein Verzeichnis aus.
4. Beenden Sie die Master Control Software.

Hinzufügen der Bosch Allegiant Kreuzschiene zum BVMS

1. Starten Sie den BVMSManagement Server-Dienst, starten Sie den Configuration Client, und fügen Sie das Allegiant Gerät hinzu. Fügen Sie dazu diese Konfigurationsdatei hinzu. (Schrittweise Anweisungen finden Sie unter Hinzufügen eines Geräts.)
2. Stellen Sie sicher, dass die im BVMS verwendete Allegiant Master Control Software-Konfigurationsdatei der aktuellen Allegiant Konfiguration entspricht.
   Das BVMS führt die erforderlichen Komponenten der Master Control Software unsichtbar im Hintergrund aus.

Konfigurieren des Benutzernamens zur Anmeldung bei Allegiant Diensten

Wenn die Allegiant Kreuzschiene an einen PC im Netzwerk und nicht an den Management Server angeschlossen ist, stellen Sie sicher, dass für die Anmeldung der Allegiant Dienste auf diesem PC und dem Management Server dasselbe Benutzerkonto verwendet wird. Dieser Benutzer muss Mitglied einer Administratorengruppe sein.

Weiterführende Informationen in der Dokumentation

Ausführliche Informationen zu den verfügbaren Fenstern finden Sie in den folgenden Abschnitten:

– *Seite Kreuzschienen, Seite 135*

Ausführliche Informationen zu den verfügbaren schrittweisen Anweisungen finden Sie in den folgenden Abschnitten:

– *Konfigurieren eines Bosch Allegiant Geräts, Seite 135*

Siehe

– *Seite Kreuzschienen, Seite 135*

6.4.3 Bosch Allegiant Satellitensystem – Konzept

Mithilfe des Satellitenkonzepts der Allegiant Kreuzschiene können mehrere Allegiant Systeme verknüpft werden. In diesem Fall erkennt BVMS mehrere Allegiant Systeme als ein großes System, das Zugriff auf alle Kameras in allen Systemen bietet.

In einem Allegiant Satellitensystem sind die Monitorausgänge einer Allegiant Slave-Kreuzschiene mit den Videoeingängen der Allegiant Master-Kreuzschiene verknüpft. Diese Verbindung wird als Trunkline bezeichnet. Zusätzlich ist ein Steuerungskanal zwischen der Master-Kreuzschiene und der Slave-Kreuzschiene eingerichtet. Wenn die Allegiant Master-Kreuzschiene die Kamera einer Allegiant Slave-Kreuzschiene anfordert, wird ein Kommando an die Slave-Kreuzschiene gesendet mit der Anweisung, die angeforderte Kamera auf eine Trunkline umzuschalten. Gleichzeitig schaltet die Allegiant Master-Kreuzschiene den Trunkline-Eingang auf den angeforderten Allegiant Master-Monitorausgang um. Dadurch wird die Videoverbindung von der angeforderten Slave-Kamera zum gewünschten Master-Monitor vollständig hergestellt.

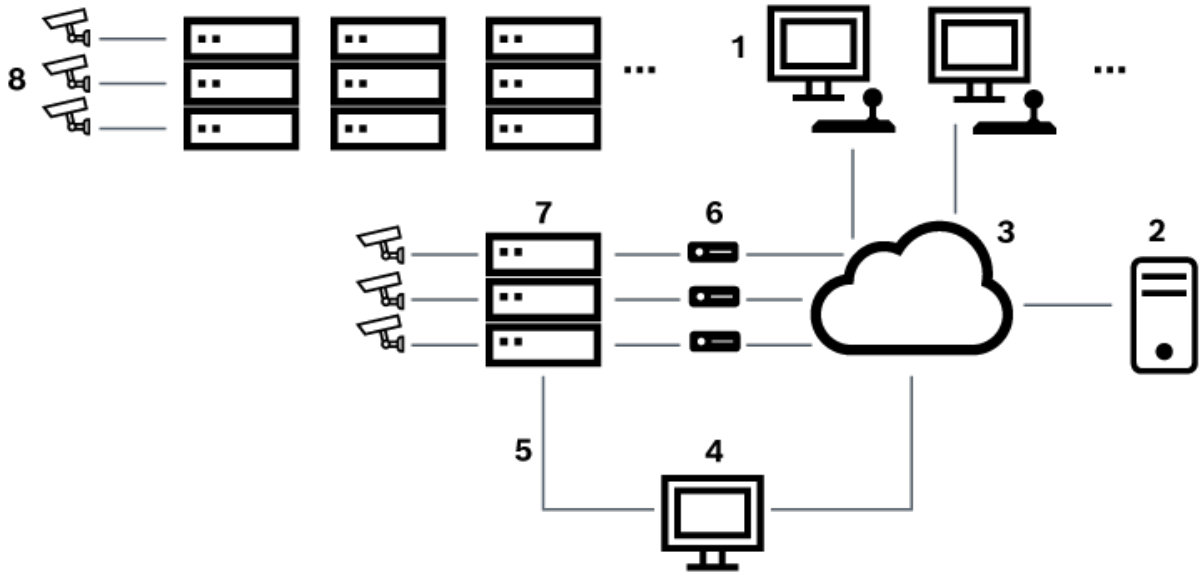


Abbildung 6.5: Mit Satellitenkreuzschienen erweitertes Bosch Allegiant System

1	BVMS Client-Arbeitsstationen
2	Management Server mit Master Control Software
3	Netzwerk
4	Allegiant PC mit Master Control Software
5	RS-232-Verbindung
6	Encoder
7	Allegiant Kreuzschiene

8	Allegiant Satellitenkreuzschiene

Sie können das Satellitenkonzept so nutzen, dass eine Allegiant Kreuzschiene sowohl als Master- als auch als Slave-Kreuzschiene fungiert. Auf diese Weise kann jede Allegiant Kreuzschiene die Kameras der anderen Kreuzschienen anzeigen. Dazu ist nur der beidseitige Anschluss der Trunklines und Steuerleitungen sowie die ordnungsgemäße Konfiguration der Allegiant Tabellen erforderlich.
Das Konzept kann nahezu ohne Einschränkung auf zahlreiche Allegiant Systeme erweitert werden. Eine Allegiant Kreuzschiene kann über viele Slave-Kreuzschienen verfügen und gleichzeitig Slave-Kreuzschiene für viele Master-Kreuzschienen sein. Sie können die Allegiant Tabellen so programmieren, dass der Benutzerzugriff auf Kameraansichten je nach Standortrichtlinie gewährt oder verweigert wird.

6.5 In BVMS unterstützte Allegiant CCL-Befehle

Um die CCL-Befehle zu verwenden, brauchen Sie das CCL-Benutzerhandbuch. Dieses Handbuch ist im Online-Produktkatalog im Dokumentenbereich jeder LTC Allegiant Kreuzschiene verfügbar.

Unterstützter Befehl	Beschreibung	Bemerkungen
Umschaltung/Sequenz		
LCM	Logische Kamera auf Monitor umstellen	LCM, LCM+ und LCM- sind äquivalent.
LCMP	Logische Kamera auf Monitor mit Vorpositionsabruf umstellen	
MON+CAM	Physische Kamera auf Monitor umstellen	
MON-RUN	Sequenz nach Monitornummer ausführen	
MON-HOLD	Sequenz nach Monitornummer anhalten	
SEQ-REQ	Sequenzanfrage	
SEQ-ULD	Sequenz entladen	
Empfänger/Treiber		
R/D	Grundlegende Steuerungsbefehle	
REMOTE-ACTION	Gleichzeitige Schwenk/ Neige/Zoom-Steuerungsbefehle	
REMOTE-TGL	Zwischen Schwenk/Neige/ Zoom-Steuerungsbefehlen wechseln	
PREPOS-SET	Vorposition einstellen	
PREPOS	Vorposition abrufen	

Unterstützter Befehl	Beschreibung	Bemerkungen
Umschaltung/Sequenz		
AUX-ON AUX-OFF	Zusätzliche Steuerungsbefehle – Zusatzfunktion einschalten – Zusatzfunktion ausschalten	
VARSPEED_PTZ	Steuerungsbefehle für variable Geschwindigkeit	
Alarm		Zur Kontrolle des virtuellen Eingangs Zum Beispiel schließt „+Alarm 1“ den virtuellen Eingang 1, „-Alarm 1“ öffnet virtuellen Eingang 1
+ALARM	Einen Alarm aktivieren	Öffnet einen virtuellen Eingang in BVMS.
-ALARM	Einen Alarm deaktivieren	Schließt einen virtuellen Eingang in BVMS.
System		
TC8x00>HEX	Hexadezimal-Modus einstellen	
TC8x00>DECIMAL	Dezimal-Modus einstellen	

7 Erste Schritte

Dieses Kapitel enthält Informationen zu den ersten Schritten mit BVMS.

7.1 Installieren der Software-Module

Hinweis!
Installieren Sie die einzelnen Softwaremodule auf dem für das jeweilige Modul vorgesehenen Computer.

So führen Sie die Installation durch:
Schließen Sie Configuration Client, bevor Sie das BVMS Setup starten.

1. Führen Sie Setup.exe aus oder starten Sie das BVMS Setup auf dem Willkommensbildschirm.
2. Wählen Sie im nächsten Dialogfeld die auf diesem Computer zu installierenden Module aus.
3. Folgen Sie den Anweisungen auf dem Bildschirm.

7.2 Verwendung von Config Wizard

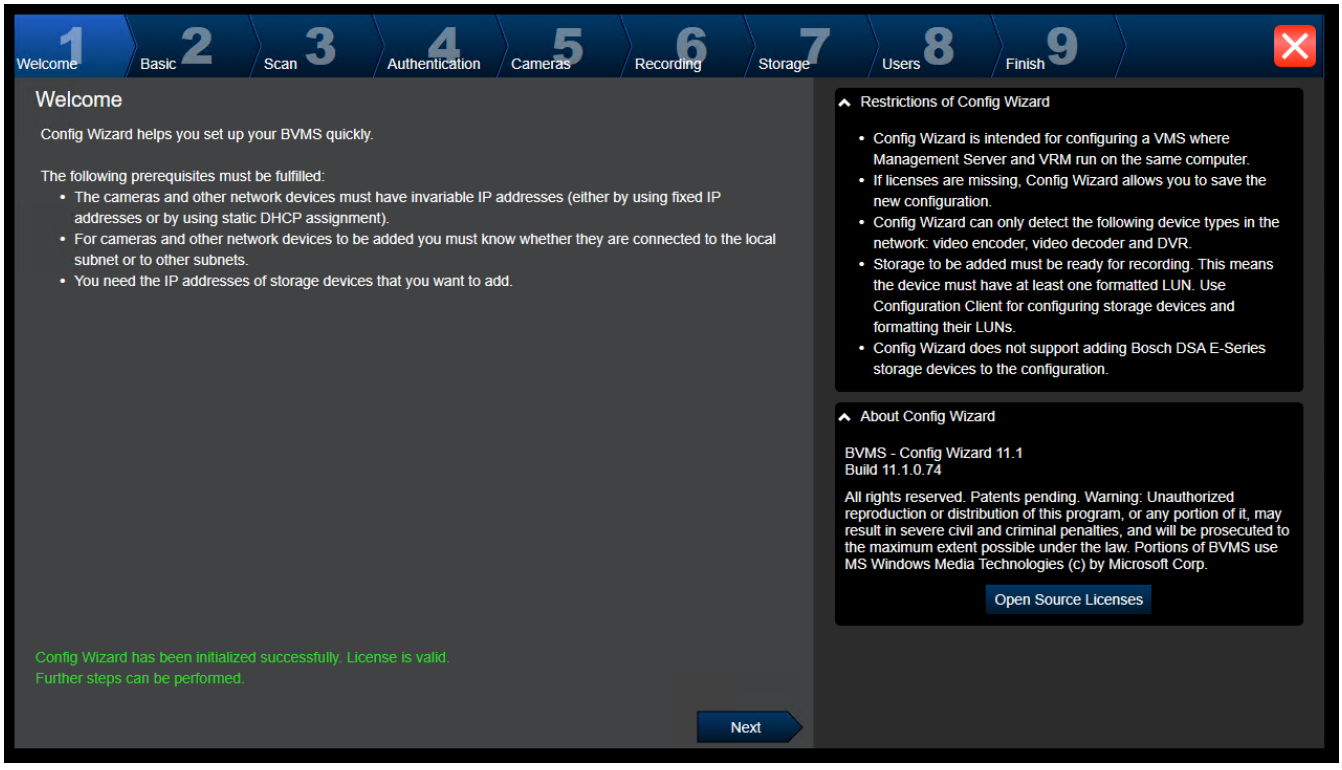
Bestimmungsgemäße Verwendung für Config Wizard ist die schnelle und einfache Konfiguration eines kleineren Systems. Config Wizard hilft Ihnen, ein konfiguriertes System zu erhalten, das Folgendes umfasst VRMiSCSI System, Kameras, Aufzeichnungsprofile und Benutzergruppen.
iSCSI-Systeme müssen Sie manuell zu einer Standard-Software-Installation hinzufügen.
Benutzergruppen und ihre Freigaben werden automatisch konfiguriert. Sie können Benutzer hinzufügen oder entfernen und Passwörter festlegen.
Der Config Wizard kann nur auf dem lokalen Computer auf Management Server zugreifen.
Sie können eine aktivierte Konfiguration als Sicherungskopie speichern und diese Konfiguration später importieren. Sie können die importierte Konfiguration nach dem Importieren ändern.
Config Wizard fügt dem lokalen VRM automatisch zu einer Standard-Software-Installation sowie in DIVAR IP hinzu.
Bei einem DIVAR IP wird das lokale iSCSI-Gerät ebenfalls automatisch hinzugefügt, falls es nicht bereits verfügbar ist.

Hinweis!
Wenn Sie für das System Decoder verwenden möchten, achten Sie darauf, dass für alle Encoder das gleiche Passwort für die user-Berechtigungsstufe verwendet wird.

So starten Sie den Config Wizard**:**

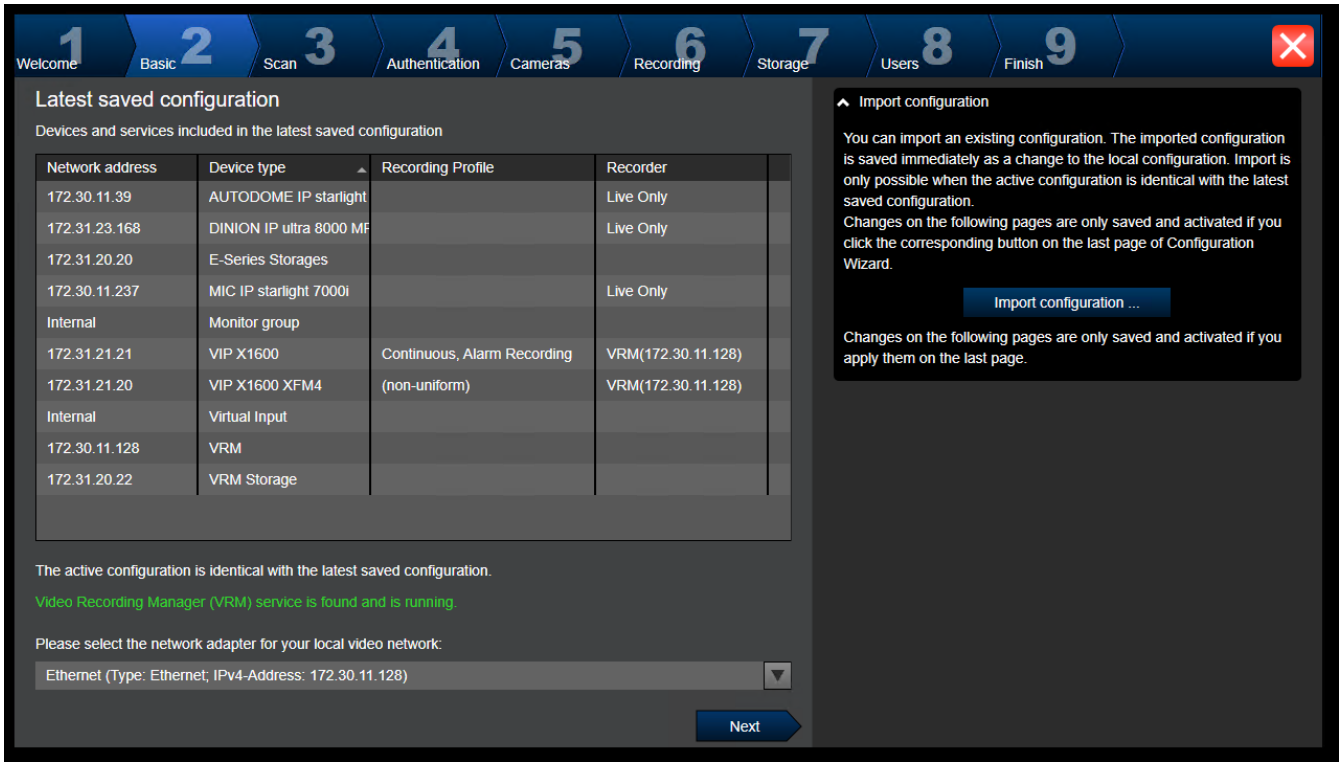
- Klicken Sie auf **Start** > **Alle Programme** > BVMS > Config Wizard.
  Die Seite Welcome wird angezeigt.

Seite Welcome



- Klicken Sie auf **Next**, um fortzufahren.

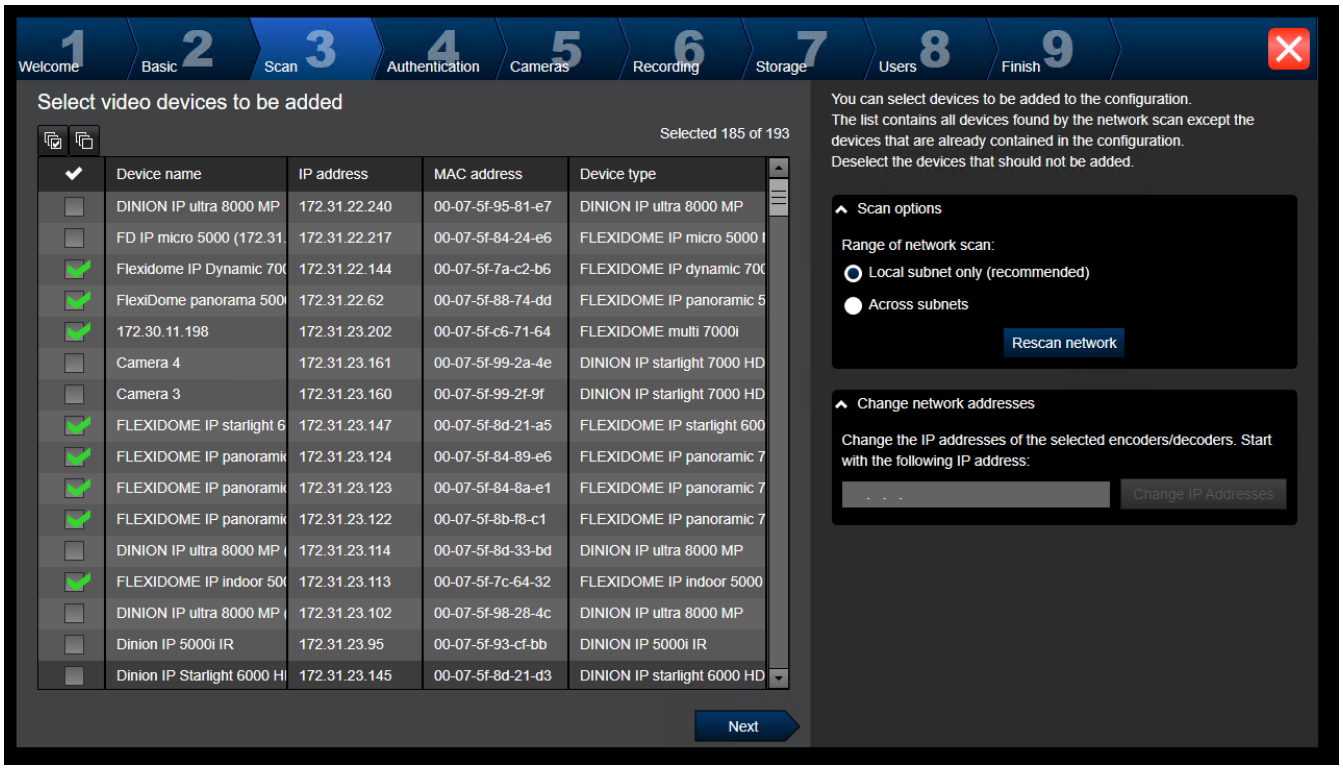
Seite Basic



Diese Seite zeigt die zuletzt gespeicherte Konfiguration an. Sie können eine BVMS-Datei als eine Änderung der vorhandenen Konfiguration importieren. Wenn Sie auf **Next** klicken, wird diese Änderung gespeichert, aber nicht aktiviert.

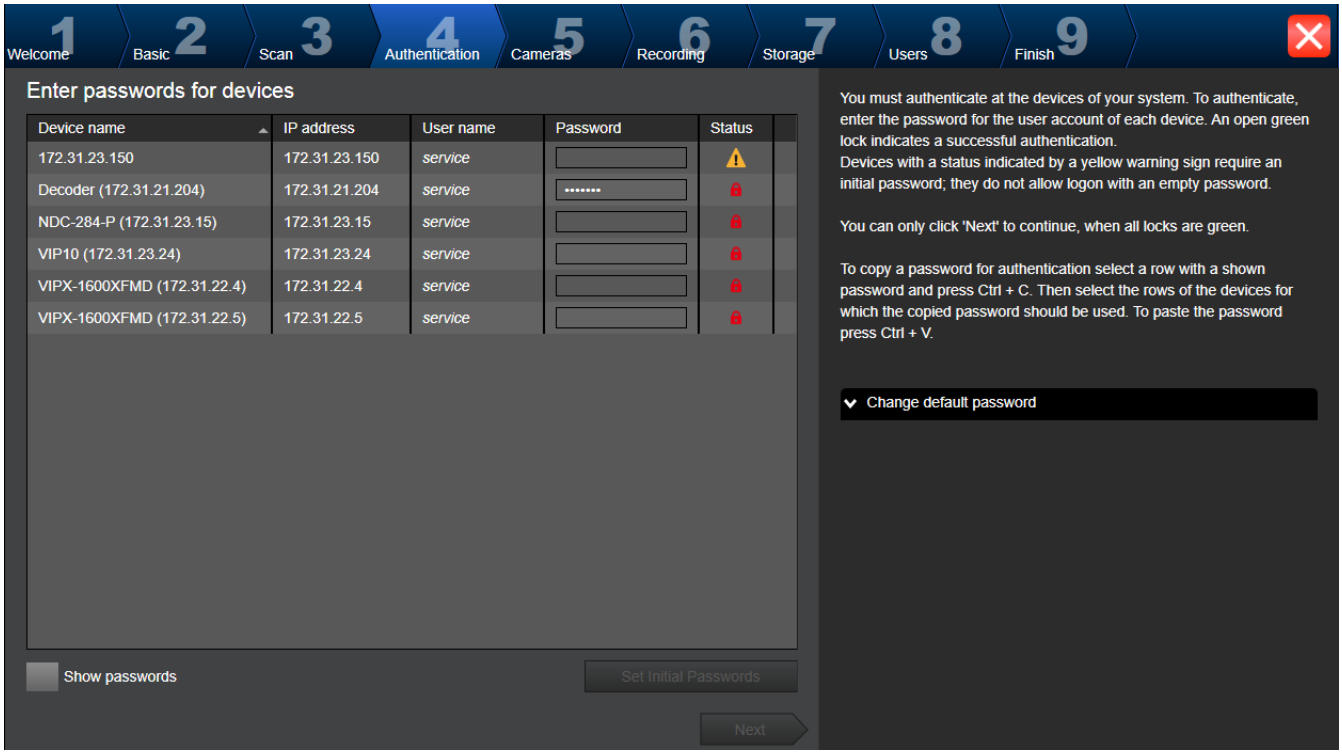
Sie können den Netzwerkadapter Ihres Computers auswählen, der mit den Videogeräten (IP-Kameras, Encodern, Decodern, iSCSI-Speichersystemen) Ihres Systems verbunden ist. Die IP-Adresse dieses Netzwerkadapters dient als IP-Adresse des VRM, des VSG und des lokalen iSCSI-Speichersystems. Klicken Sie auf **Port Mapping**, um die öffentliche IP-Adresse oder den DNS-Namen zu definieren, wenn über das Internet auf das System zugegriffen wird.

Seite Scan



Hinweis:
Die Suche nach Geräten kann eine Weile dauern. Sie können den Suchvorgang abbrechen. Alle bereits gefundenen Geräte werden in einer Tabelle angezeigt.
Auf dieser Seite werden alle Videogeräte aufgeführt, die nicht in der zuletzt gespeicherten Konfiguration enthalten sind.
Deaktivieren Sie die Kontrollkästchen für die Geräte, die nicht zur Konfiguration hinzugefügt werden sollen, und klicken Sie dann auf **Next**.
Wenn sich die ausgewählten Geräte nicht im gleichen IP-Bereich wie das DIVAR IP-System befinden, kann die IP-Adresse des Geräts geändert werden, indem eine Startadresse für den IP-Bereich des Geräts definiert wird.

Seite Authentication



Diese Seite wird für die Authentifizierung bei passwortgeschützten Videogeräten verwendet. Zur einfachen Authentifizierung mit demselben Passwort für mehrere Geräte können Sie die Zwischenablage (über CTRL+C, CTRL+V) nutzen:

1. Klicken Sie auf **Passwörter anzeigen**.
2. Wählen Sie eine Zeile mit einem erfolgreich authentifizierten Gerät aus (es wird ein grünes Schloss angezeigt) und drücken Sie CTRL+C. Wählen Sie mehrere Zeilen mit einem roten Schloss, und drücken Sie CTRL+V.

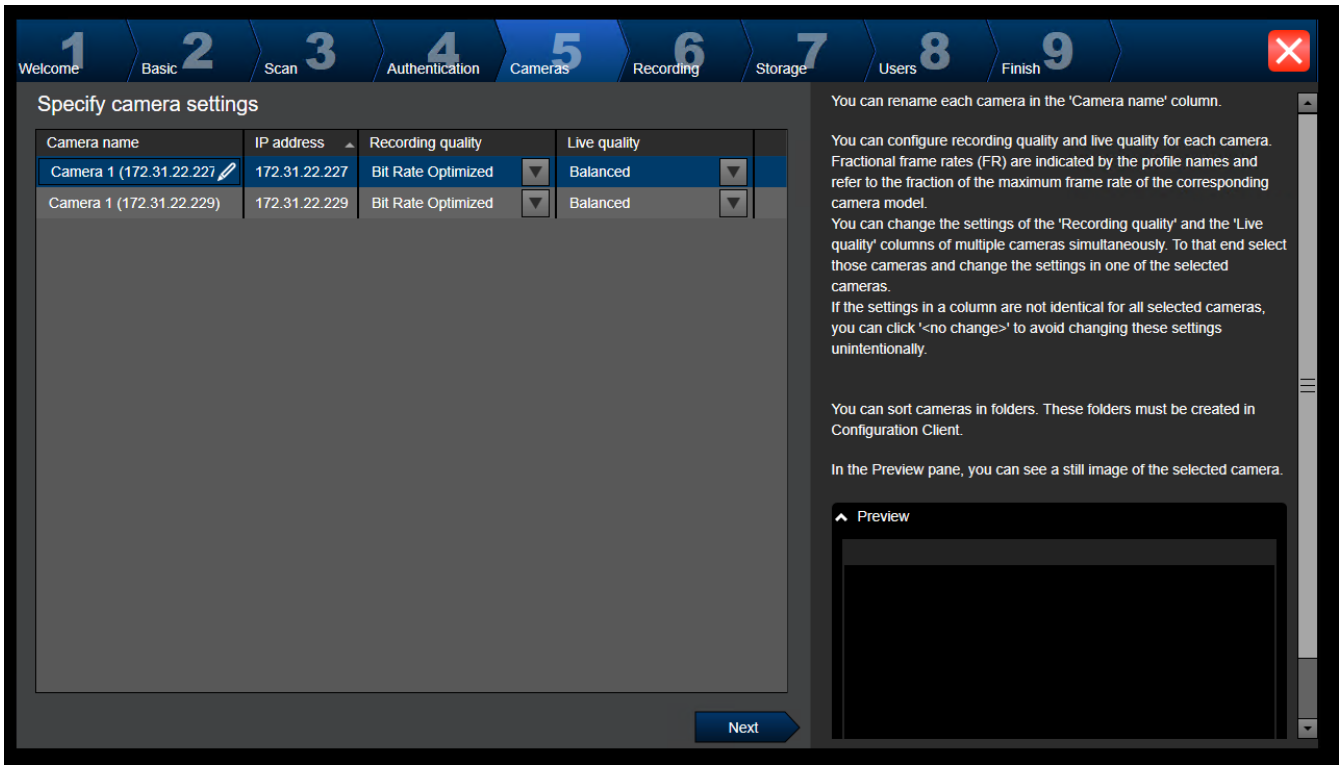
Die Passwortprüfung erfolgt automatisch, wenn Sie einige Sekunden lang kein weiteres Zeichen in dem Passwortfeld eingeben oder außerhalb des Passwortfelds klicken.
Sie können ein globales Standardpasswort für alle Geräte bereitstellen, die aktuell nicht durch ein Passwort geschützt werden.

Wenn ein Gerät ein erstes Passwort erfordert, wird angezeigt.

So legen Sie ein erstes Passwort fest:

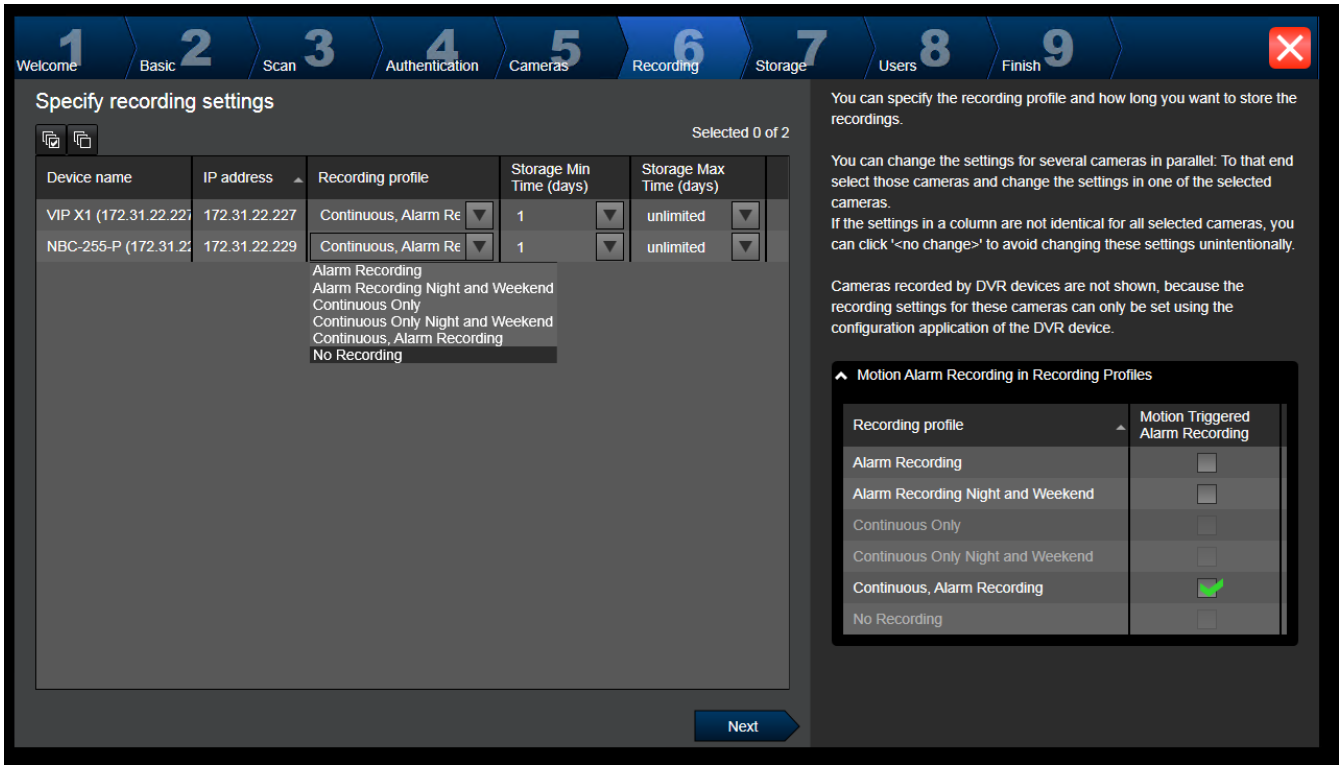
1. Geben Sie das Passwort im Feld **Passwort** ein.
2. Klicken Sie auf **Setzen Sie initiale Passwörter**.
   Das erste Passwort wird festgelegt.
   Hinweis: Solange Sie kein erstes Passwort für alle Geräte in der Liste festgelegt haben, die ein erstes Passwort benötigen, können Sie nicht fortfahren.
3. Klicken Sie auf **Weiter**, um fortzufahren.

Seite Cameras



Mithilfe dieser Seite können Sie die Kameras des Systems verwalten.

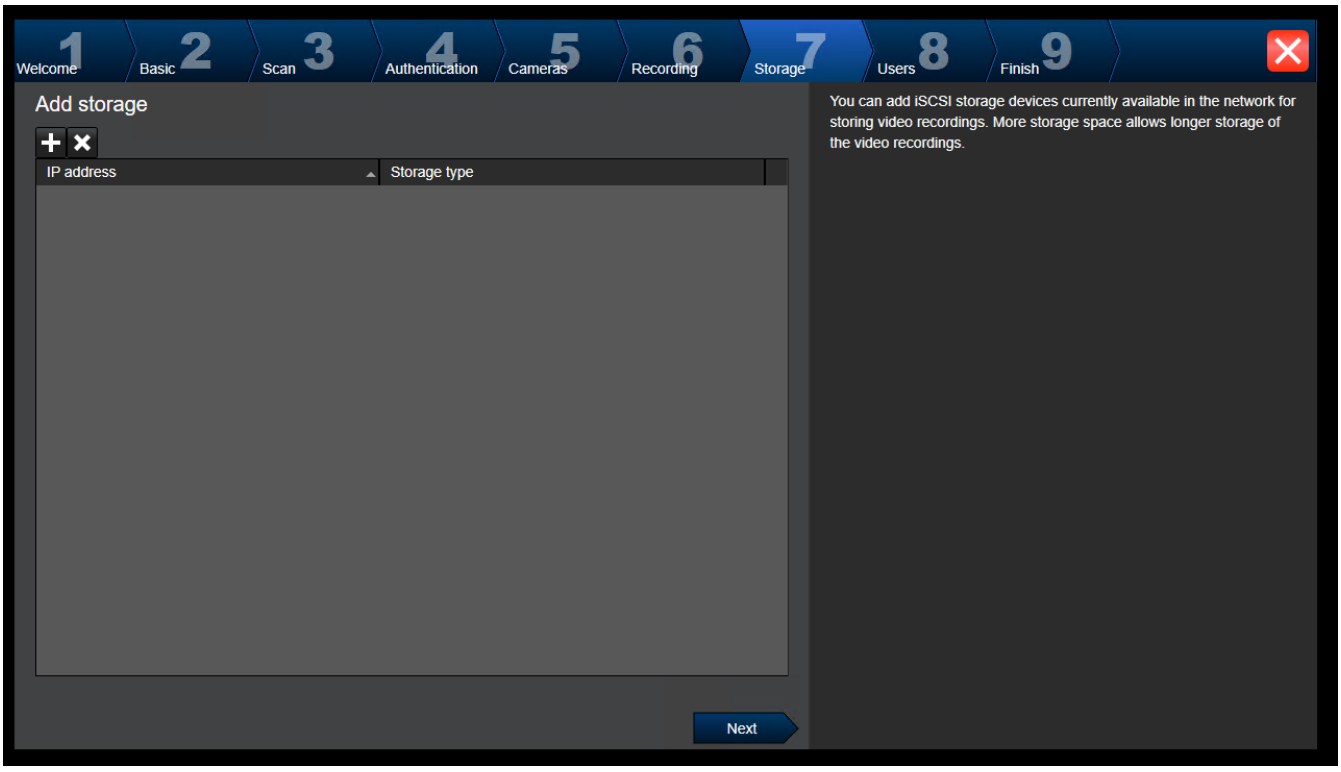
Seite Recording



Es werden auf dieser Seite nur jene Kameras angezeigt, die neu hinzugefügt wurden. Sobald Sie diese Konfiguration aktivieren, können Sie die Profilzuordnungen dieser Kameras nicht mehr ändern.

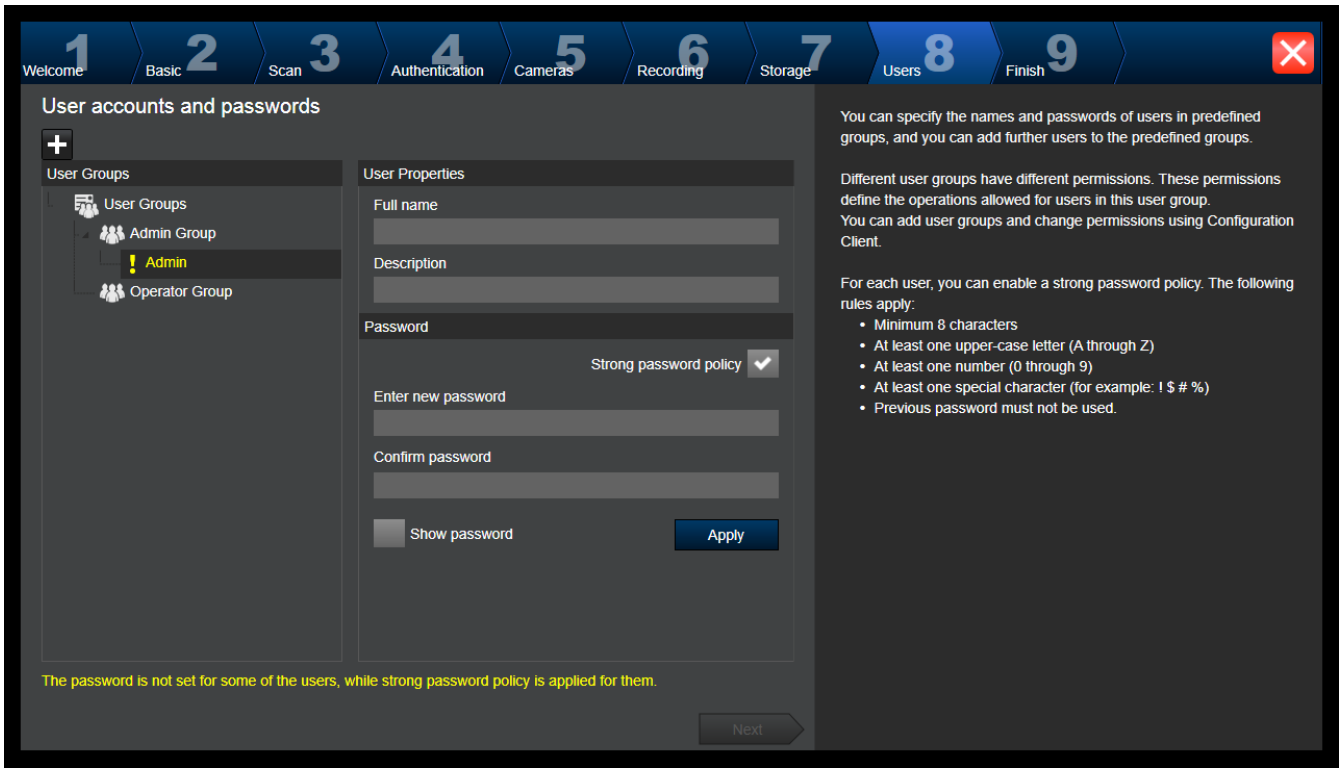
Sie können die Bewegungsaufzeichnung für die Aufzeichnung von Profilen mit aktivierter Aufzeichnung und Alarmaufzeichnung aktivieren. Konfigurieren Sie bei Bedarf die Aufzeichnung und Alarmaufzeichnung im Configuration Client (Dialogfeld **Geplante Aufzeichnungseinstellungen**). VCA ist für jede neu hinzugefügte Kamera automatisch aktiviert.

Seite Storage



Diese Seite ermöglicht das Hinzufügen von weiteren iSCSI-Speichergeräten.

Seite Users



Auf dieser Seite können Sie neue Benutzer zu den vorhandenen Benutzergruppen hinzufügen.

- ▸ Geben Sie für jeden neuen Benutzer einen Benutzernamen und eine Beschreibung ein und legen Sie ein Passwort fest.

Richtlinie für sichere Passwörter

Das Kontrollkästchen **Richtlinie für sichere Passwörter** ist bereits für alle neu erstellten Benutzergruppen aktiviert.

Es wird dringend empfohlen, diese Einstellung beizubehalten, um Ihren Computer besser vor unbefugtem Zugriff zu schützen.

Es gelten die folgenden Regeln:

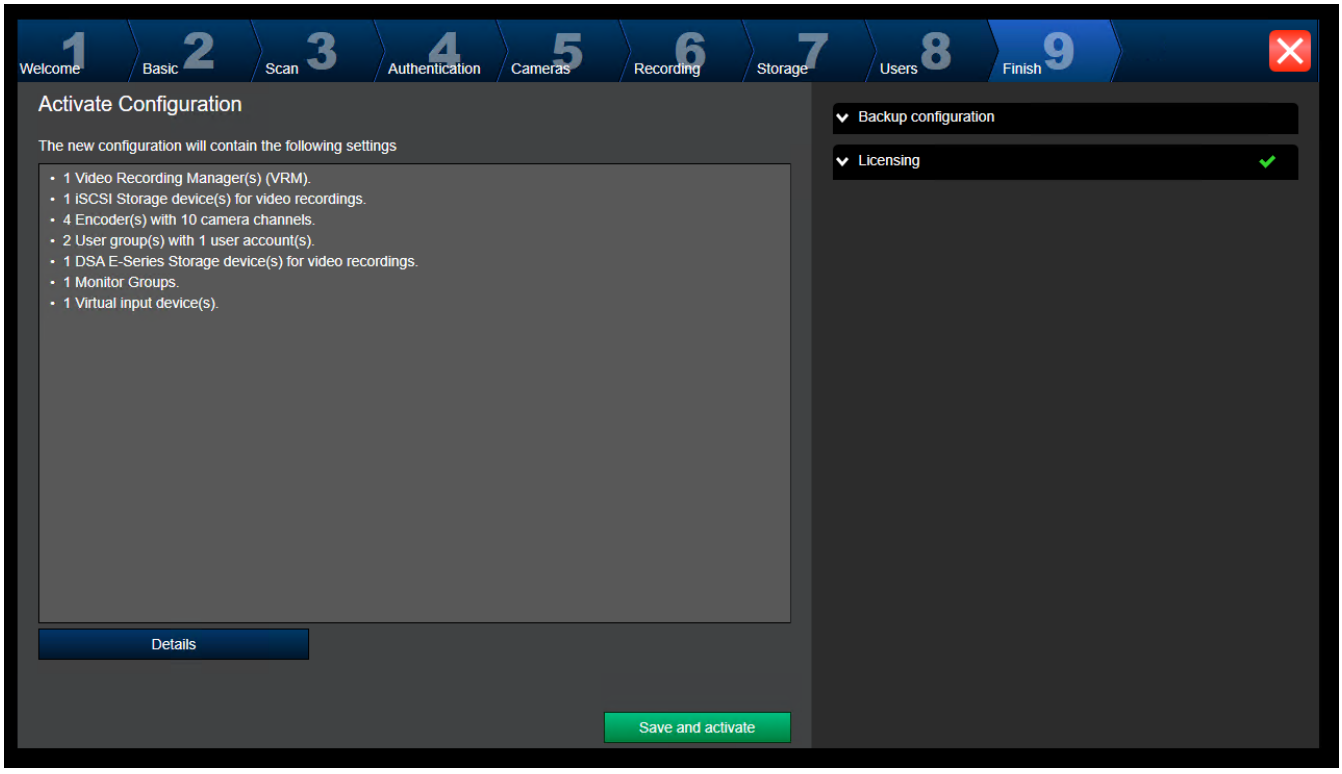
- – Mindestlänge des Passworts gemäß den Angaben auf der Seite **Kontorichtlinien** für die entsprechende Benutzergruppe.
- – Verwenden Sie keines der vorherigen Passwörter.
- – Verwenden Sie mindestens einen Großbuchstaben (A bis Z).
- – Verwenden Sie mindestens eine Ziffer (0 bis 9).
- – Verwenden Sie mindestens ein Sonderzeichen (z. B.: ! $ # %).

- ▸ Klicken Sie auf **Übernehmen**, um die Einstellungen zu übernehmen und klicken Sie anschließend zum Fortfahren auf **Weiter**.

  Hinweis: Solange Benutzer existieren, für die kein Passwort festgelegt wurde, obwohl die **Richtlinie für sichere Passwörter** aktiviert wurde, können Sie nicht fortfahren. Legen Sie zum Fortfahren die fehlenden Passwörter fest.

Verwenden Sie den Configuration Client, um Benutzergruppen hinzuzufügen und Berechtigungen für Benutzergruppen zu ändern.

Seite Finish



Bevor Sie Ihre Konfiguration aktivieren können, müssen Sie die nachfolgenden Schritte durchführen:

– Stellen Sie ein globales Standardpasswort für alle Geräte bereit, die aktuell nicht durch ein Passwort geschützt werden.
– Aktivieren Sie ggf. Ihr Lizenzpaket.

Globales Standardpasswort

Wenn in Configuration Client die Option **Passwortschutz bei Aktivierung erzwingen** (**Einstellungen** -> **Optionen**) deaktiviert ist, müssen Sie kein globales Standardpasswort zur Aktivierung bereitstellen.

Lizenzierung

Blenden Sie **Lizensieren** ein und klicken Sie **Lizenz-Assistent**, um Ihr Lizenzpaket zu überprüfen oder zu aktivieren.

Durch Klicken auf **Save and activate** wird die Konfiguration aktiviert.

Nach erfolgreicher Aktivierung wird die Seite **Fertig stellen** wieder angezeigt. Sie können nun bei Bedarf eine Sicherungskopie der Konfiguration speichern. Klicken Sie dazu auf **Save backup copy**.

Durch Klicken auf **Save and activate** wird die Konfiguration aktiviert.

Nach erfolgreicher Aktivierung wird die Seite **Fertig stellen** wieder angezeigt. Sie können nun bei Bedarf eine Sicherungskopie der Konfiguration speichern. Klicken Sie dazu auf **Save backup copy**.

7.3 Starten des Configuration Client

Hinweis!

Nur Admin-Benutzer können sich beim Configuration Client anmelden.

Der standardmäßig vorkonfigurierte Admin-Benutzer ist der Benutzer namens Admin. Nur dieser Benutzer kann sich beim Configuration Client anmelden, wenn Sie den Configuration Client zum ersten Mal starten.
Wenn Sie den Configuration Client gestartet haben, können Sie den Admin-Benutzer umbenennen und das Passwort ändern.

Hinweis:
Sie können den Configuration Client nicht starten, wenn ein anderer Benutzer den Configuration Client bereits auf einem anderen Computer im System gestartet hat.

So starten Sie den Configuration Client:

1. Wählen Sie im Menü **Start Programme** > BVMS > Configuration Client.
   Das Anmeldedialogfeld wird angezeigt.
2. Geben Sie im Feld **Benutzername:** Ihren Benutzernamen ein.
   Wenn Sie die Anwendung zum ersten Mal starten, geben Sie als Benutzernamen Admin ein. Ein Passwort ist nicht erforderlich.
3. Geben Sie im Feld **Passwort:** Ihr Passwort ein.
4. Klicken Sie auf **OK**.
   Die Anwendung wird gestartet.

Wenn der Admin-Benutzer Configuration Client zum ersten Mal startet, wird das Dialogfeld **Passwortrichtlinie verletzt** angezeigt, in dem er aufgefordert wird, ein Passwort für das Admin-Benutzerkonto festzulegen. Es wird dringend empfohlen, diese Einstellung beizubehalten und für das Admin-Benutzerkonto ein starkes Passwort entsprechend der Passwortrichtlinie festzulegen.

Siehe

- *Richtlinie für sichere Passwörter , Seite 357*
- *Konfigurieren der Admin-Gruppe, Seite 362*

7.4 Konfigurieren der Sprache des Configuration Client

Sie können die Sprache des Configuration Client unabhängig von der Sprache Ihrer Windows Installation konfigurieren.

So konfigurieren Sie die Sprache:

1. Klicken Sie im **Einstellungen**-Menü auf **Optionen...**.
   Das Dialogfeld **Optionen** wird angezeigt.
2. Wählen Sie in der Liste **Sprache** die gewünschte Sprache aus.
   Wenn Sie den Eintrag **Systemsprache** auswählen, wird die Sprache der Windows Installation verwendet.
3. Klicken Sie auf **OK**.
   Die Sprache wird beim nächsten Start der Anwendung gewechselt.

7.5 Konfigurieren der Sprache des Operator Client

Sie können die Sprache des Operator Client unabhängig von der Sprache Ihrer Windows Installation und des Configuration Client konfigurieren. Dieser Schritt wird im Configuration Client durchgeführt.

So konfigurieren Sie die Sprache:

1. Klicken Sie auf **Benutzergruppen** > . Klicken Sie auf die Registerkarte **Eigenschaften der Benutzergruppen**. Klicken Sie auf die Registerkarte **Bedienberechtigungen**.
2. Wählen Sie in der Liste **Sprache** die gewünschte Sprache aus.

3. Klicken Sie auf , um die Einstellungen zu speichern.
4. Klicken Sie auf , um die Konfiguration zu aktivieren.
   Starten Sie den Operator Client neu.

7.6 Nach Geräten suchen

Hauptfenster > **Geräte**

Sie können nach den folgenden Geräten suchen, um diese über das Dialogfeld **BVMS Scan Wizard** hinzuzufügen:

- VRM-Geräte
- Encoder
- Nur-Live-Encoder
- Nur-Live-Encoder von ONVIF
- Encoder mit lokaler Archivierung
- Decoder
- Video Streaming Gateway-(VSG-)Geräte
- DVR-Geräte

Wenn Sie Geräte per Suchvorgang hinzufügen möchten, finden Sie im Kapitel *Seite Geräte, Seite 125* beim entsprechenden Gerätethema weiterführende Informationen.

Siehe

- *Hinzufügen eines VRM-Geräts per Suchvorgang, Seite 170*
- *Hinzufügen eines Nur-Live-ONVIF-Geräts per Suchvorgang, Seite 238*
- *Hinzufügen von Nur-Live-Geräten per Suchvorgang, Seite 210*
- *Hinzufügen eines Geräts, Seite 126*

7.7 Systemzugriff

So können Sie auf ein System zugreifen:

1. Wählen Sie mit einem der folgenden Schritte die Netzwerkadresse des gewünschten Systems aus:
   - Klicken Sie auf einen vorausgewählten Listeneintrag.
   - Geben Sie eine Netzwerkadresse manuell ein.
   - Wählen Sie eine Netzwerkadresse mit Server Lookup.
2. Melden Sie sich beim gewünschten System an:
   - Single-Server-System
   - Enterprise System

7.8 Mittels Server Lookup

- Mit der BVMS Server Lookup-Funktion können Benutzer eine Verbindung mit einem BVMS Management Server aus einer bereitgestellten Server-Liste herstellen.
- Ein einzelner Benutzer von Configuration Client oder Operator Client kann nacheinander zu mehreren System-Access Points eine Verbindung herstellen.
- System-Access Points können entweder Management Server oder Enterprise Management Server sein.
- Server Lookup verwendet dedizierte Management Server zum Hosten der Server-Liste.

– Server Lookup und Management Server oder Enterprise Management Server können funktional auf einem Computer ausgeführt werden.
– Server Lookup unterstützt Sie bei der Suche von System-Access Points durch ihren Namen oder Beschreibungen.
– Sobald der Operator Client mit dem Management Server verbunden ist, empfängt er Ereignisse und Alarme vom BVMS Management Server und zeigt Live- und aufgezeichnete Inhalte an.

Zugriff:

1. Starten Sie den Operator Client oder den Configuration Client.
   Das Anmeldedialogfeld wird angezeigt.
2. Wählen Sie in der Liste **Verbindung:** die Option **<Adressbuch...>** für Configuration Client oder **<Adressbuch...>** für Operator Client.
   Wenn private und öffentliche IP-Adressen für einen Server konfiguriert wurden, wird dies angezeigt.
   Wenn Sie **<Adressbuch...>** oder **<Adressbuch...>** zum ersten Mal wählen, wird das Dialogfeld **Server lookup** angezeigt.
3. Geben Sie im Feld **(Enterprise) Management Server-Adresse** eine gültige Netzwerkadresse des gewünschten Servers an.
4. Geben Sie einen gültigen Benutzernamen und ein Passwort ein.
5. Klicken Sie gegebenenfalls auf **Einstellungen beibehalten**.
6. Klicken Sie auf **OK**.
   Das Dialogfeld **Server lookup** wird angezeigt.
7. Wählen Sie den gewünschten Server aus.
8. Klicken Sie auf **OK**.
9. Wenn der gewählte Server eine private und eine öffentliche Netzwerkadresse hat, wird ein Meldungsfeld angezeigt und gefragt, ob Sie einen Computer verwenden, der sich im privaten Netzwerk des gewählten Servers befindet.
   Der Servername wird zur Liste **Verbindung:** im Anmeldedialogfeld hinzugefügt.
10. Wählen Sie diesen Server aus der Liste **Verbindung:** aus und klicken Sie auf **OK**.
    Wenn Sie das Kontrollkästchen **Einstellungen beibehalten** aktiviert haben, können Sie diesen Server direkt auswählen, wenn Sie erneut auf diesen Server zugreifen möchten.

7.9 Aktivieren der Softwarelizenzen

Wenn Sie BVMS zum ersten Mal installieren, müssen Sie die Lizenzen für die von Ihnen bestellten Softwarepakete einschließlich des Basispakets und der Erweiterungen und/oder optionalen Funktionen aktivieren.

So aktivieren Sie das System:

1. Starten Sie BVMS Configuration Client.
2. Klicken Sie im Menü **Werkzeuge** auf **Lizenz Manager...**.
   Das Dialogfeld **Lizenz-Manager** wird angezeigt.
3. Klicken Sie auf **Hinzufügen**, um Ihre Lizenzen hinzuzufügen.
   Das Dialogfeld **Lizenz hinzufügen** wird angezeigt.
4. Befolgen Sie die Anweisungen im Dialogfeld.
5. Nach der erfolgreichen Aktivierung können Sie das Dialogfeld **Lizenz hinzufügen** schließen.
6. Schließen Sie das Dialogfeld **Lizenz-Manager**.

Weitere Informationen finden Sie im entsprechenden Whitepaper der BVMS Lizenz.

Siehe

- *Dialogfeld „License Inspector“ (Menü „Werkzeuge“), Seite 76*
- *Dialogfeld „Lizenz-Manager“ (Menü „Werkzeuge“), Seite 75*
- *Dialogfeld „Lizenz hinzufügen“, Seite 76*
- *Überblick über die BVMS Lizenzaktivierung, Seite 20*

7.9.1 Dialogfeld „Lizenz-Manager“ (Menü „Werkzeuge“)

Hauptfenster > Menü **Werkzeuge** > Befehl **Lizenz Manager...**

Dient zum Lizenzieren des von Ihnen erworbenen BVMS Pakets sowie zum Aufrüsten mit zusätzlichen Funktionen.

Lizenzstatus

Zeigt den Lizenzstatus an.

System Fingerprint

Zu Supportzwecken empfehlen wir die Angabe des **System Fingerprint**.

Installationsort

Bei Aktivierung Ihrer Basislizenz im Bosch Remote Portal geben Sie Informationen zum Installationsstandort Ihres Systems an. Diese Informationen werden hier angezeigt.

Hinweis: Sie können diese Informationen auch in anderen Lizenzen angeben, aber nur die in der Basislizenz angegebenen Informationen werden hier angezeigt.

Lizenzen

1. Klicken Sie auf **Hinzufügen**, um Ihre Lizenzen hinzuzufügen.
   Das Dialogfeld **Lizenz hinzufügen** wird angezeigt.
2. Befolgen Sie die Anweisungen im Dialogfeld.

Gültige Lizenz

Zeigt die von Ihnen aktivierte Basislizenz an.

Features

- Klicken Sie auf **Lizenz Inspektor...**.
  Das Dialogfeld **Lizenz-Inspektor** wird angezeigt.

Zeigt die Anzahl der lizenzierten Funktionen an, die derzeit installiert sind.

Sie können überprüfen, ob die Anzahl der installierten BVMS Lizenzen die Anzahl der erworbenen Lizenzen übersteigt.

Installierte BVMS Versionen

Zeigt die aktuell installierte Version von BVMS an, z. B. 11.0.

Lizenzierte BVMS Versionen

Zeigt alle BVMS Versionen an, die in der aktuell bereitgestellten Lizenzdatei enthalten sind und unterstützt werden.

Beispiel: BVMS 11.0 und alle zukünftigen Unterversionen BVMS 11.x.

Aktivierungsdatum

Zeigt das Aktivierungsdatum Ihrer installierten BVMS Version an.

Ablaufdatum

Zeigt das Ablaufdatum Ihrer installierten BVMS Version an. Ein Ablaufdatum ist nur vorhanden, wenn Sie eine Notfalllizenz oder eine Vertriebs-Demolizenz installieren.

Software Maintenance Agreement

Ablaufdatum

Wenn Sie ein Software Maintenance Agreement gekauft und aktiviert haben, wird hier das Ablaufdatum angezeigt.

Siehe

- *Aktivieren der Softwarelizenzen, Seite 74*
- *Dialogfeld „Lizenz hinzufügen“, Seite 76*
- *Dialogfeld „License Inspector“ (Menü „Werkzeuge“), Seite 76*

7.9.1.1 Dialogfeld „Lizenz hinzufügen“

Hauptfenster > Menü **Werkzeuge** > Befehl **Lizenz Manager...** > **Lizenzen** > **Hinzufügen**

Hier können Sie Ihre erworbenen Lizenzen oder Demolizenzen von der Bosch Remote Portal Website remote.boschsecurity.com zu Ihrem BVMS System hinzufügen.

Befolgen Sie die Anweisungen im Dialog, um Ihre Lizenzen hinzuzufügen.

Weitere Informationen finden Sie im entsprechenden Whitepaper der BVMS Lizenz.

7.9.2 Dialogfeld „Lizenz hinzufügen“

Hauptfenster > Menü **Werkzeuge** > Befehl **Lizenz Manager...** > **Lizenzen** > **Hinzufügen**

Hier können Sie Ihre erworbenen Lizenzen oder Demolizenzen von der Bosch Remote Portal Website remote.boschsecurity.com zu Ihrem BVMS System hinzufügen.

Befolgen Sie die Anweisungen im Dialog, um Ihre Lizenzen hinzuzufügen.

Weitere Informationen finden Sie im entsprechenden Whitepaper der BVMS Lizenz.

7.9.3 Dialogfeld „License Inspector“ (Menü „Werkzeuge“)

Hauptfenster > Menü **Werkzeuge** , Klick auf **Lizenz Inspektor...** Befehl > **Lizenz-Inspektor**

Dialogfenster

Zeigt die Anzahl der lizenzierten Funktionen an, die derzeit installiert sind.

Sie können überprüfen, ob die Anzahl der installierten BVMS Lizenzen die Anzahl der erworbenen Lizenzen übersteigt.

Hinweis: Wenn die aktuelle Systemkonfiguration die Grenzwerte der derzeit installierten Lizenzen überschreitet, können Sie die Konfiguration nicht aktivieren.

7.10 Warten von BVMS

Dieses Kapitel enthält Informationen zur Pflege eines gerade installierten oder aufgerüsteten BVMS.

Führen Sie zur Pflege des Systems folgende Aufgaben durch:

- Exportieren Sie die BVMS Konfiguration und Benutzereinstellungen. Die Versionshistorie (alle Konfigurationsversionen, die zu einem früheren Zeitpunkt aktiviert wurden) wird nicht exportiert. Es wird empfohlen, die Konfiguration vor dem Export zu aktivieren.
  - Informationen zum Verfahren finden Sie unter *So exportieren Sie Konfigurationsdaten:, Seite 77*.

oder

- Nehmen Sie eine Sicherung von elements.bvms vor. Dies ist erforderlich, wenn Sie einen (Enterprise) Management Server einschließlich der Versionshistorie wiederherstellen möchten. Benutzereinstellungen werden hierbei nicht berücksichtigt.
  - Informationen zum Verfahren finden Sie unter *So führen Sie eine Sicherung durch:, Seite 77*.
- Speichern Sie die VRM-Konfigurationsdatei (config.xml).
  - Informationen zum Verfahren finden Sie unter *So speichern Sie die VRM-Konfiguration:, Seite 77*.

Diese exportierte Konfiguration behält keine Historie des Systems. Es ist kein Rollback möglich.

Die gesamte Systemkonfiguration, einschließlich der vollständigen Historie der Systemänderungen, wird in einer Datei gespeichert:

C:\ProgramData\Bosch\VMS\Elements.bvms.

So exportieren Sie Konfigurationsdaten:

1. Klicken Sie im **System**-Menü auf **Konfiguration exportieren...**
   Das Dialogfeld **Konfigurationsdatei exportieren** wird angezeigt.

   Hinweis: Wenn die aktuelle Konfiguration der Arbeitskopie nicht aktiviert ist (aktiv ist), wird diese Arbeitskopie exportiert und nicht die aktivierte Konfiguration.
2. Klicken Sie auf **Speichern**.
3. Geben Sie einen Dateinamen ein.
   Die aktuelle Konfiguration wird exportiert. Eine ZIP-Datei mit Datenbank und Benutzerdaten wird erstellt.

So führen Sie eine Sicherung durch:

1. Beenden Sie den BVMS **Central Server**-Dienst auf dem (Enterprise) Management Server.
2. Kopieren Sie die Datei elements.bvms zur Sicherung in das gewünschte Verzeichnis.
3. Starten Sie den BVMS **Central Server**-Dienst auf dem (Enterprise) Management Server.

Die VRM-Konfiguration wird in einer einzigen verschlüsselten Datei namens config.xml gespeichert. Die Datei kann zu Sicherungszwecken kopiert und gespeichert werden, während sich der VRM-Dienst im laufenden Betrieb befindet.
Die Datei ist verschlüsselt und enthält alle für den VRM relevanten Daten wie:

- Benutzerdaten
- alle Systemgeräte und ihre für den VRM relevanten Einstellungen

Teile der VRM-Konfiguration werden ebenfalls in der BVMS Konfiguration gespeichert. Bei einer Änderung dieser Daten werden diese nach der Aktivierung der BVMS Konfiguration in die Datei config.xml geschrieben.
Die folgenden Einstellungen werden nicht in der BVMS Konfiguration gespeichert:

- **VRM-Einstellungen** > **Haupteinstellungen**
- **Netzwerk** > **SNMP**
- **Service** > **Erweitert**
- **Aufzeichnungspräferenzen**
- **Lastverteilung**

Sobald sie Änderungen an einer dieser Seiten vornehmen, werden diese umgehend auf den VRM-Server geschrieben und nicht in der BVMS Konfiguration gespeichert.

So speichern Sie die VRM-Konfiguration:

- Kopieren Sie die Datei Config.xml an einen sicheren Ort.
  Bei einem Primären VRM finden Sie diese Datei in folgendem Verzeichnis:
  C:\ProgramData\Bosch\VRM\primary
  Bei einem Sekundären VRM finden Sie diese Datei in folgendem Verzeichnis:
  C:\ProgramData\Bosch\VRM\\secondary

7.11 Austausch eines Geräts

Dieses Kapitel enthält Informationen zur Reparatur des Systems, wenn Geräte bspw. ausfallen und ausgetauscht werden müssen.

Voraussetzung
Die Pflegeaufgaben wurden vorgenommen.

Siehe

- *Warten von BVMS, Seite 76*

7.11.1 Austausch eines MS/EMS

Hierbei besteht kein Unterschied zwischen einem Austausch des Management Server und einem Austausch des Enterprise Management Server.
Sie können entweder die Konfiguration des alten Management Server bzw. Enterprise Management Server wiederherstellen oder die exportierte Konfiguration importieren.
Bei einer Wiederherstellung der Konfiguration bleibt die Server-ID unverändert.
Bei einer Import der Konfiguration wird die Server-ID des neuen Systems verwendet. Sie benötigen eine neue Server-ID, wenn Sie ein Enterprise System unter Verwendung der exportierten Konfiguration erstellen möchten, die Sie auf jeden Management Server als Vorlage importieren. Jeder Management Server in diesem Enterprise System muss eine eindeutige Server-ID besitzen.
Sie können eine exportierte Konfiguration und die Benutzereinstellungen dieser Konfiguration importieren. Die Benutzereinstellungen enthalten die Benutzer, die dieser Konfiguration hinzugefügt wurden, und deren Einstellungen im Operator Client, wie beispielsweise Fenstergrößen und Favoriten.
Hinweis: Mit dem Import einer Konfiguration wird nicht die Versionshistorie der alten Konfiguration wiederhergestellt. Wenn Sie eine Konfiguration importieren, werden keine Benutzereinstellungen importiert. Sie müssen die exportierten Benutzereinstellungen manuell wiederherstellen.

So importieren Sie die Konfiguration:

1. Klicken Sie im Menü **System** auf **Konfiguration importieren ...**.
   Das Dialogfeld **Konfigurationsdatei importieren** wird angezeigt.
2. Wählen Sie die gewünschte Datei für den Import, und klicken Sie auf **Öffnen**.
   Das Dialogfeld **Konfiguration importieren** wird angezeigt.
3. Geben Sie das entsprechende Passwort ein, und klicken Sie auf **OK**.
   Der Configuration Client wird neu gestartet. Sie müssen sich erneut anmelden.
   Die importierte Konfiguration ist nicht aktiv, kann aber mit dem Configuration Client bearbeitet werden.

So stellen Sie die exportierte Konfiguration wieder her:

Sie können auf diese Datei nur zugreifen (kopieren, löschen), wenn der BVMS **Central Server**-Dienst beendet wurde.

1. Beenden Sie den BVMS **Central Server**-Dienst auf dem (Enterprise) Management Server.
2. Falls erforderlich, benennen Sie die Sicherungsdatei in Elements.bvms um.
3. Ersetzen Sie die bestehende Datei Elements.bvms.
4. Starten Sie den BVMS **Central Server**-Dienst auf dem (Enterprise) Management Server.

Hinweis: Um das System auf eine leere Konfiguration zurückzusetzen, beenden Sie den Dienst und löschen die Datei Elements.bvms.
Weitere Konfigurationsdateien:

- Elements.bvms.bak (ab V.2.2): Automatische Sicherungsdatei der letzten Aktivierung einschließlich Versionshistorie. Spätere Änderungen an der nicht aktivierten Konfiguration sind nicht darin enthalten.
- Elements_Backup******.bvms: Konfiguration aus einer älteren Version. Diese Datei wird nach einer Softwareaktualisierung erstellt.

So stellen Sie die exportierten Benutzereinstellungen wieder her:

1. Extrahieren Sie die ZIP-Datei, die beim Wartungsexport erstellt wurde.
   Die Datei `export.bvms` und das Verzeichnis `UserData` werden extrahiert.
2. Auf dem gewünschten (Enterprise) Management Server: Kopieren Sie das Verzeichnis `UserData` nach `C:\ProgramData\Bosch\VMS\`.

7.11.2 Austausch eines VRM

Voraussetzungen

– Installiertes Betriebssystem mit korrekten Netzwerkeinstellungen und der richtigen VRM-Version.

So tauschen Sie das VRM-Gerät im BVMS aus:

1. Starten Sie BVMS Configuration Client.
2. Wählen Sie im Gerätebaum das VRM-Gerät aus.
3. Nehmen Sie die Einstellungen auf den folgenden Seiten vor. Speichern und aktivieren Sie die Konfiguration anschließend wie folgt:

– Hauptfenster > **Geräte** > erweitern > erweitern >

– Hauptfenster > **Geräte** > erweitern > erweitern > **VRM-Einstellungen** > **Haupteinstellungen**

– Hauptfenster > **Geräte** > erweitern > erweitern > **Netzwerk** > **SNMP**

– Hauptfenster > **Geräte** > erweitern > erweitern > **Service** > **Erweitert**

– Hauptfenster > **Geräte** > erweitern > erweitern > > > **Erweiterte Einstellungen** > **Aufzeichnungspräferenzen**

– Hauptfenster > **Geräte** > erweitern > erweitern > > iSCSI > **Lastverteilung**

So tauschen Sie das VRM-Gerät ohne BVMS aus:

Verwenden Sie die originale Sicherungsdatei config.xml des VRM-Geräts, die alle Konfigurationseinstellungen enthält (es sind keine weiteren Einstellungen erforderlich).

1. Beenden Sie den **Video Recording Manager**-Dienst.
2. Kopieren Sie die Datei config.xml auf dem neuen Server.
3. Starten Sie den **Video Recording Manager**-Dienst.

So tauschen Sie ein iSCSI-Gerät aus (geplanter Failover):

1. Fügen Sie das neue iSCSI-Gerät hinzu.
2. Verwenden Sie den Configuration Manager und konfigurieren Sie alle LUNs auf dem auszutauschenden iSCSI-Gerät als schreibgeschützt.

Hinweis: Sie können das alte iSCSI-Gerät entfernen, wenn die alten Aufzeichnungen nicht länger benötigt werden.

Hinweis!

Wenn Sie das neue iSCSI-Gerät konfigurieren, empfehlen wir, das CHAP-Passwort des alten Geräts zu verwenden.

Wenn Sie ein neues CHAP-Passwort verwenden, stellen Sie sicher, dass dieses neue Passwort als systemweites CHAP-Passwort festgelegt und allen iSCSI-Geräten zugewiesen wird.

Anderenfalls ist keine Authentifizierung beim iSCSI und keine direkte Wiedergabe vom iSCSI-Gerät möglich.

7.11.3 Austausch eines Encoders oder Decoders

Hinweis!
Entfernen Sie ein Gerät nicht aus dem Gerätebaum, wenn Sie dessen Aufzeichnungen aufbewahren möchten. Ersetzen Sie für den Austausch dieses Geräts die Hardware.

Austausch eines Encoders oder Decoders vom selben Typ
Voraussetzung ist ein werkseitig eingestelltes Gerät (IP-Adresse = 192.168.0.1).

1. Trennen Sie das alte Gerät vom Netzwerk.
2. Löschen Sie das Gerät im BVMS Configuration Client nicht aus dem Gerätebaum! Wenn Sie das Gerät vom VRM löschen, gehen die Aufzeichnungen verloren.
3. Schließen Sie das neue Gerät vom selben Typ an das Netzwerk an.

Hinweis!
Für die nächsten Schritte ist die zuvor genannte Standard-IP-Adresse erforderlich. Mit DHCP-zugewiesenen IP-Adressen können Sie keinen initialen Geräte-Scan durchführen.

4. Configuration Client: Klicken Sie im **Hardware**-Menü auf **Initialer Geräte-Scan...**.
   Das Dialogfeld **Initialer Geräte-Scan** wird angezeigt.
5. Klicken Sie auf eine Zelle, um die gewünschte Adresse zu ändern. Wenn Sie mehrere Geräte ändern möchten, wählen Sie die gewünschten Zeilen aus. Sie können mehrere Geräte auswählen, indem Sie die STRG- oder die UMSCHALT-Taste drücken. Klicken Sie mit der rechten Maustaste auf die ausgewählten Zeilen und klicken Sie auf **IP-Adressen vergeben ...** oder auf **Subnetzmaske einstellen...**, um die entsprechenden Werte zu ändern.
   Sie müssen die richtige Subnetzmaske und IP-Adresse eingeben.
   Subnetzmaske und IP-Adresse müssen mit den jeweiligen Adressen des ausgetauschten Geräts identisch sein.
6. Klicken Sie auf **OK**.
7. Nach einigen Sekunden können Sie auf die Geräteeinstellungen im Gerätebaum zugreifen.
8. Ändern Sie alle erforderlichen Geräteeinstellungen, die nicht von BVMS gesteuert werden (weitere Informationen hierzu finden Sie nachstehend).
9. Speichern und aktivieren Sie die Konfiguration.

Hinweise:

– Der initiale Geräte-Scan findet nur Geräte mit der Standard-IP-Adresse (192.168.0.1) oder mit duplizierten IP-Adressen.
– Verwenden Sie den VRM-Scan nicht, um nach Geräten mit Werkseinstellungen zu suchen, da Sie danach die IP-Adresse nicht mehr ändern können.

Austausch eines Encoders mit DHCP-zugewiesener IP-Adresse:
Voraussetzung ist ein werkseitig eingestellter Encoder (DHCP-zugewiesene IP).

1. Schließen Sie den Encoder direkt an den Ethernet-Port des Computers an.
2. Notieren Sie sich die TCP/IPv4-Konfiguration des Netzwerkadapters, um diese zu einem späteren Zeitpunkt wiederherzustellen.
3. Konfigurieren Sie am Netzwerkadapter des Computers die folgende feststehende IP-Adresse und Subnetzmaske für den Netzwerkadapter:
   192.168.0.2
   255.255.255.0
4. Starten Sie den Internet Explorer.
5. Geben Sie in die **Adresszeile** 192.168.0.1 ein.
   Die Web-Seite des Geräts wird angezeigt.

6. Klicken Sie auf **Einstellungen** und anschließend auf **Netzwerk**.
7. Wählen Sie auf der Seite **Netzwerk** bzw. in der **DHCP**-Liste **Off** (Aus).
8. Geben Sie in den Feldern **IP-Adresse**, **Subnetzmaske** und **Gateway-Adresse** die für das Netzwerk erforderlichen Werte ein.
9. Klicken Sie auf **Setzen u. Neustart**.
10. Stellen Sie die Netzwerkadapterkonfiguration wieder her.

Austausch eines Encoders oder Decoders eines anderen Gerätetyps

– Trennen Sie das alte Gerät vom Netzwerk.
– Löschen Sie das Gerät im BVMS Configuration Client nicht aus dem Gerätebaum!
– Schließen Sie das neue Gerät vom neuen Typ an das Netzwerk an.

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > Rechtsklick auf > Klick auf **Encoder bearbeiten** > Dialogfeld **Encoder bearbeiten**

oder

Hauptfenster > **Geräte** > erweitern > Rechtsklick auf > Klick auf **Encoder bearbeiten** > Dialogfeld **Encoder bearbeiten**

oder

Hauptfenster > **Geräte** > erweitern > Rechtsklick auf > Klick auf **Encoder bearbeiten** > Dialogfeld **Encoder bearbeiten**

oder

Hauptfenster > **Geräte** > Erweitern > Erweitern > Rechtsklicken > Klicken **Decoder bearbeiten** > **Decoder bearbeiten** Dialogfeld

Nach einem Upgrade des Geräts können Sie die Gerätefunktionen aktualisieren. Eine Textmeldung informiert Sie darüber, ob die abgerufenen Gerätefunktionen den im BVMS gespeicherten Gerätefunktionen entsprechen.

So führen Sie die Aktualisierung durch:

1. Klicken Sie auf **OK**.
   Es wird ein Meldungsfeld mit dem folgenden Text angezeigt:
   Wenn Sie die Gerätemerkmale übernehmen, können sich die Aufzeichnungs- und Ereigniseinstellungen ändern. Prüfen Sie diese Einstellungen für dieses Gerät.
2. Klicken Sie auf **OK**.
   Die Gerätefunktionen werden aktualisiert.

Austausch einer VSG-Kamera

Stellen Sie beim Austausch einer VSG-Kamera sicher, dass die ausgetauschte Kamera vom selben Typ ist und dieselbe IP-Adresse und dasselbe ONVIF-Profil wie die alte Kamera besitzt.
Darüber hinaus müssen Sie vor einem Austausch der alten AXIS-Kamera über die Webschnittstelle der VSG-Kamera die folgenden Einstellungen an der neuen AXIS-Kamera vornehmen:

– Passwort für den Benutzer „root“ festlegen
– Zeitsynchronisation konfigurieren
– Link-Local-Adresse deaktivieren
– ONVIF-Benutzer anlegen
– Schutz vor Replay-Attacken deaktivieren

Von BVMS gesteuerte Einstellungen

In einem BVMS System konfigurierte Encoder und Decoder werden durch den BVMS Server gesteuert und können daher nicht mit anderen Anwendungen geteilt werden.

Sie können zur Überprüfung, welches Gerät eine nicht übereinstimmende Konfiguration aufweist und von der BVMS Konfiguration abweicht, den BVMS Geräte-Monitor verwenden.

Im BVMS Configuration Client befinden sich Konfigurationsseiten für alle BVIP-Geräte.

Der Umfang der möglichen Einstellungen ist abhängig vom individuellen BVIP-Modell (z. B. VIPX 1600 XFM4).

BVMS überwacht alle BVIP-Einstellungen, die für eine nahtlose Integration in ein BVMS System erforderlich sind.

Von BVMS gesteuerte Einstellungen:

- Kameraname
- Zeitserver-Einstellungen
- Aufzeichnungsverwaltung (Profile, Speicherdauer, Zeitpläne)
- Definitionen von Qualitätseinstellungen
- Passwörter

Folgendes wird in der BVMS Konfiguration gespeichert, jedoch nicht auf den Geräten geändert:

- IP-Adresse (IP-Adressen können über die BVMS IP-Gerätekonfiguration geändert werden)
- Relais-/Eingangsnamen (der Unterschied zwischen Namen im Gerät und in BVMS konfigurierten Namen wird angezeigt)

Systemereignisse für eine nicht übereinstimmende Konfiguration

- Es werden SystemInfo-Ereignisse (Systeminformationen) erzeugt, sobald die Konfiguration eines Geräts im Rahmen einer regelmäßigen Überprüfung korrigiert wurde.
- Es werden SystemWarning-Ereignisse (Systemwarnung) erzeugt, sobald erstmals eine nicht übereinstimmende Konfiguration auf einem Gerät erkannt wurde. Bei nachfolgenden Überprüfungen wird dieses Ereignis so lange nicht generiert, bis die Konfiguration durch eine Aktivierung oder eine regelmäßige Reparatur korrigiert wurde.
- SystemError-Ereignisse (Systemfehler) werden erzeugt, sobald im Rahmen einer Aktivierung oder regelmäßigen Prüfung ein Fehler in Bezug auf die Konfiguration erkannt wurde. Bei nachfolgenden Überprüfungen wird dieses Ereignis so lange nicht generiert, bis die Konfiguration durch eine Aktivierung oder eine regelmäßige Reparatur korrigiert wurde.

7.11.4 Austausch eines Operator Client

So tauschen Sie eine Operator Client-Arbeitsstationen aus:

1. Tauschen Sie den Computer aus.
2. Starten Sie die BVMS-Installation auf dem neuen Computer.
3. Wählen Sie aus der Liste der zu installierenden Komponenten den Operator Client aus.
   Falls erforderlich, wählen Sie weitere Komponenten aus, die auf dem ausgetauschten Computer installiert waren.
4. Installieren Sie die Software.

7.11.5 Abschließende Tests

So überprüfen Sie den Austausch des MS/EMS und des Operator Client:

1. Aktivieren Sie die Konfiguration.
2. Starten Sie Operator Client.
3. Überprüfen Sie den Logischen Baum im Operator Client.
   Dieser muss mit dem Logischen Baum im Configuration Client identisch sein.

So überprüfen Sie den Austausch des VRM:

- Starten Sie den VRM Monitor und überprüfen Sie die aktiven Aufzeichnungen.

7.11.6 Wiederherstellen von DIVAR IP

Weitere Informationen finden Sie in den Installationshandbüchern zu DIVAR IP. Im Kapitel zur Beschreibung der Wiederherstellung des Gerätes finden Sie die Informationen zur Vorgehensweise.

7.12 Zeitsynchronisation konfigurieren

Hinweis!
Stellen Sie sicher, dass die Zeit auf allen Computern von BVMS mit dem Management Server synchronisiert ist. Andernfalls können Aufzeichnungen verloren gehen.
Konfigurieren Sie die Zeit-Server-Software auf dem Management Server. Konfigurieren Sie auf den anderen Computern die IP-Adresse des Management Server als Zeit-Server. Gehen Sie dabei gemäß der Standardvorgehensweise in Windows vor.

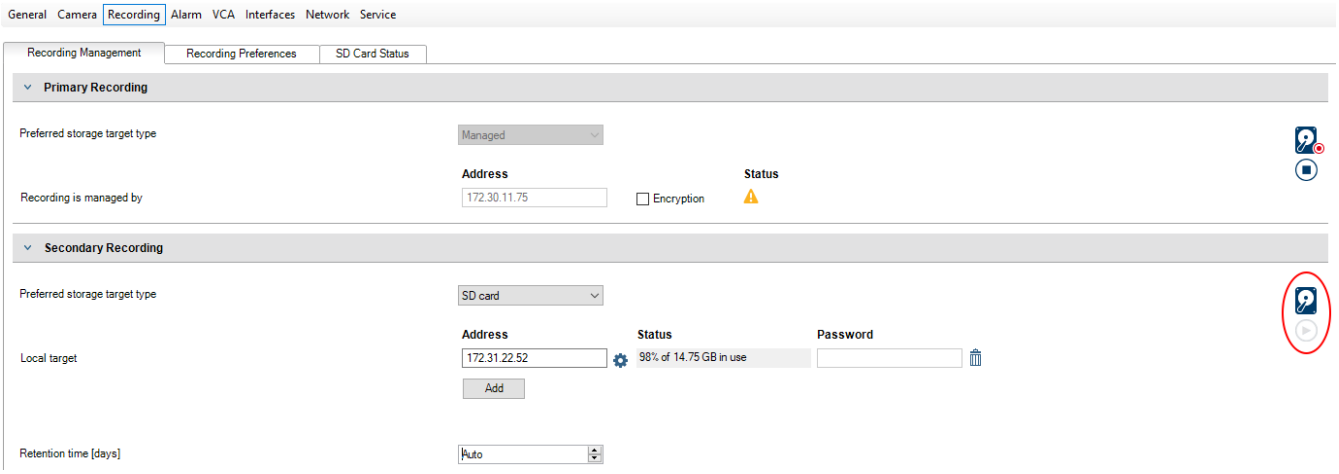
7.13 Speichermedien eines Encoders konfigurieren

Hauptfenster > **Geräte** > erweitern > erweitern > > > **Erweiterte Einstellungen** > **Aufzeichnungsverwaltung**

Hinweis: Stellen Sie sicher, dass die gewünschten Kameras dieses Encoders dem Logischen Baum hinzugefügt werden.

Um die ANR-Funktion zu nutzen, müssen die Speichermedien eines Encoders entsprechend konfiguriert werden.

Hinweis: Wenn Sie die Speichermedien eines Encoders konfigurieren möchten, der bereits dem System hinzugefügt wurde und über VRM erfasst wurde, stellen Sie sicher, dass die sekundäre Aufzeichnung gestoppt wurde:



Die ANR-Funktion ist nur zusammen mit Encodern möglich, die über eine Firmware-Version 5.90 oder höher verfügen. Nicht alle Encoder-Typen unterstützen die ANR-Funktion, selbst wenn die korrekte Firmware-Version installiert ist.

So konfigurieren Sie die Speichermedien eines Encoders:

1. Wählen Sie unter **Sekundäre Aufzeichnung** in der Liste **Bevorzugter Speicherzieltyp** das Speichermedium aus. Je nach Gerätetyp stehen verschiedene Medien zur Verfügung.
2. Klicken Sie gegebenenfalls auf die Schaltfläche „ ... ”, um die Speichermedien zu formatieren. Nach erfolgreicher Formatierung ist das Speichermedium für die Verwendung mit der ANR-Funktion bereit.

3. Konfigurieren Sie die ANR-Funktion für diesen Encoder auf der Seite **Kameras und Aufzeichnung**.

Siehe

- *Seite „Recording Management“ (Aufzeichnungsverwaltung), Seite 235*
- *ANR-Funktion konfigurieren, Seite 308*

8 Erstellung eines Enterprise Systems

Führen Sie die folgenden Schritte aus, um ein Enterprise System auf einem Enterprise Management Server und auf mehreren Management Server-Computern zu erstellen:

1. *Konfigurieren der Serverliste für Enterprise System, Seite 85*
2. *Erstellen einer Enterprise User Group, Seite 86*
3. *Erstellen eines Enterprise Accounts, Seite 86*

Für die Verwendung eines Enterprise Systems müssen gültige Lizenzen vorhanden sein.

Siehe

– *Enterprise System, Seite 25*

8.1 Konfigurieren der Serverliste für Enterprise System

Hauptfenster > **Geräte** > **Enterprise System** > **Serverliste / Adressbuch**

Konfigurieren Sie mehrere Management-Server-Computer in der Serverliste eines geeigneten Management Server.

Für den simultanen Zugriff müssen Sie eine oder mehrere Enterprise User Groups konfigurieren. Dies ändert den Management Server zu einem Enterprise Management Server.

Ein Benutzer des Operator Client kann sich mit dem Benutzernamen der Enterprise User Group anmelden, um gleichzeitig Zugriff auf die in der Serverliste konfigurierten Management Server Computer zu erhalten.

Bedienberechtigungen werden auf dem Enterprise Management Server in **Benutzergruppen**, Registerkarte Enterprise User Group konfiguriert.

Geräteberechtigungen werden auf jedem Management Server in **Benutzergruppen**, Registerkarte Enterprise Access konfiguriert.

– Klicken Sie auf , um die Einstellungen zu speichern.

– Klicken Sie auf , um die letzte Einstellung rückgängig zu machen.

– Klicken Sie auf , um die Konfiguration zu aktivieren.

So fügen Sie Server hinzu:

1. Klicken Sie auf **Server hinzufügen**.
   Das Dialogfeld **Server hinzufügen** wird angezeigt.
2. Geben Sie einen Anzeigenamen für den Server und die private Netzwerkadresse (DNS-Name oder IP-Adresse) ein.
   Hinweis: Wenn Sie eine SSH-Verbindung verwenden, geben Sie die Adresse im folgenden Format ein:
   ssh://IP-Adresse oder Servername:5322
3. Klicken Sie auf **OK**.
4. Wiederholen Sie diese Schritte, bis alle gewünschten Management Server-Computer hinzugefügt wurden.

So fügen Sie Spalten hinzu:

- Klicken Sie mit der rechten Maustaste auf die Tabellenüberschrift und klicken Sie auf **Spalte hinzufügen**.
  Sie können bis zu 10 Spalten hinzufügen.
  Um eine Spalte zu löschen, klicken Sie mit der rechten Maustaste auf die gewünschte Spalte, und klicken Sie auf **Spalte entfernen**.

⇨ Wenn Sie die Server-Liste exportieren, werden die hinzugefügten Spalten auch exportiert.

Die Management Server-Computer für Ihr Enterprise System werden konfiguriert.

Siehe

- *Enterprise System, Seite 25*
- *Seite „Server-Liste/Adressbuch“, Seite 129*
- *Seite Benutzergruppen, Seite 333*
- *Mittels Server Lookup, Seite 73*

8.2 Erstellen einer Enterprise User Group

Hauptfenster > **Benutzergruppen**

Die Aufgabe zum Erstellen einer Enterprise User Group für ein Enterprise System führen Sie auf einem Enterprise Management Server aus.

Erstellen Sie eine Enterprise User Group mit Benutzern, um deren Bedienberechtigungen zu konfigurieren. Diese Bedienberechtigungen sind auf einem Operator Client verfügbar, der mit dem Enterprise Management Server verbunden ist. Ein Beispiel für eine Bedienberechtigung ist die Benutzeroberfläche für den Alarmmonitor.

So erstellen Sie eine Enterprise User Group:

1. Klicken Sie auf die Registerkarte **Enterprise User Groups**.
   Hinweis: Die Registerkarte **Enterprise User Groups** ist nur verfügbar, wenn die entsprechende Lizenz verfügbar ist und wenn ein oder mehrere Management Server-Computer in **Geräte** > **Enterprise System** > **Serverliste / Adressbuch** konfiguriert sind.
2. Klicken Sie auf .
   Das Dialogfeld **Neue Enterprise Benutzergruppe** wird angezeigt.
3. Geben Sie den Namen und eine Beschreibung ein.
4. Klicken Sie auf **OK**.
   Die Enterprise User Group wird dem entsprechenden Baum hinzugefügt.
5. Klicken Sie mit der rechten Maustaste auf die neue Enterprise User Group, und klicken Sie auf **Umbenennen**.
6. Geben Sie den gewünschten Namen ein, und drücken Sie die Eingabetaste.
7. Konfigurieren Sie auf der Seite **Bedienberechtigungen** die Bedienberechtigungen und den Server-Zugriff für die konfigurierten Management Server-Computer nach Bedarf.

Siehe

- *Seite Eigenschaften der Benutzergruppen, Seite 335*
- *Seite mit den Bedienereigenschaften, Seite 342*
- *Seite Prioritäten, Seite 346*
- *Seite Benutzeroberfläche, Seite 346*
- *Seite „Server-Zugriff“, Seite 347*

8.3 Erstellen eines Enterprise Accounts

Hauptfenster > **Benutzergruppen**

Hinweis!
Im Gerätebaum muss mindestens ein Gerät konfiguriert sein, damit Sie einen Enterprise Account hinzufügen können.

Die Aufgabe zum Erstellen eines Enterprise Accounts führen Sie auf einem Management Server aus. Wiederholen Sie diese Aufgabe auf jedem Management Server, der Ihrem Enterprise System angehört.
Erstellen Sie einen Enterprise Account, um die Geräteberechtigungen für einen Operator Client mit einem Enterprise System zu konfigurieren.

So erstellen Sie einen Enterprise Account:

1. Klicken Sie auf die Registerkarte **Enterprise Access**.
2. Klicken Sie auf .
   Das Dialogfeld **Neuer Enterprise Account** wird angezeigt.
3. Geben Sie den Namen und eine Beschreibung ein.
4. Das Kontrollkästchen **Benutzer muss Passwort bei nächster Anmeldung ändern** ist bereits für alle neu erstellten Benutzerkonten aktiviert.
   Geben Sie den Schlüssel entsprechend der Schlüsselrichtlinie ein und bestätigen Sie ihn.
5. Klicken Sie auf **OK**.
   Ein neuer Enterprise Account wird zum entsprechenden Baum hinzugefügt.
6. Klicken Sie mit der rechten Maustaste auf den neuen Enterprise Account und klicken Sie auf **Umbenennen**.
7. Geben Sie den gewünschten Namen ein, und drücken Sie die Eingabetaste.
8. Konfigurieren Sie auf der Seite **Geräteberechtigungen** die Zugangs- und Geräteberechtigungen nach Bedarf.

Siehe

- *Richtlinie für sichere Passwörter , Seite 357*
- *Seite „Zugangsberechtigungen“, Seite 341*
- *Seite Logischer Baum, Seite 342*
- *Seite Ereignisse und Alarme, Seite 341*
- *Seite „Prioritäten für Steuerungen“, Seite 339*
- *Seite Kamerafreigaben, Seite 338*
- *Seite Decoder-Freigaben, Seite 340*

8.4 Tokenbasierte Authentifizierung

Der Enterprise Account ermöglicht Enterprise Management Clients den Zugriff auf einen Management Server, der in der Server-Zugriffsliste des Enterprise Management Server konfiguriert ist.
Der Enterprise Account ist durch einen Schlüssel gesichert. Wenn Sie diesen Schlüssel ändern müssen, müssen Sie ihn auch auf dem Management Server und auf dem Enterprise Management Server ändern. Außerdem müssen Sie die geänderte Konfiguration aktivieren.
Wenn Sie eine große Anzahl von Management Server verbunden mit einem Enterprise Management Server haben, kann dies zeitaufwendig sein.

Anstelle der Sicherung des Enterprise Account mit einem Benutzernamen und einem Schlüssel zu sichern, können Sie eine tokenbasierte Authentifizierung konfigurieren.

1. Der Enterprise Management Server erstellt das Token.
2. Das Token wird mit einem Zertifikat namens Token Issuer.
3. Der Management Server gewährt Zugriff, wenn das Token gültig ist.
   Der Management Server gewährt den Zugriff nur, wenn der Management Server so konfiguriert ist, dass es dem Token Issuer Zertifikat vertraut.

Voraussetzungen

Zum Signieren und Validieren des Tokens benötigen Sie ein Zertifikat oder eine Kette von Zertifikaten.

Hinweis: Die Zertifikate werden nicht generiert oder installiert von BVMS. Sie müssen sie selbst bereitstellen und installieren. BVMS kann Zertifikate verwenden, die im Windows Certificate Store installiert sind.

Es gibt unterschiedliche Voraussetzungen für Enterprise Management Server und Management Server Maschinen. Im Folgenden wird erläutert, welche Umgebung welche Zertifikate erfordert.

Zertifikat

- Der Enterprise Management Server benötigt das Zertifikat und seinen privaten Schlüssel.
- Der Management Server benötigt das Zertifikat.

Zertifikatkette

Eine Zertifikatskette beginnt mit einem Root Zertifikat, das Sie zum Signieren eines anderen Zertifikats verwenden. Sie können dieses Zertifikat dann erneut verwenden, um ein weiteres Zertifikat zu signieren. Sie können die Länge der Zertifikatsketten selbst festlegen.

- Der Enterprise Management Server benötigt die gesamte Zertifikatskette.
  Für das letzte Zertifikat in der Kette (Token Issuer), ist ein privater Schlüssel erforderlich.
- Der Management Server benötigt nur Teile der Zertifikatskette, abhängig von den konfigurierten Zugriffstoken-Einstellungen.

Um die tokenbasierte Authentifizierung zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Konfiguration des Enterprise Management Server
   - Definieren Sie die Zugriffstoken-Authentifizierung für den Enterprise Accounts
   - Konfigurieren Sie die Einstellungen für das Zugriffstoken
2. Konfiguration des Management Server
   - Geben Sie die vertrauenswürdigen Zertifikate an
   - Verweigern Sie den Zugriff auf das Enterprise Account durch Schlüssel

Ausführliche Informationen zu den jeweiligen Themen finden Sie im Whitepaper zur Token-basierten Authentifizierung.

Siehe

- *Dialogfeld „Zugriffstoken-Einstellungen“ (Menü Einstellungen), Seite 118*
- *Seite „Server-Zugriff“, Seite 347*

9 Konfigurieren von Kommandoskripten

In diesem Kapitel wird die Konfiguration von Kommandoskripten beschrieben. Kommandoskripte werden an verschiedenen Stellen des BVMS verwendet.

1. Klicken Sie auf , um die Einstellungen zu speichern.
2. Klicken Sie auf , um die letzte Einstellung rückgängig zu machen.
3. Klicken Sie auf , um die Konfiguration zu aktivieren.

Hinweis!
Server-Skripte werden beim Neustart des Management Server-Dienstes aktiviert, auch wenn diese nicht im Configuration Client aktiviert sind.

9.1 Verwalten von Kommandoskripten

Hauptfenster

Sie können ein Kommandoskript mit den folgenden Skriptsprachen erzeugen:

- C#
- VB.Net

Für bereits vorhandene Kommandoskripte kann die Skriptsprache nicht geändert werden.

Sie können ein Client-Skript oder ein Server-Skript erzeugen.

Sie können jedem Skript Skriptlets hinzufügen.

Um Hilfe bei der Code-Eingabe zu erhalten, klicken Sie im Dialogfeld

im **Kommandoskript-Editor**. Die Hilfe zu Bosch Script API wird angezeigt.

So fügen Sie Server-Skriptlets hinzu:

1. Im **Werkzeuge** Menü klicken Sie auf **Kommandoskript-Editor...** Befehl.
   Das **Skriptsprache auswählen** Dialogfeld wird angezeigt, wenn noch kein Kommandoskript erstellt wurde.
2. Wählen Sie aus der Liste **Skriptsprache:** den erforderlichen Eintrag.
   Das **Kommandoskript-Editor** Dialogfeld wird angezeigt.
3. Machen Sie im linken Teilfenster des Dialogfelds **Kommandoskript-Editor** einen Rechtsklick mit der Maus ServerScript und klicken Sie **Neues Scriptlet**.
   Ein neues Skriptlet wird hinzugefügt.
4. Geben Sie den Code ein.

So fügen Sie Client-Skriptlets hinzu

1. Im **Werkzeuge** Menü klicken Sie auf **Kommandoskript-Editor...** Befehl.
   Das **Skriptsprache auswählen** Dialogfeld wird angezeigt, wenn noch kein Kommandoskript erstellt wurde.
2. Wählen Sie aus der Liste **Skriptsprache:** den erforderlichen Eintrag.
   Das **Kommandoskript-Editor** Dialogfeld wird angezeigt.
3. Machen Sie im linken Teilfenster des Dialogfelds **Kommandoskript-Editor** einen Rechtsklick mit der Maus ClientScript und klicken Sie **Neues Scriptlet**.
   Ein neues Skriptlet wird hinzugefügt.
4. Geben Sie den Code ein.

So löschen Sie ein Skriptlet:

1. Öffnen Sie das Dialogfeld **Kommandoskript-Editor**.
2. Klicken Sie auf die Registerkarte **Server-Skript** bzw. **Client-Skript**.

3. Klicken Sie im Ereignisbaum mit der rechten Maustaste auf das erforderliche Ereignis, und klicken Sie auf Das Skriptlet wird entfernt.
.

So beenden Sie das Dialogfeld Kommandoskript-Editor:

- Klicken Sie auf .

Siehe

– *Dialogfeld Kommandoskript-Editor, Seite 312*

9.2 Konfigurieren eines automatisch startenden Kommandoskripts

Hauptfenster > **Alarme** > oder > **Alarmoptionen** Spalte > ...
Sie können ein Client-Kommandoskript so konfigurieren, dass es in den folgenden Fällen gestartet wird:

– Beim Starten der Arbeitsstation
– Nach der Annahme eines Alarms durch den Benutzer

So konfigurieren Sie ein Kommandoskript, das beim Starten der Arbeitsstation gestartet werden soll:

Siehe Konfigurieren eines Start-Kommandoskripts.

So konfigurieren Sie ein Kommandoskript, das nach der Annahme eines Alarms durch den Benutzer gestartet werden soll:

1. Klicken Sie auf die Registerkarte **Workflow**.
2. Wählen Sie in der Liste **Folgendes Client-Skript ausführen, wenn der Alarm angenommen worden ist:** das gewünschte Client-Skript aus.
   Dieses Skript wird gestartet, sobald ein Benutzer den gewählten Alarm annimmt.

Siehe

– *Dialogfeld Alarmoptionen, Seite 318*
– *Konfigurieren eines Start-Kommandoskripts (Seite „Einstellungen“), Seite 91*

9.3 Importieren eines Kommandoskripts

Hauptfenster

Sie können Kommandoskripte importieren, die auf einem anderen Computer entwickelt wurden. Die Datei muss in derselben Skriptsprache geschrieben sein, die Sie auf Ihrem System verwenden.

So importieren Sie ein Kommandoskript:

1. Klicken Sie im Menü **Werkzeuge** auf **Kommandoskript-Editor...**.
   Das Dialogfeld **Kommandoskript-Editor** wird angezeigt.
2. Klicken Sie .
   Das Dialogfeld zum Öffnen einer Datei wird angezeigt.
3. Wählen Sie die Skriptdatei aus, und klicken Sie auf **OK**.

Siehe

– *Dialogfeld Kommandoskript-Editor, Seite 312*

9.4 Exportieren eines Kommandoskripts

Hauptfenster

Sie können Kommandoskripte exportieren, die auf einem anderen Computer entwickelt wurden.

So exportieren Sie ein Kommandoskript:

1. Klicken Sie im Menü **Werkzeuge** auf **Kommandoskript-Editor...**.
   Das Dialogfeld **Kommandoskript-Editor** wird angezeigt.
2. Klicken Sie auf .
   Das Dialogfeld zum Speichern einer Datei wird angezeigt.
3. Geben Sie einen Namen für die Skriptdatei ein, und klicken Sie auf **OK**.

Siehe

– *Dialogfeld Kommandoskript-Editor, Seite 312*

9.5 Konfigurieren eines Start-Kommandoskripts (Seite „Einstellungen“)

Hauptfenster > **Geräte** > erweitern > > Seite **Einstellungen**

Sie können ein Kommandoskript so konfigurieren, dass es beim Starten des Operator Client auf der ausgewählten Arbeitsstation gestartet wird.

Sie müssen ein entsprechendes Kommandoskript erzeugen.

Informationen zum Erzeugen von Kommandoskripten finden Sie im *Verwalten von Kommandoskripten, Seite 89*.

So konfigurieren Sie ein Start-Skript:

- Wählen Sie in der Liste **Start-Skript:** das Kommandoskript aus.

Siehe

– *Seite Arbeitsstation, Seite 137*

10 Verwalten von Konfigurationsdaten

Hauptfenster

Sie müssen die aktuelle Konfiguration aktivieren, damit sie für den Management Server and Operator Client gültig ist. Das System weist Sie beim Beenden des Configuration Client auf die Aktivierung der Konfiguration hin.

Jede aktivierte Konfiguration wird mit Datum und gegebenenfalls mit einer Beschreibung gespeichert. Eine kürzlich aktivierte Konfiguration können Sie jederzeit wiederherstellen. Alle Konfigurationen, die in der Zwischenzeit gespeichert wurden, gehen dabei verloren.

Sie können die aktuelle Konfiguration in eine Konfigurationsdatei exportieren und diese Datei später importieren. Damit wird die exportierte Konfiguration wiederhergestellt. Alle Konfigurationen, die in der Zwischenzeit gespeichert wurden, gehen dabei verloren.

– Klicken Sie auf , um die Einstellungen zu speichern.

– Klicken Sie auf , um die letzte Einstellung rückgängig zu machen.

– Klicken Sie auf , um die Konfiguration zu aktivieren.

10.1 Aktivieren der letzten Konfiguration

Hauptfenster

Sie aktivieren die aktuelle Version der Konfiguration. Der Operator Client wendet die aktivierte Konfiguration beim nächsten Systemstart an, sofern der Benutzer diese akzeptiert hat. Falls die Aktivierung erzwungen wird, werden alle geöffneten Instanzen des Operator Client im Netzwerk geschlossen und neu gestartet. Die Benutzer der einzelnen Instanzen von Operator Client müssen sich normalerweise nicht erneut anmelden.

Sie können eine Zeit für eine verzögerte Aktivierung konfigurieren. Wenn eine verzögerte Aktivierungszeit konfiguriert ist, wird die letzte Konfiguration nicht sofort, sondern zum konfigurierten Zeitpunkt aktiviert. Wenn Sie zu einem späteren Zeitpunkt eine andere Aktivierungszeit konfigurieren (unabhängig davon, ob es sich um eine verzögerte Aktivierungszeit handelt), gilt ab diesem Zeitpunkt die neue Aktivierungszeit. Die zuerst konfigurierte Aktivierungszeit wird entfernt.

Wenn Sie den Configuration Client beenden, erhalten Sie vom System den Hinweis, die aktuelle Version der Konfiguration zu aktivieren.

Die Aktivierung einer Konfiguration, die ein Gerät ohne Passwortschutz enthält, ist nicht möglich.

Hinweis!
Falls die Aktivierung erzwungen wird, wird jede Instanz des Operator Client neu gestartet, wenn die Konfiguration aktiviert wird. Vermeiden Sie unnötige Aktivierungen. Führen Sie Aktivierungen vorzugsweise nachts oder während Zeiträumen mit geringer Aktivität durch.

Hinweis!
Enthält das System Geräte, die nicht durch ein Passwort geschützt sind, müssen Sie diese Geräte sichern, bevor Sie die Aktivierung vornehmen können. Sie können diesen Passwortzwang deaktivieren.

So aktivieren Sie die aktuelle Version der Konfiguration:

1. Klicken Sie auf .
   Das Dialogfeld **Konfiguration aktivieren** wird angezeigt.
   Enthält die Konfiguration Geräte, die nicht durch ein Passwort geschützt sind, können Sie eine Aktivierung nicht vornehmen. In diesem Fall wird das Dialogfeld **Geräte mit Standardpasswort schützen...** angezeigt.
   Befolgen Sie die Anweisungen im Dialogfeld, und klicken Sie auf **Übernehmen**.
   Das Dialogfeld **Konfiguration aktivieren** wird erneut angezeigt.
2. Geben Sie bei Bedarf eine Zeit für eine verzögerte Aktivierung ein. Standardmäßig gilt der aktuelle Zeitpunkt als Aktivierungszeit. Wenn Sie die Einstellung für die verzögerte Aktivierungszeit nicht ändern, wird die Aktivierung sofort durchgeführt.
   Aktivieren Sie bei Bedarf **Aktivierung für alle Operator Clients erzwingen**.
3. Geben Sie eine Beschreibung ein, und klicken Sie auf **OK**.
   Die aktuelle Konfiguration wird aktiviert.
   Jede Operator Client-Arbeitsstation wird sofort neu gestartet, wenn sie mit dem Netzwerk verbunden ist und die Aktivierung erzwungen wird. Wenn eine Arbeitsstation gerade nicht verbunden ist, wird sie neu gestartet, sobald sie wieder verbunden ist.
   Wenn Sie eine Zeit für eine verzögerte Aktivierung eingestellt haben, wird die Konfiguration zu einem späteren Zeitpunkt aktiviert.

Hinweis: Die verzögerte Aktivierung wird nicht ausgeführt, solange der Benutzer beim Configuration Client angemeldet ist.

Siehe

- *Dialogfeld „Geräte mit globalem Standard-Passwort schützen“ (Menü „Hardware“), Seite 105*
- *Dialogfeld „Konfiguration aktivieren“ (Menü „System“), Seite 104*

10.2 Aktivieren einer Konfiguration

Hauptfenster

Sie können eine vorherige Version der Konfiguration aktivieren, die Sie zu einem früheren Zeitpunkt gespeichert haben.

So aktivieren Sie eine Konfiguration:

1. Klicken Sie im Menü **System** auf **Aktivierungs-Manager...**.
   Das Dialogfeld **Aktivierungs-Manager** wird angezeigt.
2. Wählen Sie in der Liste die Konfiguration aus, die aktiviert werden soll.
3. Klicken Sie auf **Aktivieren**.
   Ein Meldungsfeld wird angezeigt.
4. Klicken Sie auf **OK**.
   Das Dialogfeld **Konfiguration aktivieren** wird angezeigt.
5. Falls erforderlich, aktivieren Sie **Aktivierung für alle Operator Clients erzwingen**. Jede Operator Client-Arbeitsstation wird automatisch neu gestartet, um die neue Konfiguration zu aktivieren. Der Benutzer kann die neue Konfiguration nicht ablehnen.
   Wenn **Aktivierung für alle Operator Clients erzwingen** nicht aktiviert ist, wird auf jeder Operator Client-Arbeitsstation einige Sekunden lang ein Dialogfeld angezeigt. Der Benutzer kann die neue Konfiguration ablehnen oder akzeptieren. Wenn der Benutzer untätig bleibt, wird das Dialogfeld nach einigen Sekunden geschlossen. In diesem Fall wird die neue Konfiguration nicht akzeptiert.

Siehe

- *Dialogfeld „Konfiguration aktivieren“ (Menü „System“), Seite 104*
- *Dialogfeld „Aktivierungs-Manager“ (Menü „System“), Seite 103*

10.3 Exportieren von Konfigurationsdaten

Hauptfenster

Sie können die Gerätekonfigurationsdaten des BVMS in eine .zip-Datei exportieren. Diese ZIP-Datei enthält die Datenbankdatei (`Export.bvms`) und die Benutzerdaten (`.dat`-Datei).
Mit diesen Dateien können Sie eine Systemkonfiguration wiederherstellen, die zuvor auf demselben (Enterprise) Management Server exportiert wurde, oder die Konfiguration in einen anderen (Enterprise) Management Server importieren. Die Benutzerdaten-Datei kann nicht importiert werden, allerdings können Sie die Benutzerkonfiguration manuell wiederherstellen.

So exportieren Sie Konfigurationsdaten:

1. Klicken Sie im **System**-Menü auf **Konfiguration exportieren....**
   Das Dialogfeld **Konfigurationsdatei exportieren** wird angezeigt.

   Hinweis: Wenn die aktuelle Konfiguration der Arbeitskopie nicht aktiviert ist (aktiv ist), wird diese Arbeitskopie exportiert und nicht die aktivierte Konfiguration.
2. Klicken Sie auf **Speichern**.
3. Geben Sie einen Dateinamen ein.
   Die aktuelle Konfiguration wird exportiert. Eine ZIP-Datei mit Datenbank und Benutzerdaten wird erstellt.

Siehe

- *Importieren von Konfigurationsdaten, Seite 94*

10.4 Importieren von Konfigurationsdaten

Hauptfenster

Folgende Anwendungsfälle werden behandelt:

- Import einer Konfiguration, die zuvor auf dem gleichen Server exportiert wurde (Backup durchgeführt)
- Importieren einer Konfigurationsvorlage, die auf einem anderen Server vorbereitet und exportiert wurde
- Importieren der Konfiguration einer früheren Version von BVMS.

Sie können eine Konfiguration nur importieren, wenn die letzten Änderungen der aktuellen Arbeitskopie gespeichert und aktiviert wurden.
Für den Import von Konfigurationsdaten benötigen Sie das entsprechende Passwort.
Benutzerdaten können Sie nicht importieren.

So importieren Sie die Konfiguration:

1. Klicken Sie im Menü **System** auf **Konfiguration importieren ...**.
   Das Dialogfeld **Konfigurationsdatei importieren** wird angezeigt.
2. Wählen Sie die gewünschte Datei für den Import, und klicken Sie auf **Öffnen**.
   Das Dialogfeld **Konfiguration importieren** wird angezeigt.
3. Geben Sie das entsprechende Passwort ein, und klicken Sie auf **OK**.
   Der Configuration Client wird neu gestartet. Sie müssen sich erneut anmelden.
   Die importierte Konfiguration ist nicht aktiv, kann aber mit dem Configuration Client bearbeitet werden.

Hinweis!
Wenn Sie eine Konfiguration weiterbearbeiten möchten, die für Ihren Management Server aktiviert wurde, führen Sie einen Rollback im Dialogfeld **Konfiguration aktivieren** durch.

Siehe
– *Exportieren von Konfigurationsdaten, Seite 94*

10.5 Exportieren von Konfigurationsdaten auf OPC

Hauptfenster
Sie können die Gerätekonfigurationsdaten des BVMS in eine XML-Datei exportieren, um diese in eine OPC-Server-Anwendung zu importieren. Die Datei muss im bin-Verzeichnis Ihrer BVMS Installation gespeichert werden.
Zum Konfigurieren einer BVMS-BIS-Verbindung stehen das Installationshandbuch „BVMS-BIS Connectivity“ und der technische Servicehinweis „BVMS OPC-Server“ zur Verfügung.

Hinweis!
Installieren Sie den BIS-Server und den BVMS Management Server auf verschiedenen Computern. Wenn beide Server auf demselben Computer ausgeführt werden, verringert sich die Leistung der Systeme. Außerdem kann es zu schweren Software-Fehlern kommen.

So exportieren Sie Konfigurationsdaten:
1. Klicken Sie im Menü **System** auf **OPC-Geräteinformation exportieren...**.
   Das Dialogfeld **Datei mit Geräteinformationen exportieren** wird angezeigt.
2. Geben Sie einen Dateinamen ein, und klicken Sie auf **Speichern**.
   Die Datei wird gespeichert.
   Sie können diese Datei in die OPC-Server-Anwendung importieren.

10.6 Status des Encoders/Decoders überprüfen

Hauptfenster > Menü **Hardware** > Befehl **Gerätemonitor...** > Dialogfeld **Gerätemonitor**
Sie können den Status aller aktivierten Encoder/Decoder im Gerätebaum überprüfen.

Siehe
– *Dialogfeld „Geräte-Monitor“ (Menü „Hardware“), Seite 110*

10.7 SNMP-Überwachung konfigurieren

Hauptfenster

Konfigurieren:
1. Klicken Sie im Menü **Einstellungen** auf **SNMP-Einstellungen...**.
   Das Dialogfeld **SNMP-Einstellungen** wird angezeigt.
2. Nehmen Sie die erforderlichen Einstellungen vor, und klicken Sie auf **OK**.

So deaktivieren Sie SNMP GetRequest:
- Löschen Sie im Feld **SNMP GET Port** den Feldinhalt.
  Im BVMS werden keine SNMP GetRequest-Abfragen mehr durchgeführt.

Siehe
– *Dialogfeld „SNMP-Einstellungen“ (Menü „Einstellungen“), Seite 115*

10.8 Berichte erstellen

Hauptfenster

Sie können einen einzelnen Bericht erstellen, um die Konfigurationseinstellungen eines bestimmten Dialogfelds zu speichern, oder Sie können alle Konfigurationsberichte auf einmal erstellen.

Um einen einzelnen Bericht zu erstellen:

1. Klicken Sie im Menü **Auswertungen** auf den gewünschten Befehl.
   Das entsprechende Dialogfeld wird angezeigt.
2. Klicken Sie auf **CSV-Export**.
3. Geben Sie den Pfad und den Dateinamen für die neue Auswertung ein.
4. Öffnen Sie die CSV-Datei in Microsoft Excel oder einem anderen Tabellenkalkulationsprogramm, um den Inhalt zu überprüfen.

Um alle Konfigurationsberichte auf einmal zu erstellen:

1. Klicken Sie im Menü **Auswertungen** auf **Alle Auswertungen exportieren**.
2. Wählen Sie den Zielordner, in dem Sie die Berichte speichern möchten, und klicken Sie auf **OK**.
   Die Berichte werden erstellt und im gewünschten Ordner gespeichert. Ein Fortschrittsbalken zeigt den Fortschritt der Speicherung an.

Siehe

- *Dialogfeld „Aufzeichnungszeitpläne“, Seite 113*
- *Dialogfeld „Aktionszeitpläne“, Seite 113*
- *Dialogfeld „Kameras und Aufzeichnungsparameter”, Seite 113*
- *Dialogfeld „Stream-Qualität", Seite 113*
- *Dialogfeld „Ereignis-Einstellungen”, Seite 113*
- *Dialogfeld „Einstellungen für zusammengesetztes Ereignis”, Seite 113*
- *Dialogfeld „Alarmeinstellungen“, Seite 114*
- *Dialogfeld „Konfigurierte Benutzer”, Seite 114*
- *Das Dialogfeld „Benutzergruppen und Konten”, Seite 114*
- *Dialogfeld „Bedienberechtigungen“, Seite 114*

11 Konfigurationsbeispiele

Dieses Kapitel enthält Beispiele zur Konfiguration ausgewählter Geräte im BVMS.

11.1 Hinzufügen einer Bosch ATM/POS-Bridge

In diesem Beispiel wird die Einrichtung eines Bosch ATM/POS Bridge beschrieben.

Konfigurieren des ATM/POS Bridge

1. Vergewissern Sie sich, dass das Gerät mit Strom versorgt wird.
2. Um die IP-Adresse und Subnetzmaske des Geräts zu konfigurieren, schließen Sie das Gerät mit einem RS232-Kabel an einen COM-Port Ihres Computers an. (Verwenden Sie dazu das angegebene Bosch Kabel.) Nähere Informationen finden Sie im Installationshandbuch des Bosch ATM/POS Bridge.
3. Starten Sie auf diesem Computer eine HyperTerminal Sitzung (in der Regel: **Start** > **Programme** > **Zubehör** > **Kommunikation** > **HyperTerminal**).
4. Geben Sie einen Namen für die Sitzung ein, und klicken Sie auf **OK**.
5. Wählen Sie die COM-Port-Nummer aus, und klicken Sie auf **OK**.
6. Geben Sie die folgenden COM-Port-Einstellungen ein:
   - 9600 Bits/s
   - 8 Datenbits
   - Keine Parität
   - 1 Stoppbit
   - Hardware-Flusssteuerung

   Klicken Sie auf **OK.**
7. Drücken Sie F1, um das Menü mit den Systemoptionen des Geräts anzuzeigen.
8. Geben Sie 1 ein, um nach Bedarf die IP-Adresse und Subnetzmaske einzustellen.
9. Übernehmen Sie die Standardeinstellungen für die Ports:
   - port1: **4201**
   - port2: **4200**

Hinzufügen von ATM/POS Bridgebei BVMS

1. Schließen Sie das Gerät an das BVMS Netzwerk an.
2. Starten Sie Configuration Client.
3. Klicken Sie auf **Geräte**, erweitern Sie den Logischen Baum, erweitern Sie , klicken Sie mit der rechten Maustaste auf , klicken Sie auf **Bosch ATM/POS-Bridge hinzufügen**.
   Das Dialogfeld **Bosch ATM/POS-Bridge hinzufügen** erscheint.
4. Geben Sie einen Namen sowie die zuvor konfigurierten Einstellungen ein.
5. Klicken Sie auf die Registerkarte **Eingänge**, und wählen Sie die erforderlichen Eingänge aus.
6. Klicken Sie auf , um die Einstellungen zu speichern.
7. Klicken Sie auf **Ereignisse**.
8. Erweitern Sie , erweitern Sie **POS Bridge-Eingang**, und klicken Sie auf **Daten-Input**.
9. Wählen Sie in der Liste **Alarm auslösen** die Option **Immer** aus, wenn dieses Ereignis immer einen Alarm auslösen soll. Wenn das Ereignis nur während eines bestimmten Zeitbereichs einen Alarm auslösen soll, wählen Sie einen Zeitplan aus.
10. Klicken Sie auf , um die Einstellungen zu speichern.
11. Klicken Sie auf **Alarme**.

12. Konfigurieren Sie die Alarmeinstellungen für dieses Ereignis.
13. Klicken Sie auf , um die Einstellungen zu speichern. Klicken Sie auf , um die Konfiguration zu aktivieren.
14. Führen Sie einen Testlauf durch, um sicherzustellen, dass der Alarm wunschgemäß funktioniert.

11.2 Hinzufügen eines Bosch Allegiant Kreuzschienen-Eingangsalarms

Nachdem in BVMS ein Bosch Allegiant Gerät hinzugefügt wurde, fügen Sie die Allegiant Alarmeingänge hinzu.

1. Klicken Sie im Gerätebaum auf den Eintrag Allegiant-Gerät.
2. Klicken Sie auf die Registerkarte **Eingänge** und anschließend auf **Eingang hinzufügen**.
3. Fügen Sie die gewünschten Eingangsalarme hinzu.
4. Klicken Sie auf **Ereignisse**.
5. Erweitern Sie im Ereignisbaum **Allegiant-Geräte**, erweitern Sie **Allegiant-Eingang**, und klicken Sie auf **Eingang geschlossen** oder **Eingang geöffnet** (je nach Anwendung).
6. Wählen Sie in der Liste **Alarm auslösen** die Option **Immer** aus, wenn ein Ereignis immer einen Alarm auslösen soll. Wenn das Ereignis nur während eines bestimmten Zeitbereichs einen Alarm auslösen soll, wählen Sie einen Zeitplan aus.
7. Klicken Sie auf , um die Einstellungen zu speichern. Klicken Sie auf , um die Konfiguration zu aktivieren.
8. Führen Sie einen Testlauf durch, um sicherzustellen, dass der Alarm wunschgemäß funktioniert.

11.3 Hinzufügen und Konfigurieren von 2 Dinion IP Kameras mit VRM Aufzeichnung

In diesem Abschnitt wird beschrieben, wie 2 Dinion IP Kameras für die VRM Aufzeichnung hinzugefügt werden und wie verschiedene Aufzeichnungseinstellungen sowie die Forensische Suche für diese Kameras konfiguriert werden.

Voraussetzung:
Der VRM und die iSCSI-Geräte sind ordnungsgemäß konfiguriert.
Dies bedeutet:

– Der VRM wurde dem Gerätebaum hinzugefügt.
– Dem VRM ist ein iSCSI-Gerät mit konfiguriertem Ziel und LUN zugeordnet.

So fügen Sie die IP-Kameras einem vorhandenen VRM hinzu:

Hauptfenster > **Geräte** > Erweitern

1. Klicken Sie mit der rechten Maustaste auf , und klicken Sie auf **Encoder hinzufügen**.
   Das Dialogfeld **Encoder hinzufügen** wird angezeigt.
2. Geben Sie die IP-Adresse der IP-Kamera ein, und wählen Sie den Encoder-Typ aus (Dinion IP).
   Klicken Sie auf **OK**.
   Wiederholen Sie diesen Schritt für die andere IP-Kamera.

So fügen Sie die IP-Kameras dem Logischen Baum hinzu:

Hauptfenster > **Karten und Struktur**

- Ziehen Sie die Kameras in den Logischen Baum.

So ändern Sie die Kameraeigenschaften:

Hauptfenster > **Kameras und Aufzeichnung** > > Registerkarte

1. Konfigurieren Sie in der Spalte **Live Video** die Qualität für die Liveanzeige. Für diese Geräte können Sie die Live-Qualität nur pro Kamera, nicht aber zeitplanabhängig einstellen.
2. Nehmen Sie in den anderen Spalten die erforderlichen Einstellungen vor.

So konfigurieren Sie Aufzeichnungseinstellungen für die Kameras:

1. Klicken Sie auf .
2. Wählen Sie die entsprechende Gerätefamilie aus.
3. Wählen Sie die jeweils verfügbare Aufzeichnungseinstellung.
4. Wählen Sie den entsprechenden Aufzeichnungsplan, zum Beispiel **Tag**.
5. Unter **Dauer- oder Voralarmaufzeichnung** wählen Sie den gewünschten Aufzeichnungsmodus, Stream und die Qualität.
   Wenn Sie im Aufzeichnungsmodus **Voralarm** wählen, steht das **Dauer** zur Verfügung, um die Voralarmaufzeichnungszeit in Sekunden festzulegen.
6. Unter **Alarmaufzeichnung** in der Spalte **Dauer** klicken Sie auf eine Zelle und geben Sie die gewünschte Aufzeichnungszeit in Sekunden ein, nachdem der Alarm aufgetreten ist.
7. Wiederholen Sie die vorherigen Schritte, um die Aufzeichnungseinstellungen für die andere Kamera der Gerätefamilie zu konfigurieren.

12 Allgemeine Fenster des Configuration Client

Hinweis!
BVMS Viewer bietet nur Grundfunktionen. Erweiterte Funktionen sind in BVMS Professional enthalten. Ausführliche Informationen zu den verschiedenen Versionen von BVMS finden Sie unter www.boschsecurity.com und in der BVMS Schnellauswahlhilfe: BVMS Schnellauswahlhilfe.

Dieses Kapitel enthält Informationen über einige verfügbare grundlegende Anwendungsfenster im BVMSConfiguration Client.

12.1 Konfigurationsfenster

Hauptfenster
Dient zur Systemkonfiguration. Die Schaltflächen in der Symbolleiste repräsentieren die verschiedenen Seiten, die Sie zur Inbetriebnahme des Systems konfigurieren müssen. Ihre Reihenfolge repräsentiert die empfohlene Schrittfolge bei der Konfiguration.

- Klicken Sie auf ein Baumelement, um die verfügbaren Eigenschaftsseiten anzuzeigen.

Geräte	Klicken Sie hier, um die Seite **Geräte** mit allen an das System angeschlossenen Geräten anzuzeigen.
Karten und Struktur	Klicken Sie hier, um die Seite **Karten und Struktur** mit dem Logischen Baum, Gerätebaum und den Karten anzuzeigen.
Zeitpläne	Klicken Sie hier, um die Seite **Aufzeichnungszeitpläne** und **Aktionszeitpläne** anzuzeigen.
Kameras und Aufzeichnung	Klicken Sie hier, um die Seite **Kameras und Aufzeichnung** mit der Kameratabelle und den Aufzeichnungseinstellungen aller Kameras anzuzeigen.
Ereignisse	Klicken Sie hier, um die Seite **Ereignisse** anzuzeigen.
Alarme	Klicken Sie hier, um die Seite **Alarme** anzuzeigen.
Benutzergruppen	Klicken Sie hier, um die Seite **Benutzergruppen** mit allen Benutzern anzuzeigen.
	Klicken Sie darauf, um die geänderten Einstellungen des aktuellen Fensters zu speichern.
	Klicken Sie darauf, um die gespeicherten Einstellungen des aktuellen Fensters wiederherzustellen. **Hinweis:** Nur die Einstellungen, die in BVMS vorgenommen wurden, werden wiederhergestellt, nicht die Einstellungen, die direkt auf dem Gerät vorgenommen wurden. Dies kann dazu führen, dass Geräte nicht mehr zugänglich sind.
	Klicken Sie hier, um das Dialogfeld **Konfiguration aktivieren** anzuzeigen.

	Klicken Sie darauf, um das ausgewählte Element zu löschen. (Nicht auf jeder Seite verfügbar.)
	Klicken Sie darauf, um das ausgewählte Element umzubenennen. (Nicht auf jeder Seite verfügbar.)
	Klicken Sie hier, um Hilfeinformationen zum aktuellen Fenster anzuzeigen.
	Klicken Sie hier, um die Statusinformationen für alle Geräte und die Gerätefunktionen bei Bedarf zu aktualisieren (nicht auf jeder Seite verfügbar). Sie können den Status eines einzelnen Geräts aktualisieren: Klicken Sie mit der rechten Maustaste auf das Gerät und klicken Sie dann auf **Status aktualisieren**. **Hinweis:** Wenn Sie ein großes System mit über 1.000 Geräten konfiguriert haben, kann das Aktualisieren der Status und Gerätefunktionen sehr lange dauern.

12.2 Menübefehle

System Menübefehle

Änderungen speichern	Speichert alle auf dieser Seite durchgeführten Änderungen.
Alle Änderungen auf dieser Seite rückgängig	Stellt die Einstellungen dieser Seite seit dem letzten Speichervorgang wieder her.
Aktivierungs-Manager...	Zeigt das Dialogfeld **Aktivierungs-Manager** an.
Konfiguration exportieren...	Zeigt das Dialogfeld **Konfigurationsdatei exportieren** an.
Konfiguration importieren...	Zeigt das Dialogfeld **Konfigurationsdatei importieren** an.
OPC-Geräteinformation exportieren...	Zeigt ein Dialogfeld zum Erzeugen einer Konfigurationsdatei an, die Sie in das Managementsystem eines Drittanbieters importieren können.
Beenden	Beendet das Programm.

Hardware-Menübefehle

Initialer Geräte-Scan...	Zeigt das Dialogfeld **Initialer Geräte-Scan** an.
Geräte mit Standardpasswort schützen...	Zeigt das Dialogfeld **Geräte mit globalem Standardpasswort schützen** an.
iSCSI Speichergeräte mit CHAP Passwort schützen	Zeigt das Dialogfeld **iSCSI Speichergeräte mit CHAP Passwort schützen** an.
Gerätepasswörter ändern...	Zeigt das Dialogfeld **Gerätepasswörter ändern** an.
Geräte Firmware aktualisieren...	Zeigt das Dialogfeld **Geräte-Firmware aktualisieren** an.

Geräte IP und Netzwerkeinstellungen ändern...	Zeigt das Dialogfeld **Geräte-IP und Netzwerkeinstellungen ändern** an.
Gerätemonitor...	Zeigt das Dialogfeld **Gerätemonitor** an.

Werkzeuge-Menübefehle

Kommandoskript-Editor...	Zeigt das Dialogfeld **Kommandoskript-Editor** an.
Ressourcen-Manager...	Zeigt das Dialogfeld **Ressourcen-Manager** an.
Kamerasequenzen...	Zeigt das Dialogfeld **Kamerasequenzen** an.
Lizenz Manager...	Zeigt das Dialogfeld **Lizenz-Manager** an.
Lizenz Inspektor...	Zeigt das Dialogfeld **Lizenz-Inspektor** an.
Überwachung der Arbeitsstationen...	Zeigt das Dialogfeld **Überwachung der Arbeitsstationen** an.

Auswertungen-Menübefehle

Alle Auswertungen exportieren...	Wählen Sie einen Zielordner aus, um die Auswertungen zu speichern.
Aufzeichnungszeitpläne...	Zeigt das Auswertungs-Dialogfeld **Aufzeichnungszeitpläne** an.
Geplante Aufzeichnungseinstellungen...	Zeigt das Auswertungs-Dialogfeld **Geplante Aufzeichnungseinstellungen** an.
Aktionszeitpläne...	Zeigt das Auswertungs-Dialogfeld **Aktionszeitpläne** an.
Kamera- und Aufzeichnungsparameter...	Zeigt das Auswertungs-Dialogfeld **Parameter für Kameras und Aufzeichnung** an.
Stream-Qualitätseinstellungen...	Zeigt das Auswertungs-Dialogfeld **Stream-Qualitätseinstellungen** an.
Ereigniseinstellungen...	Zeigt das Auswertungs-Dialogfeld **Ereigniseinstellungen** an.
Einstellungen für Zusammengesetzte Ereignisse...	Zeigt das Auswertungs-Dialogfeld **Einstellungen für Zusammengesetzte Ereignisse** an.
Alarmeinstellungen...	Zeigt das Auswertungs-Dialogfeld **Alarmeinstellungen** an.
Konfigurierte Benutzer...	Zeigt das Auswertungs-Dialogfeld **Konfigurierte Benutzer** an.
Benutzergruppen und Konten...	Zeigt das Auswertungs-Dialogfeld **Benutzergruppen und Konten** an.
Geräteberechtigungen...	Zeigt das Auswertungs-Dialogfeld **Geräteberechtigungen** an.
Bedienberechtigungen...	Zeigt das Auswertungs-Dialogfeld **Bedienberechtigungen** an.

Konfigurations-Berechtigungen...	Zeigt das Auswertungs-Dialogfeld **Konfigurationsberechtigungen** an.
Benutzergruppen Berechtigungen...	Zeigt das Auswertungs-Dialogfeld **Berechtigungen der Benutzergruppen** an.
Sicherheitseinstellungen...	Zeigt das Auswertungs-Dialogfeld **Sicherheitseinstellungen** an.
Berechtigungen für Anwendungen...	Zeigt das Auswertungs-Dialogfeld **Berechtigungen für Anwendungen** an.
Umgangene Geräte...	Zeigt das Auswertungs-Dialogfeld **Umgangene Geräte** an.

Befehle des Menüs Einstellungen

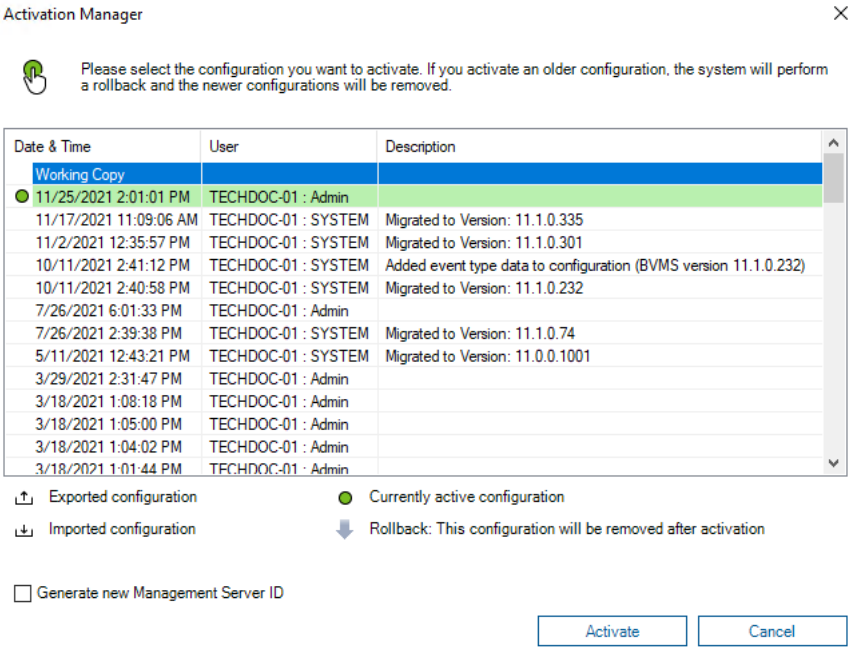
Alarmeinstellungen...	Zeigt das Dialogfeld **Alarmeinstellungen** an.
SNMP-Einstellungen...	Zeigt das Dialogfeld **SNMP-Einstellungen** an.
LDAP-Server-Einstellungen ...	Zeigt das Dialogfeld **LDAP Server-Einstellungen** an.
Reihenfolge LDAP Benutzergruppen...	Zeigt das Dialogfeld **Reihenfolge LDAP Benutzergruppen...** an.
Einstellungen Zugangstoken...	Zeigt das Dialogfeld **Zugangstoken Einstellungen** an.
Einstellungen vertrauenswürdiges Zertifikat...	Zeigt das **Einstellungen für vertrauenswürdige Zertifikate** Dialogfeld an. **Hinweis:** Das Menü **Einstellungen vertrauenswürdiges Zertifikat...** ist nur verfügbar, wenn Sie das Configuration Client mit Admin-Rechten starten und wenn der Benutzer, der sich anmeldet, die **Benutzergruppen konfigurieren/Enterprise Accounts** Berechtigung hat.
Aufzeichnungsqualitäten einstellen	Zeigt das Dialogfeld **Stream-Qualitätseinstellungen** an.
Optionen...	Zeigt das Dialogfeld **Optionen** an.

Hilfe-Menübefehle

Hilfe anzeigen	Zeigt die Anwendungshilfe zu BVMS an.
Über...	Zeigt ein Dialogfeld mit Informationen über das installierte System an, z. B. die Versionsnummer.

12.3 Dialogfeld „Aktivierungs-Manager“ (Menü „System“)

Hauptfenster > Menü **System** > Befehl **Aktivierungs-Manager...**
Dient zum Aktivieren der aktuellen Konfiguration oder zur Durchführung eines Rollbacks zu einer früheren Konfiguration.



Aktivieren

Klicken Sie hier, um das Dialogfeld **Konfiguration aktivieren** anzuzeigen.

Siehe

- *Aktivieren der letzten Konfiguration, Seite 92*
- *Aktivieren einer Konfiguration, Seite 93*

12.4 Dialogfeld „Konfiguration aktivieren“ (Menü „System“)

Hauptfenster >

Dient zum Eingeben einer Beschreibung für die zu aktivierende letzte Konfiguration.

Zeit für verzögerte Aktivierung einstellen

Klicken Sie hier, um eine Zeit für eine verzögerte Aktivierung auszuwählen.

Hinweis: Die verzögerte Aktivierung wird nicht ausgeführt, solange der Benutzer beim Configuration Client angemeldet ist.

Aktivierung für alle Operator Clients erzwingen

Wenn dieses Kontrollkästchen aktiviert ist, wird jede Operator Client-Arbeitsstation automatisch neu gestartet, um die neue Konfiguration zu aktivieren. Der Benutzer kann die neue Konfiguration nicht ablehnen.

Wenn dieses Kontrollkästchen nicht aktiviert ist, wird auf jeder Operator Client-Arbeitsstation einige Sekunden lang ein Dialogfeld angezeigt. Der Benutzer kann die neue Konfiguration ablehnen oder akzeptieren. Wenn der Benutzer untätig bleibt, wird das Dialogfeld nach einigen Sekunden geschlossen. In diesem Fall wird die neue Konfiguration nicht akzeptiert.

Siehe

- *Aktivieren der letzten Konfiguration, Seite 92*

12.5 Dialogfeld „Initialer Geräte-Scan“ (Menü „Hardware“)

Hauptfenster > Menü **Hardware** menu, Klick auf Befehl **Initialer Geräte-Scan...**

Zeigt die Geräte an, die doppelte IP-Adressen oder eine Standard-IP-Adresse (192.168.0.1) haben.
Dient zum Ändern dieser IP-Adressen und Subnetzmasken.
Sie müssen zuerst die richtige Subnetzmaske angeben, bevor Sie eine IP-Adresse ändern.

12.6 Dialogfeld „Geräte mit globalem Standard-Passwort schützen“ (Menü „Hardware“)

Hauptfenster > Menü **Hardware** > Befehl **Geräte mit Standardpasswort schützen...**
oder

Hauptfenster >

Das Dialogfeld erscheint, wenn eine Aktivierung ansteht und die Konfiguration Geräte enthält, die nicht durch ein Passwort geschützt sind. Dies ermöglicht Ihnen die Eingabe eines globalen Standard-Passworts, das für alle betreffenden Geräte gilt.

Status und Merkmale aktualisieren
Klicken Sie hier, um das Netzwerk erneut nach Geräten zu durchsuchen, die nicht passwortgeschützt sind.

Globales Standardpasswort
Geben Sie ein Passwort ein, das für alle derzeit noch nicht geschützten Geräte verwendet wird.

Passwörter anzeigen
Klicken Sie hier, damit alle Passwörter in diesem Dialog sichtbar werden.

Passwortschutz bei Aktivierung erzwingen
Klicken Sie, um das Kontrollkästchen zu aktivieren. Wenn diese Option aktiviert ist, müssen Sie ein globales Standardpasswort für Geräte übernehmen, die nicht durch ein Passwort geschützt sind.

Übernehmen
Klicken Sie hier, um das globale Standardpasswort zu übernehmen.
Das Dialogfeld **Passwörter ändern** wird angezeigt. Die Änderungen der Passwörter werden aufgeführt.
Klicken Sie zum Schließen auf **OK**.
Wenn Sie damit begonnen haben, Ihre Konfiguration zu aktivieren, wird das Dialogfeld **Aktivierungs-Manager** angezeigt.

Siehe
– *Aktivieren der letzten Konfiguration, Seite 92*

12.7 Dialogfeld „iSCSI-Speicher mit CHAP-Passwort schützen“ (Menü „Hardware“)

Verwenden Sie diesen Dialog, um CHAP-Passwörter auf iSCSI- und VRM -Geräten festzulegen. Das System überträgt diese Passwörter automatisch auf die Konten **Benutzer** und **Ziel** von Encodern, Decodern und VSG-Geräten.
Für neu hinzugefügte Geräte werden die Passwörter beim Aktivieren der Konfiguration automatisch festgelegt.
Hinweis: Durch das Festlegen eines leeren CHAP-Passworts wird das CHAP-Passwort auf iSCSI- und VRM -Geräten entfernt.

Hinweis!
- Bei allen DSA E-Series wird das CHAP-Passwort automatisch festgelegt
.- VRM Geräte übertragen das CHAP-Passwort an die Encoder. Aber Sie müssen das CHAP-Passwort auf dem jeweiligen iSCSI Gerät festlegen, um die Aufzeichnung zu gewährleisten.
- Auf allen DIVAR IP Geräten müssen Sie das CHAP-Passwort manuell festlegen. Siehe das jeweilige DIVAR IP Handbuch für weitere Anweisungen. Andernfalls bricht die Aufzeichnung ab oder die Wiedergabe funktioniert nicht.

Globalesl CHAP Passwort
Geben Sie das iSCSI-CHAP-Passwort ein, das für die Authentifizierung beim iSCSI-Speichergerät und zum Aktivieren einer direkten Wiedergabe vom iSCSI erforderlich ist.

Globales CHAP Passwort bestätigen
Bestätigen Sie das iSCSI-CHAP-Passwort.

Passwort anzeigen
Klicken Sie hier, damit das eingegebene Passwort angezeigt wird. Achten Sie darauf, dass niemand das Passwort einsehen kann.

Übernehmen
Klicken Sie, um das CHAP-Passwort zu übernehmen.
Hinweis: Überprüfen Sie das Vorgangsresultat. Ggf. müssen Sie das CHAP-Passwort bei einigen iSCSI-Geräten manuell eingeben.

12.8 Dialogfeld „Gerätepasswörter ändern“ (Menü „Hardware“)

Hauptfenster > **Geräte** > **Gerätepasswörter ändern** > **Gerätepasswörter ändern** Dialogfeld
oder
Hauptfenster > Menü **Hardware** > Befehl **Gerätepasswörter ändern...** > Dialogfeld **Gerätepasswörter ändern**

Klicken Sie darauf, um die Statusinformationen für alle Geräte zu aktualisieren. Sie können den Status eines einzelnen Geräts aktualisieren: Klicken Sie mit der rechten Maustaste auf das Gerät und klicken Sie dann auf **Status aktualisieren**.
Hinweis: Wenn Sie ein großes System mit über 1000 Geräten konfiguriert haben, kann der Aktualisierungsvorgang sehr lange dauern.

Klicken Sie darauf, um alle verfügbaren Geräte gleichzeitig auszuwählen.

Passwörter anzeigen
Aktivieren Sie das Kontrollkästchen, um die konfigurierten Passwörter lesbar anzuzeigen.

Um nach Elementen zu suchen:

- Tippen Sie im Suchfeld eine Zeichenfolge ein und drücken Sie auf den Schlüssel ENTER, um die angezeigten Elemente zu filtern.
  Nur Elemente mit der Zeichenfolge und ihre übergeordneten Elemente (nur in Bäumen) werden angezeigt. Die Anzahl der gefilterten Elemente und die gesamte Anzahl der Elemente wird angegeben.

Hinweis: Setzen Sie Zeichenfolgen zwischen doppelte Anführungszeichen, um genaue Treffer zu erhalten. Beispielsweise filtert "Camera 1" genau die Kameras mit diesem Namen, jedoch nicht camera 201.
Hinweis: Die Passwortsuche ist nur möglich, wenn das Kontrollkästchen **Passwörter anzeigen** aktiviert ist.

Die Tabelle dient zum Einstellen folgender Eigenschaften für die verfügbaren IP-Geräte:
- Service-Passwort
- Benutzer-Passwort
- Live-Passwort
- Ziel-Passwort

So ändern Sie das Passwort für IP-Geräte:
1. Wählen Sie das erforderliche Gerät aus.
2. Klicken Sie mit der rechten Maustaste auf das ausgewählte Gerät und klicken Sie dann auf **Passwort bearbeiten...**.
   Das Dialogfeld **Gerätepasswörter ändern** wird angezeigt.
3. Wählen Sie den entsprechenden Passworttyp aus.
4. Geben Sie das neue Passwort ein.
5. Klicken Sie auf **OK**.
   Das neue Passwort wird im ausgewählten Gerät aktualisiert.

So ändern Sie die Einstellungen für mehrere Geräte:
Siehe *Konfigurieren mehrerer Encoder/Decoder, Seite 232*.

12.9 Dialogfeld „Geräte-Firmware aktualisieren“ (Menü „Hardware“)

Hauptfenster > Menü **Hardware** > Befehl **Geräte Firmware aktualisieren...** > Dialogfeld **Geräte-Firmware aktualisieren**

Klicken Sie darauf, um die Statusinformationen für alle Geräte zu aktualisieren. Sie können den Status eines einzelnen Geräts aktualisieren: Klicken Sie mit der rechten Maustaste auf das Gerät und klicken Sie dann auf **Status aktualisieren**.
Hinweis: Wenn Sie ein großes System mit über 1000 Geräten konfiguriert haben, kann der Aktualisierungsvorgang sehr lange dauern.

Klicken Sie darauf, um alle verfügbaren Geräte gleichzeitig auszuwählen.

Klicken Sie darauf, um die Firmware-Version zu aktualisieren.

Um nach Elementen zu suchen:

- Tippen Sie im Suchfeld eine Zeichenfolge ein und drücken Sie auf den Schlüssel ENTER, um die angezeigten Elemente zu filtern.
  Nur Elemente mit der Zeichenfolge und ihre übergeordneten Elemente (nur in Bäumen) werden angezeigt. Die Anzahl der gefilterten Elemente und die gesamte Anzahl der Elemente wird angegeben.

Hinweis: Setzen Sie Zeichenfolgen zwischen doppelte Anführungszeichen, um genaue Treffer zu erhalten. Beispielsweise filtert "Camera 1" genau die Kameras mit diesem Namen, jedoch nicht camera 201.

So aktualisieren Sie die Firmware-Version:

1. Wählen Sie das erforderliche Gerät aus.
2. Klicken Sie auf **Firmware aktualisieren**.
   Ein Configuration Client-Informationsfenster wird angezeigt.
3. Klicken Sie auf **OK**.
   Der Explorer wird geöffnet.
4. Wählen Sie die Datei aus, die das Update enthält.
5. Klicken Sie auf **Öffnen**.
   Das Fenster **Status Firmware-Upload** wird geöffnet.
6. Klicken Sie auf **Start**, um den Upload zu starten.
7. Klicken Sie auf **Schließen**.
   Die Firmware ist aktualisiert.

So ändern Sie die Einstellungen für mehrere Geräte:
Siehe *Konfigurieren mehrerer Encoder/Decoder, Seite 232*.

12.10 Dialogfeld „Geräte-IP und Netzwerkeinstellungen ändern“ (Menü „Hardware“)

Hauptfenster > Menü **Hardware** > Befehl **Geräte IP und Netzwerkeinstellungen ändern...** > Dialogfeld **Geräte-IP und Netzwerkeinstellungen ändern**

Klicken Sie darauf, um die Statusinformationen für alle Geräte zu aktualisieren. Sie können den Status eines einzelnen Geräts aktualisieren: Klicken Sie mit der rechten Maustaste auf das Gerät und klicken Sie dann auf **Status aktualisieren**.
Hinweis: Wenn Sie ein großes System mit über 1000 Geräten konfiguriert haben, kann der Aktualisierungsvorgang sehr lange dauern.

Klicken Sie darauf, um alle verfügbaren Geräte gleichzeitig auszuwählen.

Um nach Elementen zu suchen:

- Tippen Sie im Suchfeld eine Zeichenfolge ein und drücken Sie auf den Schlüssel ENTER, um die angezeigten Elemente zu filtern.
  Nur Elemente mit der Zeichenfolge und ihre übergeordneten Elemente (nur in Bäumen) werden angezeigt. Die Anzahl der gefilterten Elemente und die gesamte Anzahl der Elemente wird angegeben.

Hinweis: Setzen Sie Zeichenfolgen zwischen doppelte Anführungszeichen, um genaue Treffer zu erhalten. Beispielsweise filtert "Camera 1" genau die Kameras mit diesem Namen, jedoch nicht camera 201.

Die Tabelle dient zum Einstellen folgender Eigenschaften für die verfügbaren IP-Geräte:
- Anzeigename
- IP-Adresse
- Subnetzmaske
- Gateway-IP

Hinweis!
Anstatt die Befehle zu verwenden, können Sie die entsprechenden Einstellungen in das erforderliche Feld eingeben.

So legen Sie den Anzeigenamen für IP-Geräte fest:
1. Wählen Sie das erforderliche Gerät aus.
2. Klicken Sie mit der rechten Maustaste auf das ausgewählte Gerät und klicken Sie dann auf **Display-Namen vergeben ...**. Das Dialogfeld **Display-Namen vergeben** wird angezeigt.
3. Geben Sie im Feld **Start bei:** die erste Zeichenfolge ein.
4. Klicken Sie auf **Berechnen**. Im Feld **Ende bei:** wird die letzte Zeichenfolge des Bereichs für das ausgewählte Gerät angezeigt.
5. Klicken Sie auf **OK**.
6. Klicken Sie im Dialogfeld **Geräte-IP und Netzwerkeinstellungen ändern** auf **Übernehmen**.
   Der berechnete Name wird im ausgewählten Gerät aktualisiert.

Dialogfeld Display-Namen einstellen

Start bei:
Geben Sie den ersten Namen ein.

Ende bei:
Zeigt den letzten Namen für die ausgewählten Geräte an, wenn Sie auf **Berechnen** geklickt haben.

Berechnen
Klicken Sie darauf, um den Bereich der Anzeigenamen für die ausgewählten Geräte zu berechnen.

So legen Sie die IP-Adresse für IP-Geräte fest:
1. Wählen Sie das erforderliche Gerät aus.
2. Klicken Sie mit der rechten Maustaste auf das ausgewählte Gerät und klicken Sie dann auf **IP-Adressen vergeben ...**. Das Dialogfeld **IP-Adressen vergeben** wird angezeigt.
3. Geben Sie im Feld **Start bei:** die erste IP-Adresse ein.
4. Klicken Sie auf **Berechnen**. Im Feld **Ende bei:** wird die letzte IP-Adresse des Bereichs für das ausgewählte Gerät angezeigt.
5. Klicken Sie auf **OK**.

6. Klicken Sie im Dialogfeld **Geräte-IP und Netzwerkeinstellungen ändern** auf **Übernehmen**.
   Die neue IP-Adresse wird im ausgewählten Gerät aktualisiert.

Dialogfeld IP-Adressen einstellen

Start bei:
Geben Sie die erste IP-Adresse ein.

Ende bei:
Zeigt die letzte IP-Adresse für die ausgewählten Geräte an, wenn Sie auf **Berechnen** geklickt haben.

Berechnen
Klicken Sie darauf, um den IP-Adressbereich für die ausgewählten Geräte zu berechnen.

So legen Sie die Subnetzmaske/Gateway-ID für IP-Geräte fest:
1. Klicken Sie in das entsprechende Feld.
2. Geben Sie den entsprechenden Wert ein.
3. Klicken Sie auf **Übernehmen**.
   Der neue Wert wird im ausgewählten Gerät aktualisiert.

Übernehmen
Klicken Sie darauf, um die Geräte mit den eingegebenen Werten zu konfigurieren, ohne das Dialogfeld zu schließen.

So ändern Sie die Einstellungen für mehrere Geräte:
Siehe *Konfigurieren mehrerer Encoder/Decoder, Seite 232*.

12.11 Dialogfeld „Geräte-Monitor“ (Menü „Hardware“)

Hauptfenster > Menü **Hardware** > Befehl **Gerätemonitor...** > Dialogfeld **Gerätemonitor**
Ermöglicht die Überprüfung des Status der Encoder/Decoder im Gerätebaum, die im BVMS aktiv sind.

Display-Name
Gerätename, der im BVMS eingestellt wurde

Netzwerkadresse
IP-Adresse des Geräts

Status
Die folgenden Zustände können angezeigt werden:
- **Konfiguriert**: Die Konfiguration dieses Geräts ist aktiviert.
- **Konfiguration stimmt nicht überein**: Die Konfiguration dieses Geräts ist nicht aktiviert.
- **Unbekannt**Der Status konnte nicht ermittelt werden.
- **Nicht verbunden**: Nicht verbunden.

Letzte Prüfung
Datum und Uhrzeit, wann der Dialog gestartet und die Prüfung durchgeführt wurde. Die Geräte werden solange nicht erneut überprüft, wie das Dialogfeld angezeigt wird.

Siehe
- *Status des Encoders/Decoders überprüfen, Seite 95*

12.12 Dialogfeld Kommandoscript-Editor (Menü „Werkzeuge“)

Weitere Informationen finden Sie unter *Dialogfeld Kommandoskript-Editor, Seite 312*.

Siehe

– *Dialogfeld Kommandoskript-Editor, Seite 312*

12.13 Dialogfeld Ressourcen-Manager (Menü „Werkzeuge“)

Weitere Informationen finden Sie unter *Dialogfeld Ressourcen-Manager, Seite 266*.

Siehe

– *Dialogfeld Ressourcen-Manager, Seite 266*

12.14 Dialogfeld Kamerasequenzen (Menü „Werkzeuge“)

Weitere Informationen finden Sie unter *Dialogfeld Kamerasequenzen, Seite 269*.

Siehe

– *Dialogfeld Kamerasequenzen, Seite 269*

12.15 Dialogfeld „Lizenz-Manager“ (Menü „Werkzeuge“)

Hauptfenster > Menü **Werkzeuge** > Befehl **Lizenz Manager...**
Dient zum Lizenzieren des von Ihnen erworbenen BVMS Pakets sowie zum Aufrüsten mit zusätzlichen Funktionen.

Lizenzstatus
Zeigt den Lizenzstatus an.

System Fingerprint
Zu Supportzwecken empfehlen wir die Angabe des **System Fingerprint**.

Installationsort
Bei Aktivierung Ihrer Basislizenz im Bosch Remote Portal geben Sie Informationen zum Installationsstandort Ihres Systems an. Diese Informationen werden hier angezeigt.
Hinweis: Sie können diese Informationen auch in anderen Lizenzen angeben, aber nur die in der Basislizenz angegebenen Informationen werden hier angezeigt.

Lizenzen

1. Klicken Sie auf **Hinzufügen**, um Ihre Lizenzen hinzuzufügen.
   Das Dialogfeld **Lizenz hinzufügen** wird angezeigt.
2. Befolgen Sie die Anweisungen im Dialogfeld.

Gültige Lizenz
Zeigt die von Ihnen aktivierte Basislizenz an.

Features

- Klicken Sie auf **Lizenz Inspektor...**.
  Das Dialogfeld **Lizenz-Inspektor** wird angezeigt.

Zeigt die Anzahl der lizenzierten Funktionen an, die derzeit installiert sind.
Sie können überprüfen, ob die Anzahl der installierten BVMS Lizenzen die Anzahl der erworbenen Lizenzen übersteigt.

Installierte BVMS Versionen
Zeigt die aktuell installierte Version von BVMS an, z. B. 11.0.

Lizenzierte BVMS Versionen
Zeigt alle BVMS Versionen an, die in der aktuell bereitgestellten Lizenzdatei enthalten sind und unterstützt werden.
Beispiel: BVMS 11.0 und alle zukünftigen Unterversionen BVMS 11.x.

Aktivierungsdatum
Zeigt das Aktivierungsdatum Ihrer installierten BVMS Version an.

Ablaufdatum
Zeigt das Ablaufdatum Ihrer installierten BVMS Version an. Ein Ablaufdatum ist nur vorhanden, wenn Sie eine Notfalllizenz oder eine Vertriebs-Demolizenz installieren.

Software Maintenance Agreement

Ablaufdatum
Wenn Sie ein Software Maintenance Agreement gekauft und aktiviert haben, wird hier das Ablaufdatum angezeigt.

Siehe
- *Aktivieren der Softwarelizenzen, Seite 74*
- *Dialogfeld „Lizenz hinzufügen“, Seite 112*
- *Dialogfeld „License Inspector“ (Menü „Werkzeuge“), Seite 112*

12.15.1 Dialogfeld „Lizenz hinzufügen“

Hauptfenster > Menü **Werkzeuge** > Befehl **Lizenz Manager...** > **Lizenzen** > **Hinzufügen**
Hier können Sie Ihre erworbenen Lizenzen oder Demolizenzen von der Bosch Remote Portal Website remote.boschsecurity.com zu Ihrem BVMS System hinzufügen.
Befolgen Sie die Anweisungen im Dialog, um Ihre Lizenzen hinzuzufügen.
Weitere Informationen finden Sie im entsprechenden Whitepaper der BVMS Lizenz.

12.16 Dialogfeld „License Inspector“ (Menü „Werkzeuge“)

Hauptfenster > Menü **Werkzeuge** , Klick auf **Lizenz Inspektor...** Befehl > **Lizenz-Inspektor**
Dialogfenster
Zeigt die Anzahl der lizenzierten Funktionen an, die derzeit installiert sind.
Sie können überprüfen, ob die Anzahl der installierten BVMS Lizenzen die Anzahl der erworbenen Lizenzen übersteigt.
Hinweis: Wenn die aktuelle Systemkonfiguration die Grenzwerte der derzeit installierten Lizenzen überschreitet, können Sie die Konfiguration nicht aktivieren.

12.17 Dialogfeld Arbeitsstationsüberwachung (Menü „Werkzeuge“)

Hauptfenster > Menü **Werkzeuge** > Befehl **Überwachung der Arbeitsstationen...** > Dialogfeld **Überwachung der Arbeitsstationen**

Zeigt eine Liste aller Arbeitsstationen an, die derzeit mit dem BVMS Management Server verbunden sind.
Hinweis: Die Liste zeigt alle verbundenen Operator Clients und Cameo SDK-Clients.

So trennen Sie eine Arbeitsstation:
1. Wählen Sie den entsprechenden Eintrag aus der Liste.
2. Klicken Sie auf **Trennen**.
   Hinweis: Die Funktion ist nur aktiv, wenn der Benutzer über die entsprechende Genehmigung verfügt.
3. Klicken Sie auf **Ja**.
   Der Listeneintrag wird entfernt, wenn sich der entsprechende Operator Client erfolgreich abmeldet.

Hinweis: Sie können nur Operator Client-Arbeitsstationen trennen.

12.18 Dialogfelder „Auswertungen“ (Menü „Auswertungen“)

Dieses Kapitel behandelt alle Dialogfelder, die für die Konfiguration von Auswertungen verfügbar sind.

Siehe

– *Berichte erstellen, Seite 96*

12.18.1 Dialogfeld „Aufzeichnungszeitpläne“

Hauptfenster > Menü **Auswertungen** > Befehl **Aufzeichnungszeitpläne...**

Listet die konfigurierten Aufzeichnungszeitpläne auf.

- Klicken Sie auf **CSV-Export**, um sämtliche in diesem Dialogfeld enthaltenen Informationen in einer CSV-Datei zu speichern.

12.18.2 Dialogfeld „Geplante Aufzeichnungseinstellungen“

Hauptfenster > Menü **Auswertungen** > Befehl **Geplante Aufzeichnungseinstellungen...**

Listet die konfigurierten geplanten Aufzeichnungseinstellungen auf.

- Klicken Sie auf **CSV-Export**, um sämtliche in diesem Dialogfeld enthaltenen Informationen in einer CSV-Datei zu speichern.

12.18.3 Dialogfeld „Aktionszeitpläne“

Hauptfenster > Menü **Auswertungen** > Befehl **Aktionszeitpläne...**

Listet die konfigurierten Aktionszeitpläne auf.

- Klicken Sie auf **CSV-Export**, um sämtliche in diesem Dialogfeld enthaltenen Informationen in einer CSV-Datei zu speichern.

12.18.4 Dialogfeld „Kameras und Aufzeichnungsparameter”

Hauptfenster > Menü **Auswertungen** > Befehl **Kamera- und Aufzeichnungsparameter...**

Listet die Aufzeichnungsparameter auf, die in der Kameratabelle und der Aufzeichnungstabelle konfiguriert sind.

- Klicken Sie auf **CSV-Export**, um sämtliche in diesem Dialogfeld enthaltenen Informationen in einer CSV-Datei zu speichern.

12.18.5 Dialogfeld „Stream-Qualität"

Hauptfenster > Menü **Auswertungen** > Befehl **Stream-Qualitätseinstellungen...**

Listet die konfigurierten Einstellungen für die Stream-Qualität aller Kameras auf.

- Klicken Sie auf **CSV-Export**, um sämtliche in diesem Dialogfeld enthaltenen Informationen in einer CSV-Datei zu speichern.

12.18.6 Dialogfeld „Ereignis-Einstellungen”

Hauptfenster > Menü **Auswertungen** > Befehl **Einstellungen für Zusammengesetzte Ereignisse...**

Listet die Ereignisse auf, für die ein Zeitplan zum Auslösen eines Alarms konfiguriert ist.

- Klicken Sie auf **CSV-Export**, um sämtliche in diesem Dialogfeld enthaltenen Informationen in einer CSV-Datei zu speichern.

12.18.7 Dialogfeld „Einstellungen für zusammengesetztes Ereignis”

Hauptfenster > Menü **Auswertungen** > Befehl **Einstellungen für Zusammengesetzte Ereignisse...**

Listet alle zusammengesetzten Ereignisse auf.

- Klicken Sie auf **CSV-Export**, um sämtliche in diesem Dialogfeld enthaltenen Informationen in einer CSV-Datei zu speichern.

12.18.8 Dialogfeld „Alarmeinstellungen“

Hauptfenster > Menü **Auswertungen** > Befehl **Alarmeinstellungen...**

Listet alle Alarmeinstellungen der konfigurierten Alarme auf, einschließlich der Einstellungen im Dialogfeld **Alarmoptionen**.

- Klicken Sie auf **CSV-Export**, um sämtliche in diesem Dialogfeld enthaltenen Informationen in einer CSV-Datei zu speichern.

12.18.9 Dialogfeld „Konfigurierte Benutzer”

Hauptfenster > Menü **Auswertungen** > Befehl **Konfigurierte Benutzer...**

Listet die Benutzer auf, die sich bei Operator Client anmelden dürfen.

- Klicken Sie auf **CSV-Export**, um sämtliche in diesem Dialogfeld enthaltenen Informationen in einer CSV-Datei zu speichern.

12.18.10 Das Dialogfeld „Benutzergruppen und Konten”

Hauptfenster > Menü **Auswertungen** > Befehl **Benutzergruppen und Konten...**

Listet die konfigurierten Benutzergruppen, Enterprise Accounts, Enterprise User Groups und 4-Augen-Gruppen auf.

- Klicken Sie auf **CSV-Export**, um sämtliche in diesem Dialogfeld enthaltenen Informationen in einer CSV-Datei zu speichern.

12.18.11 Dialogfeld „Geräteberechtigungen“

Hauptfenster > Menü **Auswertungen** > Befehl **Geräteberechtigungen...**

Listet die Berechtigungen für die Verwendung von konfigurierten Geräten für jede Benutzergruppe auf.

- Klicken Sie auf **CSV-Export**, um sämtliche in diesem Dialogfeld enthaltenen Informationen in einer CSV-Datei zu speichern.

12.18.12 Dialogfeld „Bedienberechtigungen“

Hauptfenster > Menü **Auswertungen** > Befehl **Bedienberechtigungen...**

Listet für die einzelnen Benutzergruppen die Berechtigungen zur Verwendung des Operator Client auf.

- Klicken Sie auf **CSV-Export**, um sämtliche in diesem Dialogfeld enthaltenen Informationen in einer CSV-Datei zu speichern.

12.18.13 Dialogfeld „Konfigurationsberechtigungen“

Hauptfenster > Menü **Auswertungen** > Befehl **Konfigurations-Berechtigungen...**

Listet für die einzelnen Benutzergruppen die Berechtigungen zur Verwendung des Configuration Client auf.

- Klicken Sie auf **CSV-Export**, um sämtliche in diesem Dialogfeld enthaltenen Informationen in einer CSV-Datei zu speichern.

12.18.14 Dialogfeld „Berechtigungen für Benutzergruppen“

Hauptfenster > Menü **Auswertungen** > Befehl **Benutzergruppen Berechtigungen...**

Listet die Berechtigungen für die Konfiguration von Benutzergruppen für jede Benutzergruppe auf.

- Klicken Sie auf **CSV-Export**, um sämtliche in diesem Dialogfeld enthaltenen Informationen in einer CSV-Datei zu speichern.

12.18.15 Dialogfeld „Sicherheitseinstellungen”

Hauptfenster > Menü **Auswertungen** > Befehl **Sicherheitseinstellungen...**
Listet die konfigurierten Sicherheitseinstellungen für jede Benutzergruppe und Enterprise User Groups auf.

- Klicken Sie auf **CSV-Export**, um sämtliche in diesem Dialogfeld enthaltenen Informationen in einer CSV-Datei zu speichern.

12.18.16 Dialogfeld Anwendungsberechtigungen

Hauptfenster > Menü **Auswertungen** > Befehl **Berechtigungen für Anwendungen...**

Listet alle Benutzergruppen und deren Anwendungsberechtigungen auf.

- Klicken Sie auf **CSV-Export**, um sämtliche in diesem Dialogfeld enthaltenen Informationen in einer CSV-Datei zu speichern.

12.18.17 Dialogfeld „Umgangene Geräte“

Hauptfenster > Menü **Auswertungen** > Befehl **Umgangene Geräte...**
Listet alle konfigurierten Geräte und die umgangenen Geräte auf.

- Klicken Sie auf **CSV-Export**, um sämtliche in diesem Dialogfeld enthaltenen Informationen in einer CSV-Datei zu speichern.

12.19 Dialogfeld „Alarmeinstellungen“ (Menü „Einstellungen“)

Siehe *Dialogfeld „Alarmeinstellungen“, Seite 316* .

12.20 Dialogfeld „SNMP-Einstellungen“ (Menü „Einstellungen“)

Hauptfenster > Menü **Einstellungen** > Befehl **SNMP-Einstellungen...**
Ermöglicht die Konfiguration der SNMP-Überwachung auf dem Management Server-Computer. Sie legen fest, für welches Ereignis ein SNMP-Trap gesendet wird. Darüber hinaus legen Sie einige zusätzliche Informationen zum System und die IP-Adressen der Computer fest, die SNMP-Traps vom BVMS erhalten sollen.
Der Server sendet SNMP-Traps, sobald Ereignisse eintreten. Sie können diese Traps über den SNMP-Empfänger im Configuration Client empfangen, der das **SNMP Trap Logger**-Tool verwendet. Sie können auch eine andere Software verwenden, die SNMP-Traps empfangen kann.
Der SNMP-Agent im BVMS unterstützt SNMP GetRequest. Sobald eine SNMP-Manager-Software (bspw. iReasoning MIB Browser) eine SNMP GetRequest an den BVMS Management Server sendet, sendet der Management Server eine entsprechende Antwortmeldung.
Die MIB-Datei befindet sich in folgendem Verzeichnis:

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

Es werden nur die Versionen SNMPv1 und v2 unterstützt.
Hinweis: SNMPv1 und SNMPv2 sind nicht vollständig kompatibel. Daher empfehlen wir, SNMPv1 und SNMPv2 nicht zusammen zu verwenden.

SNMP GET Port
Geben Sie die Port-Nummer für SNMP GetRequest ein. Dies ist der Port, an dem der SNMP-Agent des BVMS Management Server die SNMP GetRequest abruft.

Hinweis: Das BVMS verwendet für die SNMP GetRequest nicht die Standard-Port-Nummer 161, da dieser Port möglicherweise durch den SNMP-Agenten des Computers, auf dem das BVMS Management Server installiert ist, verwendet wird.
Der Standardwert ist `12544`.

Systemkontakt
Geben Sie die Kontaktdaten für das BVMS ein. Sie können diese Informationen über eine SNMP GetRequest unter Verwendung der OID .1.3.6.1.2.1.1.4 abrufen.

Systembeschreibung
Geben Sie eine Beschreibung für das BVMS ein. Sie können diese Informationen über eine SNMP GetRequest unter Verwendung der OID .1.3.6.1.2.1.1.5 abrufen.

Systemort
Geben Sie den Ort des BVMS ein. Mit dieser Zeichenfolge sollte der physische Standort des Server-Computers angegeben werden, bspw. das Gebäude, die Zimmernummer, Racknummer usw.
Sie können diese Informationen über eine SNMP GetRequest unter Verwendung der OID .1.3.6.1.2.1.1.6 abrufen.

Trap-Empfänger
Geben Sie die IP-Adresse des Computers ein, an den das BVMS die SNMP-Traps senden soll.

Trap-Filter
Wählen Sie die Ereignisse im Ereignisbaum durch Anklicken aus, anhand derer die gesendeten SNMP-Traps gefiltert werden.

Siehe
– *SNMP-Überwachung konfigurieren, Seite 95*

12.21 Dialogfeld „LDAP-Server-Einstellungen“ (Menü „Einstellungen“)

Hauptfenster > Menü **Einstellungen** > Befehl **LDAP-Server-Einstellungen ...**
In diesem Dialogfeld werden die LDAP-Server-Einstellungen eingegeben, die außerhalb von BVMS konfiguriert wurden. Für die folgenden Angaben benötigen Sie die Unterstützung des IT-Administrators, der den LDAP-Server eingerichtet hat.
Mit Ausnahme der Felder im Gruppenfeld **Benutzer / Benutzergruppe testen** sind alle Felder obligatorisch.

LDAP Server-Einstellungen

LDAP-Server
Geben Sie den Namen oder die IP-Adresse des LDAP-Servers ein.

Port
Geben Sie die Port-Nummer des LDAP-Servers ein (Standard-HTTP: 389, HTTPS: 636).

Sichere Verbindung
Wählen Sie das Kontrollkästchen aus, um die sichere Datenübertragung zu aktivieren.

Authentifizierungs-Verfahren
Durch „Negotiate“ wird das entsprechende Authentifizierungsprotokoll automatisch ausgewählt.
Mit „Simple“ werden die Anmeldeinformationen unverschlüsselt als Klartext übermittelt.

Proxy Authentifizierung

Anonymus
Dient zur Anmeldung als Gast. Wählen Sie diese Option aus, wenn sie vom LDAP-Server unterstützt wird und Sie keinen bestimmten Proxy-Benutzer konfigurieren können.

Verwenden Sie die folgenden Anmeldeinformationen

Benutzername
Geben Sie den eindeutigen Namen des Proxy-Benutzers ein. Dieser Benutzer ist erforderlich, um den Benutzern dieser BVMS Benutzergruppe den Zugriff auf den LDAP-Server zu ermöglichen.

Passwort
Geben Sie das Passwort des Proxy-Benutzers ein.

Test
Klicken Sie darauf, um zu testen, ob der Proxy-Benutzer Zugriff auf den LDAP-Server hat.

LDAP-Basis für Benutzer:
Geben Sie den eindeutigen Namen (DN = Distinguished Name) des LDAP-Pfads ein, in dem Sie nach einem Benutzer suchen können.
Beispiel für einen DN der LDAP-Basis: CN=Users,DC=Security,DC=MyCompany,DC=com

Filter für Benutzer
Wählen Sie einen Filter für die Suche nach einem eindeutigen Benutzernamen aus. Es sind vordefinierte Beispiele vorhanden. Ersetzen Sie %username% durch den tatsächlichen Benutzernamen.

LDAP-Basis für Gruppe
Geben Sie den eindeutigen Namen des LDAP-Pfads ein, in dem Sie nach Gruppen suchen können.
Beispiel für einen DN der LDAP-Basis: CN=Users,DC=Security,DC=MyCompany,DC=com

Filter für Suche nach Gruppenmitgliedern
Wählen Sie einen Filter für die Suche nach Gruppenmitgliedern aus.
Es sind vordefinierte Beispiele vorhanden. Ersetzen Sie %usernameDN% durch den tatsächlichen Benutzernamen und den zugehörigen DN.

Filter für Gruppensuche
Lassen Sie dieses Feld nicht leer. Wenn diese Angabe fehlt, können Sie einer BVMS Benutzergruppe keine LDAP-Gruppe zuordnen.
Wählen Sie einen Filter für die Suche nach einer Benutzergruppe aus.
Es sind vordefinierte Beispiele vorhanden.

Benutzer / Benutzergruppe testen
Die Angaben in diesem Gruppenfeld werden nicht gespeichert, wenn Sie auf **OK** klicken. Sie dienen lediglich zu Testzwecken.

Benutzername
Geben Sie den Namen eines Testbenutzers ein. Die Eingabe des DN ist nicht erforderlich.

Passwort
Geben Sie das Passwort des Testbenutzers ein.

Benutzer testen
Klicken Sie darauf, um zu testen, ob die Kombination aus Benutzername und Passwort korrekt ist.

Gruppe (DN):
Geben Sie den eindeutigen Namen der Gruppe ein, der der Benutzer zugeordnet ist.

Gruppe testen
Klicken Sie darauf, um die Zugehörigkeit des Benutzers zur Gruppe zu testen.

Siehe
– *Auswählen einer zugeordneten LDAP-Gruppe, Seite 363*

12.21.1 Zuordnen einer LDAP-Gruppe

Eine LDAP-Gruppe wird einer BVMS Benutzergruppe zugeordnet, um den Benutzern dieser LDAP-Gruppe Zugriff auf den Operator Client zu gewähren. Die Benutzer der LDAP-Gruppe verfügen über die Zugriffsrechte der Benutzergruppe, für die die LDAP-Gruppe konfiguriert ist.
Sie benötigen möglicherweise die Unterstützung des IT-Administrators, der für den LDAP-Server verantwortlich ist.
Sie können LDAP-Gruppen in Standardbenutzergruppen oder in Enterprise User Groups konfigurieren.

Hinweis!
Wenn eine LDAP-Gruppe einer BVMS Benutzergruppe zugeordnet ist, können Benutzer dieser LDAP-Gruppe den Operator Client über die einmalige Anmeldung starten.

Hinweis!
Ein LDAP-Benutzer kann mehreren LDAP-Benutzergruppen zugeordnet werden, die wiederum einer bestimmten BVMS Benutzergruppe zugeordnet sind.
Der LDAP-Benutzer erhält die Berechtigungen der BVMS Benutzergruppe, die den anderen LDAP-Benutzergruppen übergeordnet ist, die diesem LDAP-Benutzer zugeordnet sind.

So ordnen Sie eine LDAP-Gruppe zu:

1. Klicken Sie auf **LDAP-Server-Einstellungen ...**.
   Das Dialogfeld **LDAP Server-Einstellungen** wird angezeigt.
2. Geben Sie die Einstellungen des LDAP-Servers ein und klicken Sie auf **OK**.

Detaillierte Informationen zu den verschiedenen Feldern erhalten Sie, wenn Sie unten auf den Link des entsprechenden Anwendungsfensters klicken.

Siehe

- *Dialogfeld „LDAP-Server-Einstellungen“ (Menü „Einstellungen“), Seite 116*
- *Seite Eigenschaften der Benutzergruppen, Seite 335*

12.22 Dialogfeld „LDAP-Benutzergruppenreihenfolge definieren“ (Menü „Einstellungen“)

Zeigt die Liste **LDAP Nutzergruppenreihenfolge ändern** an. In der Liste werden die LDAP-Benutzergruppen mit den zugehörigen BVMS Benutzergruppen und Enterprise User Groups angezeigt. Per Drag & Drop oder mit den Pfeil-nach-oben- oder Pfeil-nach-unten-Schaltflächen können Sie die Reihenfolge der Gruppen ändern.

Hinweis!
Ein LDAP-Benutzer kann mehreren LDAP-Benutzergruppen zugeordnet werden, die wiederum einer bestimmten BVMS Benutzergruppe zugeordnet sind.
Der LDAP-Benutzer erhält die Berechtigungen der BVMS Benutzergruppe, die den anderen LDAP-Benutzergruppen übergeordnet ist, die diesem LDAP-Benutzer zugeordnet sind.

12.23 Dialogfeld „Zugriffstoken-Einstellungen“ (Menü Einstellungen)

Hauptfenster > Menü **Einstellungen** > Befehl **Einstellungen Zugangstoken...**
Wenn Sie die Anmeldung bei dem Management Server mit einem Zugriffstoken konfiguriert haben, müssen Sie zuerst die Token-Einstellungen definieren.

Ein Token wird von dem Enterprise Management Server erstellt und muss mit einem Zertifikat aus einem Zertifikatspeicher auf dem lokalen Computer signiert sein. Sie müssen das Zertifikat identifizieren, um zu wissen, welches Zertifikat Sie verwenden müssen.
Hinweis: BVMS unterstützt keine Zertifikate, die den Secure Hash Algorithmus SHA-1 verwenden und eine Schlüssellänge von weniger als 2048 Bit haben.

Eigenschaften von Signaturzertifikaten
Geben Sie eine Eigenschaftszeichenfolge ein, um das jeweilige Zertifikat zu identifizieren.
Hinweis: Wenn mehr als ein Zertifikat den Kriterien entspricht, wird das neueste, derzeit gültige Zertifikat verwendet.

Befolgen Sie die Regeln, um eine gültige Zeichenfolge für Eigenschaften in das Feld **Eigenschaften von Signaturzertifikaten** einzugeben:
- Die Zeichenfolge besteht aus einer oder mehreren Bedingungen.
- Bedingungen werden durch Semikolon (;) getrennt.
- Bedingungen sind Paare aus dem Namen der Zertifikateigenschaft und dem erwarteten Wert, getrennt durch ein Gleichheitszeichen (=).
- Die Namen der Zertifikateigenschaften können aus einem oder mehreren Teilen bestehen, die durch einen Punkt (.) getrennt sind.
- Bei den Namen der Zertifikateigenschaften und den erwarteten Werten wird nicht zwischen Groß- und Kleinschreibung unterschieden.

Beispiele:
`SubjectName.CN=BVMS Token Issuer;Parent.SubjectName.CN=BVMS Intermediate`
- Der Teil Common Name (`CN`) des Subject-Namens des Zertifikats muss gleich dem `BVMS Token Issuer` sein.
- Außerdem muss der Common Name-Teil des Subject Name des übergeordneten Zertifikats gleich dem `BVMS Intermediate` sein. Das übergeordnete Zertifikat ist das Zertifikat, das zum Signieren des aktuellen Zertifikats verwendet wurde.

`Parent.Thumbprint=A95FF7C6EC374127174D3AFA8EA67C94E8E66C3F`
- Der Fingerabdruck des übergeordneten Zertifikats des Zertifikats muss wie angegeben sein.

Liste der unterstützten Eigenschaftsnamen von Zertifikaten:

Name	Rückgabetyp
Thumbprint	String
SerialNumber	String
SubjectName	Distinguierter Name des Subjekts
IssuerName	Unterscheidungsmerkmal des Emittenten
Parent	Zertifikat, das zum Signieren des aktuellen Zertifikats verwendet wurde (Issuer CA)

Liste der unterstützten Eigenschaftsnamen auf distinguished name:

Name	Rückgabetyp
CN	String: Allgemeiner Name

Name	Rückgabetyp
OU	String: Name der organisatorischen Einheit
O	String: Name der Organisation
L	String: Name der Ortschaft
S	String: Name des Bundeslandes oder der Provinz
C	String: Name des Landes

Beispiele für die Verwendung von distinguished name:

- `SubjectName.CN=verisign authority`
- `IssuerName.C=DE`
- `Parent.Parent.SubjectName.O=Bosch Security Systems`

Zertifikatskette

Aktivieren Sie das Kontrollkästchen, um die Zertifikatskette einzuschließen.
Hinweis: Wenn der Management Server genau das gleiche Zertifikat installiert hat, müssen Sie die Zertifikatskette nicht unbedingt mit einbeziehen.

Anzahl der inbegriffenen Zertifikate

Geben Sie die genaue Anzahl der Zertifikate ein, die im Zugriffstoken enthalten sind.
Hinweis: Sie dürfen das Root Zertifikat nicht mitschicken.

Zugangstoken Laufzeit

Geben Sie die Zeit in Stunden ein, um festzulegen, wie lange die Token gültig sind, nachdem sie von dem Enterprise Management Server erstellt wurden.

Siehe

- *Tokenbasierte Authentifizierung, Seite 87*

12.24 Dialogfeld Einstellungen für vertrauenswürdige Zertifikate (Menü Einstellungen)

Hauptfenster > Menü **Einstellungen** > Befehl **Einstellungen vertrauenswürdiges Zertifikat...**
In diesem Dialogfeld können Sie den Zertifikats-Thumbprint eingeben, der vom Management Server zur Authentifizierung des Zugriffstokens verwendet wird.

Hinweis: Das Menü **Einstellungen vertrauenswürdiges Zertifikat...** ist nur verfügbar, wenn Sie den Configuration Client mit Administratorrechten starten und wenn der Benutzer, der sich anmeldet, die Berechtigung **Benutzergruppen konfigurieren/Enterprise Accounts** hat.

Thumbprint von vertrauenswürdigem Zertifikat

Zeigt einen bereits konfigurierten Fingerabdruck oder einen leeren Fingerabdruck an, wenn in der Registrierung keine Konfiguration gefunden wird. Geben Sie den Thumbprint des Stammzertifikats ein oder ändern Sie ihn.
Der angegebene Fingerabdruck wird in den Pfad `HKEY_LOCAL_MACHINE\SOFTWARE\Bosch Sicherheitssysteme GmbH\Bosch Video Management System\TrustedCertificates` zum Schlüssel „BvmsTrustedCertificate“ geschrieben.
Hinweis: Der Fingerabdruck wird beim Exportieren der Konfiguration nicht mit exportiert.

Hinweis: BVMS unterstützt keine Zertifikate, die den Secure Hash Algorithmus SHA-1 verwenden und eine Schlüssellänge von weniger als 2048 Bit haben.

12.25 Dialogfeld „Optionen“ (Menü „Einstellungen“)

Hinweis: Für einige Funktionen muss die entsprechende Lizenz erworben werden.

Hauptfenster > Menü **Einstellungen** > Befehl **Optionen...**

Allgemein

Configuration Client

Sprache
Dient zum Konfigurieren der Sprache des Configuration Client. Wenn Sie die Option **Systemsprache** auswählen, wird die Sprache der Windows-Installation verwendet.
Diese Einstellung wird bei jedem Start des Configuration Client wiederhergestellt.

Automatische Abmeldung
Dient zum Konfigurieren der automatischen Abmeldung des Configuration Client. Configuration Client meldet sich nach dem konfigurierten Zeitraum ab.
Änderungen in den Konfigurationsseiten der nachfolgenden Geräte auf der Seite **Geräte** werden nicht automatisch gespeichert und gehen bei der Abmeldung aufgrund von Inaktivität verloren:
- Encoder
- Decoder
- VRM-Geräte
- iSCSI-Geräte
- VSG-Geräte

Alle anderen anstehenden Konfigurationsänderungen werden automatisch gespeichert.
Hinweis: Änderungen in Dialogfeldern, die nicht durch Klicken von **OK** bestätigt wurden, werden nicht gespeichert.

Scan-Optionen
Dient zum Konfigurieren der Möglichkeit, ob der Scan nach Geräten im entsprechenden Subnetz oder in verschiedenen Subnetzen möglich ist.

Operator Client

Mehrfachanmeldung

Mehrfache Anmeldungen mit demselben Benutzernamen erlauben
Damit können Sie konfigurieren, dass ein Benutzer des BVMS SDK, von BVMS des Web Client, der BVMS Mobile App oder des Operator Client mehrere synchrone Anmeldungen mit demselben Benutzernamen ausführen können.

Central Server

Datenbank-Verbindungszeichenfolge
Dient zum Konfigurieren des Connection Strings für die Logbuchdatenbank.

Hinweis!
Ändern Sie diesen String nur, wenn Sie einen entfernten SQL-Server für das Logbuch konfigurieren möchten und mit der SQL-Server-Technologie vertraut sind.

Aufbewahrungsfrist
Dient zum Definieren einer maximalen Speicherdauer für Einträge im Logbuch. Nach dieser festgelegten Speicherdauer werden die Einträge automatisch gelöscht.
Diese Einstellung wird nach der Aktivierung der Konfiguration aktiviert.

Geräte

Monitorgruppe
Dient zum Konfigurieren der Benutzersteuerung aller Monitorgruppen für jeden BVMS Client-Computer. In diesem Fall müssen diese Computer nicht als Arbeitsstation im Gerätebaum konfiguriert werden.

Decoderstream Auswahl
Dies ermöglicht es Ihnen, die Konfiguration so einzustellen, dass alle Decoder im System nicht notwendigerweise den Live-Stream verwenden müssen, sondern einen kompatiblen Stream verwenden können.
Diese Einstellung wird nach der Aktivierung der Konfiguration aktiviert.
Monitorgruppen-Layout und Kamerazuordnung
Hier können Sie festlegen, ob das Layout der Monitorgruppe und die Einstellungen für die Kamerazuweisung nach einem Fehler auf die Standardeinstellungen zurückgesetzt werden sollen. Central Server neu starten oder wenn die letzten Einstellungen, die in Operator Client sollten beibehalten werden.
Wenn Sie die letzten Einstellungen beibehalten möchten, aktivieren Sie das Kontrollkästchen **Einstellungen nach Neustart des Central Server beibehalten**.
Note: Die Kamerasequenz beginnt mit der ersten Kamera in der Sequenz.

Zeitserver für Encoder
Ermöglicht Ihnen die Konfiguration der Zeitserver-Einstellungen für Encoder. Standardmäßig wird die Central Server IP-Adresse verwendet wird.

Systemfunktionen

Audit Trail
Sie benötigen eine Berechtigung, um die folgenden Einstellungen zu bearbeiten:
Audit Trail
Aktivieren oder deaktivieren Sie die Audit Trail-Funktion.
Hinweis: Die Audit Trail-Seite ist nur verfügbar, wenn die Configuration Client-Funktion aktiviert ist.
Maximale Retentionszeit
Dient zum Definieren einer maximalen Speicherdauer für Audit Trail-Einträge. Nach dieser festgelegten Speicherdauer werden die Einträge automatisch gelöscht.
Sprache
Wählen Sie die Sprache für die Audit Trail-Einträge aus.
Ausnahme: Alle Audit Trail-Einträge aus der Filterkategorie **Geräte (Kamera-Konfiguration)** werden in der konfigurierten Sprache des Configuration Client angezeigt.
Hinweis: Achten Sie darauf, die Audit Trail-Datenbank zu installieren, indem Sie sie in der BVMS-Einrichtung auswählen (optionale Konfigurationsfunktion).
Die Audit Trail-Einstellungen werden erst nach Aktivierung der Konfiguration aktiviert.

Karten

Art der Hintergrundkarte
Hier können Sie den Hintergrundkartentyp für die globale Karte auswählen. Die folgenden Kartentypen sind mit Internetzugriff verfügbar (Online-Modus):
- **HERE Straßenkarte**
- **HERE Straßenkarte dunkel**
- **HERE Satellitenkarte**

Wenn Sie keinen Internetzugriff haben (Offline-Modus), wählen Sie **Kein Eintrag** aus.

Hinweis!
Wenn Sie den Typ der Hintergrundkarte von offline auf (**Kein Eintrag**) zu online (**HERE** Maps), überprüfen Sie, ob die Position der Submaps und der Kamera-Hotspots noch korrekt ist.

Map-based tracking assistant

Systemfunktion aktivieren
Hier können Sie konfigurieren, dass ein Benutzer des Operator Client den Map-based tracking assistant verwenden kann.

Erweiterte Statusanzeige

Hotspot-Färbung auf Karten deaktivieren
Dient zum Deaktivieren der blinkenden Hotspots in Karten.

Erweiterte Statusanzeige aktiviert (Hot-Spot-Färbung in Karten in abhängig von Status)
Ermöglicht Ihnen, für alle Statusereignisse zu konfigurieren, dass die Hotspots der Geräte dieses Ereignisses mit einer Hintergrundfarbe und einem Blinken beim Auftreten des Ereignisses angezeigt werden.

Erweiterte Alarmanzeige aktivieren (Hot-Spot-Färbung in Karten in abhängig von Alarm)
Ermöglicht Ihnen, für alle Alarme zu konfigurieren, dass die Hotspots der Geräte dieses Alarms mit einer Hintergrundfarbe und einem Blinken beim Auftreten des Alarms angezeigt werden.
Die Konfiguration der erweiterten Statusanzeige kann nach dem Speichern der Konfiguration angezeigt werden. Die Hotspots werden nach der Aktivierung der Konfiguration im Operator Client auf einer Karte angezeigt.

Privacy overlay
Systemfunktion aktivieren
Hier können Sie konfigurieren, dass ein Benutzer des Operator Client ein Video mit Privacy overlay exportieren kann.

Identity provider
Identity provider
Wählen Sie Ihren Identitätsanbieter. Nach der Auswahl werden weitere Optionen angezeigt.
Tenant ID (für Identitätsanbiete **Microsoft**)
Geben Sie die Informationen abhängig von Ihrem externen Identity Provider ein.
Dieses Feld ist optional.
***Aussteller-URL** (für Identitätsanbieter **Amazon Federation**)
Geben Sie die Informationen abhängig von Ihrem externen Identity Provider ein.
***Anwendungs-ID**
Geben Sie die Informationen abhängig von Ihrem externen Identity Provider ein.
Anwendungsgeheimnis

Füllen Sie dieses Feld aus, wenn Sie eine vertraulichen Zeichenfolge verwenden möchten, um Ihre Verbindung beim externen Identity Provider zu identifizieren.
Dieses Feld ist optional.
Externe Adresse
Füllen Sie das Feld bei Bedarf mit einer externen Netzwerkadresse für eine geroutete Verbindung zu BVMS Management Server,wie z. B. eine SSH-Verbindung oder eine Internetverbindung.
Dieses Feld ist optional.
Klicken Sie auf **OK**, um die Änderungen zu speichern.

Metadaten-Verarbeitung
Objektvisualisierung auf der Karte
Aktivieren Sie das Kontrollkästchen, um die Objektverfolgungsfunktion allgemein zu aktivieren.

Wenn die Funktion aktiviert ist, wird auf der Seite **Kameras und Aufzeichnung** > die Spalte **Objektverfolgung** angezeigt, in der Sie die Objektverfolgung für die gewünschten Kameras aktivieren oder deaktivieren können.

Hinweis!
Objektverfolgung ist nur für Kameras mit CPP6 oder höher verfügbar, die dem logischen Baum und der globalen Karte hinzugefügt werden.

Siehe
– *Seite Kameras, Seite 290*

13 Seite Geräte

Hauptfenster > **Geräte**

Hinweis!
BVMS Viewer unterstützt keine Decodergeräte.

Zeigt den Gerätebaum und die Konfigurationsseiten an.
Die Anzahl der einem Eintrag untergeordneten Elemente wird in eckigen Klammern angezeigt.
Ermöglicht Ihnen die Konfiguration der verfügbaren Geräte, wie z. B. ONVIF Drehgeber, Bosch Video Streaming Gateway Geräte, Kodierer, Dekodierer, VRMs,lokale Speicher-Encoder, analoge Matrizen oder Peripheriegeräte wie ATM/POS Bridge.
Hinweis:
Die Geräte werden in einem Baum dargestellt und nach physischer Netzwerkstruktur und Gerätekategorien gruppiert.
Videoquellen wie Encoder werden unter VRMs gruppiert.

Um nach Elementen zu suchen:

- Tippen Sie im Suchfeld eine Zeichenfolge ein und drücken Sie auf den Schlüssel ENTER, um die angezeigten Elemente zu filtern.
  Nur Elemente mit der Zeichenfolge und ihre übergeordneten Elemente (nur in Bäumen) werden angezeigt. Die Anzahl der gefilterten Elemente und die gesamte Anzahl der Elemente wird angegeben.

Hinweis: Setzen Sie Zeichenfolgen zwischen doppelte Anführungszeichen, um genaue Treffer zu erhalten. Beispielsweise filtert "Camera 1" genau die Kameras mit diesem Namen, jedoch nicht camera 201.

- Klicken Sie auf ein Baumelement, um die entsprechende Seite anzuzeigen.

13.1 Aktualisieren von Gerätestatus und -funktionen

Hauptfenster > **Geräte**
Nach einem Firmware-Update kann es beispielsweise notwendig sein, die Funktionen aller konfigurierten Decoder, Encoder und VSGs zu synchronisieren. Mit dieser Funktion werden die Funktionen jedes Geräts mit den bereits in BVMS gespeicherten Funktionen verglichen. Sie können die Gerätefunktionen aller Geräte gleichzeitig im Gerätebaum aktualisieren.
Es ist auch möglich, eine Liste der Geräte in die Zwischenablage zu kopieren, deren Funktionen geändert wurden. Anschließend können Sie die Liste z. B. in einen Texteditor einfügen, um die Änderungen im Detail zu untersuchen.
Die Geräteliste aus der Zwischenablage ist als CSV formatiert und enthält die folgenden Informationen:

- Gerät
- Gerätetyp
- IP-Adresse

Hinweis: Wenn Sie ein großes System mit über 1.000 Geräten konfiguriert haben, kann das Aktualisieren von Gerätestatus und -funktionen sehr lange dauern.

Hinweis!
Die Funktionen werden nur für erreichbare Geräte abgerufen. Anhand des Gerätestatus können Sie die Erreichbarkeit eines Geräts prüfen.

So aktualisieren Sie die Gerätestatus und -funktionen:

1. Klicken Sie auf .
   Das Dialogfeld **Gerätefähigkeiten aktualisieren** wird angezeigt. Die Statusinformationen aller Geräte werden aktualisiert und die Gerätefunktionen werden abgerufen.
   Nur wenn die Gerätefunktionen nicht auf dem neuesten Stand sind, werden die entsprechenden Geräte in einer Liste angezeigt und die Schaltfläche **Aktualisieren** wird aktiviert.
2. Klicken Sie gegebenenfalls auf **Geräteliste in die Zwischenablage kopieren.**.
3. Klicken Sie auf **Aktualisieren**.
4. Klicken Sie auf **OK**.

⇨ Die Gerätefunktionen sind nun aktualisiert.

Hinweis!
Die Statusinformationen aller Geräte werden immer aktualisiert, auch wenn Sie den Dialog **Gerätefunktionen aktualisieren** abbrechen.

13.2 Ändern des Passworts für IP-Geräte

Hauptfenster > **Geräte** > **Gerätepasswörter ändern** > **Gerätepasswörter ändern** Dialogfeld
oder
Hauptfenster > Menü **Hardware** > Befehl **Gerätepasswörter ändern...** > Dialogfeld **Gerätepasswörter ändern**

So ändern Sie das Passwort für IP-Geräte:

1. Wählen Sie das erforderliche Gerät aus.
2. Klicken Sie mit der rechten Maustaste auf das ausgewählte Gerät und klicken Sie dann auf **Passwort bearbeiten...**.
   Das Dialogfeld **Gerätepasswörter ändern** wird angezeigt.
3. Wählen Sie den entsprechenden Passworttyp aus.
4. Geben Sie das neue Passwort ein.
5. Klicken Sie auf **OK**.
   Das neue Passwort wird im ausgewählten Gerät aktualisiert.

Weitere Informationen finden Sie unter *Dialogfeld „Gerätepasswörter ändern“ (Menü „Hardware“), Seite 106*.

So ändern Sie die Einstellungen für mehrere Geräte:
Siehe *Konfigurieren mehrerer Encoder/Decoder, Seite 232*.

Siehe

– *Dialogfeld „Gerätepasswörter ändern“ (Menü „Hardware“), Seite 106*

13.3 Hinzufügen eines Geräts

Hauptfenster > **Geräte**
Sie fügen die folgenden Geräte manuell zum Gerätebaum hinzu, weswegen Sie die Netzwerkadresse des Geräts kennen müssen, um es hinzuzufügen:

– Video-IP-Gerät von Bosch
– Analoge Kreuzschiene
  Zum Hinzufügen eines Bosch Allegiant-Geräts benötigen Sie eine gültige Allegiant-Konfigurationsdatei.

- BVMS Arbeitsstation
  Auf der Arbeitsstation muss die Operator Client-Software installiert sein.
- Übertragungsgerät
- Bosch ATM/POS Bridge, DTP-Gerät
- Virtueller Eingang
- Netzwerküberwachungsgerät
- Bosch IntuiKey Keyboard
- KBD-Universal XF Keyboard
- Monitorgruppe
- I/O-Modul
- Allegiant CCL-Emulation
- Einbruchmeldezentrale von Bosch
- Server-basiertes Analysegerät
- Zutrittskontrollsysteme von Bosch

Sie können nach den folgenden Geräten suchen, um diese über das Dialogfeld **BVMS Scan Wizard** hinzuzufügen:

- VRM-Geräte
- Encoder
- Nur-Live-Encoder
- Nur-Live-Encoder von ONVIF
- Encoder mit lokaler Archivierung
- Decoder
- Video Streaming Gateway-(VSG-)Geräte
- DVR-Geräte

Hinweis!

Wenn Sie ein Gerät hinzugefügt haben, klicken Sie auf , um die Einstellungen zu speichern.

Hinweis!
Fügen Sie über das Administrator-Konto des Geräts einen DVR hinzu. Die Verwendung eines DVR-Benutzerkontos mit eingeschränkten Berechtigungen kann dazu führen, dass manche Funktionen in BVMS nicht verwendbar sind, z. B. die Steuerung einer PTZ-Kamera.

Dialogfeld BVMS Scan Wizard

Hauptfenster > **Geräte** > Erweitern > Rechtsklick > Klicken Sie auf **Nach Encodern scannen** > **BVMS Scan Wizard** Dialogfeld

Hauptfenster > **Geräte** > Erweitern > Rechtsklick > Klicken Sie auf **Nach Video Streaming Gateways scannen** > **BVMS Scan Wizard** Dialogfeld

Hauptfenster > **Geräte** > Rechtsklick > Klicken Sie auf **Nach Nur Live-Encodern scannen**> **BVMS Scan Wizard** Dialogfeld

Hauptfenster > **Geräte** > Rechtsklick > Klicken Sie auf **Nach Encodern mit lokaler Archivierung scannen** > **BVMS Scan Wizard** Dialogfeld

Hauptfenster > **Geräte** > Erweitern > Erweitern > Rechtsklick > Klicken Sie auf **Nach Decodern scannen** > **BVMS Scan Wizard** Dialogfeld

Das Dialogfeld ermöglicht es Ihnen, in nur einem Vorgang nach verfügbaren Geräten im Netzwerk zu suchen, diese zu konfigurieren und dem System hinzuzufügen.

Benutzung

Klicken Sie, um ein Gerät zum Hinzufügen zum System auszuwählen.

Typ (nicht für VSG-Geräte verfügbar)

Zeigt den Gerätetyp an.

Display-Name

Zeigt den Gerätenamen an, der in den Gerätebaum eingegeben wurde.

Netzwerkadresse

Zeigt die IP-Adresse des Geräts an.

Benutzername

Zeigt den Benutzernamen an, der auf dem Gerät konfiguriert wurde.

Passwort

Geben Sie das Passwort zur Authentifizierung mit diesem Gerät ein.

Status

Zeigt den Status der Authentifizierung.

: Erfolgreich

: Fehlgeschlagen

Hauptfenster > **Geräte** > Rechtsklick > Klicken Sie auf **Nach VRM-Geräten scannen**> BVMS Scan Wizard Dialogfeld

Hinweis!

Zur Konfiguration eines Sekundären VRM muss auf dem Computer zunächst die entsprechende Software installiert werden. Führen Sie die Datei Setup.exe aus und wählen Sie **Sekundärer VRM**.

Rolle

Wählen Sie in der Liste den gewünschten Eintrag aus.

In der folgenden Tabelle wird aufgeführt, welche Rollen jeder VRM-Typ besitzen kann:

Rolle/Typ	Primärer VRM	Sekundärer VRM
Primärer (Normal)	X	
Sekundärer (Normal)		X
Primärer Failover	X	
Sekundärer Failover		X
Gespiegelt		X

Sie können einem Primären VRM ein VRM-Gerät mit folgenden Rollen hinzufügen:
– Failover-VRM
– Gespiegelte VRM
Sie können VRM-Geräte mit folgenden Rollen zu einem Sekundären VRM hinzufügen:
– Failover-VRM

Master-VRM
Wählen Sie in der Liste den gewünschten Eintrag aus.

Benutzername
Zeigt den Benutzernamen an, der auf dem VRM-Gerät konfiguriert wurde.
Sie können bei Bedarf einen anderen Benutzernamen eingeben.

Siehe
– *Hinzufügen eines VRM-Geräts per Suchvorgang, Seite 170*
– *Hinzufügen eines Encoders zu einem VRM-Pool, Seite 220*
– *Hinzufügen eines Nur-Live-Encoders, Seite 220*
– *Hinzufügen eines Encoders mit lokaler Archivierung, Seite 220*
– *Nach Geräten suchen, Seite 73*

13.4 Seite „Server-Liste/Adressbuch“

Hauptfenster > **Geräte** > **Enterprise System** > **Serverliste / Adressbuch**
Sie können mehrere Management-Server-Computer für den simultanen Zugriff in einem BVMS Enterprise System hinzufügen. Sie können auch mehrere Management Server-Computer für den sequenziellen Zugriff auf Server Lookup hinzufügen.
Sie können in der Server-Liste zusätzliche Spalten hinzufügen. Dies ermöglicht das Hinzufügen weiterer Informationen, nach denen der Benutzer bei Verwendung von Server Lookup suchen kann. Die hinzugefügten Spalten sind ebenfalls auf der Seite **Serverzugriff** sichtbar (Hauptfenster > **Benutzergruppen** > Registerkarte **Enterprise User Groups** > > Registerkarte **Serverzugriff**).

Server hinzufügen
Klicken Sie hier, um das Dialogfeld **Server hinzufügen** anzuzeigen.

Server entfernen
Klicken Sie hier, um die Management Server Einträge zu entfernen.

Management Server
Zeigt die Namen aller hinzugefügten Management Server-Computer an. Sie können jeden Eintrag ändern.

Hinweis: Wenn Sie eine SSH-Verbindung verwenden, geben Sie die Adresse im folgenden Format ein:
ssh://IP oder Servername:5322

Private Netzwerkadresse
Zeigt die privaten Netzwerkadressen aller hinzugefügten Management Server-Computer an. Sie können jeden Eintrag ändern.

Server-Nummer
Zeigt die logischen Nummern aller hinzugefügten Management Server-Computer an. Sie können jeden Eintrag ändern.

Server-Beschreibung
Geben Sie eine Beschreibung für diesen Management Server ein. Sie benötigen diese Beschreibung, um die Liste aller verfügbaren Server zu finden, wenn Sie exklusiv auf den Management Server zugreifen möchten, beispielsweise um einem Alarm aus einem anderen Management-System nachzugehen.

Klicken Sie hier, um detaillierte Anweisungen zu erhalten:
- *Konfigurieren der Serverliste für Enterprise System, Seite 85*
- *Konfigurieren von Server Lookup, Seite 130*
- *Export der Server-Liste, Seite 131*
- *Import einer Server-Liste, Seite 131*

Siehe
- *SSH-Tunneling, Seite 50*

13.4.1 Dialogfeld „Server hinzufügen“

Hauptfenster > **Geräte** > **Enterprise System** > **Serverliste / Adressbuch**

Server-Name
Geben Sie den Anzeigenamen des Management-Servers ein.

Hinweis: Wenn Sie eine SSH-Verbindung verwenden, geben Sie die Adresse im folgenden Format ein:
ssh://IP oder Servername:5322

Private Netzwerkadresse
Geben Sie die private IP-Adresse oder den DNS-Namen des Management Server ein.

Öffentliche Netzwerkadresse
Geben Sie die Adresse des öffentlichen Netzwerks ein.

Server-Beschreibung
Geben Sie eine Beschreibung für den Management Server ein.

13.4.2 Konfigurieren von Server Lookup

Für den Server Lookup meldet sich der Benutzer eines Operator Client oder Configuration Client mit einem Benutzernamen einer normalen Benutzergruppe an, nicht als Benutzer einer Enterprise User Group.

Siehe
- *Server Lookup, Seite 26*
- *Seite „Server-Liste/Adressbuch“, Seite 129*
- *Mittels Server Lookup, Seite 73*

13.4.3 Konfigurieren der Server-Liste

Hauptfenster > **Geräte** > **Enterprise System** > **Serverliste / Adressbuch**

So fügen Sie Server hinzu:
1. Klicken Sie auf **Server hinzufügen**.
   Das Dialogfeld **Server hinzufügen** wird angezeigt.

2. Geben Sie einen Anzeigenamen für den Server und die private Netzwerkadresse (DNS-Name oder IP-Adresse) ein.
   Hinweis: Wenn Sie eine SSH-Verbindung verwenden, geben Sie die Adresse im folgenden Format ein:
   ssh://IP-Adresse oder Servername:5322
3. Klicken Sie auf **OK**.
4. Wiederholen Sie diese Schritte, bis alle gewünschten Management Server-Computer hinzugefügt wurden.

So fügen Sie Spalten hinzu:

- Klicken Sie mit der rechten Maustaste auf die Tabellenüberschrift und klicken Sie auf **Spalte hinzufügen**.
  Sie können bis zu 10 Spalten hinzufügen.
  Um eine Spalte zu löschen, klicken Sie mit der rechten Maustaste auf die gewünschte Spalte, und klicken Sie auf **Spalte entfernen**.

⇨ Wenn Sie die Server-Liste exportieren, werden die hinzugefügten Spalten auch exportiert.

Siehe

– *Konfigurieren der Serverliste für Enterprise System, Seite 85*

13.4.4 Export der Server-Liste

Hauptfenster > **Geräte** > **Enterprise System** > **Serverliste / Adressbuch**

Sie können die Server-Liste mit allen konfigurierten Eigenschaften für die Bearbeitung und einen späteren Import exportieren.

Für den Fall, dass Sie die exportierte CSV-Datei in einem externen Editor bearbeiten, beachten Sie die im Kapitel Server-Liste beschriebenen Beschränkungen.

So führen Sie einen Export durch:

1. Klicken Sie mit der rechten Maustaste auf die Tabellenüberschrift und klicken Sie auf **Serverliste exportieren...**
2. Geben Sie einen Namen für die Exportdatei ein, und klicken Sie auf **Speichern**.

⇨ Alle Spalten der Server-Liste werden als CSV-Datei exportiert.

Verwandte Themen

– *Server Lookup, Seite 26*
– Server-Liste
– *Seite „Server-Liste/Adressbuch“, Seite 129*

13.4.5 Import einer Server-Liste

Hauptfenster > **Geräte** > **Enterprise System** > **Serverliste / Adressbuch**

Für den Fall, dass Sie die exportierte CSV-Datei in einem externen Editor bearbeitet haben, beachten Sie die im Kapitel Server-Liste beschriebenen Beschränkungen.

So importieren Sie:

1. Klicken Sie mit der rechten Maustaste auf die Tabellenüberschrift und klicken Sie auf **Serverliste importieren...**.
2. Klicken Sie auf die gewünschte Datei, und klicken Sie auf **Öffnen**.

Verwandte Themen

– *Server Lookup, Seite 26*
– Server-Liste
– *Seite „Server-Liste/Adressbuch“, Seite 129*

13.5 Seite DVR (Digital-Videorekorder)

Hauptfenster > **Geräte** > >

Zeigt die Eigenschaftsseiten eines ausgewählten DVR an.

Dient zum Integrieren eines DVR in das System.

- Klicken Sie auf eine Registerkarte, um die entsprechende Eigenschaftsseite anzuzeigen.

Hinweis!
Sie konfigurieren nicht den DVR selbst, sondern nur die Integration des DVR-Geräts in BVMS.

Hinweis!
Fügen Sie über das Administrator-Konto des Geräts einen DVR hinzu. Die Verwendung eines DVR-Benutzerkontos mit eingeschränkten Berechtigungen kann dazu führen, dass manche Funktionen in BVMS nicht verwendbar sind, z. B. die Steuerung einer PTZ-Kamera.

Siehe

- *DVR-Geräte, Seite 132*
- *Konfigurieren der Integration eines DVR, Seite 134*

13.5.1 DVR-Geräte

Dieses Kapitel enthält Hintergrundinformationen über die DVR-Geräte, die in BVMS integriert werden können.

Einige DVR-Modelle unterstützen die Aufzeichnung von Encodern/IP-Kameras. Andere DVR-Modelle unterstützen nur analoge Kameras.

Ein Encoder/eine IP-Kamera darf nicht in der Konfiguration von zwei Video-Systemen (DVR oder Video-Management-Systeme) integriert werden.

Wenn Encoder/IP-Kameras mit einem DVR verbunden werden, der bereits in BVMS integriert ist, werden diese Encoder/IP-Kameras beim BVMS Netzwerkgeräte-Scan nicht erkannt. Dies gilt für den Netzwerkscan innerhalb des Configuration Client und innerhalb des Config Wizard.

Wenn ein DVR mit angeschlossenen Encoder/IP-Kameras in BVMS integriert wird und diese Encoder/IP-Kameras BVMS bereits hinzugefügt wurden, wird eine Warnung angezeigt. Entfernen Sie diese Encoder/IP-Kameras vom DVR oder aus BVMS.

Der Config Wizard fügt der Konfiguration keine Geräte mit widersprüchlichen IP-Kameras hinzu.

DVR-Geräte unterstützen eine begrenzte Anzahl von gleichzeitigen Verbindungen. Diese Nummer definiert die maximale Anzahl der Operator Client Benutzer, die gleichzeitig Videos von diesem DVR anzeigen können, ohne dass schwarze Bildfenster angezeigt werden.

Hinweis!
Fügen Sie über das Administrator-Konto des Geräts einen DVR hinzu. Die Verwendung eines DVR-Benutzerkontos mit eingeschränkten Berechtigungen kann dazu führen, dass manche Funktionen in BVMS nicht verwendbar sind, z. B. die Steuerung einer PTZ-Kamera.

Hinweis!
DIVAR AN 3000/5000: Beachten Sie beim Löschen von Videodaten vom DVR, dass Sie mindestens die volle Stunde an Videodaten löschen. Wenn Sie beispielsweise einen Zeitbereich zwischen 6:50 Uhr und 7:05 Uhr wählen, löschen Sie tatsächlich die Videodaten zwischen 6:00 Uhr und 8:00 Uhr.

Bosch 700 Serie Hybrid- und HD-Netzwerkrekorder: Der Löschvorgang beginnt stets mit dem Anfang der Aufzeichnungen aller Kameras, die im Operator Client angezeigt werden, und endet mit dem eingegebenen Zeitpunkt.

Siehe
- *Seite DVR (Digital-Videorekorder), Seite 132*
- *Konfigurieren der Integration eines DVR, Seite 134*

13.5.2 Hinzufügen eines DVR-Geräts per Suchvorgang

So fügen Sie DVR-Geräte über den Suchvorgang hinzu:

1. Klicken Sie mit der rechten Maustaste auf und klicken Sie auf **DVRs scannen**.
   Das Dialogfeld **BVMS Scan Wizard** wird angezeigt.
2. Aktivieren Sie die Kontrollkästchen der Geräte, die hinzugefügt werden sollen.
3. Klicken Sie auf **Weiter >>**.
   Das Dialogfeld des Assistenten für die **Authentifizierung der Geräte** wird angezeigt.
4. Geben Sie das Passwort für jedes Gerät ein, das von einem Passwort geschützt ist.
   Passwortüberprüfungen erfolgen automatisch, wenn Sie während ein paar Sekunden keine weiteren Zeichen im Passwortfeld eingeben oder außerhalb des Passwortfelds klicken.
   Wenn die Passwörter aller Geräte identisch sind, können Sie es im ersten Feld **Passwort** eingeben. Klicken Sie mit der rechten Maustaste auf das Feld und klicken Sie auf **Zellinhalt in Spalte kopieren**.

   In der Spalte **Status** wird die erfolgreiche Anmeldung mit angezeigt.

   Fehlgeschlagene Anmeldungen werden mithilfe von angezeigt.
5. Klicken Sie auf **Fertig stellen**.
   Das Gerät wird zum Gerätebaum hinzugefügt.

13.5.3 Dialogfeld „Add DVR“ (DVR hinzufügen)

Hauptfenster > **Geräte** > erweitern > > **DVR hinzufügen**
Ermöglicht das manuelle Hinzufügen eines DVR-Geräts.

Netzwerkadresse / Port
Geben Sie die IP-Adresse Ihres DVR ein. Ändern Sie bei Bedarf die Port-Nummer.

Benutzername:
Geben Sie den Benutzernamen für die Verbindung zum DVR an.

Passwort:
Geben Sie das Passwort für die Verbindung zum DVR an.

Sicherheit
Das Kontrollkästchen **Sichere Verbindung** ist standardmäßig aktiviert.
Wenn keine sichere Verbindung möglich ist, erscheint eine Meldung. Klicken Sie darauf, um das Häkchen zu entfernen.

Hinweis!
Wenn das Kontrollkästchen **Sichere Verbindung** aktiviert ist, sind Befehl und Steuerungsverbindungen gesichert. Das Streaming von Videodaten ist nicht gesichert.

Siehe
– *Hinzufügen eines Geräts, Seite 126*

13.5.4 Registerkarte „Einstellungen“

Hauptfenster > **Geräte** > > > Registerkarte **Einstellungen**
Zeigt die Netzwerkeinstellungen des an Ihr System angeschlossenen DVR an. Dient zum Ändern der Einstellungen.

13.5.5 Registerkarte „Kameras“

Hauptfenster > **Geräte** > > > Registerkarte **Kameras**
Zeigt alle Videokanäle des DVR als Kameras. Dient zum Entfernen von Kameras.
Ein in einem DVR-Gerät deaktivierter Videoeingang wird im BVMS als aktive Kamera angezeigt, da für diesen Eingang frühere Aufnahmen existieren können.

13.5.6 Registerkarte „Eingänge“

Hauptfenster > **Geräte** > > > Registerkarte **Eingänge**
Zeigt alle Eingänge des DVR an.
Dient zum Entfernen von Elementen.

13.5.7 Registerkarte „Relais“

Hauptfenster > **Geräte** > > > Registerkarte **Relais**
Zeigt alle Relais des DVR an. Dient zum Entfernen von Elementen.

13.5.8 Konfigurieren der Integration eines DVR

Hauptfenster > **Geräte** > erweitern >

Hinweis!
Fügen Sie über das Administrator-Konto des Geräts einen DVR hinzu. Die Verwendung eines DVR-Benutzerkontos mit eingeschränkten Berechtigungen kann dazu führen, dass manche Funktionen in BVMS nicht verwendbar sind, z. B. die Steuerung einer PTZ-Kamera.

Hinweis!
Sie konfigurieren nicht den DVR selbst, sondern nur die Integration des DVR-Geräts in BVMS.

So entfernen Sie ein Element:
1. Klicken Sie auf die Registerkarte **Einstellungen**, die Registerkarte **Kameras**, die Registerkarte **Eingänge** oder die Registerkarte **Relais**.

2. Klicken Sie mit der rechten Maustaste auf ein Element und klicken Sie auf **Entfernen**. Das Element wird entfernt.

Hinweis!
Zur Wiederherstellung eines entfernten Elements klicken Sie mit der rechten Maustaste auf das DVR-Gerät und klicken dann auf **DVRs erneut scannen**.

So benennen Sie ein DVR-Gerät um:
1. Klicken Sie mit der rechten Maustaste auf ein DVR-Gerät und klicken Sie auf **Umbenennen**.
2. Geben Sie einen neuen Namen für das Element ein.

Siehe
- *Hinzufügen eines Geräts, Seite 126*
- *Seite DVR (Digital-Videorekorder), Seite 132*

13.6 Seite Kreuzschienen

Hauptfenster > **Geräte** > >
Zeigt die Eigenschaftsseiten des Bosch Allegiant Geräts an.
Das Bosch Allegiant Gerät selbst wird nicht konfiguriert. Es werden lediglich die Eigenschaften bezogen auf das BVMS festgelegt. Informationen zum Verbinden von Allegiant-Geräten mit BVMS finden Sie im Kapitel **Konzepte** dieser Online-Hilfe. Dieses Kapitel enthält Hintergrundinformationen zu ausgewählten Themen.
Sie können außerdem Steuerungsprioritäten für Allegiant Trunklines konfigurieren.
- Klicken Sie auf eine Registerkarte, um die entsprechende Eigenschaftsseite anzuzeigen.

Siehe
- *Konfigurieren eines Bosch Allegiant Geräts, Seite 135*
- *Verbinden einer Bosch Allegiant Kreuzschiene mit BVMS, Seite 57*

13.6.1 Hinzufügen eines Bosch Allegiant Geräts

So fügen Sie ein Bosch Allegiant Gerät hinzu:

1. Klicken Sie mit der rechten Maustaste auf , und klicken Sie auf **Allegiant hinzufügen**. Das Dialogfeld **Öffnen** wird angezeigt.
2. Wählen Sie die entsprechende Allegiant Konfigurationsdatei aus, und klicken Sie auf **OK**. Das Bosch Allegiant Gerät wird zum System hinzugefügt.

Hinweis: Sie können nur eine Bosch Allegiant Kreuzschiene hinzufügen.

13.6.2 Konfigurieren eines Bosch Allegiant Geräts

Hauptfenster > **Geräte** > erweitern >
Das Bosch Allegiant Gerät selbst wird nicht konfiguriert. Es werden lediglich die Eigenschaften bezogen auf das BVMS festgelegt.
So ordnen Sie einem Encoder einen Ausgang zu:
1. Klicken Sie auf die Registerkarte **Ausgänge**.
2. Klicken Sie in der Spalte **Benutzung** in den gewünschten Zellen auf **Trunkline**.
3. Wählen Sie in der Spalte **Encoder** den gewünschten Encoder aus.

So fügen Sie einem Bosch Allegiant Gerät einen Eingang hinzu:

1. Klicken Sie auf die Registerkarte **Eingänge**.
2. Klicken Sie auf **Eingänge hinzufügen**. In die Tabelle wird eine neue Zeile eingefügt.
3. Geben Sie die erforderlichen Einstellungen in die Zellen ein.

So löschen Sie einen Eingang:

1. Klicken Sie auf die Registerkarte **Eingänge**.
2. Klicken Sie auf die erforderliche Tabellenzeile.
3. Klicken Sie auf **Eingang löschen**. Die Zeile wird aus der Tabelle gelöscht.

Siehe

- *Verbinden eines Bosch IntuiKey Keyboards mit BVMS, Seite 53*
- *Seite Verbindung, Seite 137*
- *Seite Kameras, Seite 137*
- *Seite Ausgänge, Seite 136*
- *Seite Eingänge, Seite 137*

13.6.3 Seite Ausgänge

Hauptfenster > **Geräte** > erweitern > > Registerkarte **Ausgänge**

Dient zum Konfigurieren der Verwendung eines Bosch Allegiant Geräteausgangs sowie zum Zuordnen eines Encoders zu einem Ausgang.

Um die Videodaten eines Bosch Allegiant Geräteausgangs im BVMS speichern zu können, müssen Sie dem Ausgang einen Encoder zuordnen. Dieser Encoder muss an den Ausgang angeschlossen sein.

Nr.

Zeigt die Nummer des Ausgangs an.

Allegiant Logische Nr.

Zeigt die logische Nummer des Ausgangs im Allegiant System an.

BVMS Logische Nr.

Dient zum Ändern der logischen Nummer des Ausgangs im BVMS. Wenn Sie eine bereits vergebene Nummer eingeben, wird eine Meldung angezeigt.

Name

Zeigt den Namen des Ausgangs an.

Benutzung

Dient zum Ändern der Verwendung des Ausgangs.

Wenn Sie **Trunkline** auswählen, können Sie diesem Ausgang im Feld **Encoder** einen Encoder zuordnen. Der Allegiant Ausgang wird kompatibel mit dem Netzwerk.

Wenn Sie **Allegiant-Monitor** auswählen, kann der Benutzer im Operator Client das Kamerasignal einem Monitor zuordnen. Die PTZ-Kamerasteuerung ist möglich, wenn die Kamera als PTZ-Kamera konfiguriert ist. In Operator Client kann der Benutzer diese Kamera nicht in ein Bildfenster ziehen.

Wenn Sie **Inaktiv** auswählen, kann der Benutzer einer Allegiant Kamera keinen Monitor zuordnen.

Encoder

Dient zum Zuordnen eines Ausgangs zu einem Encoder. Sie können einen Encoder nur auswählen, wenn Sie **Trunkline** aktiviert haben. Der Encoder ist für den Logischen Baum gesperrt. Wenn Sie einen Encoder zuordnen, der sich bereits im Logischen Baum befindet, wird er aus dem Logischen Baum entfernt. Im Operator Client kann der Benutzer die Kamera in ein Bildfenster ziehen.

Siehe

- *Konfigurieren eines Bosch Allegiant Geräts, Seite 135*

13.6.4 Seite Eingänge

Hauptfenster > **Geräte** > erweitern > > Registerkarte **Eingänge**
Dient zum Hinzufügen von Eingängen zu einem Bosch Allegiant Gerät.

Eingang hinzufügen
Klicken Sie darauf, um zur Angabe eines neuen Eingangs eine neue Zeile in die Tabelle einzufügen.

Eingang löschen
Klicken Sie darauf, um eine Zeile aus der Tabelle zu löschen.

Eingang-Nr.
Geben Sie die erforderliche Nummer des Eingangs ein. Wenn Sie eine bereits vergebene Nummer eingeben, wird eine Meldung angezeigt.

Eingangsname
Geben Sie den erforderliche Namen des Eingangs ein.

Siehe
– *Konfigurieren eines Bosch Allegiant Geräts, Seite 135*

13.6.5 Seite Verbindung

Hauptfenster > **Geräte** > erweitern > > Registerkarte **Verbindung**
Zeigt den Namen der Bosch Allegiant Konfigurationsdatei an.
Das BVMS kann eine Konfigurationsdatei mit den Namen und Konfigurationsinformationen aller an das Bosch Allegiant Gerät angeschlossenen Kameras in strukturiertem Speicherformat auslesen.

Konfiguration aktualisieren
Klicken Sie darauf, um eine aktualisierte Bosch Allegiant Konfigurationsdatei auszuwählen.

Siehe
– *Konfigurieren eines Bosch Allegiant Geräts, Seite 135*

13.6.6 Seite Kameras

Hauptfenster > **Geräte** > erweitern > > Registerkarte **Kameras**
Zeigt eine Tabelle mit den Kameras an, die an das Bosch Allegiant Gerät angeschlossen sind.

Nr.
Zeigt die fortlaufende Nummer der Kamera an.

Allegiant Logische Nr.
Zeigt die logische Nummer der Kamera an.

Kameraname
Zeigt den Namen der Kamera an.

Siehe
– *Konfigurieren eines Bosch Allegiant Geräts, Seite 135*

13.7 Seite Arbeitsstation

Hauptfenster > **Geräte** > erweitern >
Auf der Arbeitsstation muss die Operator Client-Software installiert sein.

Dient zum Konfigurieren der folgenden Einstellungen für eine Arbeitsstation:

- Anschließen eines CCTV-Keyboards, das an eine Bosch Video Management System-Arbeitsstation angeschlossen ist
- Zuweisen eines Kommandoskripts, das beim Starten der Arbeitsstation ausgeführt wird
- Auswahl des Standard-Streams zur Live-Anzeige Sie können Streams für Dual-Stream-Kameras und für Multi-Stream-Kameras auswählen.

Hinweis: Sie können kein CCTV-Keyboard für eine Standard-Arbeitsstation konfigurieren. Dies ist nur für bestimmte konfigurierte Arbeitsstationen möglich.

Um ein Bosch IntuiKey Keyboard anzuschließen, das mit einem Decoder verbunden ist, erweitern Sie und klicken Sie dann auf .

Siehe

- *Manuelles Hinzufügen einer Arbeitsstation, Seite 138*
- *Konfigurieren eines Start-Kommandoskripts (Seite „Einstellungen“), Seite 139*

13.7.1 Manuelles Hinzufügen einer Arbeitsstation

So fügen Sie eine BVMS Arbeitsstation hinzu:

1. Klicken Sie mit der rechten Maustaste auf .
2. Klicken Sie auf **Arbeitsstation hinzufügen**.
   Das Dialogfeld **Arbeitsstation hinzufügen** wird angezeigt.
3. Geben Sie den erforderlichen Wert ein.
4. Klicken Sie auf **OK**.
   Die Arbeitsstation wird zu Ihrem System hinzugefügt.

So fügen Sie eine BVMS Standard-Arbeitsstation hinzu:

- Klicken Sie mit der rechten Maustaste auf .

Klicken Sie auf **Standard-Arbeitsstation hinzufügen**.

Die Arbeitsstation wird zu Ihrem System hinzugefügt.

Hinweis!
Sie können nur eine einzige Standard-Arbeitsstation hinzufügen.

Wenn eine Standard-Arbeitsstation konfiguriert ist, gelten ihre Einstellungen für jede Arbeitsstation, die mit diesem Server verbunden ist und nicht separat konfiguriert wurde.
Wenn eine Arbeitsstation konfiguriert wird, gelten die Einstellungen für diese spezifische Arbeitsstation und nicht die Einstellungen der Standard-Arbeitsstation.

13.7.2 Konfigurieren eines Bosch IntuiKey Keyboards (Seite „Einstellungen“) (Arbeitsstation)

Hauptfenster > **Geräte**> erweitern >

So konfigurieren Sie ein Bosch IntuiKey Keyboard, das an eine Arbeitsstation angeschlossen ist:

1. Klicken Sie auf die Registerkarte **Einstellungen**.

2. Nehmen Sie im Feld **Keyboard-Einstellungen** die erforderlichen Einstellungen vor.

Detaillierte Informationen zu den verschiedenen Feldern finden Sie in der Online-Hilfe unter dem entsprechenden Anwendungsfenster.

Siehe

– *Seite Arbeitsstation, Seite 137*

13.7.3 Konfigurieren eines Start-Kommandoskripts (Seite „Einstellungen“)

Hauptfenster > **Geräte** > erweitern > > Seite **Einstellungen**

Sie können ein Kommandoskript so konfigurieren, dass es beim Starten des Operator Client auf der ausgewählten Arbeitsstation gestartet wird.

Sie müssen ein entsprechendes Kommandoskript erzeugen.

Informationen zum Erzeugen von Kommandoskripten finden Sie im *Verwalten von Kommandoskripten, Seite 89*.

So konfigurieren Sie ein Start-Skript:

- Wählen Sie in der Liste **Start-Skript:** das Kommandoskript aus.

Siehe

– *Seite Arbeitsstation, Seite 137*

13.7.4 Seite Einstellungen

Hauptfenster > **Geräte** > Erweitern > > Registerkarte **Einstellungen**

Dient zum Konfigurieren eines Skripts, das beim Starten des Operator Client auf der Arbeitsstation ausgeführt wird.

Ermöglicht Ihnen, TCP oder UDP als Übertragungsprotokoll zu konfigurieren, das für alle Kameras verwendet wird, die auf Ihrer Arbeitsstation im Live-Modus angezeigt werden.

Dient zum Konfigurieren des Streams eines IP-Geräts für die Live-Anzeige.

Dient zum Aktivieren der Forensischen Suche für diese Arbeitsstation.

Sie können auch das Keyboard konfigurieren, das an diese Arbeitsstation angeschlossen ist.

Netzwerkadresse

Geben Sie den DNS-Namen oder die IP-Adresse der Arbeitsstation ein.

Start-Skript:

Wählen Sie das Skript aus, das beim Starten des Operator Client auf der Arbeitsstation gestartet werden soll. Das Skript wird auf der Seite **Ereignisse** erzeugt oder importiert.

Voreingestelltes Kameraprotokoll:

Wählen Sie das Standard-Übertragungsprotokoll für alle Kameras, die dem Logischen Baum dieser Arbeitsstation zugeteilt sind.

Einstellungen aus der Tabelle "Kameras und Aufzeichnung" überschreiben

Aktivieren Sie das Kontrollkästchen, um die Auswahl des gewünschten Streams für die Live-Anzeige zu aktivieren.

Hinweis: Für DVR-Geräte mit mehr als 1 Stream (z. B. DIVAR AN 3000/5000) wird die Live-Stream-Einstellung von diesem DVR auch hier geändert. Live-Stream-Einstellungen für DVR-Geräte sind auf der Seite **Kameras und Aufzeichnung** nicht verfügbar.

Live-Stream

Wählen Sie den gewünschten Stream für die Live-Ansicht. Sie können Streams für Dual-Stream-Kameras und für Multi-Stream-Kameras auswählen.

Bei der Auswahl von **Bildfenstergröße optimiert** wird die Auflösung der angezeigten Kamera automatisch auf die Größe des Bildfensters angepasst, abhängig von der Auflösung des verwendeten Monitors. Dies ist nützlich für die Anzeige mehrerer Kameras mit großer Auflösung, z. B. 4K ultra HD-Kameras. Nur bei Kameras mit Streams, deren Auflösung unabhängig voneinander konfiguriert werden kann, kann die Auflösung an das Bildfenster angepasst werden. Der Benutzer des Operator Client kann die Streamauswahl für jede Kamera individuell ändern.

Zweifachstream Kameras
Wählen Sie den Standard-Stream für die Live-Anzeige für Dual-Stream-Kameras.

Mehrfachstream Kameras
Wählen Sie den Standard-Stream für die Live-Anzeige bei Multistream-Kameras.

Stattdessen transkodierten Stream verwenden, wenn verfügbar
Aktivieren Sie das Kontrollkästchen, um die Verwendung eines transcodierten Streams, falls verfügbar, zu aktivieren. Dieser transcodierte Stream wird anstelle des gewählten Streams für die Live-Ansicht verwendet.
Für einen transkodierten Stream, der in BVMS, Ihr VRM Der Computer muss über einen eingebauten Hardware-Transcoder verfügen.
Wenn eine Kamera im Live Modus angezeigt wird, dann wird der Standard-Stream-Satz für die Arbeitsstation verwendet. Wenn die Kamera keinen Stream 2 besitzt oder der Transcoder-Dienst (Software und Hardware) nicht verfügbar ist, dann wird Stream 1 verwendet, auch wenn in den Einstellungen der Arbeitsstation eine andere Einstellung konfiguriert ist.

Direktes Playback aus dem Speicher verwenden
Aktivieren Sie dieses Kontrollkästchen, um den Video-Stream direkt vom Archivierungsgerät an diese Arbeitsstation zu senden. Der Stream wird dann nicht über VRM gesendet. Die Arbeitsstation muss dennoch mit dem VRM verbunden sein, um eine korrekte Wiedergabe zu gewährleisten.
Hinweis: Sie können die direkte Wiedergabe vom iSCSI-Speichergerät nur verwenden, wenn Sie das globale iSCSI-CHAP-Passwort festgelegt haben.

Live-Video von Video Streaming Gateway Stream 1 holen für Kameras mit Live-Video "Direkt von Kamera"
Zeigt die Liste der Video Streaming Gateway-Geräte an. Wählen Sie die gewünschten Einträge zum Aktivieren der Übertragung von Videodaten von der Videoquelle zu dieser Arbeitsstation über Segmente mit geringer Bandbreite.
Hinweis: Wenn Sie ein Video Streaming Gateway Gerät für den Abruf von Live-Video auswählen, wird das **Live Video** – **Profil** auf der **Kameras und Aufzeichnung** Seite überflüssig. Stattdessen wird die **Aufzeichnung** – **Profil** Einstellung auch für Live-Video verwendet.

Keyboard-Typ
Wählen Sie den Typ des Keyboards aus, das an die Arbeitsstation angeschlossen ist.

Port:
Wählen Sie den COM-Port aus, an den das Keyboard angeschlossen wird.

Baudrate:
Wählen Sie die maximale Rate (in Bits pro Sekunde) aus, mit der Daten über diesen Port übertragen werden sollen. In der Regel wird die maximale Rate eingestellt, die vom Computer oder Gegengerät unterstützt wird.

Datenbits:
Zeigt die Anzahl der Datenbits an, die für die einzelnen übertragenen und empfangenen Zeichen verwendet werden sollen.

Stoppbits:
Zeigt die Zeit zwischen den einzelnen übertragenen Zeichen an (gemessen in Bits).

Parität:
Zeigt die Art der Fehlerprüfung an, die für den ausgewählten Port verwendet werden soll.

Port-Typ:
Zeigt den Verbindungstyp für den Anschluss des Bosch IntuiKey Keyboards an die Arbeitsstation an.

Siehe
– *Konfigurieren eines Start-Kommandoskripts (Seite „Einstellungen“), Seite 139*

13.7.5 Ändern der Netzwerkadresse einer Arbeitsstation

Hauptfenster > **Geräte** > erweitern
So ändern Sie die IP-Adresse:

1. Klicken Sie mit der rechten Maustaste auf , und klicken Sie auf **Netzwerkadresse ändern**. Das Dialogfeld **Netzwerkadresse ändern** wird angezeigt.
2. Ändern Sie den Eintrag im Feld nach Ihren Anforderungen.

13.8 Seite "Decoder"

Hauptfenster > **Geräte** > Erweitern >
Dient zum Hinzufügen und Konfigurieren von Decodern.

Hinweis!
BVMS Viewer unterstützt keine Decodergeräte.

Hinweis!
Wenn Sie für das System Decoder verwenden möchten, achten Sie darauf, dass für alle Encoder das gleiche Passwort für die user-Berechtigungsstufe verwendet wird.

Siehe
– *Nach Geräten suchen, Seite 73*
– *Seite „Bosch Encoder/Decoder/Kamera“, Seite 217*

13.8.1 Manuelles Hinzufügen eines Encoders

Hauptfenster > **Geräte** > Erweitern > Erweitern > Rechtsklicken > Klicken **Encoder hinzufügen** > **Encoder hinzufügen** Dialogfeld
oder

Hauptfenster > **Geräte** > Rechtsklicken > Klicken **Encoder hinzufügen** > **Encoder hinzufügen** Dialogfeld
oder

Hauptfenster > **Geräte** > Rechtsklicken > Klicken **Encoder hinzufügen** > **Encoder hinzufügen** Dialogfeld
oder

Hauptfenster > **Geräte** > Erweitern > Rechtsklicken > Klicken **Decoder hinzufügen** > **Encoder hinzufügen** Dialogfeld

Dient zum manuellen Hinzufügen eines Encoders. Dies ist insbesondere dann hilfreich, wenn Sie ein beliebiges Video-IP-Gerät von Bosch hinzufügen möchten (nur für VRM).

Hinweis:
Wenn Sie einen Video-IP-Encoder von Bosch mit der **<Automatisch erkennen>**-Auswahl hinzufügen, muss dieses Gerät im Netzwerk verfügbar sein.

So fügen Sie ein Video IP-Gerät von Bosch hinzu:

1. Erweitern Sie , erweitern Sie , und klicken Sie mit der rechten Maustaste auf .
   Oder
   Klicken Sie mit der rechten Maustaste auf .
   Oder
   Klicken Sie mit der rechten Maustaste auf .
2. Klicken Sie auf **Encoder hinzufügen**.
   Das Dialogfeld **Encoder hinzufügen** wird angezeigt.
3. Geben Sie die entsprechende IP-Adresse ein.
4. Wählen Sie in der Liste **<Automatisch erkennen>** aus, geben Sie das Passwort des Geräts ein, und klicken Sie auf **Authentifizieren.**
   Oder:
   Wählen Sie in der Liste einen konkreten Encoder-Typ oder **<Einzel Platzhalter Kamera>** aus.
5. Klicken Sie auf **OK**.
   Das Gerät wird dem System hinzugefügt.

Das ⚠ Symbol weist auf einen Fehler hin, um den Sie sich kümmern müssen. In der QuickInfo finden Sie weitere Informationen zu dem jeweiligen Fehler.

Dialogfeld Encoder hinzufügen

Netzwerkadresse
Geben Sie eine gültige IP-Adresse ein.

Port-Nummer
Geben Sie die Port-Nummer des Geräts ein.

Encodertyp
Wählen Sie für ein Gerät mit bekanntem Gerätetyp den entsprechenden Eintrag aus. Das Gerät muss nicht im Netzwerk verfügbar sein.
Wenn Sie ein beliebiges Video-IP-Gerät von Bosch hinzufügen möchten, wählen Sie **<Automatisch erkennen>**. Das Gerät muss im Netzwerk verfügbar sein.
Wenn Sie eine Kamera für die Offline-Konfiguration hinzufügen möchten, wählen Sie **<Einzel Platzhalter Kamera>**.

Benutzername
Zeigt den Benutzernamen für die Authentifizierung auf dem Gerät an.

Passwort
Geben Sie ein gültiges Passwort für die Authentifizierung beim Gerät ein.

Passwort anzeigen
Klicken Sie hier, damit das eingegebene Passwort angezeigt wird. Achten Sie darauf, dass niemand das Passwort einsehen kann.

Authentifizieren
Klicken Sie hier, um sich mit den oben eingegebenen Anmeldeinformationen auf dem Gerät zu authentifizieren.

13.8.2 Dialogfeld „Encoder/Decoder bearbeiten“

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > Rechtsklick auf > Klick auf **Encoder bearbeiten** > Dialogfeld **Encoder bearbeiten**
oder
Hauptfenster > **Geräte** > erweitern > Rechtsklick auf > Klick auf **Encoder bearbeiten** > Dialogfeld **Encoder bearbeiten**
oder
Hauptfenster > **Geräte** > erweitern > Rechtsklick auf > Klick auf **Encoder bearbeiten** > Dialogfeld **Encoder bearbeiten**
oder
Hauptfenster > **Geräte** > Erweitern > Erweitern > Rechtsklicken > Klicken **Decoder bearbeiten** > **Decoder bearbeiten** Dialogfeld
Erlaubt die Überprüfung und Aktualisierung der Funktionalitäten eines Geräts. Beim Öffnen dieses Dialogfeldes wird das Gerät verbunden. Das Passwort wird geprüft, und die Funktionalitäten dieses Geräts werden mit denen im BVMS gespeicherten Gerätefunktionen verglichen.

Name
Zeigt den Gerätenamen an. Wenn Sie ein Video-IP-Gerät von Bosch hinzufügen, wird der Gerätename generiert. Ändern Sie den Eintrag bei Bedarf.

Netzwerkadresse / Port
Geben Sie die Netzwerkadresse des Geräts ein. Ändern Sie bei Bedarf die Port-Nummer.

Benutzername
Zeigt den Benutzernamen für die Authentifizierung auf dem Gerät an.

Passwort
Geben Sie ein gültiges Passwort für die Authentifizierung beim Gerät ein.

Passwort anzeigen
Klicken Sie hier, damit das eingegebene Passwort angezeigt wird. Achten Sie darauf, dass niemand das Passwort einsehen kann.

Authentifizieren
Klicken Sie hier, um sich mit den oben eingegebenen Anmeldeinformationen auf dem Gerät zu authentifizieren.

Sicherheit
Das Kontrollkästchen **Sichere Verbindung** ist standardmäßig aktiviert.
Wenn keine sichere Verbindung möglich ist, erscheint eine Meldung. Klicken Sie darauf, um das Häkchen zu entfernen.

Die folgenden Decoder unterstützen eine sichere Verbindung:

- VJD 7000
- VJD 8000
- VIP XD HD

Hinweis!
Die Verbindung zwischen einem Decoder und einem Encoder ist nur sicher, wenn beide mit einer sicheren Verbindung konfiguriert werden.

Videostream
UDP: Ermöglicht verschlüsseltes Muticast-Streaming für unterstützte Decoder-Geräte.
TCP: Ermöglicht verschlüsseltes Unicast-Streaming für unterstützte Decoder-Geräte.
Hinweis: Wenn für einen Encoder keine Multicast-Adresse konfiguriert ist, ruft der Decoder den Stream per Unicast ab.

Hinweis!
BVMS unterstützt nicht Bosch Kameras, die mit einem VSG verbunden sind.
BVMS unterstützt nur UDP Verschlüsselung für Plattformen, die älter sind als CPP13.

Gerätemerkmale
Sie können die angezeigten Gerätefunktionen nach Kategorien oder alphabetisch sortieren.
Eine Textmeldung informiert Sie darüber, ob die erkannten Gerätefunktionen den aktuellen Gerätefunktionen entsprechen.
Klicken Sie auf **OK**, um nach einem Upgrade des Geräts die Änderungen der Gerätefunktionen zu übernehmen.

Siehe
- *Verschlüsseln von Live-Video (Encoder bearbeiten), Seite 223*
- *Aktualisieren der Gerätefunktionen (Encoder bearbeiten), Seite 224*

13.8.3 Ändern des Passworts für einen Encoder/Decoder (Passwort ändern/Passwort eingeben)

Hauptfenster> **Geräte** > Erweitern > Erweitern > >
oder
Hauptfenster > **Geräte** > >
oder
Hauptfenster > **Geräte** > >
oder
Hauptfenster > **Geräte** > erweitern > erweitern >
Definieren Sie für jede Berechtigungsstufe ein eigenes Passwort, oder ändern Sie das jeweilige Passwort entsprechend. Geben Sie das Passwort (max. 19 Zeichen, keine Sonderzeichen) für die ausgewählte Berechtigungsstufe ein.

So ändern Sie das Passwort:

1. Klicken Sie mit der rechten Maustaste auf und anschließend auf **Passwort ändern...**.
   Das Dialogfeld **Passwort eingeben** wird angezeigt.

2. Wählen Sie aus der Liste **Benutzername auswählen** den gewünschten Benutzer aus, für den Sie das Passwort ändern möchten.
3. Geben Sie im Feld **Passwort für Benutzer** das neue Passwort ein.
4. Klicken Sie auf **OK**.

⇨ Das Passwort wird auf dem Gerät umgehend geändert.

Durch ein Passwort wird ein unbefugter Zugriff auf das Gerät verhindert. Über verschiedene Berechtigungsstufen können Sie den Zugriff einschränken.
Ein ordnungsgemäßer Passwortschutz ist nur gewährleistet, wenn auch alle höheren Berechtigungsstufen durch ein Passwort geschützt sind. Deshalb müssen Sie beim Vergeben von Passwörtern stets mit der höchsten Berechtigungsstufe beginnen.
Wenn Sie mit dem service-Benutzerkonto angemeldet sind, können Sie ein Passwort für jede Berechtigungsstufe festlegen und ändern.
Das Gerät hat drei Berechtigungsstufen: service, user und live.

- service ist die höchste Berechtigungsstufe. Die Eingabe des richtigen Passworts ermöglicht den Zugriff auf alle Funktionen und die Änderung aller Konfigurationseinstellungen.
- user ist die mittlere Berechtigungsstufe. Auf dieser Stufe können Sie das Gerät bedienen, Aufzeichnungen wiedergeben und z. B. auch die Kamera steuern, nicht jedoch die Konfiguration ändern.
- live ist die niedrigste Berechtigungsstufe. Auf dieser Stufe können Sie nur das Live-Videobild anschauen und zwischen den verschiedenen Livebild-Darstellungen wechseln.

Bei einem Decoder ersetzen die folgenden Berechtigungsstufen die live-Berechtigungsstufe:

- destination password (nur bei Decodern verfügbar)
  Wird für den Zugriff auf einen Encoder verwendet.

Siehe

- *Angeben des Ziel-Passworts für einen Decoder (Authentifizieren ...), Seite 212*

13.8.4 Decoderprofil

Dient zum Einstellen der verschiedenen Optionen zur Videobildanzeige auf einem VGA-Monitor.

Monitorname

Geben Sie den Namen des Monitors ein. Der Monitorname erleichtert die Identifizierung des Orts eines entfernten Monitors. Verwenden Sie einen Namen, mit dem der Ort möglichst leicht identifiziert werden kann.

Klicken Sie auf , um den Namen im Gerätebaum zu aktualisieren.

Norm

Wählen Sie das Videoausgangssignal Ihres Monitors aus. Zusätzlich zur PAL- und NTSC-Option für analoge Videomonitore stehen acht vorkonfigurierte Einstellungen für VGA-Monitore zur Verfügung.

Hinweis!
Eine VGA-Einstellung, deren Werte nicht im Bereich der technischen Spezifikationen des Monitors liegen, kann zu schweren Schäden am Monitor führen. Nähere Informationen finden Sie in der technischen Dokumentation Ihres Monitors.

Fensteranordnung

Legen Sie die Standardbildanordnung für den Monitor fest.

VGA-Bildschirmgröße
Geben Sie das Bildformat des Bildschirms (z. B. 4 x 3) oder die physische Größe des Bildschirms in Millimetern ein. Anhand dieser Informationen erfolgt eine genaue Skalierung des Videobilds, um eine verzerrungsfreie Anzeige zu erzielen.

13.8.5 Monitor-Anzeige

Das Gerät erkennt Übertragungsunterbrechungen und zeigt eine Warnmeldung auf dem Monitor an.

Anzeige von Übertragungsstörungen
Wählen Sie **Ein**, um bei Übertragungsunterbrechungen eine Warnmeldung anzuzeigen.

Störungs-Empfindlichkeit
Verschieben Sie den Schieberegler, um den Störungsgrad einzustellen, bei dem eine Warnung ausgelöst werden soll.

Störungs-Anzeigetext
Geben Sie den Text der Warnmeldung ein, der auf dem Monitor angezeigt werden soll, wenn die Verbindung unterbrochen wird. Der Text darf maximal 31 Zeichen umfassen.

13.8.6 Konfigurieren eines Bosch IntuiKey Keyboards (Decoder)

Hauptfenster > **Geräte**> erweitern >

Hinweis!
Sie können ein KBD-Universal XF Keyboard nicht an einen Decoder anschließen.

So konfigurieren Sie ein Bosch IntuiKey Keyboard, das an einen Decoder angeschlossen ist:

1. Klicken Sie in der Spalte **Verbindung** auf eine Zelle, und wählen Sie den gewünschten Decoder aus.
   Sie können auch eine Arbeitsstation auswählen, wenn das Bosch IntuiKey Keyboard an sie angeschlossen ist.
   Eine Arbeitsstation muss auf der Seite konfiguriert sein.
2. Nehmen Sie im Feld **Verbindungseinstellungen** die erforderlichen Einstellungen vor.

Detaillierte Informationen zu den verschiedenen Feldern finden Sie in der Online-Hilfe unter dem entsprechenden Anwendungsfenster.

Siehe
- *Seite „Assign Keyboard“ (Tastatur zuweisen), Seite 157*
- *Szenarios für Bosch IntuiKey Keyboard-Anschlüsse, Seite 54*
- *Anschluss eines Bosch IntuiKey Keyboards an einen Decoder, Seite 56*

13.8.7 Konfigurieren eines Decoders für den Einsatz mit einem Bosch IntuiKey Keyboard

Hauptfenster > **Geräte** > erweitern > erweitern
Führen Sie die folgenden Schritte zur Konfiguration eines VIP XD Decoders durch, an den ein Bosch IntuiKey-Keyboard angeschlossen ist.

So konfigurieren Sie einen Decoder:

1. Klicken Sie auf den Decoder, an den ein Bosch IntuiKey-Keyboard angeschlossen wird.

2. Klicken Sie auf die Registerkarte **Peripherie**.
3. Stellen Sie sicher, dass folgende Werte eingestellt sind:
   - Schnittstellenfunktion: **Transparent**
   - Baudrate: **19.200**
   - Stoppbits: **1**
   - Parität: **Keine**
   - Schnittstellenmodus: **RS232**
   - Halbduplex-Modus: **Aus**

Siehe
- *Szenarios für Bosch IntuiKey Keyboard-Anschlüsse, Seite 54*
- *Anschluss eines Bosch IntuiKey Keyboards an einen Decoder, Seite 56*
- *Aktualisierung der Bosch IntuiKey Keyboard-Firmware, Seite 56*

13.8.8 Löschen des Decoder-Logos

Klicken Sie hier, um das Logo zu löschen, das auf der Webseite des Decoders konfiguriert wurde.

13.9 Seite „Monitorgruppen“

Hauptfenster > **Geräte** > erweitern >

Ermöglicht Ihnen, Monitorgruppen hinzuzufügen und zu konfigurieren. Sie weisen einer BVMS Arbeitsstation in eine Monitorgruppe zu.

Hinweis!
Sie können eine Monitorgruppe nicht von einem Operator Client wenn die Verbindung zu Central Server is lost.

Siehe
- *Manuelles Hinzufügen einer Monitorgruppe, Seite 147*
- *Konfigurieren einer Monitorgruppe, Seite 148*
- *Konfigurieren von voreingestellten Positionen und AUX-Kommandos, Seite 305*
- *Konfigurieren eines Alarms, Seite 327*
- *Dialogfeld Alarmoptionen, Seite 318*
- *Dialogfeld „Bildfensterinhalt auswählen“ (MG), Seite 318*

13.9.1 Manuelles Hinzufügen einer Monitorgruppe

Hauptfenster > **Geräte** > erweitern > Rechtsklick auf > Klick auf **Monitorgruppe hinzufügen**

1. Klicken Sie auf **Monitorgruppe hinzufügen**.
   Das Dialogfeld **Monitorgruppe hinzufügen** wird angezeigt. Geben Sie den Namen für Ihre neue Monitorgruppe ein.
2. Klicken Sie auf „OK“.
   Die Monitorgruppe wird zum System hinzugefügt.

3. Klicken Sie auf **Karten und Struktur**.
4. Ziehen Sie die Monitorgruppe zum Logischen Baum.

13.9.2 Konfigurieren einer Monitorgruppe

Hauptfenster > **Geräte** > erweitern > >

Hinweis!
Sie können eine Monitorgruppe nicht von einem Operator Client wenn die Verbindung zu Central Server is lost.

Die Monitore einer Monitorgruppe werden logisch in Reihen und Spalten konfiguriert. Diese Anordnung muss nicht der physischen Anordnung der Monitore entsprechen.

So konfigurieren Sie eine Monitorgruppe:

1. Ziehen Sie die entsprechenden Monitore von der Registerkarte **Nicht-zugeordnete Monitore** zum Feld „Monitorgruppen“.
2. Wählen Sie in der Registerkarte **Layout** die entsprechende Anordnung aus.
3. Ziehen Sie alle verfügbaren Kamera aus der Registerkarte **Kameras** auf ein Monitorfenster auf der linken Seite.
   Die logische Nummer der Kamera wird als schwarze Zahl im Monitorfenster angezeigt und die Farbe des Fensters ändert sich.
4. Ändern Sie bei Bedarf die logischen Nummern der Bildfenster. Wenn Sie eine bereits vergebene Nummer eingeben, wird ein Meldungsfeld angezeigt.
5. Auf der Registerkarte **Optionen** können Sie auswählen, ob Kameraname und -nummer im Monitorfenster sichtbar sind. Sie können auch die Position dieser Informationen auswählen.
   Hinweis: Für VIDEOJET decoder 7513, VIDEOJET decoder 7523 und VIDEOJET decoder 8000 sind diese Optionen nur gültig, nachdem Sie die entsprechenden Decodereinstellungen konfiguriert haben.
   Siehe
   – *Konfigurieren von Decodern für das On-Screen-Display (OSD), Seite 235*

Hinweis!
Sie können festlegen, ob die konfigurierten Überwachungsgruppeneinstellungen nach einem Ausfall wiederhergestellt werden sollen Central Serverneu starten oder wenn die letzten Monitorgruppeneinstellungen, die in Operator Client sollten beibehalten werden.
Siehe *Dialogfeld „Optionen“ (Menü „Einstellungen“), Seite 121*.

Monitorsymbol
Die schwarze fett formatierte Zahl, sofern vorhanden, zeigt die logische Nummer der Erstkamera an.
Die schwarze normal formatierte Zahl zeigt die logische Nummer des Monitors an.
Wenn Sie die Zuordnung einer Kamera aufheben möchten, klicken Sie mit der rechten Maustaste auf das Monitorfenster und klicken Sie anschließend auf **Monitor löschen** oder ziehen Sie die Kamera außerhalb des Bildfensters.

Siehe
– *Manuelles Hinzufügen einer Monitorgruppe, Seite 147*

13.10 Seite Kommunikationsgeräte

Hauptfenster > **Geräte** > erweitern >
Dient zum Hinzufügen oder Konfigurieren eines Kommunikationsgeräts.
Sie können folgende Kommunikationsgeräte konfigurieren:
– E-Mail

Siehe
– *Konfigurieren eines Kommunikationsgeräts, Seite 150*

13.10.1 Hinzufügen eines E-Mail-/SMTP-Servers

So fügen Sie ein Kommunikationsgerät hinzu:

1. Erweitern Sie , klicken Sie mit der rechten Maustaste auf und klicken Sie auf **E-Mail/ SMTP-Gerät hinzufügen**.
   Das Dialogfeld **E-Mail/SMTP-Gerät hinzufügen** wird angezeigt.
2. Geben Sie die erforderlichen Einstellungen ein.
3. Klicken Sie auf **OK**.
   Das Kommunikationsgerät wird dem System hinzugefügt.

Dialogfeld E-Mail/SMTP-Gerät hinzufügen

Name:
Geben Sie den Anzeigenamen des E-Mail-Servers ein.

13.10.2 Seite SMTP-Server

Hauptfenster > **Geräte** > erweitern > erweitern >
Dient zum Konfigurieren der E-Mail-Einstellungen Ihres Systems. Auf der Seite **Ereignisse** können Sie einer E-Mail ein Ereignis zuordnen. Wenn dieses Ereignis eintritt, sendet das System eine E-Mail-Nachricht. Der Empfang von E-Mail-Nachrichten ist im BVMS nicht möglich.

SMTP-Server-Name
Geben Sie den Namen des E-Mail-Servers ein. Sie erhalten die erforderlichen Informationen hierzu von Ihrem Service Provider. Gewöhnlich handelt es sich um die IP-Adresse oder den DNS-Namen des E-Mail-Servers.

Senderadresse
Geben Sie die als Absenderadresse zu verwendende E-Mail-Adresse ein, wenn das System zum Beispiel bei einem Alarm eine E-Mail sendet.

SSL/TLS
Aktivieren Sie das Kontrollkästchen, um die Verwendung einer sicheren SSL/TLS-Verbindung zu ermöglichen. In diesem Fall wechselt der Netzwerk-Port automatisch zu 587.

Port
Geben Sie die erforderliche Netzwerk-Port-Nummer für ausgehende E-Mails ein. Sie erhalten die erforderlichen Informationen hierzu von Ihrem Provider.
Port 25 wird automatisch ausgewählt, wenn Sie die **SSL/TLS**-Einstellung deaktivieren.
Bei Bedarf können Sie einen anderen Port wählen.

Verbindungs-Timeout [s]
Geben Sie die Zeit in Sekunden ein, die das System inaktiv sein muss, bevor die Verbindung getrennt wird.

Authentifizierung
Aktivieren Sie ein Optionsfeld für das erforderliche Verfahren der Berechtigungsprüfung. Sie erhalten die erforderlichen Informationen hierzu von Ihrem Service Provider.

Benutzername
Geben Sie den Benutzernamen für die Berechtigungsprüfung auf dem E-Mail-Server ein. Sie erhalten die erforderlichen Informationen hierzu von Ihrem Service Provider.

Passwort:
Geben Sie das Passwort für die Berechtigungsprüfung auf dem E-Mail-Server ein. Sie erhalten die erforderlichen Informationen hierzu von Ihrem Service Provider.

Test-E-Mail senden
Klicken Sie hier, um das Dialogfeld **Test-E-Mail senden** anzuzeigen.

Siehe
– *Konfigurieren eines Kommunikationsgeräts, Seite 150*

13.10.3 Konfigurieren eines Kommunikationsgeräts

Hauptfenster > **Geräte** > erweitern > erweitern

So konfigurieren Sie ein Kommunikationsgerät:

1. Klicken Sie auf .
2. Nehmen Sie die erforderlichen Einstellungen vor.

Detaillierte Informationen zu den verschiedenen Feldern finden Sie in der Online-Hilfe unter dem entsprechenden Anwendungsfenster.

Siehe
– *Hinzufügen eines E-Mail-/SMTP-Servers, Seite 149*
– *Seite SMTP-Server, Seite 149*

13.10.4 Dialogfeld Test-E-Mail senden

Hauptfenster > **Geräte** > erweitern > erweitern > > Schaltfläche **Test-E-Mail senden**

Dient zum Senden einer Test-E-Mail.

Von:
Geben Sie die E-Mail-Adresse des Absenders ein.

An
Geben Sie die E-Mail-Adresse des Empfängers ein.

Betreff
Geben Sie den Betreff der E-Mail ein.

Nachricht
Geben Sie die Nachricht ein.

Test-E-Mail senden
Klicken Sie darauf, um die E-Mail zu senden.

Siehe

– *Konfigurieren eines Kommunikationsgeräts, Seite 150*

13.11 Seite „ATM/POS“

Hauptfenster > **Geräte** > erweitern >

Dient zum Hinzufügen und Konfigurieren von Peripheriegeräten, beispielsweise einer Bosch ATM/POS Bridge.

Wenn Sie mehrere Bridges auf einem Server hinzufügen möchten, müssen Sie verschiedene Ports verwenden.

Siehe

– *Hinzufügen einer Bosch ATM/POS-Bridge, Seite 97*

– *Konfigurieren eines Peripheriegeräts, Seite 152*

13.11.1 Manuelles Hinzufügen einer Bosch ATM/POS-Bridge

Hauptfenster > **Geräte** > Erweitern > Rechtsklick > **Bosch ATM/POS-Bridge hinzufügen** .

Ermöglicht das Hinzufügen eines Bosch ATM.

So fügen Sie ein Peripheriegerät hinzu:

1. Erweitern Sie , klicken Sie mit der rechten Maustaste auf und klicken Sie auf **Bosch ATM/POS-Bridge hinzufügen**.
   Das Dialogfeld **Bosch ATM/POS-Bridge hinzufügen** wird angezeigt.
2. Geben Sie die erforderlichen Einstellungen ein.
3. Klicken Sie auf **OK**.
   Das Peripheriegerät wird dem System hinzugefügt.

Dialogfeld Bosch ATM/POS-Bridge hinzufügen

Name:
Geben Sie den entsprechenden Namen für das Gerät ein.

IP-Adresse:
Geben Sie die IP-Adresse des Geräts ein.

Port 1:
Geben Sie die entsprechende Port-Nummer ein, die als Überwachungsport von ATM/POS Bridge verwendet wird.

Port 2:
Geben Sie die entsprechende Port-Nummer ein, die als Überwachungsport von BVMS Management Server verwendet wird.

Hinweis!
Achten Sie beim Hinzufügen mehrerer ATM/POS Bridges zu Ihrem System darauf, dass die Nummern für Port 2 für jedes Gerät unterschiedlich sind. Wenn Sie dieselbe Nummer mehrmals für Port 2 verwenden, können ATM/POS-Daten verloren gehen.

Siehe

– *Hinzufügen einer Bosch ATM/POS-Bridge, Seite 97*

13.11.2 Seite Bosch ATM/POS-Bridge

Hauptfenster > **Geräte** > Erweitern > Erweitern > > Registerkarte **Bosch ATM/POS-Bridge**

Ermöglicht die Konfiguration einer ATM/POS Bridge.

IP-Adresse:

Geben Sie die IP-Adresse des Geräts ein.

Port 1:

Geben Sie die entsprechende Port-Nummer ein, die als Überwachungsport von ATM/POS Bridge verwendet wird.

Port 2:

Geben Sie die entsprechende Port-Nummer ein, die als Überwachungsport von BVMS Management Server verwendet wird.

Hinweis!

Achten Sie beim Hinzufügen mehrerer ATM/POS Bridges zu Ihrem System darauf, dass die Nummern für Port 2 für jedes Gerät unterschiedlich sind. Wenn Sie dieselbe Nummer mehrmals für Port 2 verwenden, können ATM/POS-Daten verloren gehen.

Siehe

- *Konfigurieren eines Peripheriegeräts, Seite 152*
- *Hinzufügen einer Bosch ATM/POS-Bridge, Seite 97*

13.11.3 Konfigurieren eines Peripheriegeräts

Hauptfenster > **Geräte** > erweitern > erweitern > **Bosch ATM/POS-Bridge**

oder

Hauptfenster > **Geräte** > erweitern > erweitern > **DTP-Gerät** >

So konfigurieren Sie ein Peripheriegerät:

- Ändern Sie die erforderlichen Einstellungen.

Detaillierte Informationen zu den verschiedenen Feldern erhalten Sie, wenn Sie unten auf den Link des entsprechenden Anwendungsfensters klicken.

Siehe

- *Seite „ATM-Einstellungen“, Seite 153*
- *Seite Bosch ATM/POS-Bridge, Seite 152*
- *Seite „DTP-Einstellungen“, Seite 152*

13.11.4 Seite „DTP-Einstellungen“

Hauptfenster > **Geräte** > erweitern > erweitern >

Ermöglicht die Konfiguration eines DTP-Geräts mit maximal 4 mit dem DTP-Gerät verbundenen ATM-Geräten.

Serieller Port

Wählen Sie den entsprechenden Port in der Liste aus.

Siehe

- *Seite „ATM-Einstellungen“, Seite 153*

– *Konfigurieren eines Peripheriegeräts, Seite 152*

13.11.5 Seite „ATM-Einstellungen“

Hauptfenster> **Geräte** > erweitern > erweitern > >

Ermöglicht die Konfiguration eines ATM-Geräts, das mit einem DTP-Gerät verbunden ist.

Inputnummer des DTP-Gerätes

Wählen Sie die gewünschte Eingangsnummer. Wird die Nummer bereits durch ein anderes ATM-Gerät verwendet, können Sie die Eingangsnummern austauschen.

Verbindungs-Timeout [Stunden]:

Geben Sie die gewünschte Anzahl der Stunden ein. Wenn das ATM-Gerät in diesem Zeitraum keine Transaktionsdaten gesendet hat, nimmt das BVMS an, dass die Verbindung getrennt wurde. Es wird ein entsprechendes Ereignis ausgelöst. Das **Nicht authentifiziert**-Ereignis ist verfügbar für ein ATM-Gerät, aber nicht relevant.

Die Eingabe einer **0** bedeutet, dass kein Verbindungstest durchgeführt wird.

Daten-Inputs

Klicken Sie, um die gewünschten Eingänge zu aktivieren, und geben Sie den gewünschten Namen für die Eingänge ein.

Siehe

– *Konfigurieren eines Peripheriegeräts, Seite 152*

13.11.6 Seite Eingänge

Hauptfenster > **Geräte** > erweitern > erweitern > > Registerkarte **Eingänge**

Dient zum Konfigurieren von Eingängen einer Bosch ATM/POS Bridge.

Siehe

– *Konfigurieren eines Peripheriegeräts, Seite 152*
– *Hinzufügen einer Bosch ATM/POS-Bridge, Seite 97*

13.12 Foyer-Kartenleser

Hauptfenster > **Geräte** > erweitern > > Registerkarte **Globale Einstellungen für Foyerkartenleser**

Sie können die Einstellungen konfigurieren, die für alle Foyer-Kartenleser im System gelten.

Serieller Port

Wählen Sie den seriellen Port aus, mit dem der Foyer-Kartenleser verbunden ist.

Gesperrt

Dient dem Hinzufügen einer Bankleitzahl zur Sperrung. Dies bedeutet, dass Karten mit den hier eingetragenen Sperrvermerken keine Zugangsberechtigung besitzen. Der Zutritt wird durch den Foyer-Kartenleser verweigert. Die Standardeinstellung für die elektrische Türverriegelung des Foyer-Kartenlesers muss auf **Automatisch** eingestellt sein.

Die Liste kann Einträge mit Platzhaltern enthalten.

? steht für beliebige oder keine Zeichen an dieser Stelle.

* steht für eine Abfolge (ein oder mehrere Zeichen) beliebiger oder keiner Zeichen (Ausnahme: * alleinstehend bedeutet, dass sämtliche Bankleitzahlen gesperrt sind).

Länder-Code bei EC-Karten ignorieren
Klicken Sie hier, um zu aktivieren, dass das BVMS keine Kartendaten analysiert, die zur Identifikation dienen, in welchem Land die Karte verwendet wurde. Der Zutritt für Karten mit einem anderen Ländercode ist möglich.

13.12.1 Dialogfeld „Foyer-Kartenleser hinzufügen“

Hauptfenster > **Geräte** > erweitern > Rechtsklick auf > Befehl **Foyerkartenleser hinzufügen**
Sie können einen Foyer-Kartenleser hinzufügen.

Name
Geben Sie einen Namen für das Gerät ein.

Geräteidentifikation
Wählen Sie eine einmalige Nummer für das Gerät. Stehen keine Nummern zu Verfügung, wurde dem System bereits die maximale Anzahl an Foyer-Kartenlesern hinzugefügt.

13.12.2 Einstellungen für Foyer-Kartenleser-Seite

Hauptfenster > **Geräte** > erweitern > > > Registerkarte **Einstellungen für Foyerkartenleser**
Sie können einen Foyer-Kartenleser konfigurieren.

Geräteidentifikation
Zeigt die einmalige Nummer des Geräts an.

Skimming-Schutz aktivieren
Klicken Sie hier, um zu aktivieren, dass das BVMS ein Ereignis auslöst, sobald ein angehängtes Skimming-Gerät Skimming erkennt. Dies wird nicht von allen Foyerkartenlesertypen unterstützt.

Standardmodus der Freigabe des elektrischen Türschlosses
Öffnen: Die Tür ist offen und alle Personen können ohne Karte eintreten.
Geschlossen: Die Tür ist geschlossen, unabhängig davon, ob eine Karte eingeführt wird.
Automatisch: Die Tür öffnet sich nur, wenn eine Karte mit einer entsprechenden Zugangsberechtigung in den Leser eingeführt wird.

Zeitsteuerung aktivieren
Klicken Sie hier, um die Möglichkeit zu aktivieren, dem ausgewählten Freigabemodus der Türverriegelung einen Zeitplan zuweisen zu können.
Sobald der Zeitplan aktiv wird, schaltet das BVMS den Foyerkartenleser in den entsprechenden Freigabemodus.
Überschneiden sich die ausgewählten Zeitpläne, wird der wirksame Türfreigabemodus durch die folgenden Prioritätsmodi bestimmt: 1. **Öffnen** 2. **Geschlossen** 3. **Automatisch**

13.13 Seite Virtuelle Eingänge

Hauptfenster > **Geräte** > Erweitern >
Zeigt die im System konfigurierten virtuellen Eingänge an.
Dient zum Hinzufügen neuer virtueller Eingänge sowie zum Löschen vorhandener virtueller Eingänge.

Eingänge hinzufügen
Klicken Sie darauf, um ein Dialogfeld zum Hinzufügen neuer virtueller Eingänge anzuzeigen.

Eingang löschen
Klicken Sie darauf, um einen ausgewählten virtuellen Eingang zu löschen.

Nummer
Zeigt die Nummer des virtuellen Eingangs an.

Name
Klicken Sie auf eine Zelle, um den Namen des virtuellen Eingangs zu ändern.

13.13.1 Manuelles Hinzufügen virtueller Eingänge

Hauptfenster > **Geräte** > erweitern > Schaltfläche **Eingänge hinzufügen**
Dient zum Hinzufügen neuer virtueller Eingänge.

So fügen Sie einen virtuellen Eingang hinzu:

1. Erweitern Sie und klicken Sie auf .
   Die entsprechende Seite wird angezeigt.
2. Klicken Sie auf **Eingänge hinzufügen**.
   In die Tabelle wird eine Zeile eingefügt.
3. Nehmen Sie die erforderlichen Einstellungen vor.
4. Klicken Sie auf **Hinzufügen**.
   Der virtuelle Eingang wird zum System hinzugefügt.

Dialogfeld Eingänge hinzufügen

Start:
Wählen Sie die erste Nummer der neuen virtuellen Eingänge aus.

Ende:
Wählen Sie die letzte Nummer der neuen virtuellen Eingänge aus.

Name
Geben Sie den Namen jedes einzelnen neuen virtuellen Eingangs ein. An den Namen wird eine fortlaufende Nummer angehängt.

Hinzufügen
Klicken Sie darauf, um neue virtuelle Eingänge hinzuzufügen.

13.14 Seite SNMP

Hauptfenster > **Geräte** > erweitern >
Dient zum Hinzufügen oder Konfigurieren einer SNMP-Messung zur Aufrechterhaltung der Netzwerkqualität.

Siehe
– *Konfigurieren eines SNMP Trap Receivers (Seite „SNMP Trap Receiver“), Seite 156*

13.14.1 Manuelles Hinzufügen eines SNMP

Hauptfenster > **Geräte** > erweitern > Rechtsklick auf > Befehl **SNMP hinzufügen**
Dient zum Hinzufügen eines Systems zur Netzwerküberwachung zum BVMS.

So fügen Sie ein Netzwerküberwachungsgerät hinzu:

1. Erweitern Sie , klicken Sie mit der rechten Maustaste auf und klicken Sie auf **SNMP hinzufügen**.
   Das Dialogfeld **SNMP hinzufügen** wird angezeigt.
2. Geben Sie einen Namen für das SNMP-Gerät ein.
   Das Netzwerküberwachungsgerät wird zum System hinzugefügt.

Dialogfeld SNMP hinzufügen

Name:
Geben Sie einen Namen für das Netzwerküberwachungsgerät ein.

Siehe
– *Konfigurieren eines SNMP Trap Receivers (Seite „SNMP Trap Receiver“), Seite 156*

13.14.2 Konfigurieren eines SNMP Trap Receivers (Seite „SNMP Trap Receiver“)

Hauptfenster > **Geräte** > erweitern

So konfigurieren Sie den SNMP trap receiver:

1. Klicken Sie auf , um die Seite **SNMP Trap Receiver** anzuzeigen.
2. Nehmen Sie die erforderlichen Einstellungen vor.

Detaillierte Informationen zu den verschiedenen Feldern finden Sie in der Online-Hilfe unter dem entsprechenden Anwendungsfenster.

Seite SNMP Trap Receiver

Hauptfenster > **Geräte** > erweitern > erweitern
Dient zum Auswählen der zu überwachenden Geräte sowie der SNMP-Trap-OIDs, die bei Eingang ein Ereignis für das ausgewählte Gerät auslösen sollen.

Hinweis!
Sie müssen die IP-Adresse des BVMS Management Servers als Trap-Receiver in den zu überwachenden Geräten eingeben.

SNMP Trap sendende Geräte:
Dient zum Eingeben eines IP-Adressbereichs für die zu überwachenden Netzwerkgeräte. Geben Sie zur Überwachung eines einzelnen Geräts die entsprechende IP-Adresse in die Zelle **Bereich von** ein. Gehen Sie beim Ändern dieser Adressen mit Vorsicht vor. Bei Eingabe einer falschen Adresse erfolgt keine Netzwerküberwachung für dieses Gerät.

SNMP Trap Filterregeln:
Dient zum Eingeben von OIDs und der entsprechenden Werte. Sie können Platzhalter wie * und ? verwenden, um den Filterbereich zu erweitern. Wenn Sie OIDs und Werte in mehreren Zeilen eingeben, müssen alle diese Filterregeln gleichzeitig zutreffen, um ein Ereignis auszulösen. In beiden Spalten können Sie einen regulären Ausdruck in {} eingeben. Befinden sich Zeichen außerhalb der Klammern, wird der reguläre Ausdruck nicht ausgewertet.

Trap Logger Tool anzeigen
Klicken Sie hier, um das Dialogfeld **SNMP Trap Logger** anzuzeigen und SNMP-Trap-OIDs zu verfolgen.

13.14.3 Dialogfeld SNMP Trap Logger

Hauptfenster > **Geräte** > erweitern > erweitern > einen generischen SNMP-Trap-Receiver auswählen > Klick auf **Trap Logger Tool anzeigen**

Dient zur Verfolgung von SNMP-Trap-OIDs. Sie können Traps von allen Geräten im Netzwerk oder nur von ausgewählten empfangen. Sie können die eingehenden Traps filtern sowie OIDs und Werte ausgewählter Traps in die Tabelle **SNMP Trap Filterregeln:** einfügen.

Start/Pause

Klicken Sie darauf, um eine Verfolgung zu starten bzw. anzuhalten.

Nur Traps vom Sender

Geben Sie die IP-Adresse oder den DNS-Namen eines Geräts ein. Nur die Traps dieses Geräts werden verfolgt.

Nur Traps, die enthalten

Geben Sie eine Zeichenfolge ein, die ein Trap enthalten kann. Sie können * und ? als Platzhalter verwenden. Zeichenfolgen in {} werden als reguläre Ausdrücke behandelt. Nur die Traps werden verfolgt, die diese Zeichenfolge enthalten.

Empfangene Traps

Zeigt die Traps an, die bei einer Verfolgung eingegangen sind.

Klicken Sie hier, um alle Einträge aus dem Feld **Empfangene Traps** zu entfernen.

Trap-Details

Zeigt die Trap-Details an. Sie können die OID- und Werteinträge in die Tabelle **SNMP Trap Filterregeln:** kopieren.

Siehe

– *Konfigurieren eines SNMP Trap Receivers (Seite „SNMP Trap Receiver“), Seite 156*

13.15 Seite „Assign Keyboard“ (Tastatur zuweisen)

Hauptfenster > **Geräte** > erweitern >

Dient zum Hinzufügen eines KBD-Universal XF-Keyboards (das an eine BVMS-Arbeitsstation angeschlossen ist) oder eines Bosch IntuiKey Keyboards (das an eine BVMS-Arbeitsstation oder einen Decoder angeschlossen ist).

So fügen Sie ein CCTV-Keyboard hinzu:

Hinweis: Zum Hinzufügen eines Keyboards müssen Sie eine Arbeitsstation hinzugefügt haben.

1. Erweitern Sie und klicken Sie auf .
   Die entsprechende Seite wird angezeigt.
2. Klicken Sie auf **Keyboard hinzufügen**.
   In die Tabelle wird eine Zeile eingefügt.
3. Wählen Sie im entsprechenden Feld der Spalte **Keyboard-Typ** den gewünschten Keyboard-Typ:
   IntuiKey-Keyboard
   KBD-Universal XF Keyboard
4. Wählen Sie im entsprechenden Feld der Spalte **Verbindung** die Arbeitsstation, die mit dem Keyboard verbunden ist.
5. Nehmen Sie die erforderlichen Einstellungen vor.
   Das Keyboard wird zum System hinzugefügt.

Keyboard hinzufügen
Klicken Sie darauf, um für die Konfiguration eines Keyboards eine Zeile in die Tabelle einzufügen.

Keyboard entfernen
Klicken Sie darauf, um die ausgewählte Zeile zu entfernen.

Keyboard-Typ
Zeigt den Typ des Keyboards an, das mit Ihrer Arbeitsstation oder Ihrem Decoder verbunden ist.
Klicken Sie auf eine Zelle, um den erforderlichen Keyboardtyp auszuwählen.

- **IntuiKey**
  Wählen Sie diesen Typ, wenn Sie ein IntuiKey Keyboard von Bosch angeschlossen haben.
- **KBD-Universal XF Keyboard**
  Wählen Sie diesen Typ, wenn Sie ein KBD-Universal XF Keyboard angeschlossen haben.

Verbindung
Wählen Sie in einer Zelle das Gerät, an das Ihr Keyboard angeschlossen ist. Wenn Sie eine Arbeitsstation auswählen, wird das Keyboard auch zur Seite > hinzugefügt.

Port
Wählen Sie in einer Zelle den gewünschten COM-Port aus.

Baudrate
Wählen Sie in einer Zelle die maximale Rate (in Bits pro Sekunde) aus, mit der Daten über diesen Port übertragen werden sollen. In der Regel wird die maximale Rate eingestellt, die vom Computer oder Gegengerät unterstützt wird.

Datenbits
Zeigt die Anzahl der Datenbits an, die für die einzelnen übertragenen und empfangenen Zeichen verwendet werden sollen.

Stoppbits
Zeigt die Zeit zwischen den einzelnen übertragenen Zeichen an (gemessen in Bits).

Parität
Zeigt die Art der Fehlerprüfung an, die für den ausgewählten Port verwendet werden soll.

Port-Typ
Zeigt den Verbindungstyp für den Anschluss des Bosch IntuiKey Keyboards an die Arbeitsstation an.

Siehe
- *Konfigurieren eines Decoders für den Einsatz mit einem Bosch IntuiKey Keyboard, Seite 146*
- *Konfigurieren eines Bosch IntuiKey Keyboards (Seite „Einstellungen“) (Arbeitsstation), Seite 138*
- *Konfigurieren eines Bosch IntuiKey Keyboards (Decoder), Seite 146*

13.16 Seite Input / Output-Module

Hauptfenster > **Geräte** > erweitern >
Dient zum Hinzufügen oder Konfigurieren eines I/O-Moduls.
Zur Zeit werden nur ADAM-Geräte unterstützt.

Siehe
- *Konfigurieren eines I/O-Moduls, Seite 159*

13.16.1 Manuelles Hinzufügen eines I/O-Moduls

So fügen Sie ein I/O-Modul hinzu:

1. Erweitern Sie , klicken Sie mit der rechten Maustaste auf , und klicken Sie auf **Neues ADAM-Gerät hinzufügen**.
   Das Dialogfeld **ADAM hinzufügen** wird angezeigt.
2. Geben Sie die IP-Adresse des Geräts ein.
3. Wählen Sie den Gerätetyp aus.
   Die entsprechende Seite wird angezeigt.
4. Klicken Sie auf die Registerkarte **ADAM-Gerät**, um die Anzeigenamen der Eingänge bei Bedarf zu ändern.
5. Klicken Sie auf die Registerkarte **Name**, um die Anzeigenamen der Relais bei Bedarf zu ändern.

Hinweis!
Sie können auch nach ADAM-Geräten scannen (**ADAM-Geräte scannen**). Die IP-Adressen der Geräte werden erkannt. Der Gerätetyp (sofern verfügbar) wird voreingestellt. Sie müssen diese Einstellung bestätigen.

13.16.2 Konfigurieren eines I/O-Moduls

Hauptfenster > **Geräte** > erweitern > erweitern >

So konfigurieren Sie ein I/O-Modul:

Hinweis!
Ändern Sie den Gerätetyp nicht.
Wenn Sie die Anzahl der Eingänge oder Relais reduzieren, werden alle Konfigurationsdaten für die entfernten Eingänge oder Relais gelöscht.

1. Klicken Sie auf die Registerkarte **ADAM-Gerät**.
2. Wählen Sie in der Liste **ADAM-Typ:** den erforderlichen Gerätetyp aus.
3. Klicken Sie auf die Registerkarte **Eingänge**.
4. Ändern Sie in der Spalte **Name** bei Bedarf den Anzeigenamen der Eingänge.
5. Klicken Sie auf die Registerkarte **Relais**.
6. Ändern Sie in der Spalte **Relais** bei Bedarf die Relaisnamen.

So ändern Sie eine IP-Adresse:

1. Klicken Sie im Gerätebaum mit der rechten Maustaste auf ein ADAM-Gerät.
2. Wählen Sie **Netzwerkadresse ändern**.
3. Geben Sie die neue IP-Adresse ein und klicken Sie auf **OK**.
4. Aktivieren Sie die Konfiguration.

⇨ Die neue IP-Adresse wird für den Zugriff auf das Gerät verwendet.

Siehe

– *Seite Input / Output-Module, Seite 158*

13.16.3 Seite ADAM-Gerät

Hauptfenster > **Geräte** > erweitern > > > Registerkarte **ADAM-Gerät**

Zeigt Informationen zum ausgewählten ADAM-Gerät an.
Dient zum Ändern des Display-Namens eines ADAM-Geräts.

ADAM-Typ:
Wählen Sie den gewünschten Gerätetyp aus.

Eingänge insgesamt:
Zeigt die Anzahl der für diesen Gerätetyp verfügbaren Eingänge an.

Relais/Ausgänge insgesamt:
Zeigt die Anzahl der für diesen Gerätetyp verfügbaren Relais an.

13.16.4 Seite Eingänge

Hauptfenster > **Geräte** > erweitern > > > Registerkarte **Eingänge**
Dient zum Ändern der Display-Namen der Eingänge des ausgewählten ADAM-Geräts.

Nummer
Zeigt die logische Nummer des Eingangs an.

Name
Klicken Sie auf eine Zelle, um den Display-Namen eines Eingangs zu ändern.

13.16.5 Seite Relais

Hauptfenster > **Geräte** > erweitern > > > Registerkarte **Relais**
Dient zum Ändern der Display-Namen der Relais des ausgewählten ADAM-Geräts.

Nummer
Klicken Sie auf eine Zelle, um die logische Nummer eines Relais zu ändern.

Name
Geben Sie den Display-Namen des Relais ein.

13.17 Seite "Allegiant CCL-Emulation"

Hauptfenster > **Geräte** > erweitern >
Dient zum Aktivieren der Allegiant CCL-Emulation.
In BVMS unterstützte Allegiant CCL-Befehle, Seite 62 enthält die CCL-Befehle, die im Bosch Video Management System unterstützt werden.

Hinweis:
Konfigurieren Sie die Allegiant CCL-Emulation und ein Allegiant Gerät nicht am selben COM-Port. Wenn derselbe COM-Port für beide Geräte konfiguriert wird, hat das Allegiant Gerät Priorität. Beim Zugriff des Allegiant CCL-Emulationsgeräts tritt ein Fehler mit der entsprechenden Meldung auf. Um dieses Problem zu lösen, muss der Management-Server über zwei unterschiedliche COM-Ports verfügen oder das Allegiant-Gerät mit einem anderen Computer verbunden werden.

Allegiant CCL-Emulation aktivieren
Wählen Sie das Kontrollkästchen aus, um die Emulation zu aktivieren.

Baud-Rate
Wählen Sie den Wert für die Übertragungsrate in Bit/s aus.

Stoppbits
Wählen Sie die Anzahl der Stoppbits pro Zeichen aus.

Parität
Wählen Sie die Parität aus.

Handshaking
Wählen Sie die gewünschte Methode für die Flusssteuerung aus.

Modell
Wählen Sie das Allegiant-Modell aus, das Sie emulieren möchten.

Siehe
– *Konfigurieren einer Allegiant CCL-Emulation, Seite 161*

13.17.1 Manuelles Hinzufügen einer Allegiant CCL-Emulation

So fügen Sie eine Allegiant CCL-Emulation hinzu:

1. Erweitern Sie und klicken Sie auf .
   Die Registerkarte **Allegiant CCL-Emulation** wird angezeigt.
2. Aktivieren Sie **Allegiant CCL-Emulation aktivieren**.
3. Nehmen Sie die erforderlichen Einstellungen vor.
   Der Allegiant CCL-Emulationsdienst wird auf dem Management Server gestartet.

13.17.2 Allegiant CCL-Befehle

Um in BVMS konfigurierte IP-Kameras oder Encoder auf IP-Decoder umzuschalten, verwenden Sie CCL-Befehle. Sie können keine CCL-Befehle verwenden, um Analogkameras oder die Allegiant-Kreuzschiene selbst direkt zu steuern.
Die Allegiant CCL-Emulation startet einen internen BVMS Dienst, der CCL-Befehle des Kreuzschienen-Umschalters in BVMS übersetzt. Für den Empfang der CCL-Befehle wird ein COM-Port am Management Server konfiguriert. Durch die CCL-Emulation können vorhandene Allegiant Geräte mit dem Bosch Video Management System ausgetauscht oder das Bosch Video Management System mit Anwendungen verwendet werden, die Allegiant CCL-Befehle unterstützen. Alte in BVMS konfigurierte Allegiant-Hardware kann nicht mit diesen Befehlen gesteuert werden.

13.17.3 Konfigurieren einer Allegiant CCL-Emulation

Hauptfenster > **Geräte**> Erweitern >
Um die CCL-Befehle zu verwenden, brauchen Sie das CCL-Benutzerhandbuch. Dieses Handbuch ist im Online-Produktkatalog im Dokumentenbereich jeder LTC Allegiant Kreuzschiene verfügbar.
Die *In BVMS unterstützte Allegiant CCL-Befehle, Seite 62* listet die CCL-Befehle auf, die vom Bosch Video Management System unterstützt werden.

So konfigurieren Sie eine Allegiant CCL-Emulation:

1. Klicken Sie auf **Allegiant CCL-Emulation aktivieren**.
2. Konfigurieren Sie die Kommunikationseinstellungen nach Bedarf.

Detaillierte Informationen zu den verschiedenen Feldern finden Sie in der Online-Hilfe unter dem entsprechenden Anwendungsfenster.

Siehe
– *Seite "Allegiant CCL-Emulation", Seite 160*

13.18 Seite „Einbruchmeldezentralen”

Hauptfenster > **Geräte** > erweitern >

Dient zum Hinzufügen und Konfigurieren von Einbruchmeldezentralen von Bosch. Das Gerät muss verbunden und verfügbar sein.
Wenn Sie eine Einbruchmeldezentrale hinzugefügt haben, werden die Bereiche, Melder, Türen und Relais im Gerätebaum hierarchisch angezeigt.
Sie können das Fenster, jeden Bereich, jeden Melder, jede Tür und jedes Relais entfernen oder umbenennen.
Wenn die Konfiguration der Einbruchmeldezentrale geändert wurde, müssen Sie das Gerät erneut scannen, um die Änderungen in BVMS anzuzeigen.

Hinweis!
Alle Alarmereignisse, die bei einem Melder entstehen können, werden automatisch als BVMS-Alarm konfiguriert.
Beispiel: Feueralarm

Hinweis!
Wenn eine Tür in der Konfiguration einer Einbruchmeldezentrale, die zu Ihrem BVMS hinzugefügt wird, nicht einem Punkt zugewiesen wird, wird für diese Tür kein BVMS Alarmereignis und deshalb auch kein BVMS Alarm ausgelöst.

13.18.1 Manuelles Hinzufügen einer Einbruchmeldezentrale

Hauptfenster > **Geräte** > erweitern > Kontextmenü von > Befehl **Zentrale hinzufügen**
Dient zum Hinzufügen einer Einbruchmeldezentrale von Bosch.

So fügen Sie eine Einbruchmeldezentrale hinzu:

1. Erweitern Sie , klicken Sie mit der rechten Maustaste auf und klicken Sie auf **Zentrale hinzufügen**.
   Das Dialogfeld **Einbruchmeldezentrale hinzufügen** wird angezeigt.
2. Geben Sie die erforderlichen Werte ein.
3. Klicken Sie auf **OK**.
   Die Einbruchmeldezentrale wird zum System hinzugefügt.

Dialogfeld Einbruchmeldezentrale hinzufügen

Netzwerkadresse
Geben Sie die IP-Adresse des Geräts ein.

Netzwerkport
Wählen Sie im Gerät die konfigurierte Port-Nummer aus.

Automatisierungs-Passcode
Geben Sie den Passcode zur Authentifizierung auf dem Gerät ein.

13.18.2 Seite "Einstellungen"

Hauptfenster > **Geräte** > erweitern > erweitern > > Registerkarte **Einstellungen**
Dient zum Ändern der Verbindungseinstellungen der Einbruchmeldezentrale.

13.19 Seite „Zutrittskontrollsysteme“

Hauptfenster > **Geräte** > erweitern >

Dient zum Hinzufügen und Konfigurieren von Zutrittskontrollsystemen von Bosch. Das Gerät muss verbunden und verfügbar sein. Wenn Sie ein Zutrittskontrollsystem hinzugefügt haben, werden Controller, Eingänge, Leser und Türen hierarchisch im Gerätebaum angezeigt.
Sie können Controller, Eingänge, Leser und Türen auf der Seite **Karten und Struktur** entfernen oder umbenennen.
Wenn die Konfiguration oder Hierarchie von Controllern, Lesern oder Türen des Zutrittskontrollsystems geändert wurde, müssen Sie das Gerät erneut suchen, damit die Änderungen in BVMS angezeigt werden.

HTTPS-Zertifikat für Client
Um die Verbindung zwischen dem Zutrittskontrollsystem und BVMS zu sichern, müssen Sie ein Client-Zertifikat aus dem Zutrittskontrollsystem exportieren und es in BVMS importieren. Dieser Vorgang wird im Abschnitt **HTTPS-Zertifikat für Client** der Dokumentation für das Zutrittskontrollsystem beschrieben.

Hinweis!
Wenn das Zertifikat nicht hinzugefügt wird, können die Systeme keine Informationen miteinander austauschen.

13.19.1 Hinzufügen eines Zutrittskontrollsystems

Hauptfenster > **Geräte** > erweitern >

So fügen Sie ein Zutrittskontrollsystem hinzu:

1. Klicken Sie mit der rechten Maustaste auf .
2. Klicken Sie auf **Zutrittskontrollsystem hinzufügen**.
   Das Dialogfeld **Zutrittskontrollsystem hinzufügen** wird angezeigt.

Hinweis: Wenn ein Zutrittskontrollsystem hinzugefügt wird, werden die konfigurierten Türen, Leser, Eingänge und Relais im Gerätebaum auf der Seite **Karten und Struktur** aufgelistet.

Dialogfeld Zutrittskontrollsystem hinzufügen

Hostname / HTTPS Port
Geben Sie den Host-Name des Geräts ein. Ändern Sie bei Bedarf die Port-Nummer.

Benutzername
Zeigt den Benutzernamen für die Authentifizierung auf dem Gerät an.

Passwort
Geben Sie ein gültiges Passwort für die Authentifizierung beim Gerät ein.

So testen Sie die Verbindung:

1. Klicken Sie auf „Verbinden“.
   Der BVMS Configuration Client versucht, eine Verbindung mit dem Zutrittskontrollsystem herzustellen und die relevanten Informationen abzurufen.
2. Klicken Sie auf „OK“.
   Das Zutrittskontrollsystem wird basierend auf den angezeigten Informationen zum System hinzugefügt.

13.19.2 Bearbeiten eines Zutrittskontrollsystems

Hauptfenster > **Geräte** > erweitern > >

So bearbeiten Sie ein Zutrittskontrollsystem:

1. Klicken Sie mit der rechten Maustaste auf .
2. Klicken Sie auf **Zutrittskontrollsystem bearbeiten**.
   Das Dialogfeld **Zutrittskontrollsystem bearbeiten** wird angezeigt.

13.19.3 Seite „Einstellungen“

Hauptfenster > **Geräte** > erweitern > > > Registerkarte **Einstellungen**
Dient zum Ändern der Verbindungseinstellungen des Zutrittskontrollsystems.

13.20 Seite „Video Analytics“

Hauptfenster > > **Geräte** > Erweitern Sie >
Ermöglicht Ihnen das Hinzufügen von Videoanalytik , Person Identification (PID) Geräte undTattile LPR Geräte.

13.20.1 Seite „Videoanalyse-Einstellungen“

Hauptfenster > > **Geräte** > erweitern > Erweitern > **Video Analytics** > Seite **Video Analytics-Einstellungen**
Sie können ein Server-basiertes Video Analytics-Gerät hinzufügen.
Die Zugangsdaten und der Installationspfad zur Analytics-Viewer-Anwendung, die für das Videoanalysegerät verwendet wird, müssen verfügbar sein.

Netzwerkadresse
Geben Sie die IP-Adresse des Videoanalysegeräts ein. DNS-Name ist nicht zulässig.

Benutzername
Geben Sie den Benutzernamen ein, wie er im Videoanalysegerät konfiguriert ist.

Passwort
Geben Sie das Passwort ein, wie es im serverbasierten Analysegerät konfiguriert ist.

Analytics Viewer-Pfad
Geben Sie den relativen Pfad des Installationspfades der Analytics-Viewer-Anwendung ein. Der Pfad ist relativ zu `C:\Program Files (x86)\` auf dem Computer, auf dem die Viewer-Anwendung verwendet wird.
Beispiel: Die Analytics-Viewer-Anwendung (`AnalyticsViewer.exe`) ist in folgendem Verzeichnis installiert:

```
C:\Program Files (x86)\VideoAnalytics\
```

Konfigurieren den folgenden Pfad im **Analytics Viewer-Pfad**-Feld:

```
VideoAnalytics\AnalyticsViewer.exe
```

13.20.2 Hinzufügen eines Videoanalysegeräts

Hauptfenster > > **Geräte** > Rechtsklick auf > Befehl **Video Analytics-Gerät hinzufügen** > Dialogfeld **Video Analytics-Gerät hinzufügen**

Beim Hinzufügen eines Server-basierten Analyse-Geräts geben Sie die Zugangsdaten für das neue Gerät ein.

So fügen Sie ein Server-basiertes Analysegerät hinzu:

1. Erweitern Sie , klicken Sie mit der rechten Maustaste auf , und klicken Sie auf **Video Analytics-Gerät hinzufügen**.
   Das Dialogfeld **Video Analytics-Gerät hinzufügen** wird angezeigt.
2. Geben Sie die erforderlichen Werte ein.
3. Klicken Sie auf **OK**.
   Das Gerät wird zu Ihrem System hinzugefügt.

Dialogfeld Video Analytics-Gerät hinzufügen

Netzwerkadresse
Geben Sie die IP-Adresse des Videoanalysegeräts ein. DNS-Name ist nicht zulässig.

Benutzername
Geben Sie den Benutzernamen ein, wie er im Videoanalysegerät konfiguriert ist.

Passwort
Geben Sie das Passwort ein, wie es im serverbasierten Analysegerät konfiguriert ist.

13.20.3 Seite „Person Identification Device“

Hauptfenster > > **Geräte** > erweitern > erweitern > Seite Person Identification Devices
Dient zum Hinzufügen eines Person Identification Device. Das Gerät muss verbunden und verfügbar sein. Sie können Kameras zu Ihrem Person Identification Device hinzufügen und Person Identification-Ereignisse und -Alarme konfigurieren.

Personengruppe
Auf der Registerkarte **Personengruppe** können Sie Personengruppen hinzufügen und konfigurieren.

Kameras
Auf der Registerkarte **Kameras** können Sie Kameras zu Ihrem Person Identification Device hinzufügen. Die hinzugefügten Kameras werden in einer Liste angezeigt.
Hinweis: Fügen Sie zunächst die entsprechenden Kameras zum Logischen Baum hinzu.

13.20.4 Hinzufügen eines Person Identification Device (PID)

Hinweis!
Bei einem Ausfall des Management Server müssen Sie die BVMS-Konfiguration und das Zertifikat Bosch VMS CA wiederherstellen. Anderenfalls können Sie ein vorhandenes PID nicht ohne Zurücksetzen verwenden, wodurch alle gespeicherten Personen gelöscht werden.
Es wird empfohlen, eine Sicherungskopie der BVMS-Konfiguration und des Zertifikats Bosch VMS CA zu erstellen.

Stellen Sie beim Hinzufügen eines Person Identification Device sicher, dass das im Dialogfeld **Person Identification Device hinzufügen** angezeigte Zertifikat dem PID entspricht, das Sie hinzufügen möchten.
Ab BVMS 10.1 können mehrere Person Identification Devices (PIDs) hinzugefügt werden.

Das erste hinzugefügte PID ist das führende Gerät, das mit dem BVMS System verbunden ist. Dieses erste PID stellt die Verbindung zu den anderen PIDs her und die Personendatenbank wird darauf gespeichert.
Hinweis: Bevor Sie das erste PID löschen können, müssen Sie erst alle anderen konfigurierten PIDs löschen.

So fügen Sie ein Person Identification Device hinzu:

1. Erweitern Sie .
2. Klicken Sie mit der rechten Maustaste auf .
3. Klicken Sie auf **Person Identification Device hinzufügen**.
   Das Dialogfeld **Person Identification Device hinzufügen** wird angezeigt.
4. Geben Sie die erforderlichen Werte ein.
5. Klicken Sie auf **Zertifikat anzeigen...**, um zu überprüfen, ob das Zertifikat dem PID entspricht.
6. Klicken Sie zum Bestätigen auf **OK**.
7. Klicken Sie auf **OK**.
   Das Gerät wird zu Ihrem System hinzugefügt.

Dialogfeld Person Identification Device hinzufügen

Netzwerkadresse
Geben Sie die IP-Adresse des Geräts ein.

Port-Nummer
Geben Sie die Port-Nummer des Geräts ein.

Siehe
- *Wiederherstellung des PID-Zugriffs nach Ausfall eines BVMS Management Servers, Seite 166*
- *So exportieren Sie Konfigurationsdaten:, Seite 94*

13.20.5 Seite „PID“

Hauptfenster > **Geräte** > erweitern > erweitern > Person Identification Devices > Seite PID

Verbindung
Auf der Registerkarte **Verbindung** werden die Netzwerkadresse und Port-Nummer Ihres Person Identification Device angezeigt. Die Verbindungseinstellungen eines Person Identification Device sind schreibgeschützt.

13.20.6 Wiederherstellung des PID-Zugriffs nach Ausfall eines BVMS Management Servers

Hinweis!
Bei einem Ausfall des Management Server müssen Sie die BVMS-Konfiguration und das Zertifikat Bosch VMS CA wiederherstellen. Anderenfalls können Sie ein vorhandenes PID nicht ohne Zurücksetzen verwenden, wodurch alle gespeicherten Personen gelöscht werden.
Es wird empfohlen, eine Sicherungskopie der BVMS-Konfiguration und des Zertifikats Bosch VMS CA zu erstellen.

Weitere Informationen zum Speichern der BVMS-Konfiguration finden Sie unter *So exportieren Sie Konfigurationsdaten:, Seite 77*. Zertifikate werden außerhalb von BVMS in der Windows-Anwendung **Computerzertifikate verwalten** verwaltet.

Hinweis!
Zertifikate enthalten vertrauliche Informationen. Schützen Sie sie wie folgt:
– Legen Sie ein starkes Passwort fest.
– Speichern Sie das Zertifikat in einem geschützten Bereich, z. B. auf einem nicht öffentlichen Server.
– Stellen Sie sicher, dass nur autorisierte Personen auf das Zertifikat zugreifen können.

So erstellen Sie eine Sicherung des Zertifikats Bosch VMS CA:

1. Öffnen Sie die Windows-Anwendung **Computerzertifikate verwalten**.
2. Wählen Sie im Ordner **Vertrauenswürdige Stammzertifizierungsstellen** das Zertifikat Bosch VMS CA aus.
3. Exportieren Sie das Zertifikat mit dem privaten Schlüssel, indem Sie **Ja, privaten Schlüssel exportieren** auswählen.
4. Verwenden Sie das Format „Privater Informationsaustausch“.
5. Legen Sie ein starkes Passwort fest.
6. Speichern Sie das Zertifikat als PFX-Datei.

So stellen Sie den Zugriff auf das PID von einem neu installierten BVMS Management Server wieder her:

1. Öffnen Sie die Windows-Anwendung **Computerzertifikate verwalten**.
2. Importieren Sie die PFX-Datei, die das Zertifikat Bosch VMS CA enthält, in den Ordner **Vertrauenswürdige Stammzertifizierungsstellen** des neuen Management Server. Schließen Sie alle erweiterten Eigenschaften ein.
3. Importieren Sie die BVMS Konfigurationssicherung.

Siehe

– *Exportieren von Konfigurationsdaten, Seite 94*

13.20.7 Hinzufügen von Kameras zu einem Person Identification Device (PID)

Sie können Kameras zu Ihrem Person Identification Device hinzufügen, wenn diese bereits zum Logischen Baum hinzugefügt wurden.

So fügen Sie Kameras zu einem Person Identification Device hinzu:

1. Erweitern Sie .
2. Erweitern Sie .
3. Klicken Sie auf .
4. Klicken Sie auf die Registerkarte **Kameras**.
5. Ziehen Sie die entsprechenden Kameras vom Fenster **Logischer Baum** in das Fenster **Kameras**.
   oder
   Doppelklicken Sie auf die entsprechenden Kameras im Fenster **Logischer Baum**.
   Die Kameras werden zu Ihrem Person Identification Device hinzugefügt und in der Liste **Kameras** angezeigt.

13.20.8 Konfigurieren von Kameraparametern für Person Identification-Alarme

Sie können für jede verfügbare Kamera die Kameraparameter für Person Identification-Alarme konfigurieren, um Fehlalarme zu reduzieren.

Kameraparameter

Name	Wertinformationen	Beschreibung
Schwellenwert Wahrscheinlichkeit (%)	Standard: 55 % Minimum: 0 % Maximum: 100 %	Die minimale Wahrscheinlichkeit der positiven Identifikation eines Gesichts, um ein Person Identification-Ereignis zu generieren.
Gesichtsgröße (%)	Standard: 7,5 % Minimum: 5 % Maximum: 100 %	Die Mindestgröße eines zu erkennenden Gesichts im Vergleich zur Größe des gesamten Videobilds.
Min. Bildanzahl	Standard: 4 Minimum: 1	Die Mindestanzahl aufeinander folgender Videobilder, in denen ein Gesicht erscheinen muss, um erkannt zu werden.
Zu analysierende Frames (%)	Standard: 100 % Minimum: 10 % Maximum: 100 %	Der Prozentsatz der Frames, die zur Identifikation von Personen analysiert werden. Ein Wert von 50 % bedeutet, dass jeder zweite Frame analysiert wird.

13.20.9 Konfigurieren von Personengruppen

Hauptfenster > > **Geräte** > Erweitern Sie >

So konfigurieren Sie Personengruppen:

1. Öffnen Sie die Registerkarte **Personengruppe**.
2. Klicken Sie auf , um eine neue Personengruppe hinzuzufügen.
3. Geben Sie die erforderlichen Werte ein.
4. Klicken Sie auf , um eine Personengruppe zu löschen.

Hinweis!

Sie können die Werte der Standardgruppe nicht löschen oder ändern.

Tabelle „Personengruppen“

Personengruppe	Geben Sie den Namen der Personengruppe ein.
Alarmfarbe	Doppelklicken Sie, um die Alarmfarbe auszuwählen.
Alarmtitel	Geben Sie den Titel des Alarms ein, der im Operator Client angezeigt wird.

So ändern Sie die Werte der Tabelle „Personengruppen“:

1. Doppelklicken Sie in das entsprechende Tabellenfeld.
2. Ändern Sie den Wert.

Alarmpriorität

Sie können die Alarmpriorität für Person Identification-Alarme auf der Seite **Alarme** festlegen.

Hinweis!
Sie können verschiedene Alarmprioritäten für jede Kamera der entsprechenden Personengruppe festlegen.
Sie können auch die Alarmpriorität der Standard-Personengruppe ändern.

Siehe

– *Seite Alarme, Seite 315*

13.20.10 Hinzufügen eines Tattile LPR-Geräts

Hauptfenster > > **Geräte** > Erweitern Sie > >

Tattile LPR Geräte identifizieren und erkennen Nummernschilder. Sie können LPR-Ereignisse und -Alarme entsprechend konfigurieren.
Wenn die Tattile LPRGerät bestimmte Kfz-Kennzeichen erkennen soll, müssen Sie zunächst eine Liste der relevanten Kfz-Kennzeichen direkt in der Tattile LPR Gerät. Ausführliche Informationen finden Sie in der Benutzerdokumentation des Geräts.

Hinweis!
Das Gerät muss verbunden und verfügbar sein.
BVMS stellt nur dann eine Verbindung her, wenn die Authentifizierung auf dem Tattile LPR Gerät, Benutzername und Kennwort sind angegeben. Benutzername und Passwort dürfen nicht leer sein.

Zum Hinzufügen einer Tattile LPR Gerät:

1. Klicken Sie mit der rechten Maustaste auf .
2. Klicken Sie auf **Tattile LPR-Gerät hinzufügen**.
   Das Dialogfeld **Tattile LPR-Gerät hinzufügen** wird angezeigt.
3. Geben Sie die erforderlichen Werte ein.
4. Klicken Sie auf **Authentifizieren**.
5. Klicken Sie auf **OK**.
   Das Gerät wird zu Ihrem System hinzugefügt.

Hinweis!
Sie müssen die IP-Adresse des BVMS Management Server in der LPR-Gerätekonfiguration angeben. Anderenfalls ruft das BVMS-System keine Ereignisse von diesem LPR-Gerät ab.

Dialogfeld Tattile LPR-Gerät hinzufügen

Netzwerkadresse
Geben Sie die IP-Adresse des Geräts ein.

Port-Nummer
Geben Sie die Port-Nummer des Geräts ein.

Benutzername
Geben Sie den gültigen Benutzernamen für die Authentifizierung auf dem Gerät ein.

Passwort
Geben Sie ein gültiges Passwort für die Authentifizierung beim Gerät ein.

Authentifizieren
Klicken Sie hier, um sich mit den oben eingegebenen Anmeldeinformationen auf dem Gerät zu authentifizieren.

13.21 Seite VRM-Geräte

Hauptfenster > **Geräte** > erweitern >
Dient zum Hinzufügen und Konfigurieren von VRM Geräten. Für ein VRM Gerät sind mindestens ein Encoder, ein iSCSI-Gerät, eine dem iSCSI-Gerät zugeordnete LUN und ein Speicherpool erforderlich. Aktuelle Firmware-Versionen finden Sie in den Release-Hinweisen und dem Datenblatt.

Hinweis!
Wenn Sie dem BVMS ein iSCSI-Gerät mit Encodern hinzugefügt haben, müssen Sie diesem iSCSI-Gerät die IQN der einzelnen Encoder hinzufügen (gültig für bestimmte iSCSI-Gerätetypen).
Weitere Informationen finden Sie unter *Konfigurieren eines iSCSI-Geräts, Seite 194*.

Hinweis!
Stellen Sie sicher, dass die Systemzeit des VRM-Computers mit der des Management Server synchronisiert ist. Andernfalls können Aufzeichnungen verloren gehen.
Konfigurieren Sie die Zeitserver-Software auf dem Management Server. Konfigurieren Sie auf dem VRM-Computer die IP-Adresse des Management Server als Zeitserver. Gehen Sie dabei gemäß der Standardvorgehensweise in Windows vor.

Siehe
- *Konfigurieren von Multicast, Seite 236*
- *Synchronisieren der BVMS Konfiguration, Seite 180*
- *Seite VRM-Einstellungen, Seite 174*
- *Seite „Pool“, Seite 180*
- *Seite iSCSI-Gerät, Seite 190*
- *Passwort für ein VRM-Gerät ändern, Seite 176*

13.21.1 Hinzufügen eines VRM-Geräts per Suchvorgang

Hauptfenster > **Geräte** >
Im Netzwerk benötigen Sie einen auf einem Computer ausgeführten VRM-Dienst sowie ein iSCSI-Gerät.

Hinweis!
Wenn Sie ein iSCSI-Gerät hinzufügen, für das keine Ziele und LUNs konfiguriert sind, starten Sie eine Standardkonfiguration und fügen Sie dem iSCSI-Gerät den IQN der einzelnen Encoder hinzu.
Wenn Sie ein iSCSI-Gerät hinzufügen, für das Ziele und LUNs vorkonfiguriert sind, fügen Sie diesem iSCSI-Gerät den IQN der einzelnen Encoder hinzu.
Weitere Informationen finden Sie unter *Konfigurieren eines iSCSI-Geräts, Seite 194*.

So fügen Sie VRM-Geräte per Suchvorgang hinzu:

1. Klicken Sie mit der rechten Maustaste auf und klicken Sie auf **Nach VRM-Geräten scannen**.
   Das Dialogfeld **BVMS Scan Wizard** wird angezeigt.
2. Aktivieren Sie die Kontrollkästchen der Geräte, die hinzugefügt werden sollen.
3. Wählen Sie in der Liste **Rolle** die gewünschte Rolle aus.
   Die Auswahlmöglichkeit der neuen Rolle hängt vom aktuellen Typ des VRM-Geräts ab.
   Wenn Sie **Gespiegelt** oder **Failover** wählen, ist zusätzlich der nächste Konfigurationsschritt erforderlich.
4. Wählen Sie in der Liste **Rolle** die gewünschte Rolle aus.
   Welche neue Rolle Sie auswählen können, hängt vom aktuellen Typ des VRM-Geräts ab.
5. Klicken Sie auf **Weiter >>**.
6. Wählen Sie aus der Liste **Master-VRM** den Master-VRM für den ausgewählten gespiegelten oder Failover-VRM.
7. Klicken Sie auf **Weiter >>**.
   Das Dialogfeld des Assistenten für die **Authentifizierung der Geräte** wird angezeigt.
8. Geben Sie das Passwort für jedes Gerät ein, das von einem Passwort geschützt ist.
   Passwortüberprüfungen erfolgen automatisch, wenn Sie während ein paar Sekunden keine weiteren Zeichen im Passwortfeld eingeben oder außerhalb des Passwortfelds klicken.
   Wenn die Passwörter aller Geräte identisch sind, können Sie es im ersten Feld **Passwort** eingeben. Klicken Sie mit der rechten Maustaste auf das Feld und klicken Sie auf **Zellinhalt in Spalte kopieren**.
   In der Spalte **Status** wird die erfolgreiche Anmeldung mit angezeigt.
   Fehlgeschlagene Anmeldungen werden mithilfe von angezeigt.
9. Klicken Sie auf **Fertig stellen**.
   Das Gerät wird zum Gerätebaum hinzugefügt.

Hinweis: Standardmäßig werden alle VRM-Geräte mit sicherer Verbindung hinzugefügt.

So ändern Sie eine sichere/unsichere Verbindung:

1. Klicken Sie mit der rechten Maustaste auf .
2. Klicken Sie auf **VRM-Gerät bearbeiten**.
   Das Dialogfeld **VRM-Gerät bearbeiten** wird angezeigt.
3. Aktivieren Sie das Kontrollkästchen **Sichere Verbindung**.
   Der verwendete Port wird automatisch zum HTTPS-Port geändert.
   oder
   Deaktivieren Sie das Kontrollkästchen **Sichere Verbindung**.
   Der verwendete Port wird automatisch zum rcpp-Port geändert.

Siehe

- *Hinzufügen eines Geräts, Seite 126*
- *Seite VRM-Geräte, Seite 170*
- *Konfigurieren eines iSCSI-Geräts, Seite 194*
- *Duale/Failover-Aufzeichnung, Seite 31*

13.21.2 Manuelles Hinzufügen eines primären oder sekundären VRMs

Hauptfenster > **Geräte** > Rechtsklick auf > Klick auf **VRM hinzufügen** > Dialogfeld **VRM hinzufügen**

Ermöglicht das Hinzufügen eines VRM-Geräts. Sie können den Gerätetyp auswählen und die Zugangsdaten eingeben.

Sie können einen Failover-VRM einem Master-VRM nur dann hinzufügen, wenn beide online sind und beide erfolgreich authentifiziert wurden. Die Passwörter werden dann synchronisiert.

Wenn Ihnen die IP-Adresse und das Passwort bekannt sind, können Sie ein primäres VRM-Gerät manuell hinzufügen.

So fügen Sie ein primäres VRM-Gerät hinzu:

1. Nehmen Sie die erforderlichen Einstellungen für das VRM-Gerät vor.
2. Wählen Sie aus der Liste **Typ** den Eintrag **Primär** aus.
3. Klicken Sie auf **OK**.

Das VRM-Gerät wird hinzugefügt.

Wenn Ihnen die IP-Adresse und das Passwort bekannt sind, können Sie ein sekundäres VRM-Gerät manuell hinzufügen.

Hinweis!
Zur Konfiguration eines Sekundären VRM muss auf dem Computer zunächst die entsprechende Software installiert werden. Führen Sie die Datei Setup.exe aus und wählen Sie **Sekundärer VRM**.

So fügen Sie ein sekundäres VRM-Gerät hinzu:

1. Nehmen Sie die erforderlichen Einstellungen für das VRM-Gerät vor.
2. Wählen Sie aus der Liste **Typ** den Eintrag **Sekundär** aus.
3. Klicken Sie auf **OK**.

Das VRM-Gerät wird hinzugefügt.

Nun können Sie den sekundären VRM wie einen primären VRM konfigurieren.

Dialogfeld VRM hinzufügen

Name

Geben Sie einen Anzeigenamen für das Gerät ein.

Netzwerkadresse / Port

Geben Sie die IP-Adresse des Geräts ein.

Wenn das Kontrollkästchen **Sichere Verbindung** aktiviert ist, wird der Port automatisch zum HTTPS-Port geändert.

Sie können die Port-Nummer ändern, wenn keine Standardports verwendet werden.

Typ

Wählen Sie den gewünschten Gerätetyp aus.

Benutzername

Geben Sie zur Authentifizierung einen Benutzernamen ein.

Passwort
Geben Sie zur Authentifizierung das Passwort ein.

Passwort anzeigen
Klicken Sie hier, um das Passwort sichtbar zu machen.

Sicherheit
Das Kontrollkästchen **Sichere Verbindung** ist standardmäßig aktiviert, wenn HTTPS unterstützt wird.

Hinweis!
Wenn Sie zu BVMS Version 10.0 und höher migrieren, ist das Kontrollkästchen **Sichere Verbindung** nicht standardmäßig aktiviert und die Verbindung ist unsicher (rcpp).

Verwenden Sie zum Ändern einer sicheren oder unsicheren Verbindung den Befehl **VRM-Gerät bearbeiten** und aktivieren oder deaktivieren Sie das Kontrollkästchen **Sichere Verbindung**.

Test
Klicken Sie hier, um zu überprüfen, ob das Gerät verbunden ist und die Authentifizierung erfolgreich war.

Eigenschaften
Ändern Sie bei Bedarf die Port-Nummern für den HTTP- und den HTTPS-Port. Dies ist nur möglich, wenn Sie einen VRM, der nicht verbunden ist, hinzufügen oder bearbeiten. Ist der VRM verbunden, werden die Werte abgerufen, und Sie können diese nicht ändern.
Sofern zutreffend, zeigt die **Master-VRM**-Tabellenzeile das ausgewählte Gerät.

Siehe
- *Bearbeiten eines VRM-Geräts, Seite 173*
- *Manuelles Hinzufügen eines gespiegelten VRM, Seite 177*
- *Manuelles Hinzufügen eines Failover-VRM, Seite 177*

13.21.3 Bearbeiten eines VRM-Geräts

Hauptfenster > **Geräte**
Ermöglicht das Bearbeiten eines VRM-Geräts.

So ändern Sie eine sichere/unsichere Verbindung:

1. Klicken Sie mit der rechten Maustaste auf .
2. Klicken Sie auf **VRM-Gerät bearbeiten**.
   Das Dialogfeld **VRM-Gerät bearbeiten** wird angezeigt.
3. Aktivieren Sie das Kontrollkästchen **Sichere Verbindung**.
   Der verwendete Port wird automatisch zum HTTPS-Port geändert.
   oder
   Deaktivieren Sie das Kontrollkästchen **Sichere Verbindung**.
   Der verwendete Port wird automatisch zum rcpp-Port geändert.

Hinweis!
Nach dem Upgrade auf eine neuere Version wird empfohlen, zu einer sicheren Verbindung zu wechseln.

Ausführliche Informationen zum Parameter des Dialogfelds **VRM-Gerät bearbeiten** finden Sie im Kapitel „Manuelles Hinzufügen eines primären oder sekundären VRMs“.

Siehe

– *Manuelles Hinzufügen eines primären oder sekundären VRMs, Seite 172*

13.21.4 Seite VRM-Einstellungen

Hauptfenster > **Geräte** > erweitern > > **Haupteinstellungen** > **VRM-Einstellungen**

Server-Initiatorname
Zeigt den iSCSI-Initiatornamen des VRM Server an.

13.21.5 Seite SNMP

Hauptfenster > **Geräte** > erweitern > erweitern > **Netzwerk** > **SNMP**

1. SNMP-Zieladresse 2. SNMP-Zieladresse
VRM unterstützt SNMP (Simple Network Management Protocol) zum Verwalten und Überwachen von Netzwerkkomponenten und kann SNMP-Nachrichten (Traps) an IP-Adressen senden. Diese Einheit unterstützt SNMP MIB II im Einheitscode. Wenn SNMP-Traps gesendet werden sollen, geben Sie hier die IP-Adressen von einem oder zwei Zielgeräten ein.
Manche Ereignisse werden nur als SNMP-Traps gesendet. Eine Beschreibung finden Sie in der MIB-Datei.

13.21.6 Seite „Konten“

Um das Posting von Bildern zu konfigurieren und Videos im MP4-Dateiformat zu exportieren, müssen Sie ein Konto erstellen, in dem die Bilder gespeichert werden und für den Zugriff bereitstehen. Sie können maximal vier Konten erstellen.

Typ
Wählen Sie den Kontentyp aus: **FTP** oder **Dropbox**.

IP-Adresse
Geben Sie die IP-Adresse des Servers ein, auf dem die Bilder gespeichert werden sollen.

Benutzername
Geben Sie den Benutzernamen für den Server ein.

Passwort
Geben Sie das Passwort für den Zugriff auf den Server ein. Um das Passwort zu überprüfen, klicken Sie rechts auf **Prüfen**.

Prüfen
Klicken Sie darauf, um das Passwort zu überprüfen.

Pfad
Geben Sie den genauen Pfad für die Speicherung der Bilder und Videos auf dem Server ein.

13.21.7 Seite Erweitert

Hauptfenster > **Geräte** > erweitern > erweitern > **Service** > **Erweitert**

RCP+-Protokollierung / Debug-Protokollierung / Wiedergabe-Protokollierung / VDP-Protokollierung / Leistungs-Protokollierung
Aktivieren Sie die verschiedenen Protokolle für den VRM Server und den Configuration Manager.
Die Protokolldateien für VRM Server werden auf dem Computer gespeichert, auf dem VRM Server gestartet wurde. Sie können mit VRM Monitor angezeigt oder heruntergeladen werden.
Die Protokolldateien für Configuration Manager werden lokal in folgendem Verzeichnis gespeichert:

%USERPROFILE%\My Documents\Bosch\Video Recording Manager\Log

Speicherzeit (Tage)
Legen Sie die Speicherzeit für die Protokolldateien in Tagen fest.

Kompletter Hauptspeicherauszug
Aktivieren Sie dieses Kontrollkästchen nur bei Bedarf, beispielsweise wenn der technische Kundendienst eine vollständige Hauptspeicherübersicht anfordert.

Telnet-Unterstützung
Aktivieren Sie dieses Kontrollkästchen, wenn Zugriffe über das Telnet-Protokoll unterstützt werden sollen. Aktivieren Sie dieses Kontrollkästchen nur bei Bedarf.

Hinweis!
Die umfassende Protokollierung benötigt erhebliche Prozessorleistung und Festplattenkapazität. Verwenden Sie die umfassende Protokollierung nicht im Dauerbetrieb.

13.21.8 Verschlüsseln der Aufzeichnung für VRM

Die verschlüsselte Aufzeichnung für VRM-Encoder ist nicht standardmäßig aktiviert.
Sie müssen die verschlüsselte Aufzeichnung für den primären und sekundären VRM separat aktivieren.

Hinweis!
Sie müssen einen Redundanzschlüssel (Zertifikatsicherung) erstellen, bevor Sie die verschlüsselte Aufzeichnung zum ersten Mal aktivieren. Sie müssen für jedes VRM-Gerät nur einmal einen Redundanzschlüssel erstellen.
Falls der reguläre Verschlüsselungsschlüssel verloren geht, können Sie die Aufzeichnungen mit dem Redundanzschlüssel entschlüsseln.

Es wird empfohlen, eine Kopie des Redundanzschlüssels an einem sicheren Ort aufzubewahren (z. B. in einem Tresor).

So erstellen Sie einen Redundanzschlüssel:
1. Wählen Sie das gewünschte VRM-Gerät aus.
2. Öffnen Sie die Registerkarte **Service**.
3. Öffnen Sie die Registerkarte **Aufzeichnungs-Verschlüsselung**.
4. Klicken Sie auf **Redundanzschlüssel**.
5. Wählen Sie den Zertifikatspeicherort aus.
6. Geben Sie ein Passwort ein, das den Komplexitätsvoraussetzungen für Passwörter entspricht, und bestätigen Sie es.
7. Klicken Sie auf **Erstellen**.
   Der Redundanzschlüssel (Zertifikatsicherung) wird erstellt.

So aktivieren/deaktivieren Sie die verschlüsselte Aufzeichnung:
1. Wählen Sie das gewünschte VRM-Gerät aus.
2. Öffnen Sie die Registerkarte **Service**.
3. Öffnen Sie die Registerkarte **Aufzeichnungs-Verschlüsselung**.
4. Aktivieren/Deaktivieren Sie das Kontrollkästchen **Verschlüsselte Aufzeichnung aktivieren**.
5. Klicken Sie auf .

Hinweis: Die Verschlüsselung wird erst nach der nächsten Blockänderung aktiviert. Dies kann eine Weile dauern.
Vergewissern Sie sich, dass die Encoder die Verschlüsselung vornehmen.

So überprüfen Sie die Verschlüsselung durch die VRM-Encoder:

1. Wählen Sie das gewünschte VRM-Gerät aus.
2. Öffnen Sie die Registerkarte **Service**.
3. Öffnen Sie die Registerkarte **Aufzeichnungs-Verschlüsselung**.

Hinweis: Siehe auch Registerkarte **Überwachung** des VRM Monitor.

Hinweis!
Alle VRM-Encoder, die die Verschlüsselung unterstützen, verschlüsseln die Aufzeichnung automatisch, nachdem die Verschlüsselung in VRM aktiviert wurde.
Die Verschlüsselung kann für einen einzelnen Encoder deaktiviert werden.
VSG-Encoder werden immer verschlüsselt, wenn die Verschlüsselung in VRM aktiviert ist.

So aktivieren/deaktivieren Sie die verschlüsselte Aufzeichnung für einen einzelnen VRM-Encoder:

1. Wählen Sie den gewünschten VRM-Encoder.
2. Öffnen Sie die Registerkarte **Aufzeichnung**.
3. Öffnen Sie die Registerkarte **Aufzeichnungsverwaltung**.
4. Aktivieren/deaktivieren Sie das Kontrollkästchen **Verschlüsselung**.
5. Klicken Sie auf .

13.21.9 Passwort für ein VRM-Gerät ändern

Hauptfenster > **Geräte** > erweitern >

So ändern Sie das Passwort:

1. Klicken Sie mit der rechten Maustaste auf und klicken Sie dann auf **VRM-Passwort ändern**.
   Das Dialogfeld **Passwort ändern** wird angezeigt.
2. Geben Sie im Feld **Altes Passwort** das entsprechende Passwort ein.
3. Geben Sie im Feld **Neues Passwort** das neue Passwort ein, klicken Sie und wiederholen Sie die Eingabe im zweiten Feld **Neues Passwort**.

Klicken Sie auf **OK**.

- Bestätigen Sie das nächste Dialogfeld.

⇨ Das Passwort wird auf dem Gerät umgehend geändert.

13.21.10 Hinzufügen eines VRM-Pools

Hauptfenster > **Geräte** > erweitern

Um einen VRM-Pool hinzuzufügen:

- Klicken Sie mit der rechten Maustaste auf oder und klicken Sie dann auf **Pool hinzufügen**.
  Ein neuer Pool wird dem System hinzugefügt.

Siehe

– *iSCSI-Speicherpool, Seite 190*

13.21.11 Manuelles Hinzufügen eines Failover-VRM

Hauptfenster > **Geräte** > erweitern > Rechtsklick auf > Klick auf **Failover-VRM hinzufügen** > Dialogfeld **Failover-VRM hinzufügen**

Hinweis!
Zur Konfiguration eines Sekundären VRM muss auf dem Computer zunächst die entsprechende Software installiert werden. Führen Sie die Datei Setup.exe aus und wählen Sie **Sekundärer VRM**.

Es kann entweder ein Primärer VRM oder ein Sekundärer VRM die Rolle eines Failover-VRM übernehmen. Sie können einen Primären Failover-VRM einem Primären VRM hinzufügen, oder Sie fügen einen Sekundären Failover-VRM einem Sekundären VRM hinzu.
Wenn Ihnen die IP-Adresse und das Passwort bekannt sind, können Sie ein Failover-VRM-Gerät manuell hinzufügen. Der zuerst gewählte VRM stellt den Master-VRM für diesen Failover-VRM dar.
Sie können ein Failover-VRM-Gerät hinzufügen. Sie können es entweder manuell hinzufügen oder ein Gerät aus der Liste der gefundenen VRM-Geräte auswählen.
Sie können einen Failover-VRM einem Master-VRM nur dann hinzufügen, wenn beide online sind und beide erfolgreich authentifiziert wurden. Die Passwörter werden dann synchronisiert.

So fügen Sie ein Failover-VRM-Gerät hinzu:

1. Nehmen Sie die erforderlichen Einstellungen für das VRM-Gerät vor.
2. Stellen Sie sicher, dass der richtige Master-VRM ausgewählt wurde. Ist dies nicht der Fall, brechen Sie den Vorgang ab.
3. Klicken Sie auf **OK**.

⇨ Das Failover-VRM-Gerät wird zum ausgewählten Master-VRM hinzugefügt.

Dialogfeld Failover-VRM hinzufügen

Netzwerkadresse
Geben Sie die IP-Adresse des Geräts ein oder wählen Sie eine Netzwerkadresse aus der Liste **Gefundene VRMs**.

Gefundene VRMs
Zeigt die Liste der gefundenen VRM-Computer an. Um den Suchvorgang zu wiederholen, schließen Sie das Dialogfeld und lassen sich das Dialogfeld erneut anzeigen.

Hinweis!
Das Failover-VRM-Gerät übernimmt die Einstellungen, die im Master-VRM konfiguriert sind. Wenn die Einstellungen des Master-VRM geändert werden, werden die Einstellungen des Failover-VRM-Geräts entsprechend geändert.

Siehe

– *Duale/Failover-Aufzeichnung, Seite 31*

13.21.12 Manuelles Hinzufügen eines gespiegelten VRM

Hauptfenster > **Geräte** > erweitern > Rechtsklick auf > Klick auf **Gespiegelten VRM hinzufügen** > Dialogfeld **VRM hinzufügen**

Hinweis!
Zur Konfiguration eines Sekundären VRM muss auf dem Computer zunächst die entsprechende Software installiert werden. Führen Sie die Datei Setup.exe aus und wählen Sie **Sekundärer VRM**.

Nur ein sekundärer VRM kann die Rolle eines gespiegelten VRM übernehmen. Fügen Sie einen gespiegelten VRM einem Primären VRM hinzu.
Wenn Ihnen die IP-Adresse und das Passwort bekannt sind, können Sie ein gespiegeltes VRM-Gerät manuell hinzufügen. Der zuerst gewählte VRM stellt den Master VRM für diesen Gespiegelten VRM dar.

So fügen Sie ein gespiegeltes VRM-Gerät hinzu:

1. Nehmen Sie die erforderlichen Einstellungen für das VRM-Gerät vor.
2. Stellen Sie sicher, dass der richtige Master-VRM ausgewählt wurde. Ist dies nicht der Fall, brechen Sie den Vorgang ab.
3. Klicken Sie auf **OK**.

Das Gespiegelte VRM-Gerät wird dem ausgewählten Primären VRM hinzugefügt.

Dialogfeld VRM hinzufügen

Name
Geben Sie einen Anzeigenamen für das Gerät ein.

Netzwerkadresse / Port
Geben Sie die IP-Adresse des Geräts ein.
Wenn das Kontrollkästchen **Sichere Verbindung** aktiviert ist, wird der Port automatisch zum HTTPS-Port geändert.
Sie können die Port-Nummer ändern, wenn keine Standardports verwendet werden.

Typ
Wählen Sie den gewünschten Gerätetyp aus.

Benutzername
Geben Sie zur Authentifizierung einen Benutzernamen ein.

Passwort anzeigen
Klicken Sie hier, um das Passwort sichtbar zu machen.

Passwort
Geben Sie zur Authentifizierung das Passwort ein.

Sicherheit
Das Kontrollkästchen **Sichere Verbindung** ist standardmäßig aktiviert, wenn HTTPS unterstützt wird.

Hinweis!
Wenn Sie zu BVMS Version 10.0 und höher migrieren, ist das Kontrollkästchen **Sichere Verbindung** nicht standardmäßig aktiviert und die Verbindung ist unsicher (rcpp).

Verwenden Sie zum Ändern einer sicheren oder unsicheren Verbindung den Befehl **VRM-Gerät bearbeiten** und aktivieren oder deaktivieren Sie das Kontrollkästchen **Sichere Verbindung**.

Test
Klicken Sie hier, um zu überprüfen, ob das Gerät verbunden ist und die Authentifizierung erfolgreich war.

Eigenschaften
Ändern Sie bei Bedarf die Port-Nummern für den HTTP- und den HTTPS-Port. Dies ist nur möglich, wenn Sie einen VRM, der nicht verbunden ist, hinzufügen oder bearbeiten. Ist der VRM verbunden, werden die Werte abgerufen, und Sie können diese nicht ändern.
Sofern zutreffend, zeigt die **Master-VRM**-Tabellenzeile das ausgewählte Gerät.

Siehe

– *Manuelles Hinzufügen eines primären oder sekundären VRMs, Seite 172*

– *Duale/Failover-Aufzeichnung, Seite 31*

13.21.13 Hinzufügen von Encodern per Suchvorgang

So fügen Sie Encoder per Suchvorgang hinzu:

1. Klicken Sie mit der rechten Maustaste auf und klicken Sie auf **Nach Encodern scannen**.
   Das Dialogfeld **BVMS Scan Wizard** wird angezeigt.
2. Wählen Sie die erforderlichen Encoder sowie den gewünschten VRM-Pool aus und klicken Sie auf **Zuordnen**, um diese dem VRM-Pool zuzuweisen.
3. Klicken Sie auf **Weiter >>**.
   Das Dialogfeld des Assistenten für die **Authentifizierung der Geräte** wird angezeigt.
4. Geben Sie das Passwort für jedes Gerät ein, das von einem Passwort geschützt ist.
   Passwortüberprüfungen erfolgen automatisch, wenn Sie während ein paar Sekunden keine weiteren Zeichen im Passwortfeld eingeben oder außerhalb des Passwortfelds klicken.
   Wenn die Passwörter aller Geräte identisch sind, können Sie es im ersten Feld **Passwort** eingeben. Machen Sie mit der Maus einen Rechtsklick und klicke Sie dann auf **Zellinhalt in Spalte kopieren**.
   In der **Status** Spalte wird die erfolgreiche Anmeldung mit angezeigt. Fehlgeschlagene Anmeldungen werden mithilfe von angezeigt.
5. Klicken Sie auf **Fertig stellen**.
   Das Gerät wird zum Gerätebaum hinzugefügt.

Das ⚠ Symbol weist auf einen Fehler hin, um den Sie sich kümmern müssen. In der QuickInfo finden Sie weitere Informationen zu dem jeweiligen Fehler.

13.21.14 Hinzufügen von VSG-Geräten per Suchvorgang

So fügen Sie VSG-Geräte über den Suchvorgang hinzu:

1. Klicken Sie mit der rechten Maustaste auf und klicken Sie auf **Nach Video Streaming Gateways scannen**.
   Das Dialogfeld **BVMS Scan Wizard** wird angezeigt.
2. Wählen Sie die erforderlichen VSG-Geräte und anschließend den gewünschten VRM-Pool aus und klicken Sie auf **Zuordnen**, um diese dem VRM-Pool zuzuweisen.
3. Klicken Sie auf **Weiter >>**.
   Das Dialogfeld des Assistenten für die **Authentifizierung der Geräte** wird angezeigt.
4. Geben Sie das Passwort für jedes Gerät ein, das von einem Passwort geschützt ist.
   Passwortüberprüfungen erfolgen automatisch, wenn Sie während ein paar Sekunden keine weiteren Zeichen im Passwortfeld eingeben oder außerhalb des Passwortfelds klicken.
   Wenn die Passwörter aller Geräte identisch sind, können Sie es im ersten Feld **Passwort** eingeben. Klicken Sie mit der rechten Maustaste auf das Feld und klicken Sie auf **Zellinhalt in Spalte kopieren**.
   In der Spalte **Status** wird die erfolgreiche Anmeldung mit angezeigt.
   Fehlgeschlagene Anmeldungen werden mithilfe von angezeigt.

5. Klicken Sie auf **Fertig stellen**.
   Das Gerät wird zum Gerätebaum hinzugefügt.

13.21.15 Synchronisieren der BVMS Konfiguration

Hauptfenster > **Geräte** > erweitern > Rechtsklick auf > Befehl **BVMS Konfiguration synchronisieren**

Ab BVMS 6.0 wird VRM 3.50 unterstützt. Wenn Sie VRM nicht auf Version 3.50 aktualisieren, wird während der Aktualisierung auf BVMS 6.0 die Aufzeichnung fortgesetzt, aber Sie können die Konfiguration des alten VRM nicht ändern.

Wenn Sie Ihre VRM-Software auf Version 3.50 aktualisiert haben, müssen Sie die BVMS Konfiguration manuell synchronisieren.

13.21.16 Importieren der Konfiguration von VRM

Hauptfenster > **Geräte** > erweitern >

Falls Sie ein primäres VRM -Gerät austauschen müssen, können Sie die Konfiguration des vorherigen primären VRM -Geräts importieren.

Hinweis: Dies ist nur bei primären VRM -Geräten möglich.

Voraussetzung: Es wurde eine Sicherung der vorherigen VRM -Gerätekonfigurationsdatei (config.xml) erstellt. Informationen zum Erstellen einer Sicherung finden Sie unter *Warten von BVMS, Seite 76*.

So importieren Sie die Konfiguration von VRM:

1. Kopieren Sie die gesicherte VRM -Konfigurationsdatei (config.xml) in C:\ProgramData\Bosch\VRM\primary.
2. Klicken Sie mit der rechten Maustaste auf .
3. Wählen Sie **Import der VRM Konfiguration** aus.
   Die Konfiguration des vorherigen VRM wird importiert.

Hinweis!
Es werden nur die Konfigurationen von Encoder, VSG und iSCSI importiert.
Alle weiteren Konfigurationen müssen Sie manuell vornehmen, z. B. das Hinzufügen der erforderlichen Geräte zum **Logischer Baum**, die Konfiguration der Alarme oder der Aufzeichnungseinstellungen.

13.22 Seite „Pool“

Hauptfenster > **Geräte** > erweitern > erweitern >

Ermöglicht das Konfigurieren von Aufzeichnungseinstellungen, die für alle Geräte in diesem Speicherpool gültig sind.

Pool-Identifizierung
Zeigt die Pool-Nummer an.

Modus Aufzeichnungspräferenzen

– **Failover**
  Aufzeichnungen werden nur auf dem Primärziel gespeichert. Ist ein Speichern auf diesem Ziel nicht möglich, werden die Aufzeichnungen auf dem unter „Sekundärziel“ angegebenen Ziel gespeichert.

Eine Ausfallsituation tritt dann ein, wenn das Primärziel keine Speicherblöcke mehr zur Verfügung stellt, z. B. aufgrund von Systemausfall, Netzwerkfehler oder mangelnder verbleibender Kapazität.
Sie können die Liste „Sekundärziel“ leer lassen. In diesem Fall ist kein Failover möglich, aber die Anzahl der erforderlichen iSCSI-Sitzungen verringert sich und es ist kein Speicherplatz auf dem Sekundärziel zugeordnet. Dadurch verringert sich der System-Overhead und die Systemspeicherzeit wird verlängert.
Hinweis: Sie müssen dann das Primär- und Sekundärziel für jede Kamera und jeden Encoder konfigurieren.

– **Automatisch**
Die Lastverteilung wird automatisch konfiguriert. Im Modus **Automatisch** wird automatisch versucht, die Speicherzeit der verfügbaren iSCSI-Targets zu optimieren. Um die Blöcke des zweiten iSCSI-Targets zuzuweisen, wählen Sie in der Liste **Nutzung Zweit-Target** die Option **Ein** aus.

Plausibilitätsprüfungsperiode (Tage)
Geben Sie den erforderlichen Zeitraum ein. Nach diesem Zeitraum analysiert der Video Recording Manager, ob die Speicherverteilung im Modus **Automatisch** noch optimal ist. Andernfalls nimmt Video Recording Manager Änderungen vor.

Nutzung Zweit-Target
Hier können Sie auswählen, ob Blöcke von einem Sekundärziel verteilt werden.
Wählen Sie **Ein** oder **Aus** aus, um die Verwendung eines Sekundärziels ein- oder auszuschalten.

– **Ein**: Wählen Sie **Ein** aus, um ein Sekundärziel zu verwenden, damit die Aufzeichnungslücke bei einem Ausfall des Primärziels reduziert wird. Wenn das Primärziel verfügbar ist, werden die Blöcke auf dem Sekundärziel nicht verwendet, aber der Speicher wird zugewiesen. Diese Redundanz reduziert die Speicherzeit des Systems.
– **Aus**: Wählen Sie **Aus** aus, wenn Sie kein Sekundärziel verwenden möchten. Bei einem Ausfall des Primärziels benötigt Video Recording Manager mehr Zeit für die Neuorganisation. Dies bedeutet, dass die Aufzeichnungslücke größer ist.

Block-Reservierung für Ausfallzeit
Geben Sie die Anzahl der Tage ein, für die die zugeordneten Encoder aufgezeichnet werden, obwohl der VRM Server außer Betrieb ist.
Wenn Sie z. B. 4 eingeben, werden die Encoder bei außer Betrieb befindlichem VRM Server etwa vier Tage lang aufgezeichnet.
Wenn Ihr System mit Encodern mit niedriger Bitrate ausgestattet ist, kann der reservierte Festplattenspeicher erheblich verringert werden. Dadurch wird eine sichere Verteilung der Speicherkapazitäten gewährleistet und die Speicherzeit verlängert.

LUNs größer als 2 TB erlauben
Klicken zur Aktivierung der Verwendung von LUNs, die größer als 2 TB sind.
Folgende Geräte unterstützen keine LUNs größer als 2 TB („große LUNs“):

– VRM-Geräte vor 3.60
– VSG-Geräte mit Firmware-Version älter als 6.30
– Encoder mit Firmware-Version älter als 6.30

BVMS verhindert, dass Sie die folgenden Schritte durchführen:

– Hinzufügen oder Verschieben von Geräten mit einer Firmware-Version älter als 6.30 zu einem Pool, der große LUNs ermöglicht.
– Hinzufügen oder Verschieben von Geräten, die derzeit nicht mit dem Netzwerk verbunden sind, zu einem Pool, der große LUNs ermöglicht.

– Hinzufügen oder Verschieben eines iSCSI-Geräts, das große LUNs enthält, zu einem Pool, der keine großen LUNs zulässt.
– Ermöglichen großer LUNs in einem Pool, der Geräte mit Firmware-Version älter als 6.30 enthält.
– Deaktivieren großer LUNs in einem Pool mit einem iSCSI-Gerät, das große LUNs enthält.

Verschieben Sie Geräte mit einer Firmware-Version älter als 6.30 in einen Pool, der keine großen LUNs zulässt.

Siehe
– *Hinzufügen einer LUN, Seite 198*
– *Hinzufügen eines VRM-Pools, Seite 176*

13.22.1 Konfigurieren des automatischen Aufzeichnungsmodus auf einem Pool

Hauptfenster > **Geräte** > erweitern > erweitern >

Hinweis:
Wenn Sie zuvor einen Failover-Aufzeichnungsmodus konfiguriert haben, wird diese Konfiguration überschrieben.

So führen Sie die Konfiguration durch:

- Wählen Sie aus der **Modus Aufzeichnungspräferenzen**-Liste die **Automatisch**.
  Nach der Aktivierung der Konfiguration des **Automatisch** ist der Aufnahmemodus aktiv. Auf der **Aufzeichnungspräferenzen**-Seite eines Encoders sind die Primär- und Sekundärziel-Liste deaktiviert.

Verwandte Themen
– *Konfigurieren des Failover-Aufzeichnungsmodus auf einem Encoder, Seite 234*

13.22.2 Manuelles Hinzufügen eines Encoders

Hauptfenster > **Geräte** > Erweitern > Erweitern > Rechtsklicken > Klicken **Encoder hinzufügen** > **Encoder hinzufügen** Dialogfeld
oder

Hauptfenster > **Geräte** > Rechtsklicken > Klicken **Encoder hinzufügen** > **Encoder hinzufügen** Dialogfeld
oder

Hauptfenster > **Geräte** > Rechtsklicken > Klicken **Encoder hinzufügen** > **Encoder hinzufügen** Dialogfeld
oder

Hauptfenster > **Geräte** > Erweitern > Rechtsklicken > Klicken **Decoder hinzufügen** > **Encoder hinzufügen** Dialogfeld

Dient zum manuellen Hinzufügen eines Encoders. Dies ist insbesondere dann hilfreich, wenn Sie ein beliebiges Video-IP-Gerät von Bosch hinzufügen möchten (nur für VRM).

Hinweis:
Wenn Sie einen Video-IP-Encoder von Bosch mit der **<Automatisch erkennen>**-Auswahl hinzufügen, muss dieses Gerät im Netzwerk verfügbar sein.

So fügen Sie ein Video IP-Gerät von Bosch hinzu:

1. Erweitern Sie , erweitern Sie , und klicken Sie mit der rechten Maustaste auf .
   Oder
   Klicken Sie mit der rechten Maustaste auf .
   Oder
   Klicken Sie mit der rechten Maustaste auf .
2. Klicken Sie auf **Encoder hinzufügen**.
   Das Dialogfeld **Encoder hinzufügen** wird angezeigt.
3. Geben Sie die entsprechende IP-Adresse ein.
4. Wählen Sie in der Liste **<Automatisch erkennen>** aus, geben Sie das Passwort des Geräts ein, und klicken Sie auf **Authentifizieren.**
   Oder:
   Wählen Sie in der Liste einen konkreten Encoder-Typ oder **<Einzel Platzhalter Kamera>** aus.
5. Klicken Sie auf **OK**.
   Das Gerät wird dem System hinzugefügt.

Das ⚠ Symbol weist auf einen Fehler hin, um den Sie sich kümmern müssen. In der QuickInfo finden Sie weitere Informationen zu dem jeweiligen Fehler.

Dialogfeld Encoder hinzufügen

Netzwerkadresse
Geben Sie eine gültige IP-Adresse ein.

Port-Nummer
Geben Sie die Port-Nummer des Geräts ein.

Encodertyp
Wählen Sie für ein Gerät mit bekanntem Gerätetyp den entsprechenden Eintrag aus. Das Gerät muss nicht im Netzwerk verfügbar sein.
Wenn Sie ein beliebiges Video-IP-Gerät von Bosch hinzufügen möchten, wählen Sie **<Automatisch erkennen>**. Das Gerät muss im Netzwerk verfügbar sein.
Wenn Sie eine Kamera für die Offline-Konfiguration hinzufügen möchten, wählen Sie **<Einzel Platzhalter Kamera>**.

Benutzername
Zeigt den Benutzernamen für die Authentifizierung auf dem Gerät an.

Passwort
Geben Sie ein gültiges Passwort für die Authentifizierung beim Gerät ein.

Passwort anzeigen
Klicken Sie hier, damit das eingegebene Passwort angezeigt wird. Achten Sie darauf, dass niemand das Passwort einsehen kann.

Authentifizieren
Klicken Sie hier, um sich mit den oben eingegebenen Anmeldeinformationen auf dem Gerät zu authentifizieren.

13.22.3 Manuelles Hinzufügen eines iSCSI-Geräts

Hauptfenster > **Geräte** > > erweitern > Rechtsklick auf > **iSCSI-Gerät hinzufügen** > Dialogfeld **iSCSI-Gerät hinzufügen**

Dient zum Hinzufügen eines iSCSI-Geräts zu einem VRM.

So fügen Sie ein iSCSI-Gerät hinzu:

1. Klicken Sie mit der rechten Maustaste auf und klicken Sie anschließend auf **iSCSI-Gerät hinzufügen**.
   Das Dialogfeld **iSCSI-Gerät hinzufügen** wird angezeigt.
2. Geben Sie den gewünschten Anzeigenamen, die Netzwerkadresse des iSCSI-Geräts sowie den Gerätetyp ein, und klicken Sie auf **OK**.
   Das iSCSI-Gerät wird dem ausgewählten VRM-Pool hinzugefügt.
   Falls erforderlich, fügen Sie die Ziele und LUNs hinzu.

Dialogfeld iSCSI-Gerät hinzufügen

Name
Geben Sie einen Anzeigenamen für das Gerät ein.

Netzwerkadresse
Geben Sie eine gültige Netzwerkadresse des Geräts ein.

iSCSI-Gerätetyp
Wählen Sie den gewünschten Gerätetyp aus.

Benutzername
Geben Sie zur Authentifizierung einen Benutzernamen ein.

Passwort
Geben Sie zur Authentifizierung das Passwort ein.

Monitoring aktivieren
Wenn für ein DIVAR IP Gerät der iSCSI-Gerätetyp ausgewählt ist und jede SNMP (Simple Network Management Protocol)-Überwachung für diesen DIVAR IP Gerätetyp unterstützt wird, ist das Kontrollkästchen **Monitoring aktivieren** aktiviert.
Aktivieren Sie das Kontrollkästchen, damit der Systemzustand des DIVAR IP Geräts überwacht wird. BVMS erhält und analysiert nun automatisch SNMP-Traps vom DIVAR IP Gerät und aktiviert Ereignisse und Alarme für die Systemzustandsüberwachung (z. B. CPU, Speicher, Lüfter ...). Standardmäßig werden nur kritische Alarme ausgelöst.
Hinweis: Sie müssen zuerst SNMP auf dem DIVAR IP Gerät konfigurieren.
Hinweis: Diese Einstellung ist nur für unterstützte Geräte verfügbar.
Weitere Informationen zur Konfiguration von SNMP auf einem DIVAR IP Gerät finden Sie in der entsprechenden DIVAR IP Dokumentation.

Verwandte Themen
– *Hinzufügen eines VRM-Geräts per Suchvorgang, Seite 170*

Siehe
– *Seite SNMP, Seite 155*
– *SNMP-Überwachung konfigurieren, Seite 95*

13.22.4 Manuelles Hinzufügen eines Video Streaming Gateway

Hauptfenster > **Geräte** > erweitern >

Sie können ein VSG Gerät einem VRM-Pool zuordnen.

So fügen Sie ein VSG-Gerät manuell hinzu:

1. Klicken Sie mit der rechten Maustaste auf und klicken Sie dann auf **Video Streaming Gateway hinzufügen**.
   Das Dialogfeld **Video Streaming Gateway hinzufügen** wird angezeigt.
2. Nehmen Sie die erforderlichen Einstellungen für das VSG-Gerät vor.
3. Klicken Sie auf **Hinzufügen**.

⇨ Das VSG-Gerät wird dem System hinzugefügt. Die diesem VSG-Gerät zugewiesenen Kameras werden aufgezeichnet.

Dialogfeld Video Streaming Gateway hinzufügen

Machen Sie einen Rechtsklick im > **Video Streaming Gateway hinzufügen** > **Video Streaming Gateway hinzufügen** Dialogfeld

Port-Nummer
Geben Sie die Port-Nummer des Geräts ein.

Benutzername
Geben Sie den Benutzernamen für die Authentifizierung auf dem Gerät ein. In der Regel: service.

Netzwerkadresse / Port
Geben Sie die IP-Adresse des Geräts ein.
Wenn das Kontrollkästchen **Sichere Verbindung** aktiviert ist, wird der Port automatisch zum HTTPS-Port geändert.
Sie können die Port-Nummer ändern, wenn keine Standardports verwendet werden oder die VSG-Instanzen in einer anderen Reihenfolge konfiguriert sind.

Standardports

VSG-Instanz	rcpp-Port	HTTPS-Port
1	8756	8443
2	8757	8444
3	8758	8445
4	8759	8446
5	8760	8447
6	8761	8448
7	8762	8449

Passwort
Geben Sie ein gültiges Passwort für die Authentifizierung auf dem Gerät ein.

Passwort anzeigen
Klicken Sie hier, um das eingegebene Passwort anzuzeigen. Achten Sie darauf, dass niemand das Passwort einsehen kann.

Sicherheit
Das Kontrollkästchen **Sichere Verbindung** ist standardmäßig aktiviert, wenn HTTPS unterstützt wird. Ab VSG Version 7.0 unterstützt VSG sichere Verbindungen.

Hinweis!
Wenn Sie zu BVMS Version 10.0 und höher migrieren, ist das Kontrollkästchen **Sichere Verbindung** nicht standardmäßig aktiviert und die Verbindung ist unsicher (rcpp).

Verwenden Sie zum Ändern einer sicheren oder unsicheren Verbindung den Befehl **Video Streaming Gateway bearbeiten** und aktivieren oder deaktivieren Sie das Kontrollkästchen **Sichere Verbindung**.

Authentifizieren
Klicken Sie hier, um sich mit den oben eingegebenen Anmeldeinformationen beim Gerät zu authentifizieren.

Siehe
– *Bearbeiten eines Video Streaming Gateway, Seite 202*

13.22.5 Manuelles Hinzufügen eines iSCSI-Geräts der DSA E-Series

Hauptfenster > **Geräte** > > Erweitern >
Sie können entweder ein E-Series iSCSI-Gerät hinzufügen, das bereits initialisiert ist, oder Sie fügen ein nicht initialisiertes E-Series iSCSI-Gerät hinzu.
Sie können LUNs größer als 2 TB hinzufügen, wenn der Pool für große LUNs aktiviert ist.
Folgende Geräte unterstützen keine LUNs größer als 2 TB („große LUNs“):
– VRM-Geräte vor 3.60
– VSG-Geräte mit Firmware-Version älter als 6.30
– Encoder mit Firmware-Version älter als 6.30

BVMS verhindert, dass Sie die folgenden Schritte durchführen:
– Hinzufügen oder Verschieben von Geräten mit einer Firmware-Version älter als 6.30 zu einem Pool, der große LUNs ermöglicht.
– Hinzufügen oder Verschieben von Geräten, die derzeit nicht mit dem Netzwerk verbunden sind, zu einem Pool, der große LUNs ermöglicht.
– Hinzufügen oder Verschieben eines iSCSI-Geräts, das große LUNs enthält, zu einem Pool, der keine großen LUNs zulässt.
– Ermöglichen großer LUNs in einem Pool, der Geräte mit Firmware-Version älter als 6.30 enthält.
– Deaktivieren großer LUNs in einem Pool mit einem iSCSI-Gerät, das große LUNs enthält.

Verschieben Sie Geräte mit einer Firmware-Version älter als 6.30 in einen Pool, der keine großen LUNs zulässt.

So fügen Sie ein initialisiertes iSCSI-Gerät hinzu:

1. Klicken Sie mit der rechten Maustaste auf und klicken Sie dann auf **DSA E-Series-Gerät hinzufügen**.
   Das Dialogfeld **DSA E-Series-Gerät hinzufügen** wird angezeigt.
2. Geben Sie die Management-IP-Adresse und das Passwort ein.
3. Klicken Sie auf **Verbinden** .
   Wenn die Verbindung hergestellt wurde, sind die Felder in der Gruppe **Controller** und/oder der Gruppe **Zweiter Controller** ausgefüllt.
4. Klicken Sie auf **OK**.
   Das Gerät wird dem System hinzugefügt.
   Die verfügbaren Ziele werden automatisch gescannt und die LUNs angezeigt.
   Sie können das iSCSI-Gerät verwenden.

Wenn der Pool für große LUNs aktiviert ist und das iSCSI-Gerät für große LUNs konfiguriert ist, erscheint in der Spalte **Große LUN** ein Häkchen für die betroffenen LUNs.

So fügen Sie ein nicht initialisiertes iSCSI-Gerät hinzu:

1. Klicken Sie mit der rechten Maustaste auf und klicken Sie dann auf **DSA E-Series-Gerät hinzufügen**.
   Das Dialogfeld **DSA E-Series-Gerät hinzufügen** wird angezeigt.
2. Geben Sie die Management-IP-Adresse und das Passwort ein.
3. Klicken Sie auf **Verbinden** .
   Wenn die Verbindung hergestellt wurde, sind die Felder in der Gruppe **Controller** und/oder der Gruppe **Zweiter Controller** ausgefüllt.
4. Klicken Sie auf **OK**.
   Das Gerät wird dem System hinzugefügt.
5. Klicken Sie auf und anschließend auf .
6. Klicken Sie auf die Registerkarte **Basiskonfiguration**.
7. Geben Sie die gewünschte LUN-Kapazität ein.
   Wenn Sie einen Wert von mehr als 2 TB eingeben, müssen Sie Ihren Pool für LUNs mit mehr als 2 TB aktivieren.
8. Klicken Sie auf **Initialisieren**.
   Die LUNs werden erstellt.
9. Klicken Sie auf **Schließen**.
10. Klicken Sie mit der rechten Maustaste auf das iSCSI-Gerät, und klicken Sie dann auf **Ziel scannen**.
    Die LUNs mit einem unbekannten Zustand werden angezeigt.
11. Speichern und aktivieren Sie die Konfiguration.
12. Formatieren Sie alle LUNs.
13. Wenn Sie ein iSCSI-Gerät mit Dual-Controllern hinzugefügt haben, entfernen Sie die gewünschte LUNs des ersten Controllers, klicken Sie mit der rechten Maustaste auf den zweiten Controller und dann auf **Ziel scannen**, um diese LUNs hinzuzufügen.

Dialogfeld DSA E-Series-Gerät hinzufügen

Hauptfenster > **Geräte** > > erweitern > Rechtsklick auf > **DSA E-Series-Gerät hinzufügen** > Dialogfeld **DSA E-Series-Gerät hinzufügen**

Dient zum Hinzufügen eines DSA E-Series iSCSI-Gerätes. Dieses Gerät verfügt über eine Management-IP-Adresse, die von der IP-Adresse des iSCSI-Speichers abweicht. Über diese Management-IP-Adresse wird das Gerät automatisch erkannt und konfiguriert.

Name

Geben Sie einen Anzeigenamen für das Gerät ein.

Management-Adresse

Geben Sie die IP-Adresse für die automatische Konfiguration des Geräts ein.

Passwort

Geben Sie das Passwort für dieses Gerät ein.

DSA E-Series Typ:

Zeigt den Gerätetyp an.

Netzwerkadresse iSCSI Ch
Zeigt die IP-Adresse des iSCSI-Ports des Geräts an. Sofern verfügbar, können Sie eine andere IP-Adresse auswählen.

Management-Adresse
Zeigt die IP-Adresse für die automatische Konfiguration des zweiten Controllers an, sofern verfügbar. Sofern verfügbar, können Sie eine andere IP-Adresse auswählen.

Netzwerkadresse iSCSI Ch
Zeigt die IP-Adresse für den iSCSI-Port des zweiten Controllers an, sofern verfügbar. Sofern verfügbar, können Sie eine andere IP-Adresse auswählen.

Verbinden
Hier klicken, um die Geräteeinstellungen zu ermitteln.
Wenn die Verbindung hergestellt wurde, sind die Felder in der Gruppe **Controller** und der Gruppe **2. Controller** ausgefüllt.

Siehe
- *Seite „Basic Configuration“ (Grundkonfiguration), Seite 195*
- *Formatieren einer LUN, Seite 199*

13.22.6 Hinzufügen von Encodern per Suchvorgang

So fügen Sie Encoder per Suchvorgang hinzu:

1. Klicken Sie mit der rechten Maustaste auf und klicken Sie auf **Nach Encodern scannen**.
   Das Dialogfeld **BVMS Scan Wizard** wird angezeigt.
2. Wählen Sie die erforderlichen Encoder sowie den gewünschten VRM-Pool aus und klicken Sie auf **Zuordnen**, um diese dem VRM-Pool zuzuweisen.
3. Klicken Sie auf **Weiter >>**.
   Das Dialogfeld des Assistenten für die **Authentifizierung der Geräte** wird angezeigt.
4. Geben Sie das Passwort für jedes Gerät ein, das von einem Passwort geschützt ist.
   Passwortüberprüfungen erfolgen automatisch, wenn Sie während ein paar Sekunden keine weiteren Zeichen im Passwortfeld eingeben oder außerhalb des Passwortfelds klicken.
   Wenn die Passwörter aller Geräte identisch sind, können Sie es im ersten Feld **Passwort** eingeben. Machen Sie mit der Maus einen Rechtsklick und klicke Sie dann auf **Zellinhalt in Spalte kopieren**.
   In der **Status** Spalte wird die erfolgreiche Anmeldung mit angezeigt. Fehlgeschlagene Anmeldungen werden mithilfe von angezeigt.
5. Klicken Sie auf **Fertig stellen**.
   Das Gerät wird zum Gerätebaum hinzugefügt.

Das ⚠ Symbol weist auf einen Fehler hin, um den Sie sich kümmern müssen. In der QuickInfo finden Sie weitere Informationen zu dem jeweiligen Fehler.

13.22.7 Hinzufügen von VSG-Geräten per Suchvorgang

So fügen Sie VSG-Geräte über den Suchvorgang hinzu:

1. Klicken Sie mit der rechten Maustaste auf und klicken Sie auf **Nach Video Streaming Gateways scannen**.
   Das Dialogfeld **BVMS Scan Wizard** wird angezeigt.
2. Wählen Sie die erforderlichen VSG-Geräte und anschließend den gewünschten VRM-Pool aus und klicken Sie auf **Zuordnen**, um diese dem VRM-Pool zuzuweisen.
3. Klicken Sie auf **Weiter >>**.
   Das Dialogfeld des Assistenten für die **Authentifizierung der Geräte** wird angezeigt.
4. Geben Sie das Passwort für jedes Gerät ein, das von einem Passwort geschützt ist.
   Passwortüberprüfungen erfolgen automatisch, wenn Sie während ein paar Sekunden keine weiteren Zeichen im Passwortfeld eingeben oder außerhalb des Passwortfelds klicken.
   Wenn die Passwörter aller Geräte identisch sind, können Sie es im ersten Feld **Passwort** eingeben. Klicken Sie mit der rechten Maustaste auf das Feld und klicken Sie auf **Zellinhalt in Spalte kopieren**.

   In der Spalte **Status** wird die erfolgreiche Anmeldung mit angezeigt.

   Fehlgeschlagene Anmeldungen werden mithilfe von angezeigt.
5. Klicken Sie auf **Fertig stellen**.
   Das Gerät wird zum Gerätebaum hinzugefügt.

13.22.8 Duale Aufzeichnung im Gerätebaum konfigurieren

Hauptfenster > **Geräte** > erweitern > >

Um die duale Aufzeichnung konfigurieren zu können, muss die ANR-Funktion deaktiviert werden.
Wenn Sie die duale Aufzeichnung für eine Kamera eines Mehrkanal-Encoders konfigurieren, stellt das System sicher, dass für alle Kameras dieses Encoders dasselbe Aufzeichnungsziel konfiguriert wird.
Sie können die duale Aufzeichnung konfigurieren, indem sie Encoder, die durch einen Primären VRM erfasst werden, einem Sekundären VRM zuweisen. Dieses ist beispielsweise sinnvoll, wenn Sie nur einen Teil der Encoder, die von einem Primären VRM erfasst werden, zuweisen möchten.
Dazu muss bereits ein Sekundärer VRM hinzugefügt worden sein.

Konfigurieren:

1. Klicken Sie mit der rechten Maustaste auf und klicken Sie dann auf **Encoder vom Primären VRM hinzufügen**.
   Das Dialogfeld **Encoder hinzufügen** wird angezeigt.
2. Wählen Sie die gewünschten Encoder durch Anklicken aus.
   Bei Auswahl eines Pools oder VRM werden alle untergeordneten Elemente automatisch ausgewählt.
3. Klicken Sie auf **OK**.
   Die ausgewählten Encoder werden dem Sekundären VRM hinzugefügt.

Siehe

- *Duale Aufzeichnung in der Kameratabelle konfigurieren, Seite 308*
- *ANR-Funktion konfigurieren, Seite 308*
- *Duale/Failover-Aufzeichnung, Seite 31*

13.23 Bosch Encoder-/Decoder-Seite

Informationen zur Konfiguration eines Bosch Encoders/Decoders finden Sie unter *Seite „Bosch Encoder/Decoder/Kamera“, Seite 217*.

13.24 Seite iSCSI-Gerät

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > erweitern
Sie können entweder ein iSCSI-Gerät der E-Serie hinzufügen oder ein anderes unterstütztes iSCSI-Gerät.

Siehe
- *Manuelles Hinzufügen eines iSCSI-Geräts, Seite 191*
- *Manuelles Hinzufügen eines iSCSI-Geräts der DSA E-Series, Seite 192*
- *Konfigurieren eines iSCSI-Geräts, Seite 194*
- *Hinzufügen einer LUN, Seite 198*
- *Formatieren einer LUN, Seite 199*

13.24.1 iSCSI-Speicherpool

Ein Speicherpool kann verwendet werden, um eine logische Abbildung der Netzwerktopologie zum Video Recording Manager zu erhalten. Wenn Sie z. B. zwei Gebäude haben, die beide über Speicher und Geräte verfügen, ist es wünschenswert, die Weiterleitung des Netzwerkverkehrs von einem Gebäude zum anderen zu vermeiden.
Speicherpools können auch verwendet werden, um Kameras und Speichersysteme unter dem Gesichtspunkt der Wichtigkeit zu gruppieren. Angenommen, dass ein System einige sehr wichtige Kameras und eine größere Anzahl von weniger wichtigen Kameras umfasst. In diesem Fall ist es möglich, diese in zwei Speicherpools zu gruppieren: in einem mit vielen Redundanzfunktionen und in einem mit weniger Redundanz.
Sie können die folgenden Eigenschaften für die Lastverteilung eines Speicherpools konfigurieren:
- Aufzeichnungspräferenzen (**Automatisch** oder **Failover**)
- Verwendung eines Sekundärziels
  Das Sekundärziel wird im **Failover**-Modus verwendet, wenn das zugewiesene Primärziel ausfällt. Wenn diese Option ausgeschaltet ist, wird die Aufzeichnung auf allen Geräten angehalten, die diesem ausgefallenen Primärziel zugewiesen sind.
  Im Modus **Automatisch**: Wenn ein Ziel ausfällt, führt der VRM Server eine automatische Neuzuweisung der zugehörigen Geräte an andere Speicher durch. Wenn der VRM Server während des Ausfalls eines Ziels außer Betrieb ist, wird die Aufzeichnung auf den Geräten angehalten, die derzeit auf dem ausgefallenen Ziel aufzeichnen.
- Block-Reservierung für Ausfallzeit
- Zeitraum für Plausibilitätsprüfung

Jeder Pool kann so konfiguriert werden, dass dieser LUNs größer als 2 TB ermöglicht.
Folgende Geräte unterstützen keine LUNs größer als 2 TB („große LUNs“):
- VRM-Geräte vor 3.60
- VSG-Geräte mit Firmware-Version älter als 6.30
- Encoder mit Firmware-Version älter als 6.30

BVMS verhindert, dass Sie die folgenden Schritte durchführen:
- Hinzufügen oder Verschieben von Geräten mit einer Firmware-Version älter als 6.30 zu einem Pool, der große LUNs ermöglicht.

– Hinzufügen oder Verschieben von Geräten, die derzeit nicht mit dem Netzwerk verbunden sind, zu einem Pool, der große LUNs ermöglicht.
– Hinzufügen oder Verschieben eines iSCSI-Geräts, das große LUNs enthält, zu einem Pool, der keine großen LUNs zulässt.
– Ermöglichen großer LUNs in einem Pool, der Geräte mit Firmware-Version älter als 6.30 enthält.
– Deaktivieren großer LUNs in einem Pool mit einem iSCSI-Gerät, das große LUNs enthält.

Verschieben Sie Geräte mit einer Firmware-Version älter als 6.30 in einen Pool, der keine großen LUNs zulässt.

Wenn eine primäre VRM über einen Speicherpool verfügt, der große LUNs ermöglicht, erbt die entsprechende gespiegelte VRM diese Einstellung und Sie können das entsprechende Kontrollkästchen **LUNs größer als 2 TB erlauben** des gespiegelten VRM-Pools nicht aktivieren bzw. deaktivieren. Wenn Sie ein iSCSI-Gerät mit großen LUNs zu einem gespiegelten VRM hinzugefügt haben, können Sie das Kontrollkästchen **LUNs größer als 2 TB erlauben** des entsprechenden Pools der primären VRM nicht löschen.

Siehe

– *Seite „Pool“, Seite 180*

13.24.2 Manuelles Hinzufügen eines iSCSI-Geräts

Hauptfenster > **Geräte** > > erweitern > Rechtsklick auf > **iSCSI-Gerät hinzufügen** > Dialogfeld **iSCSI-Gerät hinzufügen**

Dient zum Hinzufügen eines iSCSI-Geräts zu einem VRM.

So fügen Sie ein iSCSI-Gerät hinzu:

1. Klicken Sie mit der rechten Maustaste auf und klicken Sie anschließend auf **iSCSI-Gerät hinzufügen**.
   Das Dialogfeld **iSCSI-Gerät hinzufügen** wird angezeigt.
2. Geben Sie den gewünschten Anzeigenamen, die Netzwerkadresse des iSCSI-Geräts sowie den Gerätetyp ein, und klicken Sie auf **OK**.
   Das iSCSI-Gerät wird dem ausgewählten VRM-Pool hinzugefügt.
   Falls erforderlich, fügen Sie die Ziele und LUNs hinzu.

Dialogfeld iSCSI-Gerät hinzufügen

Name
Geben Sie einen Anzeigenamen für das Gerät ein.

Netzwerkadresse
Geben Sie eine gültige Netzwerkadresse des Geräts ein.

iSCSI-Gerätetyp
Wählen Sie den gewünschten Gerätetyp aus.

Benutzername
Geben Sie zur Authentifizierung einen Benutzernamen ein.

Passwort
Geben Sie zur Authentifizierung das Passwort ein.

Monitoring aktivieren
Wenn für ein DIVAR IP Gerät der iSCSI-Gerätetyp ausgewählt ist und jede SNMP (Simple Network Management Protocol)-Überwachung für diesen DIVAR IP Gerätetyp unterstützt wird, ist das Kontrollkästchen **Monitoring aktivieren** aktiviert.

Aktivieren Sie das Kontrollkästchen, damit der Systemzustand des DIVAR IP Geräts überwacht wird. BVMS erhält und analysiert nun automatisch SNMP-Traps vom DIVAR IP Gerät und aktiviert Ereignisse und Alarme für die Systemzustandsüberwachung (z. B. CPU, Speicher, Lüfter ...). Standardmäßig werden nur kritische Alarme ausgelöst.
Hinweis: Sie müssen zuerst SNMP auf dem DIVAR IP Gerät konfigurieren.
Hinweis: Diese Einstellung ist nur für unterstützte Geräte verfügbar.
Weitere Informationen zur Konfiguration von SNMP auf einem DIVAR IP Gerät finden Sie in der entsprechenden DIVAR IP Dokumentation.

Verwandte Themen
– *Hinzufügen eines VRM-Geräts per Suchvorgang, Seite 170*

Siehe
– *Seite SNMP, Seite 155*
– *SNMP-Überwachung konfigurieren, Seite 95*

13.24.3 Manuelles Hinzufügen eines iSCSI-Geräts der DSA E-Series

Hauptfenster > **Geräte** > > Erweitern >
Sie können entweder ein E-Series iSCSI-Gerät hinzufügen, das bereits initialisiert ist, oder Sie fügen ein nicht initialisiertes E-Series iSCSI-Gerät hinzu.
Sie können LUNs größer als 2 TB hinzufügen, wenn der Pool für große LUNs aktiviert ist.
Folgende Geräte unterstützen keine LUNs größer als 2 TB („große LUNs“):
– VRM-Geräte vor 3.60
– VSG-Geräte mit Firmware-Version älter als 6.30
– Encoder mit Firmware-Version älter als 6.30

BVMS verhindert, dass Sie die folgenden Schritte durchführen:
– Hinzufügen oder Verschieben von Geräten mit einer Firmware-Version älter als 6.30 zu einem Pool, der große LUNs ermöglicht.
– Hinzufügen oder Verschieben von Geräten, die derzeit nicht mit dem Netzwerk verbunden sind, zu einem Pool, der große LUNs ermöglicht.
– Hinzufügen oder Verschieben eines iSCSI-Geräts, das große LUNs enthält, zu einem Pool, der keine großen LUNs zulässt.
– Ermöglichen großer LUNs in einem Pool, der Geräte mit Firmware-Version älter als 6.30 enthält.
– Deaktivieren großer LUNs in einem Pool mit einem iSCSI-Gerät, das große LUNs enthält.

Verschieben Sie Geräte mit einer Firmware-Version älter als 6.30 in einen Pool, der keine großen LUNs zulässt.

So fügen Sie ein initialisiertes iSCSI-Gerät hinzu:

1. Klicken Sie mit der rechten Maustaste auf und klicken Sie dann auf **DSA E-Series-Gerät hinzufügen**.
   Das Dialogfeld **DSA E-Series-Gerät hinzufügen** wird angezeigt.
2. Geben Sie die Management-IP-Adresse und das Passwort ein.
3. Klicken Sie auf **Verbinden** .
   Wenn die Verbindung hergestellt wurde, sind die Felder in der Gruppe **Controller** und/oder der Gruppe **Zweiter Controller** ausgefüllt.
4. Klicken Sie auf **OK**.
   Das Gerät wird dem System hinzugefügt.
   Die verfügbaren Ziele werden automatisch gescannt und die LUNs angezeigt.
   Sie können das iSCSI-Gerät verwenden.

Wenn der Pool für große LUNs aktiviert ist und das iSCSI-Gerät für große LUNs konfiguriert ist, erscheint in der Spalte **Große LUN** ein Häkchen für die betroffenen LUNs.

So fügen Sie ein nicht initialisiertes iSCSI-Gerät hinzu:

1. Klicken Sie mit der rechten Maustaste auf und klicken Sie dann auf **DSA E-Series-Gerät hinzufügen**.
   Das Dialogfeld **DSA E-Series-Gerät hinzufügen** wird angezeigt.
2. Geben Sie die Management-IP-Adresse und das Passwort ein.
3. Klicken Sie auf **Verbinden** .
   Wenn die Verbindung hergestellt wurde, sind die Felder in der Gruppe **Controller** und/oder der Gruppe **Zweiter Controller** ausgefüllt.
4. Klicken Sie auf **OK**.
   Das Gerät wird dem System hinzugefügt.
5. Klicken Sie auf und anschließend auf .
6. Klicken Sie auf die Registerkarte **Basiskonfiguration**.
7. Geben Sie die gewünschte LUN-Kapazität ein.
   Wenn Sie einen Wert von mehr als 2 TB eingeben, müssen Sie Ihren Pool für LUNs mit mehr als 2 TB aktivieren.
8. Klicken Sie auf **Initialisieren**.
   Die LUNs werden erstellt.
9. Klicken Sie auf **Schließen**.
10. Klicken Sie mit der rechten Maustaste auf das iSCSI-Gerät, und klicken Sie dann auf **Ziel scannen**.
    Die LUNs mit einem unbekannten Zustand werden angezeigt.
11. Speichern und aktivieren Sie die Konfiguration.
12. Formatieren Sie alle LUNs.
13. Wenn Sie ein iSCSI-Gerät mit Dual-Controllern hinzugefügt haben, entfernen Sie die gewünschte LUNs des ersten Controllers, klicken Sie mit der rechten Maustaste auf den zweiten Controller und dann auf **Ziel scannen**, um diese LUNs hinzuzufügen.

Dialogfeld DSA E-Series-Gerät hinzufügen

Hauptfenster > **Geräte** > > erweitern > Rechtsklick auf > **DSA E-Series-Gerät hinzufügen** > Dialogfeld **DSA E-Series-Gerät hinzufügen**

Dient zum Hinzufügen eines DSA E-Series iSCSI-Gerätes. Dieses Gerät verfügt über eine Management-IP-Adresse, die von der IP-Adresse des iSCSI-Speichers abweicht. Über diese Management-IP-Adresse wird das Gerät automatisch erkannt und konfiguriert.

Name

Geben Sie einen Anzeigenamen für das Gerät ein.

Management-Adresse

Geben Sie die IP-Adresse für die automatische Konfiguration des Geräts ein.

Passwort

Geben Sie das Passwort für dieses Gerät ein.

DSA E-Series Typ:

Zeigt den Gerätetyp an.

Netzwerkadresse iSCSI Ch
Zeigt die IP-Adresse des iSCSI-Ports des Geräts an. Sofern verfügbar, können Sie eine andere IP-Adresse auswählen.

Management-Adresse
Zeigt die IP-Adresse für die automatische Konfiguration des zweiten Controllers an, sofern verfügbar. Sofern verfügbar, können Sie eine andere IP-Adresse auswählen.

Netzwerkadresse iSCSI Ch
Zeigt die IP-Adresse für den iSCSI-Port des zweiten Controllers an, sofern verfügbar. Sofern verfügbar, können Sie eine andere IP-Adresse auswählen.

Verbinden
Hier klicken, um die Geräteeinstellungen zu ermitteln.
Wenn die Verbindung hergestellt wurde, sind die Felder in der Gruppe **Controller** und der Gruppe **2. Controller** ausgefüllt.

Siehe
- *Seite „Basic Configuration“ (Grundkonfiguration), Seite 195*
- *Formatieren einer LUN, Seite 199*

13.24.4 Konfigurieren eines iSCSI-Geräts

Hauptfenster > **Geräte** > Erweitern > Erweitern >
Führen Sie nach dem Hinzufügen von VRM-Geräten, iSCSI-Geräten und Encodern die folgenden Aufgaben aus, damit die Videodaten der Encoder auf den iSCSI-Geräten gespeichert oder Videodaten von diesen iSCSI-Geräten abgerufen werden können:
- Führen Sie die Standardkonfiguration durch, um auf jedem Ziel des iSCSI-Geräts LUNs zu erzeugen.
  Dieser Schritt ist optional. Bei einem iSCSI-Gerät mit vorkonfigurierten LUNs muss dieser Schritt nicht durchgeführt werden.
- Durchsuchen Sie das iSCSI-Gerät nach Abschluss der Standardkonfiguration, um die Ziele und LUNs im Gerätebaum hinzuzufügen.

Hinweis:
Nicht alle iSCSI-Geräte unterstützen die Standardkonfiguration und das automatische IQN-Mapping.
Voraussetzung:
Das iSCSI-Gerät muss mit gültigen IP-Adressen konfiguriert werden.

Durchführung der Grundkonfiguration eines DSA E-Series iSCSI-Geräts:

- Erweitern Sie das entsprechende VRM-Gerät und , und klicken Sie auf das entsprechende iSCSI-Gerät .

1. Klicken Sie auf die Registerkarte **Basiskonfiguration**.
2. Geben Sie die gewünschte LUN-Kapazität ein.
   Wenn Sie einen Wert von mehr als 2 TB eingeben, müssen Sie Ihren Pool für LUNs mit mehr als 2 TB aktivieren.
3. Klicken Sie auf **Initialisieren**.
   Die LUNs werden erstellt.
4. Klicken Sie auf **Schließen**.

5. Klicken Sie mit der rechten Maustaste auf das iSCSI-Gerät, und klicken Sie dann auf **Ziel scannen**.
   Die LUNs mit einem unbekannten Zustand werden angezeigt.
6. Speichern und aktivieren Sie die Konfiguration.
7. Formatieren Sie alle LUNs.
8. Wenn Sie ein iSCSI-Gerät mit Dual-Controllern hinzugefügt haben, entfernen Sie die gewünschte LUNs des ersten Controllers, klicken Sie mit der rechten Maustaste auf den zweiten Controller und dann auf **Ziel scannen**, um diese LUNs hinzuzufügen.

Durchführung einer Grundkonfiguration auf anderen iSCSI-Geräten:

1. Klicken Sie auf die Registerkarte **Basiskonfiguration**.
2. Geben Sie die gewünschte LUN-Anzahl ein.
3. Klicken Sie auf **Setzen**.
   Die LUNs werden erstellt.
4. Klicken Sie auf **Schließen**.
5. Klicken Sie mit der rechten Maustaste auf das iSCSI-Gerät, und klicken Sie dann auf **Ziel scannen**.
   Die LUNs mit einem unbekannten Zustand werden angezeigt.
6. Speichern und aktivieren Sie die Konfiguration.
7. Formatieren Sie alle LUNs.

IQN-Mapping für andere iSCSI-Geräte durchführen:

1. Erweitern Sie das entsprechende VRM-Gerät und , und klicken Sie auf das entsprechende iSCSI-Gerät .
2. Klicken Sie mit der rechten Maustaste auf , und klicken Sie auf **IQN-Mapping starten**.
   Das Dialogfeld iqn-Mapper wird angezeigt, und der Vorgang wird gestartet.
   Die dem ausgewählten VRM-Gerät zugeordneten Encoder werden ausgewertet, und ihre IQNs werden dem iSCSI-Gerät hinzugefügt.
3. Klicken Sie auf , um die Einstellungen zu speichern.
4. Klicken Sie auf , um die Konfiguration zu aktivieren.

Siehe

- *Seite „Basic Configuration“ (Grundkonfiguration), Seite 195*
- *Dialogfeld „Lastverteilung“, Seite 197*
- *Dialogfeld iqn-Mapper, Seite 199*
- *Formatieren einer LUN, Seite 199*

13.24.5 Seite „Basic Configuration“ (Grundkonfiguration)

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > Klicken auf > Registerkarte **Basiskonfiguration**

Die angezeigten Optionen variieren je nach Art des verwendeten iSCSI-Speichersystems.

Dient zum Durchführen einer Grundkonfiguration für das iSCSI-Gerät. Sie erzeugen LUNs auf der iSCSI-Festplatte und formatieren die LUNs.

Wird nur angezeigt, wenn das Gerät eines der iSCSI-Archivierungssysteme ist, die von Bosch unterstützt werden, beispielsweise DSA oder DLS 1x00.

Hinweis!
Nach der Grundkonfiguration einer E-Serie benötigt das System viele Stunden (oder auch Tage) für die Initialisierung. In dieser Phase ist die volle Leistung nicht verfügbar, und in Phase 1.5 kann die Formatierung fehlschlagen.

Physikalische Kapazität [GB]
Informationen zur Gesamtkapazität des Archivierungssystems.

Anzahl der LUNs
Sie können die Anzahl der LUNs ändern.

Hinweis!
Wenn Sie die Anzahl der LUNs ändern, wird das gesamte iSCSI-System neu organisiert und alle im System gespeicherten Sequenzen gehen verloren.
Überprüfen Sie daher die Aufzeichnungen und sichern Sie wichtige Sequenzen, bevor Sie Änderungen durchführen.

Kapazität für neue LUNs [GB]
Da 256 die maximale Anzahl der LUNs eines Speicherarrays ist, darf die Größe der LUNs nicht zu klein gewählt werden. Andernfalls können in der Zukunft keine weiteren LUNs erstellt werden, wenn ein zusätzliches Fach installiert wird.

Target-Spare-Disks
Die Anzahl der vom Benutzer gewählten Reservefestplatten des Systems.

Tatsächliche Spare-Disks
Anzahl der Reservefestplatten, über die das System derzeit verfügt. Diese Anzahl kann von der Anzahl oben abweichen, z. B. wenn das Speichersystem manuell neu konfiguriert wurde oder Festplatten defekt sind.

Initialisierungsstatus (%)
Zusätzliche Informationen werden während der Initialisierung angezeigt. Wenn die Initialisierung abgeschlossen ist (100 %), erhalten Sie auch die Möglichkeit, alle LUNs wieder zu löschen.

RAID-DP (Schwerpunkt: Ausfallsicherheit)
Aktivieren Sie diese Option, wenn Sie statt des angegebenen RAID-Typs RAID 4 lieber den zuverlässigeren RAID-Typ RAID DP verwenden möchten.

RAID 6 (Schwerpunkt: Ausfallsicherheit)
Wählen Sie diese Option aus, wenn Sie statt des angegebenen RAID-Typs RAID 5 lieber den zuverlässigeren RAID-Typ RAID 6 verwenden möchten.

Zusatzinformationen
Zeigt weitere Informationen an, z. B. Informationen darüber, dass das Speichersystem nicht richtig konfiguriert ist und daher keine Einrichtung möglich ist.

Siehe
– *Manuelles Hinzufügen eines iSCSI-Geräts der DSA E-Series, Seite 192*

13.24.6 Dialogfeld „Lastverteilung“

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > Rechtsklick auf > Befehl **Lastverteilung...** > Dialogfeld **Lastverteilung**

Voraussetzung: Konfigurieren Sie den Aufzeichnungsmodus **Automatisch**.

Hier können Sie die oberen Grenzwerte für die zulässige Bitrate und die Anzahl der gleichzeitigen iSCSI-Verbindungen für jedes iSCSI-System einstellen. Bei einer Überschreitung dieser Grenzwerte werden keine Daten mehr auf dem iSCSI-System gespeichert. Die entsprechenden Daten gehen verloren.

Verwenden Sie für unterstützte Systeme (zum Beispiel Bosch RAID, NetApp DLA) die Standardwerte. Falls andere Geräte verwendet werden, finden Sie weitere Informationen in der zugehörigen Dokumentation. Testen Sie zunächst kleine Werte.

13.24.7 Verschieben eines iSCSI-Systems in einen anderen Pool (Pool ändern)

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern >

Sie verschieben das Gerät von einem Pool in den anderen innerhalb des gleichen VRM Geräts, ohne Aufzeichnungsverlust.

Zum Verschieben:

1. Klicken Sie mit der rechten Maustaste auf / / und klicken Sie auf **Pool ändern...**.
   Das Dialogfeld **Pool ändern** wird angezeigt.
2. Wählen Sie in der Liste **Neuer Pool:** den gewünschten Pool aus.
3. Klicken Sie auf **OK**.
   Das Gerät wird in den ausgewählten Pool verschoben.

13.24.8 Seite LUNs

Hauptfenster > **Geräte** > Erweitern > Erweitern > > Erweitern > Erweitern >

Erlaubt das Hinzufügen, Entfernen oder Formatieren von LUNs und zeigt Informationen über die LUNs an.

Hinzufügen

Klicken Sie hier, um das Dialogfeld **LUN hinzufügen** anzuzeigen.

Entfernen

Klicken Sie, um die ausgewählten Zeilen zu entfernen. Klicken Sie zur Auswahl einer Zeile auf die linke Zeilenüberschrift auf der linken Seite. Jede Zeile steht für eine LUN.

Ein Meldungsfeld wird angezeigt.

LUN formatieren

Klicken Sie darauf, um die ausgewählte LUN zu formatieren. Ein Meldungsfeld wird angezeigt.

Format

Klicken Sie auf das Kontrollkästchen, um die LUN auszuwählen, und anschließend auf **LUN formatieren**.

LUN

Zeigt den Namen der LUN an.

Größe [GB]
Zeigt die maximale Kapazität der LUN an.

Große LUN
Jede Zelle zeigt an, ob diese LUN größer als 2 TB ist oder nicht.

Status
Zeigt den Status der LUN an.

Fortschritt
Zeigt den Fortschritt der Formatierung an.

Siehe
- *Seite „Pool“, Seite 180*
- *Hinzufügen einer LUN, Seite 198*
- *Hinzufügen eines VRM-Geräts per Suchvorgang, Seite 170*

13.24.9 Hinzufügen einer LUN

Hauptfenster > **Geräte** > Erweitern > Erweitern >
In der Regel werden die gewünschten iSCSI-Geräte beim Netzwerk-Scan automatisch mit ihren Zielen und LUNs hinzugefügt. Wenn der Netzwerk-Scan nicht erfolgreich ausgeführt wurde oder Sie ein iSCSI-Gerät vor der Integration im Netzwerk offline konfigurieren möchten, konfigurieren Sie für das iSCSI-Gerät das Ziel und für dieses Ziel ein oder mehrere LUNs.
Sie können LUNs größer als 2 TB hinzufügen, wenn der Pool für große LUNs aktiviert ist.
Folgende Geräte unterstützen keine LUNs größer als 2 TB („große LUNs“):
- VRM-Geräte vor 3.60
- VSG-Geräte mit Firmware-Version älter als 6.30
- Encoder mit Firmware-Version älter als 6.30

BVMS verhindert, dass Sie die folgenden Schritte durchführen:
- Hinzufügen oder Verschieben von Geräten mit einer Firmware-Version älter als 6.30 zu einem Pool, der große LUNs ermöglicht.
- Hinzufügen oder Verschieben von Geräten, die derzeit nicht mit dem Netzwerk verbunden sind, zu einem Pool, der große LUNs ermöglicht.
- Hinzufügen oder Verschieben eines iSCSI-Geräts, das große LUNs enthält, zu einem Pool, der keine großen LUNs zulässt.
- Ermöglichen großer LUNs in einem Pool, der Geräte mit Firmware-Version älter als 6.30 enthält.
- Deaktivieren großer LUNs in einem Pool mit einem iSCSI-Gerät, das große LUNs enthält.

Verschieben Sie Geräte mit einer Firmware-Version älter als 6.30 in einen Pool, der keine großen LUNs zulässt.

Zum Hinzufügen:
1. Falls erforderlich, klicken Sie zur Auswahl auf **LUNs größer als 2 TB erlauben**.
2. Klicken Sie mit der rechten Maustaste auf und klicken Sie dann auf **Ziel scannen**.
   Das Ziel wird hinzugefügt.
3. Klicken Sie auf das Ziel.
   Die Seite **LUNs** wird angezeigt.
4. Klicken Sie auf **Hinzufügen**.
   Das Dialogfeld **LUN hinzufügen** wird angezeigt.

5. Geben Sie die gewünschte LUN ein und klicken Sie auf **OK**.
   Die LUN wird als neue Zeile in der Tabelle hinzugefügt.
   Wiederholen Sie diesen Schritt für jede gewünschte LUN.

Hinweise:

– Klicken Sie zum Entfernen einer LUN auf **Entfernen**.
  Die Videodaten dieser LUN werden beibehalten.
– Klicken Sie zum Formatieren einer LUN auf **LUN formatieren**.
  Alle Daten dieser LUN werden entfernt!

Dialogfeld LUN hinzufügen

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > erweitern > > Klick auf **Hinzufügen**

Dient zum Hinzufügen einer LUN.

Id

Geben Sie die ID der LUN ein.

Siehe

– *Seite „Pool“, Seite 180*
– *Seite LUNs, Seite 197*

13.24.10 Formatieren einer LUN

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > erweitern >

Eine LUN wird zur Vorbereitung zur ersten Verwendung formatiert.

Hinweis!
Alle Daten der LUN gehen beim Formatieren verloren.

Konfigurieren:

1. Wählen Sie die gewünschte LUN aus, und aktivieren Sie das Kontrollkästchen in der Spalte **Format**.
2. Klicken Sie auf **LUN formatieren**.
3. Lesen Sie die angezeigte Meldung aufmerksam durch, und bestätigen Sie sie gegebenenfalls.
   Die ausgewählte LUN wird formatiert. Alle Daten dieser LUN gehen verloren.

Siehe

– *Seite LUNs, Seite 197*

13.24.11 Dialogfeld iqn-Mapper

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > Rechtsklick auf > **IQN-Mapping starten**

Dient zum Starten des IQN-Mappings.

Siehe

- *Hinzufügen eines VRM-Geräts per Suchvorgang, Seite 170*
- *Konfigurieren eines iSCSI-Geräts, Seite 194*

13.25 Seite „Video Streaming Gateway-Gerät“

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern >

Dieses Kapitel enthält Informationen zur Konfiguration des VSG-Geräts in Ihrem System.

Ermöglicht es Ihnen, die folgenden Encoder-Typen hinzuzufügen und zu konfigurieren:

- Bosch Encoder
- ONVIF-Encoder
- JPEG-Encoder
- RTSP-Encoder

So fügen Sie VSG-Geräte über den Suchvorgang hinzu:

1. Klicken Sie mit der rechten Maustaste auf und klicken Sie auf **Nach Video Streaming Gateways scannen**.
   Das Dialogfeld **BVMS Scan Wizard** wird angezeigt.
2. Wählen Sie die erforderlichen VSG-Geräte und anschließend den gewünschten VRM-Pool aus und klicken Sie auf **Zuordnen**, um diese dem VRM-Pool zuzuweisen.
3. Klicken Sie auf **Weiter >>**.
   Das Dialogfeld des Assistenten für die **Authentifizierung der Geräte** wird angezeigt.
4. Geben Sie das Passwort für jedes Gerät ein, das von einem Passwort geschützt ist.
   Passwortüberprüfungen erfolgen automatisch, wenn Sie während ein paar Sekunden keine weiteren Zeichen im Passwortfeld eingeben oder außerhalb des Passwortfelds klicken.
   Wenn die Passwörter aller Geräte identisch sind, können Sie es im ersten Feld **Passwort** eingeben. Klicken Sie mit der rechten Maustaste auf das Feld und klicken Sie auf **Zellinhalt in Spalte kopieren**.
   In der Spalte **Status** wird die erfolgreiche Anmeldung mit angezeigt.
   Fehlgeschlagene Anmeldungen werden mithilfe von angezeigt.
5. Klicken Sie auf **Fertig stellen**.
   Das Gerät wird zum Gerätebaum hinzugefügt.

Wenn Sie eine neue VSG Version 7.0 oder höher hinzufügen, ist das Kontrollkästchen **Sichere Verbindung** standardmäßig aktiviert.

Verwenden Sie zum Ändern einer sicheren oder unsicheren Verbindung den Befehl **Video Streaming Gateway bearbeiten** und aktivieren oder deaktivieren Sie das Kontrollkästchen **Sichere Verbindung**.

Siehe

- *Bearbeiten eines Video Streaming Gateway, Seite 202*
- *ONVIF Seite, Seite 238*

13.25.1 Manuelles Hinzufügen eines Video Streaming Gateway

Hauptfenster > **Geräte** > erweitern >

Sie können ein VSG Gerät einem VRM-Pool zuordnen.

So fügen Sie ein VSG-Gerät manuell hinzu:

1. Klicken Sie mit der rechten Maustaste auf und klicken Sie dann auf **Video Streaming Gateway hinzufügen**.
   Das Dialogfeld **Video Streaming Gateway hinzufügen** wird angezeigt.
2. Nehmen Sie die erforderlichen Einstellungen für das VSG-Gerät vor.
3. Klicken Sie auf **Hinzufügen**.

⇨ Das VSG-Gerät wird dem System hinzugefügt. Die diesem VSG-Gerät zugewiesenen Kameras werden aufgezeichnet.

Dialogfeld Video Streaming Gateway hinzufügen

Machen Sie einen Rechtsklick im > **Video Streaming Gateway hinzufügen** > **Video Streaming Gateway hinzufügen** Dialogfeld

Port-Nummer
Geben Sie die Port-Nummer des Geräts ein.

Benutzername
Geben Sie den Benutzernamen für die Authentifizierung auf dem Gerät ein. In der Regel: service.

Netzwerkadresse / Port
Geben Sie die IP-Adresse des Geräts ein.
Wenn das Kontrollkästchen **Sichere Verbindung** aktiviert ist, wird der Port automatisch zum HTTPS-Port geändert.
Sie können die Port-Nummer ändern, wenn keine Standardports verwendet werden oder die VSG-Instanzen in einer anderen Reihenfolge konfiguriert sind.

Standardports

VSG-Instanz	rcpp-Port	HTTPS-Port
1	8756	8443
2	8757	8444
3	8758	8445
4	8759	8446
5	8760	8447
6	8761	8448
7	8762	8449

Passwort
Geben Sie ein gültiges Passwort für die Authentifizierung auf dem Gerät ein.

Passwort anzeigen
Klicken Sie hier, um das eingegebene Passwort anzuzeigen. Achten Sie darauf, dass niemand das Passwort einsehen kann.

Sicherheit
Das Kontrollkästchen **Sichere Verbindung** ist standardmäßig aktiviert, wenn HTTPS unterstützt wird. Ab VSG Version 7.0 unterstützt VSG sichere Verbindungen.

Hinweis!
Wenn Sie zu BVMS Version 10.0 und höher migrieren, ist das Kontrollkästchen **Sichere Verbindung** nicht standardmäßig aktiviert und die Verbindung ist unsicher (rcpp).

Verwenden Sie zum Ändern einer sicheren oder unsicheren Verbindung den Befehl **Video Streaming Gateway bearbeiten** und aktivieren oder deaktivieren Sie das Kontrollkästchen **Sichere Verbindung**.

Authentifizieren
Klicken Sie hier, um sich mit den oben eingegebenen Anmeldeinformationen beim Gerät zu authentifizieren.

Siehe
– *Bearbeiten eines Video Streaming Gateway, Seite 202*

13.25.2 Bearbeiten eines Video Streaming Gateway

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern >

So ändern Sie eine sichere/unsichere Verbindung:

1. Klicken Sie mit der rechten Maustaste auf .
2. Klicken Sie auf **Video Streaming Gateway bearbeiten**.
   Das Dialogfeld **Video Streaming Gateway bearbeiten** wird angezeigt.
3. Aktivieren Sie das Kontrollkästchen **Sichere Verbindung**.
   Der verwendete Port wird automatisch zum HTTPS-Port geändert.
   oder
   Deaktivieren Sie das Kontrollkästchen **Sichere Verbindung**.
   Der verwendete Port wird automatisch zum rcpp-Port geändert.

Hinweis!
Nach dem Upgrade auf eine neuere Version wird empfohlen, zu einer sicheren Verbindung zu wechseln.

Siehe
– *Manuelles Hinzufügen eines Video Streaming Gateway, Seite 200*

13.25.3 Hinzufügen einer Kamera zu einem VSG

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern >

Sie können dem VSG die folgenden Geräte hinzufügen:
– Encoder von Bosch
– ONVIF-Kameras
– JPEG-Kameras
– RTSP-Encoder

Wenn Sie VSG-Encoder offline hinzufügen, können Sie deren Status aktualisieren.

So führen Sie das Hinzufügen aus:

1. Klicken Sie mit der rechten Maustaste auf , zeigen Sie mit dem Cursor auf **Encoder/Kamera hinzufügen** und klicken Sie anschließend auf den gewünschten Befehl.
2. Nehmen Sie für das Hinzufügen des Geräts die erforderlichen Einstellungen im Dialogfeld vor.

3. Klicken Sie auf **OK**.

Das Gerät wird hinzugefügt.

Zum Aktualisieren:

- Machen Sie einen Rechtsklick auf den gewünschten Encoder und klicken dann **Status aktualisieren**.
  Die Eigenschaften des Geräts werden abgerufen.

Siehe

– *Dialogfeld „Bosch Encoder hinzufügen/bearbeiten“, Seite 203*
– *Dialogfeld „ONVIF-Encoder hinzufügen/bearbeiten“, Seite 204*
– *Dialogfeld „JPEG-Kamera hinzufügen/bearbeiten“, Seite 206*
– *Dialogfeld „RTSP-Encoder hinzufügen/bearbeiten“, Seite 207*

13.25.4 Dialogfeld „Bosch Encoder hinzufügen/bearbeiten“

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > Rechtsklick auf > **Encoder/Kamera hinzufügen** > Befehl **Bosch Encoder**

oder

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > erweitern > Rechtsklick auf > Auf **Encoder bearbeiten** klicken > Dialogfeld **Bosch-Encoder bearbeiten**

Sie können Ihrem VSG-Gerät einen Encoder von Bosch hinzufügen.

Netzwerkadresse
Geben Sie die Netzwerkadresse des Geräts ein.

Port-Nummer
Geben Sie die Port-Nummer des Geräts ein.

Sichere Verbindung
Sie können die sichere Verbindung von Live-Videos aktivieren, die von einem ONVIF-Encoder zu Ihrem VSG-Gerät übertragen werden.

Hinweis:
Wenn diese Option aktiviert ist, kann der Benutzer des Operator Client einen Stream nicht auf UDP und UDP Multicast umschalten.
Wenn diese Option aktiviert ist, funktioniert das ANR des betreffenden Geräts nicht.
Wenn diese Option aktiviert ist, funktioniert die Encoder-Wiedergabe auf Encodern mit Firmware älter als 6.30 nicht.

Encodertyp
Wählen Sie für ein Gerät mit bekanntem Gerätetyp den entsprechenden Eintrag aus. Das Gerät muss nicht im Netzwerk verfügbar sein.
Wenn Sie ein beliebiges Video-IP-Gerät von Bosch hinzufügen möchten, wählen Sie **<Automatisch erkennen>**. Das Gerät muss im Netzwerk verfügbar sein.
Wenn Sie eine Kamera für die Offline-Konfiguration hinzufügen möchten, wählen Sie **<Einzel Platzhalter Kamera>**.

Benutzername
Geben Sie den Benutzernamen für die Authentifizierung auf dem Gerät ein. In der Regel: service.

Passwort
Geben Sie ein gültiges Passwort für die Authentifizierung auf dem Gerät ein.

Passwort anzeigen
Klicken Sie hier, um das eingegebene Passwort anzuzeigen. Achten Sie darauf, dass niemand das Passwort einsehen kann.

Authentifizieren
Klicken Sie hier, um sich mit den oben eingegebenen Anmeldeinformationen beim Gerät zu authentifizieren.

Kameraprotokoll
Klicken Sie, um das für dieses Gerät verfügbare gewünschte Protokoll zu aktivieren.
TCP
Dient zur Übertragung über das Internet und/oder für verlustlose Datenübertragung. Gewährleistet, dass keine Datenpakete verloren gehen. Anforderungen an die Netzwerkbandbreite können hoch sein. Verwendung, wenn sich das Gerät hinter einer Firewall befindet. Unterstützt kein Multicast.
UDP
Verwendung für verbindungslose und leichte Datenübertragung in privaten Netzwerken. Datenpakete können verloren gehen. Anforderungen an die Netzwerkbandbreite können gering sein.
Unterstützt Multicast.

Videoeingänge verwenden
Klicken Sie, um die Videoeingänge auszuwählen, wenn Sie ein Mehrkanal-Gerät konfigurieren.

Verwendete Videoeingänge
Aktivieren Sie das Kontrollkästchen, um den entsprechenden Videoeingang zu verwenden.

Siehe
– *Hinzufügen einer Kamera zu einem VSG, Seite 202*

13.25.5 Dialogfeld „ONVIF-Encoder hinzufügen/bearbeiten“

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > Rechtsklick auf > **Encoder/Kamera hinzufügen** > Befehl **ONVIF-Encoder hinzufügen**
oder
Hauptfenster > **Geräte** > Rechtsklick > Befehl **ONVIF-Encoder hinzufügen**

oder
Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > erweitern >
Rechtsklick auf > Klick auf **ONVIF-Encoder bearbeiten** > Dialogfeld **ONVIF-Encoder bearbeiten**
oder
Hauptfenster > **Geräte**> Rechtsklick auf > Rechtsklick auf > Klick auf **ONVIF-Encoder bearbeiten** > Dialogfeld **ONVIF-Encoder bearbeiten**
Sie können einen ONVIF-Encoder Ihrem VSG Geräte hinzufügen oder als Nur-Live-Encoder.
Sie müssen in der Kameratabelle das für die Aufzeichnung und Live-Video verwendete Profil konfigurieren.

Ab BVMS 10.0 können ONVIF-Encoderereignisse direkt vom VSG- oder ONVIF-Encoder abgerufen werden. Wenn Sie einen neuen ONVIF-Encoder hinzufügen, wird das Kontrollkästchen **ONVIF-Ereignisse über VSG abrufen (Profile S, T)** standardmäßig aktiviert und Profile T wird unterstützt. Die folgenden Funktionen werden nur unterstützt, wenn ein ONVIF-Encoder über ein VSG-Gerät zu Ihrem System hinzugefügt wird:

- Wenn ONVIF-Encoderereignisse von VSG abgerufen werden, sind Standard-ONVIF-Ereignisse bereits zugeordnet.
- Der Bediener kann Relais im Operator Client ein- bzw. ausschalten.

Hinweis!
Das Abrufen von ONVIF-Ereignissen von VSG ist nur in VSG Version 7.0 möglich. Wenn Sie zu BVMS Version 10.0 migrieren, werden vorhandene ONVIF-Encoderereignisse direkt vom ONVIF-Encoder abgerufen. Sie müssen VSG auf Version 7.0 aktualisieren.

Name
Geben Sie einen Anzeigenamen für das Gerät ein.

Netzwerkadresse
Geben Sie die Netzwerkadresse des Geräts ein.

Port-Nummer
Geben Sie die Port-Nummer des Geräts ein.

Sichere Verbindung
Sie können die sichere Verbindung von Live-Videos aktivieren, die von einem ONVIF-Encoder zu Ihrem VSG-Gerät übertragen werden.

Hinweis:
Wenn diese Option aktiviert ist, kann der Benutzer des Operator Client einen Stream nicht auf UDP und UDP Multicast umschalten.
Wenn diese Option aktiviert ist, funktioniert das ANR des betreffenden Geräts nicht.
Wenn diese Option aktiviert ist, funktioniert die Encoder-Wiedergabe auf Encodern mit Firmware älter als 6.30 nicht.

Hinweis!
Standardmäßig ist Port 443 festgelegt. Sie können die Port-Nummer bearbeiten, damit sie dem konfigurierten HTTPS-Port des Encoders entspricht.
Die konfigurierte Port-Nummer wird nicht gespeichert.

Benutzername
Geben Sie den Benutzernamen für die Authentifizierung auf dem Gerät ein. In der Regel: service.

Passwort
Geben Sie ein gültiges Passwort für die Authentifizierung auf dem Gerät ein.

Passwort anzeigen
Klicken Sie hier, um das eingegebene Passwort anzuzeigen. Achten Sie darauf, dass niemand das Passwort einsehen kann.

Authentifizieren
Klicken Sie hier, um sich mit den oben eingegebenen Anmeldeinformationen beim Gerät zu authentifizieren.

Kameraprotokoll
Wählen Sie das gewünschte Kameraprotokoll aus.

ONVIF Profil
Wenn diese Option unterstützt wird, wählen Sie das Profil aus, das Sie konfigurieren möchten.

ONVIF Profil G
Wenn Ihr ONVIF-Encoder Profile G unterstützt und Sie lokal aufzeichnen möchten, konfigurieren Sie die lokalen Aufzeichnungseinstellungen im herstellerspezifischen Konfigurations-Tool, und aktivieren Sie das Kontrollkästchen **Lokale Aufzeichnung aktiviert**.
Wenn das Kontrollkästchen nicht aktiviert ist, fungiert Ihr ONVIF Profile G-Encoder als regulärer ONVIF-Encoder.

Panorama-Kamera
Aktivieren Sie ggf. das Kontrollkästchen.

Montageposition
Wählen Sie die Montageposition aus.

Anzahl der Videoeingangskanäle
Geben Sie die gewünschte Anzahl von Videoeingängen ein.

Videoeingang {0} verwenden
Aktivieren Sie das Kontrollkästchen, um den entsprechenden Videoeingang zu verwenden.

Anzahl der Audioeingangskanäle
Geben Sie die gewünschte Anzahl von Audioeingängen ein.

Anzahl der Alarmeingänge
Geben Sie die gewünschte Anzahl von Alarmeingängen ein.

Anzahl der Relais
Geben Sie die gewünschte Anzahl von Relais ein.

Hinweis!
Die **Einstellungen für Video Streaming Gateway**-Optionen sind nicht für ONVIF-Encoder verfügbar, die als Nur-Live-Encoder hinzugefügt werden.

Siehe
– *Hinzufügen einer Kamera zu einem VSG, Seite 202*

13.25.6 Dialogfeld „JPEG-Kamera hinzufügen/bearbeiten“

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > Rechtsklick auf > **Encoder/Kamera hinzufügen** > Befehl **JPEG-Kamera**
oder
Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > erweitern > Rechtsklick auf > Klick auf **JPEG-Kamera bearbeiten** > Dialogfeld **JPEG bearbeiten**

Sie können eine JPEG Kamera Ihrem VSG Gerät hinzufügen.

Name
Geben Sie einen Anzeigenamen für das Gerät ein.

URL
Geben Sie die URL Ihrer JPEG-Kamera / RTSP Kamera ein.
Für eine JPEG Kamera von Bosch geben Sie den folgenden String ein:

`http://<ip-address>/snap.jpg?jpegCam=<channel_no.>`

Für eine RTSP Kamera von Bosch geben Sie folgende Zeichenfolge ein:

`rtsp://<ip-address>/rtsp_tunnel`

Benutzername

Geben Sie den Benutzernamen für die Authentifizierung auf dem Gerät ein. In der Regel: service.

Passwort

Geben Sie ein gültiges Passwort für die Authentifizierung auf dem Gerät ein.

Passwort anzeigen

Klicken Sie hier, um das eingegebene Passwort anzuzeigen. Achten Sie darauf, dass niemand das Passwort einsehen kann.

Bildrate [ips]

Geben Sie die gewünschte Bildfrequenzrate ein.

Siehe

– *Hinzufügen einer Kamera zu einem VSG, Seite 202*

13.25.7 Dialogfeld „RTSP-Encoder hinzufügen/bearbeiten“

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > Rechtsklick auf > **Encoder/Kamera hinzufügen** > Befehl **RTSP-Kamera**

oder

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > erweitern > Rechtsklick auf > Klick auf **RTSP-Kamera bearbeiten** > Dialogfeld **RTSP bearbeiten**

Sie können einen RTSP-Encoder Ihrem VSG Gerät hinzufügen.

Name

Geben Sie einen Anzeigenamen für das Gerät ein.

URL

Geben Sie die URL Ihrer JPEG-Kamera / RTSP Kamera ein.
Für eine JPEG Kamera von Bosch geben Sie den folgenden String ein:

`http://<ip-address>/snap.jpg?jpegCam=<channel_no.>`

Für eine RTSP Kamera von Bosch geben Sie folgende Zeichenfolge ein:

`rtsp://<ip-address>/rtsp_tunnel`

Hinweis: Wenn VSG zwei Streams unterstützt, geben Sie die entsprechende URL für den Stream mit hoher und niedriger Qualität ein.

Benutzername

Geben Sie den Benutzernamen für die Authentifizierung auf dem Gerät ein. In der Regel: service.

Passwort

Geben Sie ein gültiges Passwort für die Authentifizierung auf dem Gerät ein.

Passwort anzeigen

Klicken Sie hier, um das eingegebene Passwort anzuzeigen. Achten Sie darauf, dass niemand das Passwort einsehen kann.

Siehe

– *Hinzufügen einer Kamera zu einem VSG, Seite 202*

13.25.8 Verschieben eines VSG in einen anderen Pool (Pool ändern)

Hauptfenster > **Geräte** > erweitern > erweitern > >

Sie verschieben das Gerät von einem Pool in den anderen innerhalb des gleichen VRM Geräts, ohne Aufzeichnungsverlust.

Zum Verschieben:

1. Klicken Sie mit der rechten Maustaste auf / / und klicken Sie auf **Pool ändern...**.
   Das Dialogfeld **Pool ändern** wird angezeigt.
2. Wählen Sie in der Liste **Neuer Pool:** den gewünschten Pool aus.
3. Klicken Sie auf **OK**.
   Das Gerät wird in den ausgewählten Pool verschoben.

13.25.9 Konfigurieren von Multicast (Registerkarte „Multicast“)

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern >

Sie können für jede Kamera, die einem Video Streaming Gateway Gerät zugewiesen ist, eine Multicast-Adresse und einen Port konfigurieren.

So konfigurieren Sie Multicast:

1. Aktivieren Sie das gewünschte Kontrollkästchen, um Multicast zu ermöglichen.
2. Geben Sie eine gültige Multicast-Adresse und eine Port-Nummer ein.
3. Falls erforderlich, konfigurieren Sie das kontinuierliche Multicast-Streaming.

Registerkarte Multicast

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > > Registerkarte **Netzwerk** > Registerkarte **Multicast**

Dient zum Konfigurieren von Multicast für die zugewiesenen Kameras.

Aktivieren

Klicken Sie darauf, um Multicast für diese Kamera zu aktivieren.

Multicast-Adresse

Fügen Sie eine gültige Multicast-Adresse ein (im Bereich zwischen 224.0.0.0 und 239.255.255.255). Geben Sie `1.0.0.0` ein. Eine eindeutige Multicast-Adresse wird basierend auf der MAC-Adresse des Gerätes automatisch eingefügt.

Port

Wenn eine Firewall vorhanden ist, geben Sie einen Port-Wert ein, der in der Firewall als nicht gesperrter Port konfiguriert ist.

Streaming

Klicken Sie darauf, um fortlaufendes Multicast-Streaming zum Switch zu aktivieren. Dies bedeutet, dass der Multicast-Verbindung keine RCP+-Registrierung vorausgeht. Es findet immer ein Streaming aller Daten vom Encoder zum Switch statt. Falls keine IGMP-Multicast-Filterung unterstützt wird oder konfiguriert ist, sendet der Switch diese Daten wiederum an alle Ports, sodass der Switch überläuft. Sie benötigen Streaming, wenn Sie ein Fremdherstellergerät zum Empfangen eines Multicast-Streams verwenden.

13.25.10 Konfigurieren der Protokollierung (Registerkarte „Erweitert“)

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > >
Registerkarte **Service** > Registerkarte **Erweitert**
Dient zum Aktivieren der Protokollierung für Video-Streaming-Gateway.
Die Protokolldateien werden gewöhnlich in folgendem Verzeichnis gespeichert:

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

Ab VSG Version 7.0 werden die Protokolldateien gewöhnlich in folgendem Verzeichnis gespeichert:

```
C:\ProgramData\Bosch\VSG\log
```

Hinweis: Wenn Sie auf VSG Version 7.0 oder höher aktualisieren, werden vorherige Protokolldateien automatisch an diesen Speicherort verschoben.
Protokolldateien von älteren VSG Versionen werden in der Regel unter dem folgenden Pfad gespeichert:

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

Registerkarte Erweitert

RCP+-Protokollierung
Zur Aktivierung der RCP+-Protokollierung anklicken.

Debug-Protokollierung
Zur Aktivierung der Debug-Protokollierung anklicken.

RTP-Protokollierung
Zur Aktivierung der RTP-Protokollierung anklicken.

Speicherzeit (Tage)
Wählen Sie die gewünschte Anzahl an Tagen.

Kompletter Hauptspeicherauszug
Aktivieren Sie dieses Kontrollkästchen nur bei Bedarf, beispielsweise wenn der technische Kundendienst eine vollständige Hauptspeicherübersicht anfordert.

Telnet-Unterstützung
Aktivieren Sie dieses Kontrollkästchen, wenn Zugriffe über das Telnet-Protokoll unterstützt werden sollen. Aktivieren Sie dieses Kontrollkästchen nur bei Bedarf.

Hinweis!
Die umfassende Protokollierung benötigt erhebliche Prozessorleistung und Festplattenkapazität. Verwenden Sie die umfassende Protokollierung nicht im Dauerbetrieb.

13.25.11 Starten des ONVIF Camera Event Driver Tool aus dem Configuration Client

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern >
Sie können das ONVIF Camera Event Driver Tool direkt aus dem Configuration Client für das ausgewählte VSG starten.
Hinweis: Sie können das Tool auch über das Windows-Startmenü starten.
Mit dem ONVIF Camera Event Driver Tool können Sie ONVIF-Ereignisse zu VSG-BVIP-Ereignissen zuordnen. Sie können eine Verbindung zu ONVIF-Kameras herstellen und die ONVIF-Ereignisse für die Zuordnung abrufen.

Gehen Sie wie folgt vor, um das ONVIF Camera Event Driver Tool aus dem Configuration Client zu starten:

1. Klicken Sie mit der rechten Maustaste auf das entsprechende VSG.

2. Klicken Sie auf **ONVIF Camera Event Driver Tool starten**.
   Das ONVIF Camera Event Driver Tool wird angezeigt.

Hinweis!
Das ONVIF Camera Event Driver Tool unterstützt nur eine sichere Verbindung zum VSG.

So verwenden Sie das ONVIF Camera Event Driver Tool:
Weitere Informationen finden Sie unter Anleitungsvideo.

13.26 Seite Nur Live

Hauptfenster > **Geräte** > erweitern >
Ermöglicht es Ihnen, Encoder hinzuzufügen und zu konfigurieren, die für Nur-Live-Anwendungen verwendet werden. Sie können Bosch Encoder und ONVIF Netzwerk-Videosender hinzufügen.

Informationen zum Hinzufügen, Bearbeiten und Konfigurieren eines Nur-Live-ONFIV-Encoders finden Sie unter *ONVIF Seite, Seite 238*.

Siehe
- *Hinzufügen eines Nur-Live-Encoders, Seite 220*
- *Nach Geräten suchen, Seite 73*
- *Seite „Bosch Encoder/Decoder/Kamera“, Seite 217*
- *ONVIF Seite, Seite 238*
- *Konfigurieren von Multicast, Seite 236*

13.26.1 Hinzufügen von Nur-Live-Geräten per Suchvorgang

So fügen Sie Nur-Live-Geräte von Bosch per Suchvorgang hinzu:

1. Klicken Sie mit der rechten Maustaste auf und klicken Sie auf **Nach Nur Live-Encodern scannen**.
   Das Dialogfeld **BVMS Scan Wizard** wird angezeigt.
2. Aktivieren Sie die Kontrollkästchen der Geräte, die hinzugefügt werden sollen.
3. Klicken Sie auf **Weiter >>**.
   Das Dialogfeld des Assistenten für die **Authentifizierung der Geräte** wird angezeigt.
4. Geben Sie das Passwort für jedes Gerät ein, das von einem Passwort geschützt ist.
   Passwortüberprüfungen erfolgen automatisch, wenn Sie während ein paar Sekunden keine weiteren Zeichen im Passwortfeld eingeben oder außerhalb des Passwortfelds klicken.
   Wenn die Passwörter aller Geräte identisch sind, können Sie es im ersten Feld **Passwort** eingeben. Machen Sie mit der Maus einen Rechtsklick und klicke Sie dann auf **Zellinhalt in Spalte kopieren**.
   In der **Status** Spalte wird die erfolgreiche Anmeldung mit .
   angezeigt. Fehlgeschlagene Anmeldungen werden mithilfe von angezeigt.
5. Klicken Sie auf **Fertig stellen**.
   Das Gerät wird zum Gerätebaum hinzugefügt.

Das ⚠ Symbol weist auf einen Fehler hin, um den Sie sich kümmern müssen. In der QuickInfo finden Sie weitere Informationen zu dem jeweiligen Fehler.

13.26.2 Manuelles Hinzufügen eines Encoders

Hauptfenster > **Geräte** > Erweitern > Erweitern > Rechtsklicken > Klicken **Encoder hinzufügen** > **Encoder hinzufügen** Dialogfeld
oder

Hauptfenster > **Geräte** > Rechtsklicken > Klicken **Encoder hinzufügen** > **Encoder hinzufügen** Dialogfeld
oder

Hauptfenster > **Geräte** > Rechtsklicken > Klicken **Encoder hinzufügen** > **Encoder hinzufügen** Dialogfeld
oder

Hauptfenster > **Geräte** > Erweitern > Rechtsklicken > Klicken **Decoder hinzufügen** > **Encoder hinzufügen** Dialogfeld

Dient zum manuellen Hinzufügen eines Encoders. Dies ist insbesondere dann hilfreich, wenn Sie ein beliebiges Video-IP-Gerät von Bosch hinzufügen möchten (nur für VRM).

Hinweis:
Wenn Sie einen Video-IP-Encoder von Bosch mit der **<Automatisch erkennen>**-Auswahl hinzufügen, muss dieses Gerät im Netzwerk verfügbar sein.

So fügen Sie ein Video IP-Gerät von Bosch hinzu:

1. Erweitern Sie , erweitern Sie , und klicken Sie mit der rechten Maustaste auf .
   Oder
   Klicken Sie mit der rechten Maustaste auf .
   Oder
   Klicken Sie mit der rechten Maustaste auf .
2. Klicken Sie auf **Encoder hinzufügen**.
   Das Dialogfeld **Encoder hinzufügen** wird angezeigt.
3. Geben Sie die entsprechende IP-Adresse ein.
4. Wählen Sie in der Liste **<Automatisch erkennen>** aus, geben Sie das Passwort des Geräts ein, und klicken Sie auf **Authentifizieren.**
   Oder:
   Wählen Sie in der Liste einen konkreten Encoder-Typ oder **<Einzel Platzhalter Kamera>** aus.
5. Klicken Sie auf **OK**.
   Das Gerät wird dem System hinzugefügt.

Das ⚠ Symbol weist auf einen Fehler hin, um den Sie sich kümmern müssen. In der QuickInfo finden Sie weitere Informationen zu dem jeweiligen Fehler.

Dialogfeld Encoder hinzufügen

Netzwerkadresse
Geben Sie eine gültige IP-Adresse ein.

Port-Nummer
Geben Sie die Port-Nummer des Geräts ein.

Encodertyp
Wählen Sie für ein Gerät mit bekanntem Gerätetyp den entsprechenden Eintrag aus. Das Gerät muss nicht im Netzwerk verfügbar sein.
Wenn Sie ein beliebiges Video-IP-Gerät von Bosch hinzufügen möchten, wählen Sie **<Automatisch erkennen>**. Das Gerät muss im Netzwerk verfügbar sein.
Wenn Sie eine Kamera für die Offline-Konfiguration hinzufügen möchten, wählen Sie **<Einzel Platzhalter Kamera>**.

Benutzername
Zeigt den Benutzernamen für die Authentifizierung auf dem Gerät an.

Passwort
Geben Sie ein gültiges Passwort für die Authentifizierung beim Gerät ein.

Passwort anzeigen
Klicken Sie hier, damit das eingegebene Passwort angezeigt wird. Achten Sie darauf, dass niemand das Passwort einsehen kann.

Authentifizieren
Klicken Sie hier, um sich mit den oben eingegebenen Anmeldeinformationen auf dem Gerät zu authentifizieren.

13.26.3 Angeben des Ziel-Passworts für einen Decoder (Authentifizieren ...)

Hauptfenster > **Geräte** > erweitern > erweitern > Rechtsklick auf > Klick auf **Authentifizieren...** > Dialogfeld **Passwort eingeben**
Um den Zugriff eines passwortgeschützten Encoders auf einen Decoder zu ermöglichen, müssen Sie das Passwort der Benutzer-Berechtigungsstufe des Encoders als Ziel-Passwort in den Decoder eingeben.

So legen Sie ein Passwort fest:

1. Wählen Sie aus der Liste **Benutzername auswählen** die Option destination password aus.
2. Geben Sie im Feld **Passwort für Benutzer** das neue Passwort ein.
3. Klicken Sie auf **OK**.

⇨ Das Passwort wird auf dem Gerät umgehend geändert.

Siehe

– *Ändern des Passworts für einen Encoder/Decoder (Passwort ändern/Passwort eingeben), Seite 144*

13.27 Seite Lokale Archivierung

Hauptfenster > **Geräte** > Erweitern >
Ermöglicht es Ihnen, Encoder mit lokaler Archivierung hinzuzufügen und zu konfigurieren.

So fügen Sie Encoder mit lokaler Archivierung per Suchvorgang hinzu:

1. Klicken Sie im Gerätebaum mit der rechten Maustaste auf und klicken Sie anschließend auf **Nach Encodern mit lokaler Archivierung scannen**.
   Das Dialogfeld **BVMS Scan Wizard** wird angezeigt.
2. Aktivieren Sie die Kontrollkästchen der Geräte, die hinzugefügt werden sollen.
3. Klicken Sie auf **Weiter >>**.
   Das Dialogfeld des Assistenten für die **Authentifizierung der Geräte** wird angezeigt.
4. Geben Sie das Passwort für jedes Gerät ein, das von einem Passwort geschützt ist.
   Passwortüberprüfungen erfolgen automatisch, wenn Sie während ein paar Sekunden keine weiteren Zeichen im Passwortfeld eingeben oder außerhalb des Passwortfelds klicken.
   Wenn die Passwörter aller Geräte identisch sind, können Sie es im ersten Feld **Passwort** eingeben. Machen Sie mit der Maus einen Rechtsklick und klicke Sie dann auf **Zellinhalt in Spalte kopieren**.
   In der **Status** Spalte wird die erfolgreiche Anmeldung mit .
   angezeigt. Fehlgeschlagene Anmeldungen werden mithilfe von angezeigt.
5. Klicken Sie auf **Fertig stellen**.
   Das Gerät wird zum Gerätebaum hinzugefügt.

Das ⚠ Symbol weist auf einen Fehler hin, um den Sie sich kümmern müssen. In der QuickInfo finden Sie weitere Informationen zu dem jeweiligen Fehler.

Siehe
- *Konfigurieren von Multicast, Seite 236*
- *Hinzufügen eines Encoders mit lokaler Archivierung, Seite 220*
- *Seite „Bosch Encoder/Decoder/Kamera“, Seite 217*
- *Nach Geräten suchen, Seite 73*

13.28 Seite „Unmanaged Site“

Hauptfenster > **Geräte** > erweitern >

Sie können ein Videonetzwerkgerät zum **Unmanaged Sites**-Element des Gerätebaums hinzufügen. Es wird angenommen, dass alle Unmanaged Netzwerkgeräte einer unmanaged site in derselben Zeitzone angesiedelt sind.

Site-Name
Zeigt den Namen der Site an, der während der Erstellung dieses Elements eingegeben wurde.

Beschreibung
Geben Sie eine Beschreibung für diese site ein.

Zeitzone
Wählen Sie die entsprechende Zeitzone für diese unmanaged site aus.

Siehe
- *Unmanaged Site, Seite 28*
- *Manuelles Hinzufügen einer Unmanaged Site, Seite 214*
- *Importieren von Unmanaged Sites, Seite 214*

– *Konfiguration der Zeitzone, Seite 215*

13.28.1 Manuelles Hinzufügen einer Unmanaged Site

Hauptfenster > **Geräte** >

Erstellung:

1. Klicken Sie mit der rechten Maustaste auf und klicken Sie dann auf **Unmanaged Site hinzufügen**.
   Das Dialogfeld **Unmanaged Site hinzufügen** wird angezeigt.
2. Geben Sie einen Site-Namen und eine Beschreibung ein.
3. Wählen Sie in der **Zeitzone**-Liste den gewünschten Eintrag aus.
4. Klicken Sie auf **OK**.
   Dem System wird eine neue unmanaged site hinzugefügt.

Siehe

– *Unmanaged Site, Seite 28*
– *Seite „Unmanaged Site“, Seite 213*

13.28.2 Importieren von Unmanaged Sites

Hauptfenster > **Geräte** >

Sie können eine CSV-Datei mit einer Konfiguration des DVR oder anderen BVMS importieren, die Sie in Ihren BVMS als Unmanaged Site importieren möchten.

So importieren Sie die Datei:

1. Klicken Sie mit der rechten Maustaste auf , und klicken Sie dann auf **Unmanaged Sites importieren**.
2. Klicken Sie auf die gewünschte Datei, und klicken Sie auf **Öffnen**.
   Dem System wird mindestens eine neue unmanaged site hinzugefügt.
   Sie können diese unmanaged sites nun zum Logischen Baum hinzufügen.
   Hinweis: Wenn ein Fehler auftritt und die Datei nicht importiert werden kann, wird eine entsprechende Fehlermeldung angezeigt.

13.28.3 Seite „Unmanaged Site“

Site-Name
Zeigt den Namen der Site an, der während der Erstellung dieses Elements eingegeben wurde.

Beschreibung
Geben Sie eine Beschreibung für diese site ein.

Zeitzone
Wählen Sie die entsprechende Zeitzone für diese unmanaged site aus.

13.28.4 Hinzufügen eines Unmanaged Netzwerkgeräts

Hauptfenster > **Geräte** > >

1. Klicken Sie mit der rechten Maustaste auf dieses Element, und klicken Sie dann auf **Unmanaged Netzwerkgerät hinzufügen**.
   Das Dialogfeld **Unmanaged Netzwerkgerät hinzufügen** wird angezeigt.

2. Wählen Sie den gewünschten Gerätetyp aus.
3. Geben Sie eine gültige IP-Adresse oder einen Hostnamen und die Zugangsdaten für dieses Gerät ein.
4. Klicken Sie auf **OK**.
   Dem System wird ein neues **Unmanaged Netzwerkgerät** hinzugefügt.
   Sie können diese unmanaged site nun zum Logischen Baum hinzufügen.
   Beachten Sie, dass nur die Site im Logischen Baum angezeigt wird, jedoch nicht die Netzwerkgeräte, die zu dieser Site gehören.
5. Geben Sie den gültigen Benutzernamen für dieses Netzwerkgerät ein, sofern verfügbar.
6. Geben Sie das gültige Passwort ein, sofern verfügbar.

Dialogfeld Unmanaged Netzwerkgerät hinzufügen

Hauptfenster > **Geräte** > erweitern > Rechtsklick auf > Klick auf **Unmanaged Netzwerkgerät hinzufügen**

Gerätetyp:
Wählen Sie den zutreffenden Eintrag für dieses Gerät.
Verfügbare Einträge:
- **DIVAR AN / DVR**
- **DIVAR IP (AiO) / BVMS**
- **Bosch IP-Kamera/Encoder**

Netzwerkadresse:
Geben Sie eine IP-Adresse oder einen Hostnamen ein. Ändern Sie bei Bedarf die Port-Nummer.
Hinweis: Wenn Sie eine SSH-Verbindung verwenden, geben Sie die Adresse im folgenden Format ein:
ssh://IP oder Servername:5322

Sicherheit
Das Kontrollkästchen **Sichere Verbindung** ist standardmäßig aktiviert.

Hinweis!
Wenn beim Hinzufügen eines DVR das Kontrollkästchen **Sichere Verbindung** aktiviert ist, werden Befehl und Steuerungsverbindungen gesichert. Das Streaming von Videodaten ist nicht gesichert.

Benutzername:
Geben Sie den gültigen Benutzernamen für dieses Netzwerkgerät ein, sofern verfügbar. Weitere Informationen finden Sie unter *Unmanaged Site, Seite 28*.

Passwort:
Geben Sie das gültige Passwort ein, sofern verfügbar. Weitere Informationen zu Zugangsdaten finden Sie unter *Unmanaged Site, Seite 28*.

Siehe
- *Unmanaged Site, Seite 28*

13.28.5 Konfiguration der Zeitzone

Hauptfenster > **Geräte** > erweitern >
Sie können die Zeitzone einer unmanaged site konfigurieren. Dies ist nützlich, wenn ein Benutzer von Operator Client auf unmanaged site über einen Computer mit Operator Client zugreift, der sich in einer anderen Zeitzone als diese unmanaged site befindet.

So konfigurieren Sie die Zeitzone:

- Wählen Sie in der **Zeitzone**-Liste den gewünschten Eintrag aus.

Siehe

– *Seite „Unmanaged Site“, Seite 213*

14 Seite „Bosch Encoder/Decoder/Kamera“

Dieses Kapitel enthält Informationen zur Konfiguration von Encodern und Decodern in Ihrem System.

Hinweis!
BVMS Viewer unterstützt keine Decodergeräte.

Ausführliche Informationen zu den Encoder-, Decoder- oder Kameraeinstellungen, z. B. Video Content Analysis (VCA) oder Netzwerkeinstellungen, finden Sie in der Bedienungsanleitung des entsprechenden Geräts.
Die Anzahl der einem Eintrag untergeordneten Elemente wird in eckigen Klammern angezeigt.

So konfigurieren Sie einen Encoder:

Hauptfenster> **Geräte** > Erweitern > Erweitern > >
oder
Hauptfenster > **Geräte** > Erweitern > Erweitern > Erweitern >
oder
Hauptfenster > **Geräte** > >
oder
Hauptfenster > **Geräte** > >

So konfigurieren Sie einen Decoder:

Hauptfenster > **Geräte** > Erweitern > Erweitern >

Weitere Informationen finden Sie in der Online-Hilfe auf den Seiten .

So konfigurieren Sie eine Kamera:

Hauptfenster> **Geräte** > Erweitern > Erweitern > >
Hauptfenster > **Geräte** > Erweitern > Erweitern > > > >
oder
Hauptfenster> **Geräte** > Erweitern > Erweitern > erweitern> >
oder
Hauptfenster > **Geräte** > > >
oder
Hauptfenster > **Geräte** > > >

– Klicken Sie auf , um die Einstellungen zu speichern.
– Klicken Sie auf , um die letzte Einstellung rückgängig zu machen.

– Klicken Sie auf , um die Konfiguration zu aktivieren.

Die meisten Einstellungen auf den Encoder-/Decoder-/Kamera-Seiten sind sofort nach dem Klicken auf wirksam. Wenn Sie Einstellungen geändert haben und eine andere Registerkarte aufrufen, ohne zuvor auf zu klicken, werden zwei entsprechende Meldungsfelder angezeigt. Wenn Sie die Änderungen speichern möchten, bestätigen Sie beide Meldungen.

Klicken Sie zum Ändern der Passwörter eines Encoders mit der rechten Maustaste auf das Gerätesymbol und anschließend auf **Passwort ändern...**.

Klicken Sie zum Anzeigen des Geräts in einem Webbrowser mit der rechten Maustaste auf das Gerätesymbol und anschließend auf **Webseite im Browser anzeigen**.

Hinweis:

Je nach ausgewähltem Encoder oder Kamera sind nicht alle hier beschriebenen Seiten für jedes Gerät verfügbar. Die in dieser Beschreibung verwendeten Feldbezeichnungen können von Ihrer Software abweichen.

- Klicken Sie auf eine Registerkarte, um die entsprechende Eigenschaftsseite anzuzeigen.

So fügen Sie per Suchvorgang Encoder hinzu:

1. Klicken Sie mit der rechten Maustaste auf und klicken Sie auf **Nach Encodern scannen**.
   Das Dialogfeld **BVMS Scan Wizard** wird angezeigt.
2. Wählen Sie die erforderlichen Encoder sowie den gewünschten VRM-Pool aus und klicken Sie auf **Zuordnen**, um sie dem VRM-Pool zuzuweisen.
3. Klicken Sie auf **Weiter >>**.
   Das Dialogfeld des Assistenten für die **Authentifizierung der Geräte** wird angezeigt.
4. Geben Sie das Passwort für jedes Gerät ein, das von einem Passwort geschützt ist.
   Passwortüberprüfungen erfolgen automatisch, wenn Sie während ein paar Sekunden keine weiteren Zeichen im Passwortfeld eingeben oder außerhalb des Passwortfelds klicken.
   Wenn die Passwörter aller Geräte identisch sind, können Sie es im ersten Feld **Passwort** eingeben. Machen Sie mit der Maus einen Rechtsklick und klicke Sie dann auf **Zellinhalt in Spalte kopieren**.
   In der **Status** Spalte wird die erfolgreiche Anmeldung mit .

   angezeigt. Fehlgeschlagene Anmeldungen werden mithilfe von angezeigt.
5. Klicken Sie auf **Fertig stellen**.
   Das Gerät wird zum Gerätebaum hinzugefügt.

Das Symbol weist auf einen Fehler hin, um den Sie sich kümmern müssen. In der QuickInfo finden Sie weitere Informationen zu dem jeweiligen Fehler.

Siehe

– *Nach Geräten suchen, Seite 73*

14.1 Manuelles Hinzufügen eines Encoders

Hauptfenster > **Geräte** > Erweitern > Erweitern > Rechtsklicken > Klicken **Encoder hinzufügen** > **Encoder hinzufügen** Dialogfeld
oder

Hauptfenster > **Geräte** > Rechtsklicken > Klicken **Encoder hinzufügen** > **Encoder hinzufügen** Dialogfeld
oder

Hauptfenster > **Geräte** > Rechtsklicken > Klicken **Encoder hinzufügen** > **Encoder hinzufügen** Dialogfeld
oder

Hauptfenster > **Geräte** > Erweitern > Rechtsklicken > Klicken **Decoder hinzufügen** > **Encoder hinzufügen** Dialogfeld

Dient zum manuellen Hinzufügen eines Encoders. Dies ist insbesondere dann hilfreich, wenn Sie ein beliebiges Video-IP-Gerät von Bosch hinzufügen möchten (nur für VRM).

Hinweis:
Wenn Sie einen Video-IP-Encoder von Bosch mit der **<Automatisch erkennen>**-Auswahl hinzufügen, muss dieses Gerät im Netzwerk verfügbar sein.

So fügen Sie ein Video IP-Gerät von Bosch hinzu:

1. Erweitern Sie , erweitern Sie , und klicken Sie mit der rechten Maustaste auf .
   Oder
   Klicken Sie mit der rechten Maustaste auf .
   Oder
   Klicken Sie mit der rechten Maustaste auf .
2. Klicken Sie auf **Encoder hinzufügen**.
   Das Dialogfeld **Encoder hinzufügen** wird angezeigt.
3. Geben Sie die entsprechende IP-Adresse ein.
4. Wählen Sie in der Liste **<Automatisch erkennen>** aus, geben Sie das Passwort des Geräts ein, und klicken Sie auf **Authentifizieren.**
   Oder:
   Wählen Sie in der Liste einen konkreten Encoder-Typ oder **<Einzel Platzhalter Kamera>** aus.
5. Klicken Sie auf **OK**.
   Das Gerät wird dem System hinzugefügt.

Das ⚠ Symbol weist auf einen Fehler hin, um den Sie sich kümmern müssen. In der QuickInfo finden Sie weitere Informationen zu dem jeweiligen Fehler.

Dialogfeld Encoder hinzufügen

Netzwerkadresse
Geben Sie eine gültige IP-Adresse ein.

Port-Nummer
Geben Sie die Port-Nummer des Geräts ein.

Encodertyp
Wählen Sie für ein Gerät mit bekanntem Gerätetyp den entsprechenden Eintrag aus. Das Gerät muss nicht im Netzwerk verfügbar sein.
Wenn Sie ein beliebiges Video-IP-Gerät von Bosch hinzufügen möchten, wählen Sie **<Automatisch erkennen>**. Das Gerät muss im Netzwerk verfügbar sein.
Wenn Sie eine Kamera für die Offline-Konfiguration hinzufügen möchten, wählen Sie **<Einzel Platzhalter Kamera>**.

Benutzername
Zeigt den Benutzernamen für die Authentifizierung auf dem Gerät an.

Passwort
Geben Sie ein gültiges Passwort für die Authentifizierung beim Gerät ein.

Passwort anzeigen
Klicken Sie hier, damit das eingegebene Passwort angezeigt wird. Achten Sie darauf, dass niemand das Passwort einsehen kann.

Authentifizieren
Klicken Sie hier, um sich mit den oben eingegebenen Anmeldeinformationen auf dem Gerät zu authentifizieren.

14.2 Hinzufügen eines Encoders zu einem VRM-Pool

Informationen zum Hinzufügen eines Encoders zu einem VRM-Pool finden Sie unter *Hinzufügen von Encodern per Suchvorgang, Seite 179*.

Siehe
– *Hinzufügen eines Geräts, Seite 126*

14.3 Hinzufügen eines Nur-Live-Encoders

Informationen zum Hinzufügen eines Nur-Live-Encoders über den Suchvorgang finden Sie unter *Hinzufügen von Nur-Live-Geräten per Suchvorgang, Seite 210*.

Siehe
– *Hinzufügen eines Geräts, Seite 126*
– *Seite Nur Live, Seite 210*

14.4 Hinzufügen eines Encoders mit lokaler Archivierung

Informationen zum Hinzufügen eines Encoders mit lokaler Archivierung per Suchvorgang finden Sie unter *Seite Lokale Archivierung, Seite 212*.

Siehe
– *Hinzufügen eines Geräts, Seite 126*
– *Seite Lokale Archivierung, Seite 212*

14.5 Hinzufügen einer einzelnen Platzhalterkamera

Wenn Sie eine Kamera hinzufügen und konfigurieren möchten, die derzeit offline ist, können Sie stattdessen eine einzelne Platzhalterkamera hinzufügen. Sie können die einzelne Platzhalterkamera zum logischen Baum hinzufügen, um Ereignisse und Alarme zuzuordnen und zu konfigurieren.

So fügen Sie eine einzelne Platzhalterkamera hinzu

1. Klicken Sie mit der rechten Maustaste auf das Element im Gerätebaum, zu dem Sie die Platzhalterkamera hinzufügen möchten.
2. Klicken Sie auf **Encoder hinzufügen**.
   Das Dialogfeld **Encoder hinzufügen** wird angezeigt.
3. Geben Sie eine entsprechende IP-Adresse ein, die derzeit offline ist.
4. Wählen Sie den Encodertyp **<Einzel Platzhalter Kamera>**.
5. Konfigurieren Sie alle entsprechenden Einstellungen für die Platzhalterkamera.

So ersetzen Sie eine einzelne Platzhalterkamera

1. Klicken Sie mit der rechten Maustaste auf die entsprechende Platzhalterkamera.
2. Klicken Sie auf **Encoder bearbeiten**.
   Das Dialogfeld **Encoder bearbeiten** wird angezeigt.
3. Geben Sie die Netzwerkadresse der Ersatzkamera ein.
4. Geben Sie das richtige Passwort der Ersatzkamera ein.
5. Klicken Sie auf **OK**.
   Das **Gerätenamen aktualisieren** Dialogfeld wird angezeigt.
6. Klicken Sie auf **OK**.

Hinweis: Wenn die Gerätefunktionen der Ersatzkamera auf dem neuesten Stand sind, müssen Sie die Einstellungen überprüfen, die Sie in der Tabelle Kameras und Aufzeichnungen vorgenommen haben.

14.6 Importieren von Kameras aus einer CSV-Datei

Hauptfenster > **Geräte** > Erweitern > Erweitern

Sie können eine größere Anzahl von Kameras aus einer CSV-Datei importieren. Sie können Encoder- oder Kameranamen, logische Baumknoten und Benutzergruppen festlegen, die Zugriff auf die neu hinzugefügten Kameras haben.

CSV-Template

Sie können die Vorlage MassConfigurationTemplate.csvunter C:\Program Files\Bosch\VMS\Samples verwenden.

Hinweis: Verwenden Sie Komma als Trennzeichen für CSV-Spalten.

Säulenlautsprecher	Information
NetworkAddress	IP-Adresse des Encoders. Der Wert darf nicht leer und nicht dupliziert werden.
EncoderName	Name des Encoders. Der Wert darf nicht leer sein.
CameraNames	Name der Kameras des aktuellen Encoders. Der Wert darf nicht leer sein. Trennen Sie mehrere Kameras mit einem Semikolon.
UserName	Benutzername für die Authentifizierung auf dem Encoder. Der Wert kann leer sein.

Säulenlautsprecher	Information
Password	Passwort für die Berechtigungsprüfung auf dem Encoder. Der Wert kann leer sein.
LogicalTree	Pfade des logischen Baums, zu dem Sie die Kameras hinzufügen. Trennen Sie mehrere Pfade mit einem Semikolon. Wenn der Wert leer ist, werden die Kameras nicht zum logischen Baum hinzugefügt und Sie können keine Benutzergruppen zuweisen. Pfade des logischen Baumes beginnen mit „/“. Das „/“ ist nur für den Hauptknoten obligatorisch, für andere Ordner ist es optional. Sie müssen den Namen des Hauptknotens nicht zum Ordnerpfad hinzufügen. Wenn kein Pfad existiert, wird er erstellt.
Permissions	Zulässige Benutzergruppen. Trennen Sie mehrere Benutzergruppen mit einem Semikolon. Wenn der Wert leer ist, sollte für alle Gruppen auf die Kameras zugegriffen werden. Die Admin-Gruppe besitzt die Berechtigung, auf alle Kameras zu zugreifen. Wenn Sie keiner Gruppe Zugriff gewähren möchten, müssen Sie trotzdem die Gruppe „admin” hinzufügen. Wenn die Benutzergruppe nicht existiert, wird die Kamera nicht importiert. **1Hinweis:** Enterprise User Groups werden nicht unterstützt, nur Enterprise Accounts.

Beispiele:
NetworkAddress,EncoderName,CameraNames,UserName,Password,LogicalTree,Permissions
1.1.1.1,Encoder1,Camera1,service,pwd,/Folder1/Folder2;/Folder3,Admin Group
2.2.2.2,Multichannel2,Camera21;Camera22,service,pwd,/Folder1/Folder2,Admin Group;Operator

Die folgenden drei Berechtigungen sind erforderlich, bevor Sie mit dem Import beginnen:
- **Geräte-Eigenschaften ändern**
- **Logischen Baum ändern**
- **Benutzergruppen konfigurieren/Enterprise Accounts**

Hinweis: Ein Admin-Benutzer kann den Import jederzeit selbst machen.

So importieren Sie Kameras aus einer CSV-Datei:

1. Klicken Sie mit der rechten Maustaste auf und klicken Sie auf **Kameras von CSV-Datei importieren...**.
   Der Datei-Explorer öffnet sich.
2. Wählen Sie die entsprechende CSV-Datei aus und klicken Sie auf **Öffnen**.
   Hinweis: Die Verarbeitung der CSV-Datei kann eine Weile dauern, die maximale Anzahl der zu importierenden Kameras beträgt 250.
3. Der Dialog **CSV-Import** zeigt alle relevanten Informationen über erfolgreiche oder fehlgeschlagene Kameraimporte an.
   Klicken Sie auf **Nur Fehler anzeigen**, um alle fehlgeschlagenen Kameraimporte anzuzeigen.
4. Klicken Sie auf **Schließen**, um den Dialog zu schließen oder **Export-Log,** um eine Protokolldatei zu exportieren und zu speichern.

So zeigen Sie eine importierte Kamera auf dem Stadtplan an:

1. Hauptfenster >**Karten und Struktur** > Logischer Baum
2. Klicken Sie mit der rechten Maustaste auf die gewünschte Kamera und wählen Sie dann **Sichtbar auf einer Karte**.
   Die Kamera wird auf dem Stadtplan angezeigt.

14.7 Hinzufügen eines Bosch Encoders mit vorkonfigurierten Geolokalisierungseinstellungen

Wenn Sie einen Bosch Encoder mit vorkonfigurierten Geolokalisierungseinstellungen (Breitengrad, Längengrad, Azimut) hinzufügen, werden diese Einstellungen im BVMS beibehalten und ein Kamera-Hotspot wird automatisch an der entsprechenden Position auf der globalen Karte hinzugefügt.
Wenn Sie die Kameraposition auf der Karte oder die Richtung und den Sichtkegel der Kamera ändern, kommt es zu einer Diskrepanz zwischen den Geolokalisierungseinstellungen in BVMS und den Geolokalisierungseinstellungen in der Kamerakonfiguration.

- Um die Einstellungen in der Kamerakonfiguration mit den Einstellungen im BVMS zu synchronisieren, speichern und aktivieren Sie die BVMS-Konfiguration.

Wenn Sie die Geolokalisierungseinstellungen in der Kamerakonfiguration später ändern, werden sie auf die in BVMS konfigurierten Geolokalisierungseinstellungen zurückgesetzt, sobald Sie die BVMS-Konfiguration aktivieren.

Siehe

– *Konfigurieren von Kameras auf der globalen Karte, Seite 276*

14.8 Bearbeiten eines Encoders

14.8.1 Verschlüsseln von Live-Video (Encoder bearbeiten)

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > Klick auf > Dialogfeld **Encoder bearbeiten**

Hauptfenster > **Geräte** > erweitern > Rechtsklick auf > Dialogfeld **Encoder bearbeiten**

Hauptfenster > **Geräte** > erweitern > Klick auf > Dialogfeld **Encoder bearbeiten**

Sie können die sichere Verbindung von Live-Videos aktivieren, die von einem Encoder an die folgenden Geräte übertragen werden, wenn der HTTPS-Port 443 auf dem Encoder konfiguriert ist:

- Operator Client-Computer
- Management Server-Computer
- Configuration Client-Computer
- VRM-Computer
- Decoder

Hinweis:
Wenn diese Option aktiviert ist, funktioniert das ANR des betreffenden Geräts nicht.
Wenn diese Option aktiviert ist, funktioniert die Encoder-Wiedergabe auf Encodern mit Firmware älter als 6.30 nicht.
Nur Encoder mit Firmware-Version 7.0 oder höher unterstützen sicheres UDP. Wenn die sichere Verbindung in diesem Fall aktiviert ist, kann der Operator Client-Benutzer einen Stream auf UDP und auf UDP-Multicast umschalten.

Aktivieren:

1. Aktivieren Sie das Kontrollkästchen **Sichere Verbindung**.
2. Klicken Sie auf **OK**.
   Für diesen Encoder ist eine sichere Verbindung aktiviert.

Siehe

– *Konfigurieren von Multicast, Seite 236*
– *Dialogfeld „Encoder/Decoder bearbeiten“, Seite 224*

14.8.2 Aktualisieren der Gerätefunktionen (Encoder bearbeiten)

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > Rechtsklick auf > Klick auf **Encoder bearbeiten** > Dialogfeld **Encoder bearbeiten**

oder

Hauptfenster > **Geräte** > erweitern > Rechtsklick auf > Klick auf **Encoder bearbeiten** > Dialogfeld **Encoder bearbeiten**

oder

Hauptfenster > **Geräte** > erweitern > Rechtsklick auf > Klick auf **Encoder bearbeiten** > Dialogfeld **Encoder bearbeiten**

oder

Hauptfenster > **Geräte** > Erweitern > Erweitern > Rechtsklicken > Klicken **Decoder bearbeiten** > **Decoder bearbeiten** Dialogfeld

Nach einem Upgrade des Geräts können Sie die Gerätefunktionen aktualisieren. Eine Textmeldung informiert Sie darüber, ob die abgerufenen Gerätefunktionen den im BVMS gespeicherten Gerätefunktionen entsprechen.

So führen Sie die Aktualisierung durch:

1. Klicken Sie auf **OK**.
   Es wird ein Meldungsfeld mit dem folgenden Text angezeigt:
   Wenn Sie die Gerätemerkmale übernehmen, können sich die Aufzeichnungs- und Ereigniseinstellungen ändern. Prüfen Sie diese Einstellungen für dieses Gerät.
2. Klicken Sie auf **OK**.
   Die Gerätefunktionen werden aktualisiert.

Siehe

– *Dialogfeld „Encoder/Decoder bearbeiten“, Seite 224*

14.8.3 Dialogfeld „Encoder/Decoder bearbeiten“

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > Rechtsklick auf > Klick auf **Encoder bearbeiten** > Dialogfeld **Encoder bearbeiten**

oder

Hauptfenster > **Geräte** > erweitern > Rechtsklick auf > Klick auf **Encoder bearbeiten** > Dialogfeld **Encoder bearbeiten**
oder
Hauptfenster > **Geräte** > erweitern > Rechtsklick auf > Klick auf **Encoder bearbeiten** > Dialogfeld **Encoder bearbeiten**
oder
Hauptfenster > **Geräte** > Erweitern > Erweitern > Rechtsklicken > Klicken **Decoder bearbeiten** > **Decoder bearbeiten** Dialogfeld
Erlaubt die Überprüfung und Aktualisierung der Funktionalitäten eines Geräts. Beim Öffnen dieses Dialogfeldes wird das Gerät verbunden. Das Passwort wird geprüft, und die Funktionalitäten dieses Geräts werden mit denen im BVMS gespeicherten Gerätefunktionen verglichen.

Name
Zeigt den Gerätenamen an. Wenn Sie ein Video-IP-Gerät von Bosch hinzufügen, wird der Gerätename generiert. Ändern Sie den Eintrag bei Bedarf.

Netzwerkadresse / Port
Geben Sie die Netzwerkadresse des Geräts ein. Ändern Sie bei Bedarf die Port-Nummer.

Benutzername
Zeigt den Benutzernamen für die Authentifizierung auf dem Gerät an.

Passwort
Geben Sie ein gültiges Passwort für die Authentifizierung beim Gerät ein.

Passwort anzeigen
Klicken Sie hier, damit das eingegebene Passwort angezeigt wird. Achten Sie darauf, dass niemand das Passwort einsehen kann.

Authentifizieren
Klicken Sie hier, um sich mit den oben eingegebenen Anmeldeinformationen auf dem Gerät zu authentifizieren.

Sicherheit
Das Kontrollkästchen **Sichere Verbindung** ist standardmäßig aktiviert.
Wenn keine sichere Verbindung möglich ist, erscheint eine Meldung. Klicken Sie darauf, um das Häkchen zu entfernen.

Die folgenden Decoder unterstützen eine sichere Verbindung:
- VJD 7000
- VJD 8000
- VIP XD HD

Hinweis!
Die Verbindung zwischen einem Decoder und einem Encoder ist nur sicher, wenn beide mit einer sicheren Verbindung konfiguriert werden.

Videostream
UDP: Ermöglicht verschlüsseltes Muticast-Streaming für unterstützte Decoder-Geräte.
TCP: Ermöglicht verschlüsseltes Unicast-Streaming für unterstützte Decoder-Geräte.
Hinweis: Wenn für einen Encoder keine Multicast-Adresse konfiguriert ist, ruft der Decoder den Stream per Unicast ab.

Hinweis!
BVMS unterstützt nicht Bosch Kameras, die mit einem VSG verbunden sind.
BVMS unterstützt nur UDP Verschlüsselung für Plattformen, die älter sind als CPP13.

Gerätemerkmale
Sie können die angezeigten Gerätefunktionen nach Kategorien oder alphabetisch sortieren.
Eine Textmeldung informiert Sie darüber, ob die erkannten Gerätefunktionen den aktuellen Gerätefunktionen entsprechen.
Klicken Sie auf **OK**, um nach einem Upgrade des Geräts die Änderungen der Gerätefunktionen zu übernehmen.

Siehe
- *Verschlüsseln von Live-Video (Encoder bearbeiten), Seite 223*
- *Aktualisieren der Gerätefunktionen (Encoder bearbeiten), Seite 224*

14.9 Verwalten der Authentizitätsprüfung

Zur Aktivierung der Authentizitätsprüfung auf einem Encoder müssen Sie die folgenden Schritte durchführen:
- Konfigurieren Sie die Authentifizierung auf dem Encoder.
- Laden Sie ein Zertifikat vom Encoder herunter.
- Installieren Sie dieses Encoder-Zertifikat auf der Arbeitsstation, die Sie zur Authentizitätsprüfung nutzen.

Siehe
- *Überprüfung der Authentizität , Seite 226*

14.9.1 Überprüfung der Authentizität

Der Benutzer des Operator Client kann die Authentizität der Aufzeichnungen überprüfen. Die Authentizität der Exporte wird automatisch überprüft.
Der Administrator muss diese Schritte durchführen, um für eine lückenlose Zertifikatskette zu sorgen.
Für große Systeme (>30 Kameras) empfehlen wir, folgendermaßen vorzugehen:
- Lassen Sie Ihre Zertifizierungsstelle (CA) ein Zertifikat für jeden Encoder erstellen.
- Laden Sie das erstellte Zertifikat (einschließlich des privaten Schlüssels) in einer sicheren Art und Weise auf jeden Encoder hoch.
- Installieren Sie das CA-Zertifikat auf den Operator Client-Arbeitstationen, auf denen Sie die Authentizitätsprüfung durchführen möchten, oder auf anderen Computern, auf denen Exporte durchgeführt werden sollen.

Für kleine Systeme (<30 Kameras) empfehlen wir, folgendermaßen vorzugehen:
- Laden Sie das `HTTPS Server`-Zertifikat von jedem Encoder herunter.
- Installieren Sie diese Zertifikate auf den Operator Client-Arbeitsstationen, an denen Sie eine Authentizitätsprüfung durchführen möchten.

Für weitere Details wenden Sie sich an die IT-Abteilung Ihres Unternehmens.
Zur Aktivierung der sicheren Authentizitätsprüfung muss der Administrator die folgenden Schritte durchführen:
- Aktivierung der Authentifizierung auf jeder gewünschten Kamera.
- Für große Systeme: Upload und Zuweisung des entsprechenden Zertifikats zu jeder gewünschten Kamera.

– Bei kleinen Systemen: Herunterladen eines Zertifikats von jedem Encoder. Installation der Zertifikate zur Überprüfung auf einer Arbeitsstation.

Einschränkungen

Firmware-Version 6.30 oder höher ist erforderlich.
Wir empfehlen die gleichzeitige Authentizitätsprüfung von maximal 4 Kameras.
Der Benutzer des Operator Client kann die Authentizität des Live-Videos nicht überprüfen.
Hinweis: Ändern Sie das Zertifikat nicht, wenn eine Aufzeichnung läuft. Müssen Sie das Zertifikat ändern, stoppen Sie zunächst die Aufzeichnung, ändern Sie das Zertifikat und starten Sie die Aufzeichnung erneut.
Zur Authentizitätsprüfung der Aufzeichnung wird diese Aufzeichnung in einem Hintergrundprozess mit maximaler Geschwindigkeit wiedergegeben. In Netzwerken mit geringer Bandbreite kann die Wiedergabe langsam sein. Der Prüfprozess kann dann die entsprechend ausgewählte Zeitspanne dauern. Beispiel: Sie wählen Sie einen Zeitraum von einer Stunde. Der Prüfvorgang kann dann bis zu 1 Stunde dauern.
Der Benutzer kann nur überprüfen, ob eine Aufzeichnung authentisch ist. Wenn die Überprüfung nicht erfolgreich abgeschlossen wurde, bedeutet dies nicht unbedingt, dass das Video manipuliert worden ist. Viele andere Gründe, z. B. ein manuelles Löschen, können für die Fehler verantwortlich sein. Der Benutzer des Operator Client kann nicht zwischen einer beabsichtigten Änderung der Aufzeichnung oder einer betrügerischen Manipulation unterscheiden.
Video-Authentifizierung behandelt ausschließlich Methoden zur Überprüfung der Authentizität der Videos. Video-Authentifizierung behandelt in keiner Weise die Übertragung von Video und Daten.
Die Wasserzeichen-Funktion zur Authentizitätsprüfung in früheren BVMS Versionen wurde ersetzt. Die neue Authentizitätsprüfung steht automatisch nach einem Upgrade auf die neueste BVMS-Version zur Verfügung. Authentizitätsprüfungen, die in der Vergangenheit erfolgreich waren, können jetzt nicht mehr verifiziert werden, da diese Aufzeichnungen nicht die erforderlichen erweiterten Informationen enthalten.
Die Authentizitätsprüfung wird in den folgenden Fällen nicht unterstützt:

– Transcodierung
– Lokale Aufzeichnung
– VSG
– Digitaler Videorekorder
– Bosch Recording Station
– ANR

Siehe

– *Konfigurieren der Authentifizierung, Seite 227*
– *Hochladen eines Zertifikats, Seite 228*
– *Download eines Zertifikats, Seite 228*
– *Installierung eines Zertifikats auf einer Arbeitsstation, Seite 228*

14.9.2 Konfigurieren der Authentifizierung

Hauptfenster > **Geräte** > Erweitern > Erweitern > Erweitern >
oder
Hauptfenster > **Geräte** > Erweitern >
Sie können die Überprüfung der Authentizität auf einem Encoder aktivieren.

So führen Sie die Konfiguration durch:

1. Klicken Sie auf **Kamera**, und dann klicken Sie auf **Videoeingang**

2. Wählen Sie aus der Liste **Video-Authentifizierung SHA-256** aus.
3. Wählen Sie aus der Liste **Signatur-Intervalle** den gewünschten Wert aus.
   Ein kleiner Wert erhöht die Sicherheit, ein großer Wert reduziert die Belastung für den Encoder.
4. Klicken Sie auf .

14.9.3 Hochladen eines Zertifikats

Hauptfenster > **Geräte** > Erweitern > Erweitern > Erweitern >
oder
Hauptfenster > **Geräte** > Erweitern >
Sie können ein abgeleitetes Zertifikat auf einen Encoder laden.

So gehen Sie vor:

1. Klicken Sie auf **Service**, und klicken Sie dann auf **Zertifikate**.
2. Klicken Sie auf **Zertifikat-Upload**.
3. Wählen Sie die entsprechende Datei, die das Zertifikat für diesen Encoder enthält. Diese Datei muss den privaten Schlüssel enthalten, z. B. *.PEM.
   Gewährleisten Sie eine sichere Datenübertragung.
4. Klicken Sie auf **Öffnen**.
5. Wählen Sie in der Liste **Verwendung** einen **HTTPS-Server** aus, um das hochgeladene Zertifikat einem **HTTPS-Server**-Eintrag zuzuweisen.
6. Klicken Sie auf .

14.9.4 Download eines Zertifikats

Hauptfenster > **Geräte** > Erweitern > Erweitern > Erweitern >
oder
Hauptfenster > **Geräte** > Erweitern >
Sie können ein Zertifikat von einem Encoder herunterladen.

Herunterladen:

1. Klicken Sie auf **Service** und klicken Sie dann auf **Zertifikate**.
2. Wählen Sie das gewünschte Zertifikat aus und klicken Sie auf das Symbol `Save`.
3. Wählen Sie das entsprechende Verzeichnis, in dem die Zertifikatdatei gespeichert werden soll.
4. Nennen Sie die Erweiterung der Zertifikatdatei zu `*.cer` um.

Sie können dieses Zertifikat jetzt auf der Arbeitsstation installieren, auf der Sie die Authentizität prüfen möchten.

14.9.5 Installierung eines Zertifikats auf einer Arbeitsstation

Sie können das Zertifikat, das Sie von einen Encoder heruntergeladen haben, auf der Arbeitsstation installieren, auf der Sie die Authentizitätsprüfung durchführen möchten.

1. Starten Sie die `Microsoft Management Console` auf der Arbeitsstation.
2. Fügen Sie das `Certificates` Snap-In auf diesem Computer hinzu, mit der ausgewählten Option `Computer account`.
3. Erweitern Sie `Certificates (Local computer)`, dann `Trusted Root Certification Authorities`.

4. Klicken Sie mit der rechten Maustaste auf `Certificates`, zeigen Sie auf `All Tasks` und klicken Sie dann auf `Import...`.
   Der `Certificate Import Wizard` wird angezeigt.
   Die `Local Machine` Option wird voreingestellt und kann nicht geändert werden.
5. Klicken Sie auf `Next`.
6. Wählen Sie die vom Encoder heruntergeladene Zertifikatdatei aus.
7. Klicken Sie auf `Next`.
8. Lassen Sie die Einstellungen unverändert und klicken auf `Next`.
9. Lassen Sie die Einstellungen unverändert und klicken auf `Finish`.

14.10 Angeben des Ziel-Passworts für einen Decoder (Authentifizieren ...)

Hauptfenster > **Geräte** > erweitern > erweitern > Rechtsklick auf > Klick auf **Authentifizieren...** > Dialogfeld **Passwort eingeben**

Um den Zugriff eines passwortgeschützten Encoders auf einen Decoder zu ermöglichen, müssen Sie das Passwort der Benutzer-Berechtigungsstufe des Encoders als Ziel-Passwort in den Decoder eingeben.

So legen Sie ein Passwort fest:

1. Wählen Sie aus der Liste **Benutzername auswählen** die Option destination password aus.
2. Geben Sie im Feld **Passwort für Benutzer** das neue Passwort ein.
3. Klicken Sie auf **OK**.

⇨ Das Passwort wird auf dem Gerät umgehend geändert.

Siehe

– *Ändern des Passworts für einen Encoder/Decoder (Passwort ändern/Passwort eingeben), Seite 229*

14.11 Ändern des Passworts für einen Encoder/Decoder (Passwort ändern/Passwort eingeben)

Hauptfenster> **Geräte** > Erweitern > Erweitern > >

oder

Hauptfenster > **Geräte** > >

oder

Hauptfenster > **Geräte** > >

oder

Hauptfenster > **Geräte** > erweitern > erweitern >

Definieren Sie für jede Berechtigungsstufe ein eigenes Passwort, oder ändern Sie das jeweilige Passwort entsprechend. Geben Sie das Passwort (max. 19 Zeichen, keine Sonderzeichen) für die ausgewählte Berechtigungsstufe ein.

So ändern Sie das Passwort:

1. Klicken Sie mit der rechten Maustaste auf und anschließend auf **Passwort ändern...**.
   Das Dialogfeld **Passwort eingeben** wird angezeigt.

2. Wählen Sie aus der Liste **Benutzername auswählen** den gewünschten Benutzer aus, für den Sie das Passwort ändern möchten.
3. Geben Sie im Feld **Passwort für Benutzer** das neue Passwort ein.
4. Klicken Sie auf **OK**.

⇨ Das Passwort wird auf dem Gerät umgehend geändert.

Durch ein Passwort wird ein unbefugter Zugriff auf das Gerät verhindert. Über verschiedene Berechtigungsstufen können Sie den Zugriff einschränken.
Ein ordnungsgemäßer Passwortschutz ist nur gewährleistet, wenn auch alle höheren Berechtigungsstufen durch ein Passwort geschützt sind. Deshalb müssen Sie beim Vergeben von Passwörtern stets mit der höchsten Berechtigungsstufe beginnen.
Wenn Sie mit dem service-Benutzerkonto angemeldet sind, können Sie ein Passwort für jede Berechtigungsstufe festlegen und ändern.
Das Gerät hat drei Berechtigungsstufen: service, user und live.

- service ist die höchste Berechtigungsstufe. Die Eingabe des richtigen Passworts ermöglicht den Zugriff auf alle Funktionen und die Änderung aller Konfigurationseinstellungen.
- user ist die mittlere Berechtigungsstufe. Auf dieser Stufe können Sie das Gerät bedienen, Aufzeichnungen wiedergeben und z. B. auch die Kamera steuern, nicht jedoch die Konfiguration ändern.
- live ist die niedrigste Berechtigungsstufe. Auf dieser Stufe können Sie nur das Live-Videobild anschauen und zwischen den verschiedenen Livebild-Darstellungen wechseln.

Bei einem Decoder ersetzen die folgenden Berechtigungsstufen die live-Berechtigungsstufe:

- destination password (nur bei Decodern verfügbar)
  Wird für den Zugriff auf einen Encoder verwendet.

Siehe

- *Angeben des Ziel-Passworts für einen Decoder (Authentifizieren ...), Seite 229*

14.12 Verschieben eines Encoders in einen anderen Pool (Pool ändern)

Hauptfenster> **Geräte** > erweitern > erweitern > >

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > erweitern

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern >

Sie verschieben das Gerät von einem Pool in den anderen innerhalb des gleichen VRM Geräts, ohne Aufzeichnungsverlust.

Zum Verschieben:

1. Klicken Sie mit der rechten Maustaste auf / / und klicken Sie auf **Pool ändern...**.
   Das Dialogfeld **Pool ändern** wird angezeigt.
2. Wählen Sie in der Liste **Neuer Pool:** den gewünschten Pool aus.
3. Klicken Sie auf **OK**.
   Das Gerät wird in den ausgewählten Pool verschoben.

Dialogfeld Pool ändern

Dient zum Ändern der Pool-Zuordnung eines Geräts.

Aktueller Pool:
Zeigt die Nummer des Pools an, dem das ausgewählte Gerät aktuell zugewiesen ist.

Neuer Pool:
Wählen Sie die gewünschte Pool-Nummer.

14.13 Wiederherstellung von Aufzeichnungen von einem ausgetauschten Encoder (Aufzeichnungen von Vorgänger zuweisen)

Hauptfenster > **Geräte** > erweitern > erweitern > >

Wenn ein defekter Encoder ausgetauscht wird, sind die Aufzeichnungen des ausgetauschten Encoders für den neuen Encoder bei der Auswahl des neuen Encoders im Operator Client verfügbar.

Hinweis!
Ein Encoder kann nur durch einen Encoder mit derselben Anzahl an Kanälen ersetzt werden.

So stellen Sie Aufzeichnungen von einem ausgetauschten Encoder wieder her:

Hinweis!
Verwenden Sie nicht den Befehl **Encoder bearbeiten**.

1. Rechtsklick auf > Befehl **Die Aufzeichnungen des Vorgängergerätes zuordnen ...**.
2. Das Dialogfeld **Die Aufzeichnungen des Vorgängergerätes zuordnen ...** wird angezeigt.
3. Geben Sie die Netzwerkadresse und ein gültiges Passwort für das neue Gerät ein.
4. Klicken Sie auf **OK**.
5. Klicken Sie auf , um die Einstellungen zu speichern.
6. Klicken Sie auf , um die Konfiguration zu aktivieren.

Dialogfeld Die Aufzeichnungen des Vorgängergerätes zuordnen ...
Dient zum Wiederherstellen von Aufzeichnungen eines ausgetauschten Encoders. Nach der Konfiguration der Einstellungen im Dialogfeld sind die Aufzeichnungen des ausgetauschten Encoders für den neuen Encoder verfügbar, wenn der neue Encoder im Operator Client ausgewählt wird.

Netzwerkadresse / Port
Geben Sie die Netzwerkadresse des Geräts ein.

Benutzername
Zeigt den Benutzernamen für die Authentifizierung beim Gerät an.

Passwort
Geben Sie ein gültiges Passwort für die Authentifizierung beim Gerät ein.

Authentifizieren
Klicken Sie hier, um sich mit den oben eingegebenen Anmeldeinformationen beim Gerät zu authentifizieren.

14.14 Konfigurieren von Encodern/Decodern

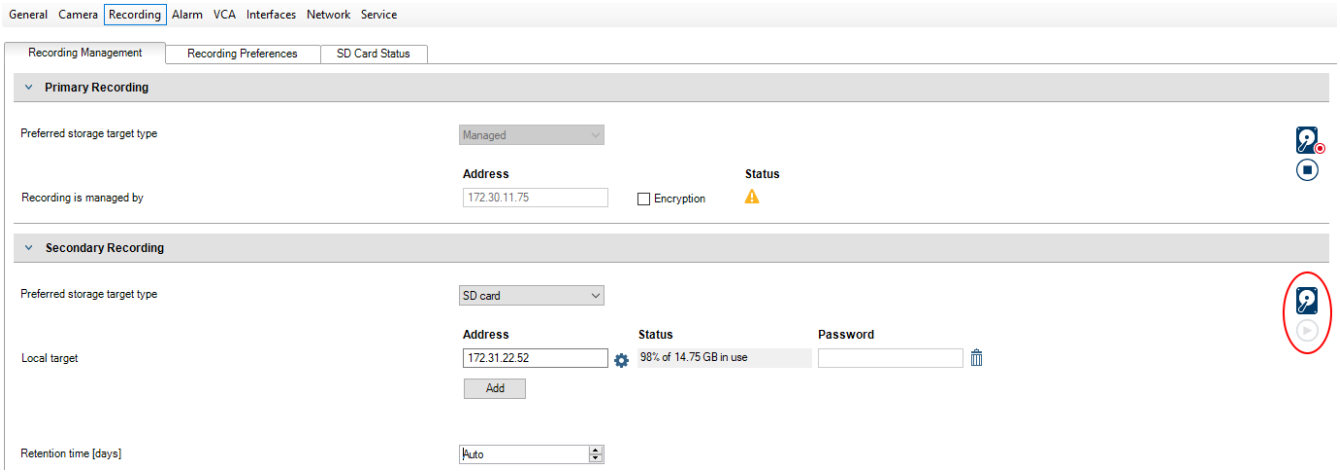
14.14.1 Speichermedien eines Encoders konfigurieren

Hauptfenster > **Geräte** > erweitern > erweitern > > > **Erweiterte Einstellungen** > **Aufzeichnungsverwaltung**

Hinweis: Stellen Sie sicher, dass die gewünschten Kameras dieses Encoders dem Logischen Baum hinzugefügt werden.

Um die ANR-Funktion zu nutzen, müssen die Speichermedien eines Encoders entsprechend konfiguriert werden.

Hinweis: Wenn Sie die Speichermedien eines Encoders konfigurieren möchten, der bereits dem System hinzugefügt wurde und über VRM erfasst wurde, stellen Sie sicher, dass die sekundäre Aufzeichnung gestoppt wurde:



Die ANR-Funktion ist nur zusammen mit Encodern möglich, die über eine Firmware-Version 5.90 oder höher verfügen. Nicht alle Encoder-Typen unterstützen die ANR-Funktion, selbst wenn die korrekte Firmware-Version installiert ist.

So konfigurieren Sie die Speichermedien eines Encoders:

1. Wählen Sie unter **Sekundäre Aufzeichnung** in der Liste **Bevorzugter Speicherzieltyp** das Speichermedium aus. Je nach Gerätetyp stehen verschiedene Medien zur Verfügung.
2. Klicken Sie gegebenenfalls auf die Schaltfläche „ ... ”, um die Speichermedien zu formatieren. Nach erfolgreicher Formatierung ist das Speichermedium für die Verwendung mit der ANR-Funktion bereit.
3. Konfigurieren Sie die ANR-Funktion für diesen Encoder auf der Seite **Kameras und Aufzeichnung**.

Siehe

- *Seite „Recording Management“ (Aufzeichnungsverwaltung), Seite 235*
- *ANR-Funktion konfigurieren, Seite 308*

14.14.2 Konfigurieren mehrerer Encoder/Decoder

Hauptfenster

Sie können die folgenden Eigenschaften für mehrere Encoder und Decoder gleichzeitig ändern:

- Gerätepasswörter
- IP-Adressen
- Anzeigenamen
- Subnetzmaske

– Gateway-ID
– Firmware-Versionen

So wählen Sie mehrere Geräte aus:

- Wählen Sie die gewünschten Geräte aus, indem Sie die STRG- oder die UMSCHALT-Taste drücken.

So wählen Sie alle verfügbaren Geräte aus:

- Klicken Sie auf den Befehl **Alles auswählen**.

So ändern Sie das Passwort für mehrere Geräte:

1. Klicken Sie im Hauptfenster **Geräte** auf den Befehl **Gerätepasswörter ändern**.
   oder
   Klicken Sie im Menü **Hardware** auf **Gerätepasswörter ändern...**
   Das Dialogfeld **Gerätepasswörter ändern** wird angezeigt.
2. Wählen Sie die erforderlichen Geräte aus.
3. Klicken Sie mit der rechten Maustaste auf die ausgewählten Geräte.
4. Klicken Sie auf **Passwort bearbeiten...**. Das Dialogfeld **Passwörter ändern** wird angezeigt.
5. Nehmen Sie die erforderlichen Einstellungen vor.

Hinweis!
Sie können nur Passworttypen auswählen, die für alle ausgewählten Geräte verfügbar sind.

So konfigurieren Sie mehrere Anzeigenamen:

1. Klicken Sie im Menü **Hardware** auf **Geräte IP und Netzwerkeinstellungen ändern...**.
   Das Dialogfeld **Geräte-IP und Netzwerkeinstellungen ändern** wird angezeigt.
2. Wählen Sie die erforderlichen Geräte aus.
3. Klicken Sie mit der rechten Maustaste auf die ausgewählten Geräte.
4. Klicken Sie auf **Display-Namen vergeben ...**.
   Das Dialogfeld **Display-Namen vergeben** wird angezeigt.
5. Nehmen Sie die erforderlichen Einstellungen vor.

So konfigurieren Sie mehrere IP-Adressen:

Hinweis!
Wird die IP-Adresse eines IP-Geräts geändert, ist eine Kommunikation mit dem Gerät unter Umständen nicht mehr möglich.

1. Klicken Sie im Menü **Hardware** auf **Geräte IP und Netzwerkeinstellungen ändern...**.
   Das Dialogfeld **Geräte-IP und Netzwerkeinstellungen ändern** wird angezeigt.
2. Wählen Sie die erforderlichen Geräte aus.
3. Klicken Sie mit der rechten Maustaste auf die ausgewählten Geräte.
4. Klicken Sie auf **IP-Adresse einstellen...**.
   Das Dialogfeld **IP-Adressen vergeben** wird angezeigt.

5. Nehmen Sie die erforderlichen Einstellungen vor.

So ändern Sie Subnetzmaske/Gateway-ID für mehrere Geräte:

1. Klicken Sie auf das gewünschte Feld eines Geräts, das Sie ändern möchten.
2. Geben Sie den entsprechenden Wert ein.
3. Wählen Sie alle erforderlichen Geräte aus.
4. Klicken Sie mit der rechten Maustaste auf das erforderliche Feld des Geräts, bei dem Sie bereits den Wert geändert haben.
5. Klicken Sie auf den Befehl **Kopiere Zellinhalt nach** und auf den Befehl **Auswahl in Spalte** .
   Oder klicken Sie bei Bedarf auf den Befehl **Ganze Spalte**.

Hinweis!
Sie können auch vollständige Zeilen kopieren, um IP-Adressen, Anzeigenamen, Subnetzmasken und Gateway-IDs für mehrere Geräte zu ändern.

So aktualisieren Sie Firmware für mehrere Geräte:

1. Klicken Sie im Menü **Hardware** auf **Geräte Firmware aktualisieren...**.
   Das Dialogfeld **Geräte-Firmware aktualisieren** wird angezeigt.
2. Wählen Sie die erforderlichen Geräte aus.
3. Klicken Sie auf den Befehl **Firmware aktualisieren**.
4. Wählen Sie die Datei aus, die das Update enthält.
5. Klicken Sie auf **OK**.

Vorgangsresultat
Zeigt den entsprechenden Status für die betroffenen Geräte an.

14.14.3 Konfigurieren des Failover-Aufzeichnungsmodus auf einem Encoder

Hauptfenster> **Geräte** > Erweitern > Erweitern > >

Voraussetzungen: Auf der **Pool** Seite, wählen Sie aus der **Modus Aufzeichnungspräferenzen**-Liste **Failover**. Wenn **Automatisch** ausgewählt ist, werden die Einstellungen automatisch durchgeführt und können nicht konfiguriert werden.
Wenn Sie sowohl für den automatischen als auch für den Failover-Modus ein Sekundärziel verwenden möchten, wählen Sie auf der Seite **Pool** in der **Nutzung Zweit-Target**-Liste **Ein** aus.
Es wird empfohlen, mindestens zwei iSCSI-Geräte für den Failover-Modus zu konfigurieren.

So führen Sie die Konfiguration durch:

1. Klicken Sie auf **Erweiterte Einstellungen**.
2. Klicken Sie auf **Aufzeichnungspräferenzen**.
3. Wählen Sie unter **Erst-Target** den Eintrag für das entsprechende Ziel aus. Alle unter **Speichersysteme** eingegebenen Speichersysteme werden in der Liste angezeigt.
4. Wählen Sie unter **Zweit-Target** den Eintrag für das entsprechende Ziel aus. Alle unter **Speichersysteme** eingegebenen Speichersysteme werden in der Liste angezeigt.
   Die Änderungen werden sofort aktiv. Eine Aktivierung ist nicht erforderlich.

Verwandte Themen

– *Konfigurieren des automatischen Aufzeichnungsmodus auf einem Pool, Seite 182*

14.14.4 Seite „Recording Management“ (Aufzeichnungsverwaltung)

Aktive Aufzeichnungen sind durch gekennzeichnet.
Punkt zum Symbol. Hier werden Details zur aktiven Aufzeichnung angezeigt.

Aufzeichnungen manuell verwaltet
Die Aufzeichnungen werden lokal auf diesem Encoder verwaltet. Alle relevanten Einstellungen müssen manuell vorgenommen werden. Encoder/IP-Kamera fungieren als Nur-Live-Gerät. Sie dürfen nicht automatisch vom VRM entfernt werden.

Aufzeichnung 1 von VRM verwaltet
Die Aufzeichnungen dieses Encoders werden vom VRM-System verwaltet.

Dual-VRM
Aufzeichnung 2 dieses Encoders wird von einem sekundären VRM verwaltet.

Registerkarte iSCSI-Medien
Klicken Sie darauf, um den verfügbaren iSCSI-Speicher anzuzeigen, der mit diesem Encoder verbunden ist.

Registerkarte Lokale Medien
Klicken Sie darauf, um den verfügbaren lokalen Speicher auf diesem Encoder anzuzeigen.

Hinzufügen
Klicken Sie, um ein Speichergerät zur Liste der verwalteten Speichermedien hinzuzufügen.

Entfernen
Klicken Sie darauf, um ein Speichergerät aus der Liste der verwalteten Speichermedien zu entfernen.

Siehe
– *Speichermedien eines Encoders konfigurieren, Seite 232*

14.14.5 Seite „Aufzeichnungspräferenzen“

Die Seite **Aufzeichnungspräferenzen** wird für jeden Encoder angezeigt. Die Anzeige der Seite erfolgt nur, wenn ein Gerät einem VRM-System zugeordnet ist.

Erst-Target
Nur sichtbar, wenn die Liste **Modus Aufzeichnungspräferenzen** auf der Seite **Pool** auf **Failover** eingestellt ist.
Wählen Sie den Eintrag für das entsprechende Ziel aus.

Zweit-Target
Nur sichtbar, wenn die Liste **Modus Aufzeichnungspräferenzen** auf der Seite **Pool** auf **Failover** und die Liste **Nutzung Zweit-Target** auf **Ein** eingestellt ist.
Wählen Sie den Eintrag für das entsprechende Ziel für die Konfiguration des Failover-Modus aus.

Siehe
– *Seite „Pool“, Seite 180*

14.14.6 Konfigurieren von Decodern für das On-Screen-Display (OSD)

Zum Aktivieren des On-Screen-Displays (OSD) für Decoder müssen Sie die entsprechenden Decodereinstellungen konfigurieren.

Konfigurieren von VIDEOJET decoder 8000

Hauptfenster > **Geräte** > erweitern > erweitern > > **Erweitert** > **Anzeige**
Konfigurieren Sie im Bereich **Bildeinblendung** die folgenden Einstellungen:

– **Alarmmodus einblenden**: Wählen Sie **Benutzerdefiniert** aus.
– Geben Sie die **X**- und **Y**-Koordinaten ein, um die Position der OSD-Einblendung festzulegen.
– Geben Sie die gewünschte Höhe, Farbe und Hintergrundfarbe für den Alarmtext an.

Konfigurieren von VIDEOJET decoder 7513, VIDEOJET decoder 7523

Hauptfenster > **Geräte** > erweitern > erweitern > > **Erweitert** > **Anzeige**

Konfigurieren Sie im Bereich **Bildeinblendung** die folgenden Einstellungen:
– **Alarmmodus einblenden**: Wählen Sie **Benutzerdefiniert** aus.
– Geben Sie die **X**- und **Y**-Koordinaten ein, um die Position der OSD-Einblendung festzulegen.
– Geben Sie die gewünschte Höhe, Farbe und Hintergrundfarbe für den Alarmtext an.

Konfigurieren Sie im Bereich **Einblendungsmodus** die folgende Einstellung:
– **Einblendungsmodus**: Wählen Sie **Text** aus.

14.15 Konfigurieren von Multicast

Sie können für jede zugewiesene Kamera eine Multicast-Adresse mit Port konfigurieren.

So konfigurieren Sie Multicast:

1. Aktivieren Sie das gewünschte Kontrollkästchen, um Multicast zu ermöglichen.
2. Geben Sie eine gültige Multicast-Adresse und eine Port-Nummer ein.
3. Falls erforderlich, konfigurieren Sie das kontinuierliche Multicast-Streaming.

Registerkarte Multicast

Hauptfenster > **Geräte** > >

oder

Hauptfenster > **Geräte** > >

oder

Hauptfenster> **Geräte** > Erweitern > Erweitern > >

> Registerkarte **Netzwerk** > Registerkarte **Multicast**

Dient zum Konfigurieren von Multicast für die zugewiesenen Kameras.

Aktivieren
Klicken Sie darauf, um Multicast für diese Kamera zu aktivieren.

Multicast-Adresse
Fügen Sie eine gültige Multicast-Adresse ein (im Bereich zwischen 224.0.0.0 und 239.255.255.255). Geben Sie `1.0.0.0` ein. Eine eindeutige Multicast-Adresse wird basierend auf der MAC-Adresse des Gerätes automatisch eingefügt.

Port
Wenn eine Firewall vorhanden ist, geben Sie einen Port-Wert ein, der in der Firewall als nicht gesperrter Port konfiguriert ist.

Streaming
Klicken Sie darauf, um fortlaufendes Multicast-Streaming zum Switch zu aktivieren. Dies bedeutet, dass der Multicast-Verbindung keine RCP+-Registrierung vorausgeht. Es findet immer ein Streaming aller Daten vom Encoder zum Switch statt. Falls keine IGMP-Multicast-Filterung unterstützt wird oder konfiguriert ist, sendet der Switch diese Daten wiederum an alle Ports, sodass der Switch überläuft.

Sie benötigen Streaming, wenn Sie ein Fremdherstellergerät zum Empfangen eines Multicast-Streams verwenden.

Hinweis!
Multicast-Streams sind nur sicher, wenn der Encoder über die Firmware-Version 7.0 oder höher verfügt und das Kontrollkästchen **Sichere Verbindung** aktiviert ist.

Siehe

– *Verschlüsseln von Live-Video (Encoder bearbeiten), Seite 223*

15 ONVIF Seite

Hauptfenster > **Geräte** > erweitern >
oder

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > >
erweitern

Siehe

- *Seite „Video Streaming Gateway-Gerät“, Seite 200*
- *Seite Nur Live, Seite 210*

15.1 Hinzufügen eines Nur-Live-ONVIF-Geräts per Suchvorgang

So fügen Sie ONVIF-Nur-Live-Geräte per Suchvorgang hinzu:

1. Klicken Sie mit der rechten Maustaste auf und klicken Sie dann auf **Nach Nur Live ONVIF-Encodern scannen**.
   Das Dialogfeld **BVMS Scan Wizard** wird angezeigt.
2. Aktivieren Sie die Kontrollkästchen der Geräte, die hinzugefügt werden sollen.
3. Klicken Sie auf **Weiter >>**.
   Das Dialogfeld des Assistenten für die **Authentifizierung der Geräte** wird angezeigt.
4. Geben Sie das Passwort für jedes Gerät ein, das von einem Passwort geschützt ist.
   Passwortüberprüfungen erfolgen automatisch, wenn Sie während ein paar Sekunden keine weiteren Zeichen im Passwortfeld eingeben oder außerhalb des Passwortfelds klicken.
   Wenn die Passwörter aller Geräte identisch sind, können Sie es im ersten Feld **Passwort** eingeben. Klicken Sie mit der rechten Maustaste auf das Feld und klicken Sie auf **Zellinhalt in Spalte kopieren**.

   In der Spalte **Status** wird die erfolgreiche Anmeldung mit angezeigt.

   Fehlgeschlagene Anmeldungen werden mithilfe von angezeigt.
5. Klicken Sie auf **Fertig stellen**.
   Das Gerät wird zum Gerätebaum hinzugefügt.

15.2 Seite „ONVIF-Encoder"

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > erweitern >
> Registerkarte **ONVIF-Encoder**
oder

Hauptfenster > **Geräte** > erweitern > > Registerkarte **ONVIF-Encoder**
Zeigt Informationen über einen ONVIF Encoder an, der Ihrem BVMS hinzugefügt wurde.

Name
Zeigt den Namen des ONVIF-Geräts an. Sie können es direkt im Gerätebaum umbenennen.

Netzwerkadresse
Zeigt die IP-Adresse des Geräts an.

Hersteller
Zeigt den Herstellernamen an.

Modell
Zeigt den Modellnamen an.

Firmware
Zeigt die Versionsnummer der Firmware an.

ONVIF Profil
Zeigt das konfigurierte Profil an.

ONVIF Profil G
Zeigt an, ob der ONVIF-Encoder Profile G unterstützt und die lokale Aufzeichnung aktiviert ist.

Zahl der Videoeingänge
Zeigt die Anzahl der Kameras, die mit diesem Encoder verbunden sind.

Zahl der Audioeingänge
Zeigt die Anzahl der Audioeingänge an, die mit diesem Encoder verbunden sind.

Anzahl der Alarmeingänge
Zeigt die Anzahl der Alarmeingänge an, die mit diesem Encoder verbunden sind.

Anzahl der Relais
Zeigt die Anzahl der Relais an, die mit diesem Encoder verbunden sind.

Siehe
- *Seite "ONVIF-Encoderereignis", Seite 239*
- *Hinzufügen eines Nur-Live-Encoders, Seite 220*
- *Konfigurieren einer ONVIF-Mapping-Tabelle, Seite 243*

15.3 Seite "ONVIF-Encoderereignis"

Ab BVMS 10.0 können ONVIF-Encoderereignisse direkt vom VSG- oder ONVIF-Encoder abgerufen werden. Wenn Sie einen neuen ONVIF-Encoder hinzufügen, wird das Kontrollkästchen **ONVIF-Ereignisse über VSG abrufen (Profile S, T)** standardmäßig aktiviert und Profile T wird unterstützt. Die folgenden Funktionen werden nur unterstützt, wenn ein ONVIF-Encoder über ein VSG-Gerät zu Ihrem System hinzugefügt wird:
- Wenn ONVIF-Encoderereignisse von VSG abgerufen werden, sind Standard-ONVIF-Ereignisse bereits zugeordnet.
- Der Bediener kann Relais im Operator Client ein- bzw. ausschalten.

Hinweis!
Das Abrufen von ONVIF-Ereignissen von VSG ist nur in VSG Version 7.0 möglich. Wenn Sie zu BVMS Version 10.0 migrieren, werden vorhandene ONVIF-Encoderereignisse direkt vom ONVIF-Encoder abgerufen. Sie müssen VSG auf Version 7.0 aktualisieren.

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > erweitern > > Registerkarte **ONVIF Encoder Ereignisse**

oder

Hauptfenster > **Geräte** > erweitern > > Registerkarte **ONVIF Encoder Ereignisse**

Sie müssen ONVIF-Ereignisse zu BVMS-Ereignissen zuordnen, wenn ONVIF-Encoderereignisse direkt vom ONVIF-Encoder abgerufen werden. Damit ist sichergestellt, dass Sie ONVIF-Ereignisse später als BVMS Alarme konfigurieren können.

Hinweis!
Wenn ONVIF-Encoderereignisse von VSG abgerufen werden, sind Standard-ONVIF-Ereignisse bereits zugeordnet.

Mapping-Tabelle
Sie können eine Mapping-Tabelle erstellen oder bearbeiten.

Klicken Sie auf , um das Dialogfeld **Mapping-Tabelle hinzufügen** anzuzeigen.

Klicken Sie auf , um das Dialogfeld **Mapping-Tabelle umbenennen** anzuzeigen.

Klicken Sie auf , um die Mapping-Tabelle mit allen Zeilen zu entfernen.

Klicken Sie auf oder , um eine ONVIF-Mapping-Tabelle zu importieren oder zu exportieren.

Ereignisse und Alarme
Wählen Sie ein BVMS Ereignis, um es mit einem ONVIF-Ereignis zusammenzuführen.

Zeile hinzufügen
Klicken Sie, um eine neue Zeile zur Mapping-Tabelle hinzuzufügen.
Wenn mehrere Zeilen verfügbar sind, erfolgt ein Ereignis, wenn eine Zeile wahr ist.

Zeile entfernen
Klicken Sie, um die gewählte Zeile aus der Mapping-Tabelle zu löschen.

ONVIF Topic
Geben Sie eine Zeichenfolge ein oder wählen Sie eine aus, zum Beispiel:

```
tns1:VideoAnalytics/tnsaxis:MotionDetection
```

ONVIF Datenname
Geben Sie eine Zeichenfolge ein oder wählen Sie eine aus.

ONVIF Datentyp
Geben Sie eine Zeichenfolge ein oder wählen Sie eine aus.

ONVIF Datenwert
Geben Sie eine Zeichenfolge oder eine Nummer ein oder wählen Sie eine aus.

Wenn ONVIF-Ereignisse von VSG abgerufen werden, werden die folgenden Ereignisse standardmäßig VSG zugeordnet:

- **Gesamtveränderung – erkannt**
- **Gesamtveränderung – nicht erkannt**
- **Bewegungserkennung** - **Bewegung erkannt**
- **Bewegungserkennung** - **Bewegung beendet**
- **Referenzbildprüfung** - **Dejustiert**
- **Referenzbildprüfung** - **Justiert**
- **Videosignalverlust** - **Videosignal verloren**

- **Videosignalverlust** - **Videosignal OK**
- **Videosignalverlust** - **Videosignalstatus unbekannt**
- **Videosignal zu unscharf – Videosignal OK**
- **Videosignal zu unscharf – Videosignal nicht OK**
- **Videosignal zu hell** - **Videosignal OK**
- **Videosignal zu hell** - **Videosignal nicht OK**
- **Videosignal zu dunkel** - **Videosignal OK**
- **Videosignal zu dunkel** - **Videosignal nicht OK**
- **Videosignal verrauscht** - **Videosignal OK Videosignal nicht OK**
- **Relais-Status** - **Relais offen**
- **Relais-Status** - **Relais geschlossen**
- **Relais-Status** - **Relaisfehler**
- **Eingangsstatus** - **Eingang geöffnet**
- **Eingangsstatus** - **Eingang geschlossen**
- **Eingangsstatus** - **Eingang Fehler**

Siehe
- *Starten des ONVIF Camera Event Driver Tool aus dem Configuration Client, Seite 209*
- *ONVIF-Ereigniszuordnung, Seite 42*
- *Konfigurieren einer ONVIF-Mapping-Tabelle, Seite 243*

15.3.1 Hinzufügen und Entfernen eines ONVIF Profils

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > erweitern > > Registerkarte **ONVIF Encoder Ereignisse**

oder

Hauptfenster > **Geräte** > erweitern > > Registerkarte **ONVIF Encoder Ereignisse**

Sie können ONVIF Profile für einen gewählten Encoder hinzufügen, entfernen oder ändern.

So fügen Sie einen Encoder hinzu:
1. Klicken Sie auf **Hinzufügen...**.
2. Im Dialogfeld **Profil hinzufügen** geben Sie einen Namen für das Profil ein.
3. Klicken Sie auf **Weiter >**.
4. Wählen Sie im nächsten Dialogfeld die gewünschte Kamera.
5. Klicken Sie auf **Weiter >**.
6. Wählen Sie im nächsten Dialogfeld das gewünschte nicht aufzeichnende Encoder-Profil.
7. Klicken Sie auf **Speichern**.
   Der neue Profilname wird gespeichert.
   Die Einstellungen dieses Profils werden mit den Werten aus dem gewählten Encoder-Profil gefüllt. Falls erforderlich, können Sie diese Werte ändern.

So entfernen Sie sie:
- Wählen Sie in der Liste ein Profil, und klicken Sie auf **Entfernen**.

So ändern Sie sie:
1. Wählen Sie in der Liste ein Profil.
2. Ändern Sie die Einstellungen nach Bedarf.

15.3.2 Exportieren einer ONVIF-Mapping-Tabelle

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > erweitern > > Registerkarte **ONVIF Encoder Ereignisse**

oder

Hauptfenster > **Geräte** > erweitern > > Registerkarte **ONVIF Encoder Ereignisse**

Sie können eine ONVIF Mapping-Tabelle als Datei (OMF-Datei) exportieren. Die Mapping-Tabelle wird für das gewählte Encoder-Modell gespeichert.

So führen Sie einen Export durch:

1. Klicken Sie auf .
2. Geben Sie einen Dateinamen ein, und klicken Sie auf **Speichern**.
   Die ONVIF Mapping-Tabelle wird als OMF-Datei für das gewählte Encoder-Modell exportiert.

Siehe

– *Seite "ONVIF-Encoderereignis", Seite 239*

15.3.3 Importieren einer ONVIF Mapping-Tabelle

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > erweitern > > Registerkarte **ONVIF Encoder Ereignisse**

oder

Hauptfenster > **Geräte** > erweitern > > Registerkarte **ONVIF Encoder Ereignisse**

Sie können eine als Datei (OMF-Datei) verfügbare ONVIF Mapping-Tabelle importieren.
Freigegebene ONVIF Mapping-Dateien werden im folgenden Configuration Client-Verzeichnis gespeichert:

– `%programdata%\Bosch\VMS\ONVIF`

Wenn dieselbe Mapping-Tabelle bereits importiert wurde, wird eine Fehlermeldung angezeigt.
Wenn eine neuere Version dieser Datei importiert wird, wird eine Warnung angezeigt. Klicken Sie auf **OK**, wenn Sie diese Datei importieren möchten. Ansonsten klicken Sie auf **Abbrechen**.

So importieren Sie die Datei:

1. Klicken Sie auf .
2. Wählen Sie die gewünschte Datei, und klicken Sie auf **Öffnen**.
   Das Dialogfeld **Mapping-Tabelle importieren** wird angezeigt.
3. Nehmen Sie die erforderlichen Einstellungen vor.
4. Klicken Sie auf **OK**.

Dialogfeld Mapping-Tabelle importieren

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > erweitern > > Registerkarte **ONVIF Encoder Ereignisse** >

oder

Hauptfenster > **Geräte** > erweitern > > Registerkarte **ONVIF Encoder Ereignisse** >

Hersteller
Zeigt den Herstellernamen an, für den diese Mapping-Tabelle gültig ist.

Modell
Zeigt den Modellnamen an, für den diese Mapping-Tabelle gültig ist.

Beschreibung
Zeigt weitere Informationen an, beispielsweise zu getesteten Kameramodellen.

Mapping-Tabelle Name
Zeigt den Namen der Mapping-Tabelle an. Ändern Sie diesen Namen, wenn er bereits in BVMS verwendet wird.
Wählen Sie eine der folgenden Optionen, um zu entscheiden, welchen ONVIF Encodern Sie die Mapping-Tabelle zuordnen möchten.

Nur auf die ausgewählten ONVIF-Encoder anwenden

Auf alle ONVIF-Encoder des gelisteten Modells anwenden

Auf alle ONVIF-Encoder des Herstellers anwenden
Die bestehende ONVIF Ereignisaufzeichnung wird fortgesetzt. Sie können OMT-Dateien aus vorherigen BVMS Versionen nicht importieren.

15.3.4 Konfigurieren einer ONVIF-Mapping-Tabelle

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > erweitern > > Registerkarte **ONVIF Encoder Ereignisse**

oder

Hauptfenster > **Geräte** > erweitern > > Registerkarte **ONVIF Encoder Ereignisse**

Sie konfigurieren Mapping-Tabellen zum Aufzeichnen von ONVIF Ereignissen für BVMS Ereignisse. Sie konfigurieren eine Mapping-Tabelle für alle ONVIF Encoder desselben Modells oder alle ONVIF Encoder desselben Herstellers.

Klicken Sie auf , um ONVIF Encoder zu aktualisieren, die offline mit der gleichen Ereignisaufzeichnung von einem bereits hinzugefügten ONVIF Encoder desselben Herstellers und/oder mit demselben Modellnamen hinzugefügt wurden.
Für Mehrkanal-Encoder können Sie die Ereignisquellen konfigurieren, beispielsweise eine spezifische Kamera oder ein Relais.

So erstellen Sie eine Mapping-Tabelle:

1. Klicken Sie auf .
   Das Dialogfeld **Mapping-Tabelle hinzufügen** wird angezeigt.
2. Geben Sie einen Namen für die Mapping-Tabelle ein.
3. Wählen Sie in der **Hersteller**- und der **Modell**-Liste aus.
   Wenn Sie in beiden Listen **<kein Eintrag>** auswählen, gilt die Ereigniszuordnung nur für dieses Gerät.
   Wenn Sie **<kein Eintrag>** in der **Modell**-Liste und den Herstellernamen in der **Hersteller**-Liste

auswählen, gilt die Ereigniszuordnung für alle Geräte mit demselben Hersteller.
Wenn Sie die verfügbaren Einträge in beiden Listen auswählen, gilt die Ereigniszuordnung für alle Geräte desselben Herstellers und desselben Modells.

4. Klicken Sie auf **OK**.
Sie können nun die Mapping-Tabelle bearbeiten, zum Beispiel eine Zeile beim Ereignis **Bewegung erkannt** hinzufügen.

So bearbeiten Sie eine Mapping-Tabelle:

1. Klicken Sie auf .
Das Dialogfeld **Mapping-Tabelle umbenennen** wird angezeigt.
2. Ändern Sie den gewünschten Eintrag.

So fügen Sie Ereignisaufzeichnungen hinzu oder entfernen sie:

1. Wählen Sie aus der Liste **Mapping-Tabelle** den gewünschten Namen aus.
2. Um eine Zeile hinzuzufügen, klicken Sie auf **Zeile hinzufügen**.
3. Wählen Sie in der Zeile die gewünschten Einträge aus.
Wenn mehrere Zeilen verfügbar sind, wird ein Ereignis ausgelöst, wenn nur eine Reihe wahr ist.
4. Um eine Zeile zu entfernen: Klicken Sie auf **Zeile entfernen**.

So entfernen Sie eine Mapping-Tabelle:

1. Klicken Sie in der Liste **Mapping-Tabelle** auf den Namen der Ereignisaufzeichnung, die Sie entfernen möchten.
2. Klicken Sie auf .

So konfigurieren Sie ein Ereignisquelle:

1. Erweitern Sie und klicken Sie auf oder oder .
2. Klicken Sie auf die Registerkarte **ONVIF Ereignisquelle**.
3. Aktivieren Sie in der Spalte **Ereignis auslösen** das in dieser Zeile konfigurierte Ereignis.
4. Wählen Sie die gewünschten Ereignisdefinitionen.

Dialogfeld „ONVIF Mapping-Tabelle hinzufügen/umbenennen“

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > erweitern > > Registerkarte **ONVIF Encoder Ereignisse** > oder

oder

Hauptfenster > **Geräte** > erweitern > > Registerkarte **ONVIF Encoder Ereignisse** > oder

Ermöglicht das Hinzufügen einer Mapping-Tabelle. Wenn diese Mapping-Tabelle als Vorlage für künftige ONVIF-Encoder desselben Herstellers oder desselben Modells dienen soll, wählen Sie die korrekten Einträge.

Mapping-Tabelle Name
Geben Sie den Namen zur einfachen Identifikation ein.

Hersteller
Wählen Sie bei Bedarf einen Eingang.

Modell
Wählen Sie bei Bedarf einen Eingang.

Siehe

- *Ermöglicht die Protokollierung von ONVIF-Ereignissen, Seite 385*
- *ONVIF-Ereigniszuordnung, Seite 42*
- *Seite "ONVIF-Encoderereignis", Seite 239*
- *Seite "ONVIF-Ereignisquelle", Seite 258*

15.4 Seite „ONVIF Konfiguration“

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > erweitern > > Registerkarte **ONVIF Konfiguration**

oder

Hauptfenster > **Geräte** > erweitern > > Registerkarte **ONVIF Konfiguration**

Sie können auf der Seite **Videoencoderprofil** mehrere ONVIF-Encoder wählen und die Einstellungen ändern. Die geänderten Einstellungen gelten für alle gewählten Geräte.

Diese Seite ist nur für ONVIF-Encoder verfügbar.

Hinweis!

Einschränkungen der ONVIF-Konfiguration

Einstellungen, die Sie auf diesen Seiten vornehmen, werden möglicherweise nicht korrekt ausgeführt, da sie nicht von der Kamera unterstützt werden. Unterstützte ONVIF-Kameras wurden nur mit den Standardeinstellungen getestet.

15.4.1 Gerätezugriff

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > erweitern > > Registerkarte **ONVIF Konfiguration** > Registerkarte **Haupteinstellungen** > Registerkarte **Gerätezugriff**

oder

Hauptfenster > **Geräte** > erweitern > > Registerkarte **ONVIF Konfiguration** > Registerkarte **Haupteinstellungen** > Registerkarte **Gerätezugriff**

Hersteller

Zeigt den Herstellernamen des gewählten Encoders an.

Modell

Zeigt den Modellnamen des gewählten Encoders an.

Hinweis: Wenn Sie Ereignisaufzeichnungen in eine ONVIF-Aufzeichnungsdatei exportieren möchten, wählen Sie diesen Modellnamen als Dateinamen aus.

Hardware-ID

Zeigt die Hardware-ID des gewählten Encoders an.

Firmware-Version

Zeigt die Firmware-Version des gewählten Encoders an.

Hinweis: Vergewissern Sie sich hinsichtlich der BVMS-Kompatibilität, ob die Firmware-Version korrekt ist.

Seriennummer

Zeigt die Seriennummer des gewählten Encoders an.

MAC-Adresse
Zeigt die MAC-Adresse des gewählten Encoders an.

ONVIF-Version
Zeigt die ONVIF Version des gewählten Encoders an.
Für BVMS ist die ONVIF-Version 2.0 erforderlich.

15.4.2 Datum/Zeit

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > erweitern > > Registerkarte **ONVIF Konfiguration** > Registerkarte **Haupteinstellungen** > Registerkarte **Datum/Zeit**
oder
Hauptfenster > **Geräte** > erweitern > > Registerkarte **ONVIF Konfiguration** > Registerkarte **Haupteinstellungen** > Registerkarte **Datum/Zeit**

Zeitzone
Wähle Sie hier die Zeitzone aus, in der sich das System befindet.
Wenn Sie mehrere Geräte in Ihrem System oder Netzwerk betreiben, müssen die internen Uhren der Geräte unbedingt synchron arbeiten. Die korrekte Identifikation und Auswertung gleichzeitiger Aufzeichnungen ist beispielsweise nur möglich, wenn alle Geräte dieselbe Uhrzeit verwenden.

1. Geben Sie das aktuelle Datum ein. Da die Gerätezeit durch die Kalenderuhr gesteuert wird, müssen Sie den Wochentag nicht eingeben – er wird automatisch hinzugefügt.
2. Geben Sie die aktuelle Uhrzeit ein, oder klicken Sie auf **Synchr. PC**, um die Systemzeit Ihres Computers auf das Gerät zu übertragen.

Hinweis:
Stellen Sie unbedingt sicher, dass Datum und Zeit für die Aufzeichnung korrekt eingestellt sind. Eine falsche Datums- und Zeiteinstellung könnte zu inkorrekten Aufzeichnungen führen.

15.4.3 Benutzerverwaltung

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > erweitern > > Registerkarte **ONVIF Konfiguration** > Registerkarte **Haupteinstellungen** > Registerkarte **Benutzerverwaltung**
oder
Hauptfenster > **Geräte** > erweitern > > Registerkarte **ONVIF Konfiguration** > Registerkarte **Haupteinstellungen** > Registerkarte **Benutzerverwaltung**
Diese Benutzereinstellungen werden für Drittanbieteranwendungen verwendet, wie direkten Web Client-Zugriff auf Encoder.
Es werden folgende Benutzerrollen für den Zugriff von Drittanbieteranwendungen unterstützt:

– **Anonymus**: Diese Rolle hat unbegrenzt Zugriff auf nur die Geräte, auf denen keine Benutzer von anderen Rollen (**Benutzer**, **Anwender**, **Administrator**) registriert sind. Bei Geräten mit mindestens einem oben erwähnten Benutzer hat der anonyme Benutzer nur die Berechtigung zum Anzeigen der Zeiteinstellungen.

– **Administrator** (nicht unterstützt von Configuration Client): Diese Rolle hat Zugriff auf alle Anwendungsabschnitte und -funktionen, die Rechte zum Neustarten des Geräts, zum Zurücksetzen der Einstellungen und zum Aktualisieren der Firmware sowie zum Erstellen anderer Benutzer mit unterschiedlichen Zugriffsrechten.

Der erste auf dem Gerät erstellte Benutzer muss **Administrator** sein.
Unterschiede bei den Standardzugriffsrechten des Bedieners und des Benutzers der **Anwender**-Rolle und der **Benutzer**-Rolle finden Sie in der folgenden Tabelle.

ONVIF-Konfigurationsabschnitt oder -funktion	Bediener	Benutzer
Identifikation	ANZEIGEN	AUSGEBLENDET
Zeiteinstellungen	ANZEIGEN	ANZEIGEN
Netzwerkeinstellungen	ANZEIGEN	ANZEIGEN
Benutzer	AUSGEBLENDET	AUSGEBLENDET
Relaiseinstellungen	ÄNDERN	ANZEIGEN
Live-Video (einschließlich RTSP-Link)	ÄNDERN	ÄNDERN
Video-Streaming	ÄNDERN	ANZEIGEN
Profile	ÄNDERN	ANZEIGEN

ÄNDERN: Aktuelle Einstellungen ändern und neue erstellen.
ANZEIGEN: Einstellungen sind nicht ausgeblendet, sie können aber nicht geändert oder erstellt werden.
AUSGEBLENDET: Bestimmte Einstellungen oder sogar ganze Abschnitte sind ausgeblendet.

Benutzer
Führt die verfügbaren Benutzer des Geräts auf.

Passwort
Geben Sie ein gültiges Passwort ein.

Passwortbestätigung
Bestätigen Sie das eingegebene Passwort.

Rolle
Wählen Sie die gewünschte Rolle für den gewählten Benutzer aus. Die Zugriffsrechte werden entsprechend angepasst.

15.4.4 Seite „Videoencoderprofil”

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > erweitern > > Registerkarte **ONVIF Konfiguration** > Registerkarte **Kamera** > Registerkarte **Videoencoderprofil**

oder

Hauptfenster > **Geräte** > erweitern > > Registerkarte **ONVIF Konfiguration** > Registerkarte **Kamera** > Registerkarte **Videoencoderprofil**

Profile sind sehr komplex und enthalten eine Reihe von Parametern, die sich gegenseitig beeinflussen. Aus diesem Grund ist es im Allgemeinen sinnvoll, die vordefinierten Profile zu verwenden. Ändern Sie ein Profil nur dann, wenn Sie mit allen Konfigurationsoptionen umfassend vertraut sind.

Profile
Klicken Sie auf den gewünschten Namen.

Hinweis!
Die hier konfigurierten Profile können im Configuration Client ausgewählt werden.

Klicken Sie im Hauptfenster auf **Kameras und Aufzeichnung** und anschließend auf oder .
Die Standardeinstellung „<Automatisch>“ kann in eines der aufgelisteten und konfigurierten Profile geändert werden.
Hinweis: Berücksichtigen Sie bei aktiver Verwendung von mehr als einem Profil eines einzelnen Geräts, dass bestimmte Leistungseinschränkungen gelten und die Kamera möglicherweise die Qualität eines Streams bei Überlastung automatisch beschränkt.

Name
Sie können einen neuen Namen für das Profil eingeben. Der Name wird anschließend in der Liste der wählbaren Profile im Feld „Aktives Profil“ angezeigt.

Encodierung
Wählen Sie den gewünschten Codec aus.

Auflösung
Wählen Sie die gewünschte Auflösung für das Videobild.

Qualität
Mit diesem Parameter können Sie die Belastung des Kanals durch Reduzierung der Bilddefinition verringern. Der Parameter wird mithilfe des Schiebereglers festgelegt: Die Position ganz links entspricht der höchsten Bilddefinition, die Position ganz rechts der niedrigsten Belastung des Videokanals.

Bildraten-Limit
Bildfrequenz (Bilder pro Sekunde) gibt an, wie viele Bilder pro Sekunde von der mit dem Gerät verbundenen Videokamera aufgenommen werden. Dieser Parameter wird nur zu Informationszwecken angezeigt.
Wenn ein Codierungsintervall vorhanden ist, wird die daraus resultierende codierte Bildfrequenz um den gegebenen Faktor verringert.

Bitraten-Limit
Je niedriger die Bitrate, desto kleiner die finale Videodateigröße. Wenn die Bitrate jedoch erheblich reduziert wird, muss das Programm stärkere Komprimierungsalgorithmen verwenden, wodurch auch die Videoqualität reduziert wird.
Wählen Sie die maximale Ausgangs-Bitrate in Kbit/s aus. Diese maximale Datenrate wird unter keinen Umständen überschritten. Dies kann je nach den Einstellungen für die Videoqualität der I- und P-Frames zum Überspringen einzelner Bilder führen.
Der hier eingegebene Wert sollte mindestens 10 % größer sein als die typische Zieldaten-Bitrate.

Encodierungsintervall
Codierungsintervall (Anzahl der Bilder) gibt an, mit welcher Rate die von der Kamera kommenden Bilder codiert werden. Wenn die Codierung des Intervalls beispielsweise 25 beinhaltet, heißt das, dass ein Bild von 25 pro Sekunde erfassten codiert und an den Benutzer übertragen wird. Der

Maximalwert reduziert die Belastung des Kanals, verursacht aber möglicherweise das Überspringen von Informationen, die nicht codiert wurden. Durch die Reduzierung des Codierungsintervalls wird die Frequenz der Bildaktualisierung sowie die Belastung des Kanal erhöht.

GOP-Länge
GOP-Länge kann nur bearbeitet werden, wenn der Encoder H.264 oder H.265 ist. Dieser Parameter kennzeichnet die Länge der Bildgruppe zwischen zwei Key-Frames. Je höher dieser Wert ist, desto geringer ist die Belastung des Netzwerks, aber die Bildqualität wird beeinträchtigt.
1 bedeutet, dass I-Frames kontinuierlich generiert werden. Eine Eingabe von 2 bedeutet, dass jedes zweite Bild ein I-Frame ist, 3 bedeutet, dass nur jedes dritte Bild ein I-Frame ist usw. Die Bilder dazwischen werden als P-Frames oder B-Frames verschlüsselt.

Sitzungs-Timeout
Das RTSP-Sitzungstimeout für den zugehörigen Videostream.
Das Sitzungstimeout dient als Hinweis für die Beibehaltung einer RTSP-Sitzung von einem Gerät.

Multicast - IP-Adresse
Geben Sie eine gültige Multicast-Adresse für den Betrieb im Multicast-Modus ein (Duplizierung des Daten-Streams im Netzwerk).

Bei der Einstellung 0.0.0.0 arbeitet der Encoder für den jeweiligen Stream im Multi-Unicast-Modus (Kopieren der Daten-Streams im Gerät). Die Kamera unterstützt Multi-Unicast-Verbindungen für bis zu fünf gleichzeitig verbundene Empfänger.

Die Duplizierung der Daten im Gerät erfordert eine hohe Rechenleistung und kann unter bestimmten Umständen zu Einbußen in der Bildqualität führen.

Multicast - Port
Wählen Sie den RTP-Multicast-Ziel-Port. Ein Gerät kann RTCP unterstützen. In diesem Fall muss der Port-Wert gerade sein, damit der entsprechende RTCP-Stream der nächst höheren (ungeraden) Ziel-Port-Nummer zugeordnet werden können, wie in den RTSP-Spezifikationen definiert.

Multicast – TTL
Hier können Sie angeben, wie lange die Multicast-Datenpakete im Netzwerk aktiv sein sollen. Wenn der Multicast-Betrieb über einen Router erfolgen soll, muss dieser Wert größer als 1 sein.

Hinweis!
Multicast-Betrieb ist nur mit dem UDP-Protokoll möglich. Das TCP-Protokoll unterstützt keine Multicast-Verbindungen.
Wenn das Gerät hinter einer Firewall betrieben wird, muss als Übertragungsprotokoll TCP (HTTP-Port) ausgewählt werden. Für die Nutzung in einem lokalen Netzwerk wählen Sie „UDP“ aus.

15.4.5 Audioencoderprofil

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > erweitern > > Registerkarte **ONVIF Konfiguration** > Registerkarte **Kamera** > Registerkarte **Audioencoderprofil**

oder

Hauptfenster > **Geräte** > erweitern > > Registerkarte **ONVIF Konfiguration** > Registerkarte **Kamera** > Registerkarte **Audioencoderprofil**

Profile sind sehr komplex und enthalten eine Reihe von Parametern, die sich gegenseitig beeinflussen. Aus diesem Grund ist es im Allgemeinen sinnvoll, die vordefinierten Profile zu verwenden. Ändern Sie ein Profil nur dann, wenn Sie mit allen Konfigurationsoptionen umfassend vertraut sind.

Encodierung
Wählen Sie die gewünschte Codierung für die Audioquelle, falls verfügbar:
- **G.711 [ITU-T G.711]**
- **G.726 [ITU-T G.726]**
- **AAC [ISO 14493-3]**

Bitrate
Wählen Sie die gewünschte Bitrate für die Übertragung des Audiosignals, zum Beispiel 64 Kbit/s

Abtastrate
Geben Sie die Ausgabe-Abtastrate in kHz an, z. B. 8 Kbit/s.

Sitzungs-Timeout
Das RTSP-Sitzungstimeout für den zugehörigen Audiostream.
Das Sitzungstimeout dient als Hinweis für die Beibehaltung einer RTSP-Sitzung von einem Gerät.

15.4.6 Imaging allgemein

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > erweitern > > Registerkarte **ONVIF Konfiguration** > Registerkarte **Kamera** > Registerkarte **Imaging allgemein**
oder
Hauptfenster > **Geräte** > erweitern > > Registerkarte **ONVIF Konfiguration** > Registerkarte **Kamera** > Registerkarte **Imaging allgemein**

Helligkeit
Passen Sie die Helligkeit des Bilds an Ihre Arbeitsumgebung an.

Farbsättigung
Passen Sie die Farbsättigung im Bild an, um die Farbwiedergabe am Monitor möglichst realitätsgetreu zu gestalten.

Kontrast
Sie können den Kontrast des Videobilds an Ihre Arbeitsumgebung anpassen.

Schärfe
Hier kann die Schärfe des Bilds eingestellt werden.
Ein niedriger Wert führt zu einem weniger scharfen Bild. Durch das Erhöhen der Bildschärfe werden einzelne Details besser erkannt. Durch zusätzliche Bildschärfe können Details bei Kennzeichen, Gesichtsmerkmalen und Kanten bestimmter Oberflächen besser erkannt werden, dies kann aber auch dazu führen, dass mehr Bandbreite benötigt wird.

IR-Sperrfilter
Wählen Sie den Status des IR-Sperrfilters.
Der AUTO-Zustand lässt den Belichtungsalgorithmus handhaben, wenn der IR-Sperrfilter geändert wird.

15.4.7 Gegenlichtkompensation

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > erweitern > > Registerkarte **ONVIF Konfiguration** > Registerkarte **Haupteinstellungen** > Registerkarte **Gegenlichtkompensation**

oder

Hauptfenster > **Geräte** > erweitern > > Registerkarte **ONVIF Konfiguration** > Registerkarte **Haupteinstellungen** > Registerkarte **Gegenlichtkompensation**

Je nach Gerätemodell können Sie hier Parameter für die Gegenlichtkompensation konfigurieren.

Modus

Wählen Sie **Aus** aus, um die Gegenlichtkompensation auszuschalten.

Wählen Sie **Ein** zum Erfassen von Details bei starkem Kontrast und extremen Hell-Dunkel-Bedingungen aus.

Ebene

Wählen Sie den gewünschten Wert aus, oder geben Sie ihn ein.

15.4.8 Belichtung

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > erweitern > > Registerkarte **ONVIF Konfiguration** > Registerkarte **Haupteinstellungen** > Registerkarte **Belichtung**

oder

Hauptfenster > **Geräte** > erweitern > > Registerkarte **ONVIF Konfiguration** > Registerkarte **Haupteinstellungen** > Registerkarte **Belichtung**

Je nach Gerätemodell können Sie hier Parameter für die Belichtung konfigurieren.

Modus

Wählen Sie **Auto** aus, um den Belichtungsalgorithmus auf dem Gerät zu aktivieren. Die Werte in den folgenden Feldern werden vom Algorithmus verwendet:

- **Priorität**
- **Fenster**
- **Min. Belichtungszeit**
- **Max. Belichtungszeit**
- **Min. Verstärkung**
- **Max. Verstärkung**
- **Min. Blende**

Wählen Sie **Manuell** aus, um den Belichtungsalgorithmus auf dem Gerät zu deaktivieren. Die Werte in den folgenden Feldern werden vom Algorithmus verwendet:

- **Belichtungszeit**
- **Verstärkung**
- **Blende**

Priorität

Konfigurieren Sie den Belichtungs-Prioritätsmodus (niedriges Rauschen/Bildfrequenz).

Fenster

Definieren Sie eine rechteckige Belichtungsmaske.

Min. Belichtungszeit
Konfigurieren Sie den Mindest-Belichtungszeitbereich [µs].

Max. Belichtungszeit
Konfigurieren Sie den Höchst-Belichtungszeitbereich [µs].

Min. Verstärkung
Konfigurieren Sie den Mindest-Sensor-Verstärkungsbereich [dB].

Max. Verstärkung
Konfigurieren Sie den Höchst-Sensor-Verstärkungsbereich [dB].

Min. Blende
Konfigurieren Sie die Mindestdämpfung der eindringenden Lichtmenge, die durch die Blende beeinträchtigt wird [dB]. 0 dB wird einer vollständig geöffneten Blende zugeordnet.

Max. Blende
Konfigurieren Sie die Höchstdämpfung der eindringenden Lichtmenge, die durch die Blende beeinträchtigt wird [dB]. 0 dB wird einer vollständig geöffneten Blende zugeordnet.

Belichtungszeit
Konfigurieren Sie die feste Belichtungszeit [µs].
Verstärkung
Konfigurieren Sie die feste Verstärkung [dB].

Blende
Konfigurieren Sie die feste Dämpfung der eindringenden Lichtmenge, die durch die Blende beeinträchtigt wird [dB]. 0 dB wird einer vollständig geöffneten Blende zugeordnet.

15.4.9 Fokus

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > erweitern > > Registerkarte **ONVIF Konfiguration** > Registerkarte **Haupteinstellungen** > Registerkarte **Fokus**
oder
Hauptfenster > **Geräte** > erweitern > > Registerkarte **ONVIF Konfiguration** > Registerkarte **Haupteinstellungen** > Registerkarte **Fokus**
Je nach Gerätemodell können Sie hier Parameter für den Fokus konfigurieren.
Diese Seite ermöglicht, das Objektiv auf eine absolute, relative oder kontinuierliche Weise zu bewegen. Fokusanpassungen über diesen Vorgang schalten den Autofokus aus. Ein Gerät mit Unterstützung für entfernte Fokussteuerung unterstützt in der Regel die Steuerung über diesen Verschiebevorgang. Die Fokusposition wird mit einem bestimmten numerischen Wert dargestellt. Der Status des Fokus kann einer der Folgenden sein:
BEWEGT
OK
UNBEKANNT
Zusätzliche Fehlerinformationen können angezeigt werden, z. B. ein von der Hardware angegebener Positionierungsfehler.

Modus
Wählen Sie **Auto** aus, um zuzulassen, dass das Objektiv automatisch den Fokus zu jeder Zeit entsprechend der Objekte in der Szene einstellt. Die Werte in den folgenden Feldern werden vom Algorithmus verwendet:

– **Vordertiefe**
– **Hintertiefe**

Wählen Sie **Manuell** aus, um den Fokus manuell anzupassen. Die Werte in den folgenden Feldern werden vom Algorithmus verwendet:

– **Standard-Geschwindigkeit**

Standard-Geschwindigkeit
Konfigurieren Sie die Standard-Geschwindigkeit für den Fokusverschiebevorgang (wenn der Geschwindigkeitsparameter nicht vorhanden ist).

Hintertiefe
Konfigurieren Sie die Vordertiefe des Objektivs [m].

Hintertiefe
Konfigurieren Sie die Hintertiefe des Objektivs [m].

15.4.10 Großer dynamischer Bereich

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > erweitern > > Registerkarte **ONVIF Konfiguration** > Registerkarte **Haupteinstellungen** > Registerkarte **Weiter Dynamikbereich**

oder

Hauptfenster > **Geräte** > erweitern > > Registerkarte **ONVIF Konfiguration** > Registerkarte **Haupteinstellungen** > Registerkarte **Weiter Dynamikbereich**

Je nach Gerätemodell können Sie hier Parameter für den großen dynamischen Bereich konfigurieren.

Modus
Wählen Sie den gewünschten Wert aus, oder geben Sie ihn ein.

Ebene
Wählen Sie den gewünschten Wert aus, oder geben Sie ihn ein.

15.4.11 Weißabgleich

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > erweitern > > Registerkarte **ONVIF Konfiguration** > Registerkarte **Haupteinstellungen** > Registerkarte **Weißabgleich**

oder

Hauptfenster > **Geräte** > erweitern > > Registerkarte **ONVIF Konfiguration** > Registerkarte **Haupteinstellungen** > Registerkarte **Weißabgleich**

Je nach Gerätemodell können Sie hier Parameter für den Weißabgleich konfigurieren.

Modus
Mit dem Auto-Modus kann die Kamera eine kontinuierliche Anpassung für eine optimale Farbwiedergabe vornehmen, wozu eine durchschnittlichen Reflektierungsmethode oder eine Umgebung mit natürlichen Lichtquellen verwendet wird.
Im Modus „Manuell“ kann die Verstärkung für Rot, Grün und Blau auf einen bestimmten Wert eingestellt werden.
Die Änderung des Offsets der Farbdarstellung ist nur für spezielle Aufnahmesituationen erforderlich:

– Innenlichtquellen und für farbige LED-Beleuchtung

– Natriumdampflichtquellen (Straßenbeleuchtung)
– für dominante Farben im Bild, zum Beispiel das Grün eines Fußballfeld oder eines Spieltischs

R-Verstärkung
Passen Sie im manuellen Weißabgleichmodus die Rotverstärkung zwischen -50 und +50 an, um die Werkseinstellung der Farbdarstellung auszugleichen (mehr Cyan, weniger Rot).

B-Verstärkung
Passen Sie im manuellen Weißabgleichmodus die Blauverstärkung an, um die Werkseinstellung der Farbdarstellung auszugleichen (mehr Gelb, weniger Blau).

15.4.12 Netzwerkzugriff

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > erweitern > > Registerkarte **ONVIF Konfiguration** > Registerkarte **Netzwerk** > Registerkarte **Netzwerkzugriff**
oder
Hauptfenster > **Geräte** > erweitern > > Registerkarte **ONVIF Konfiguration** > Registerkarte **Netzwerk** > Registerkarte **Netzwerkzugriff**
Hier können Sie verschiedene Netzwerkeinstellungen konfigurieren.

Ethernet IPv4

DHCP
Wenn im Netzwerk ein DHCP-Server für die dynamische Zuweisung von IP-Adressen eingesetzt wird, können Sie die Annahme von IP-Adressen aktivieren, die dem Encoder automatisch zugewiesen werden.
BVMS verwendet die IP-Adresse zur eindeutige Zuordnung des Encoders. Der DHCP-Server muss die feste Zuordnung zwischen IP-Adressen und MAC-Adressen unterstützen und entsprechend konfiguriert sein, damit die zugeordnete IP-Adresse nach jedem Neustart des Computers weiterhin zur Verfügung steht.

Subnetzmaske
Geben Sie die zur eingestellten IP-Adresse passende Subnetzmaske ein.
Wenn der DHCP-Server aktiviert ist, wird die Subnetzmaske automatisch zugewiesen.

Standard-Gateway
Wenn das Modul eine Verbindung mit einer Gegenstelle in einem anderen Subnetz herstellen soll, geben Sie hier die IP-Adresse des Gateways ein. Andernfalls lassen Sie das Feld leer (0.0.0.0).

Ethernet IPv6

DHCP
Wählen Sie den gewünschten Wert aus, oder geben Sie ihn ein.

IP-Adresse
Zeigt die IPv6-Adresse des Geräts an, die vom DHCP-Server bereitgestellt wird.

Präfix-Länge
Zeigt die Präfix-Länge des Geräts an, das vom DHCP-Server bereitgestellt wird.

Standard-Gateway
Zeigt das Standard-Gateway des Geräts an, das vom DHCP-Server bereitgestellt wird.

Host-Name
Wählen Sie den gewünschten Wert aus, oder geben Sie ihn ein.

DNS
Das Gerät kann mit einem DNS-Server eine Adresse finden, die als Name angegeben ist. Geben Sie hier die IP-Adresse des DNS-Servers ein.

NTP-Server
Geben Sie die IP-Adresse des gewünschten Zeit-Servers ein oder lassen Sie den DHCP-Server dies für Sie erledigen.
Der Encoder kann über verschiedene Zeitserver-Protokolle das Zeitsignal von einem Zeitserver empfangen und danach die interne Uhr stellen. Das Modul ruft das Zeitsignal automatisch einmal pro Minute ab. Geben Sie hier die IP-Adresse eines Zeitservers ein. Dieses Protokoll bietet eine hohe Genauigkeit und ist für spezielle Anwendungen.

HTTP-Ports
Wählen Sie gegebenenfalls einen anderen HTTP-Browser-Port aus. Der Standard-HTTP-Port ist 80. Wenn nur sichere Verbindungen über HTTPS zugelassen werden sollen, müssen Sie den HTTP-Port deaktivieren.
Hinweis: Nicht unterstützt von BVMS.

HTTPS-Ports
Hinweis: Nicht unterstützt von BVMS.
Wenn Sie Zugriff auf das Netzwerk über eine sichere Verbindung erteilen möchten, wählen Sie bei Bedarf einen HTTPS-Port. Der Standard-HTTPS-Port ist 443. Wählen Sie zum Deaktivieren der HTTPS-Ports die Option **Aus**. Nur unsichere Verbindungen sind nun möglich.

Standard-Gateway
Wählen Sie den gewünschten Wert aus, oder geben Sie ihn ein.

RTSP-Ports
Wählen Sie gegebenenfalls einen anderen Port für den Austausch von RTSP-Daten. Der Standard-RTSP-Port ist 554. Wählen Sie **Aus**, um die RTSP-Funktion zu deaktivieren.

Zero-Configuration-Adresse
Aktivieren bzw. deaktivieren Sie die Zero-Configuration-Erkennung der ausgewählten Kamera. Zero-Configuration ist eine alternative Vorgehensweise zum DHCP und DNS für das Zuweisen von IP-Adressen zu Kameras. Es wird automatisch eine nutzbare IP-Netzwerkadresse ohne Konfiguration oder besondere Server erstellt.
Hinweis: Im ONVIF-Standard wird nur die Serviceentdeckung der Zero-Configuration verwendet. Alternativ muss das Netzwerk ohne Zero-Configuration Services bereitstellen, wie z. B. DHCP oder DNS.
Andernfalls konfigurieren Sie die Netzwerkeinstellungen jeder IP-Kamera manuell.

ONVIF-Discovery-Modus
Wenn aktiviert, kann die Kamera im Netzwerk gefunden werden. Dies umfasst auch ihre Funktionen. Wenn deaktiviert, sendet die Kamera keine Erkennungsmeldungen, um DOS-Angriffe zu verhindern. Wir empfehlen, die Entdeckung nach dem Hinzufügen der Kamera zur Konfiguration zu deaktivieren. Wählen Sie den gewünschten Wert aus, oder geben Sie ihn ein.

DynDNS aktivieren
Dient zur Aktivierung von DynDNS.
Mit einem dynamischen Domain Name Service (DNS) können Sie das Gerät über das Internet mit einem Hostnamen ansprechen, ohne die aktuelle IP-Adresse des Geräts wissen zu müssen. Dazu müssen Sie ein Konto bei einem der dynamischen DNS-Anbieter haben und den entsprechenden Host-Namen für das Gerät auf dieser Website registriert haben.

Hinweis:
Informationen über den Dienst, das Registrierungsverfahren und die verfügbaren Hostnamen erhalten Sie von Ihrem DynDNS-Anbieter auf dyndns.org.

Typ
Wählen Sie den gewünschten Wert aus, oder geben Sie ihn ein.

Name
Geben Sie den Namen des DynDNS-Benutzerkontos ein.

TTL
Wählen Sie den gewünschten Wert aus, oder geben Sie ihn ein.

15.4.13 Bereiche

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > erweitern > > Registerkarte **ONVIF Konfiguration** > Registerkarte **Netzwerk** > Registerkarte **Bereiche**

oder

Hauptfenster > **Geräte** > erweitern > > Registerkarte **ONVIF Konfiguration** > Registerkarte **Netzwerk** > Registerkarte **Bereiche**

Sie können -Bereiche zu Ihrem ONVIF-Gerät hinzufügen oder diese entfernen. Die URIs müssen das folgende Format haben:

```
onvif://www.onvif.org/<path>
```

Das folgende Beispiel zeigt die Verwendung der Bereichswert. Dies ist nur ein Beispiel und kein Hinweis, welcher Typ des Bereichsparameters Teil einer Encoder-Konfiguration sein soll. In diesem Beispiel wird davon ausgegangen, dass der Encoder mit den folgenden Bereichen konfiguriert ist:

```
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
```

Sie können dem Gerät eine detaillierte Position und einen Gerätenamen geben, um es innerhalb der Liste von Geräten zu identifizieren.
Die Tabelle zeigt die grundlegenden Funktionen und andere Eigenschaften des Geräts, die standardisiert sind:

Kategorie	Definierte Werte	Beschreibung
Typ	video_encoder	Das Gerät ist ein Netzwerk-Video-Encoder.
	Ptz	Das Gerät ist ein PTZ-Gerät.
	audio_encoder	Das Gerät bietet Audio-Encoder-Unterstützung.
	video_analytics	Das Gerät unterstützt die Videoanalyse.
	Network_Video_Transmitter	Das Gerät ist ein Netzwerk-Videosender.
	Network_Video_Decoder	Das Gerät ist ein Netzwerk-Video-Decoder.
	Network_Video_Storage	Das Gerät ist ein Netzwerk-Video-Speichergerät.
	Network_Video_Analytic	Das Gerät ist ein Netzwerk-Video-Analysegerät.

Kategorie	Definierte Werte	Beschreibung
Speicherort	Alle Zeichenfolgen oder Pfadwerte.	Nicht unterstützt von BVMS.
Hardware	Alle Zeichenfolgen oder Pfadwerte.	Eine Zeichenfolge oder ein Pfadwert zur Beschreibung der Hardware des Geräts. Ein Gerät muss mindestens einen Hardware-Eintrag in der Liste der Bereiche enthalten.
Name	Alle Zeichenfolgen oder Pfadwerte.	Der suchbare Name des Geräts. Dieser Name wird im Geräte- und logischen Baum angezeigt.

Der Bereichsname, das Modell und der Hersteller bestimmen, wie das Gerät im Gerätebaum und in ONVIF der Encoder-Identifikation und den Haupteinstellungen angezeigt wird.

15.4.14 Relais

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > erweitern > > Registerkarte **ONVIF Konfiguration** > Registerkarte **Schnittstellen** > Registerkarte **Relais**

Hauptfenster > **Geräte** > erweitern > > Registerkarte **ONVIF Konfiguration** > Registerkarte **Schnittstellen** > Registerkarte **Relais**

Der physische Ruhezustand eines Relaisausgangs kann konfiguriert werden, indem Sie den Ruhezustand auf **offen** oder **geschlossen** festlegen (Umkehrung des Relaisverhaltens).
Die verfügbaren digitalen Ausgänge des Geräts sind mit Namen aufgelistet, z. B.:

- **AlarmOut_0**
- **AlarmOut_1**

Für jede Ereigniszuordnung von Relais innerhalb von BVMS verwenden Sie die hier aufgelisteten Namen.

Modus

Das Relais kann in zwei Relaismodi arbeiten:

- **Bistabil**: Nach dem Einstellen des Zustands bleibt das Relais in diesem Zustand.
- **Monostabil**: Nach dem Einstellen des Zustands kehrt das Relais nach der angegebenen Verzögerungszeit in den Ruhezustand zurück.

Ruhezustand

Wählen Sie **Offen** aus, wenn das Relais als normaler offener Kontakt geschaltet werden soll, oder wählen Sie **Geschlossen**, wenn das Relais als normaler geschlossener Kontakt geschaltet werden soll.

Verzögerungszeit

Stellen Sie die Verzögerungszeit ein. Nach diesem Zeitraum wechselt das Relais zurück in den Ruhezustand, wenn dies im Modus **Monostabil** konfiguriert ist.
Wenn Sie alle Konfigurationen in Bezug auf eine Relaisstatusänderung überprüfen möchten, klicken Sie auf **Aktivieren** oder **Deaktivieren**, um das Relais zu wechseln. Sie können die konfigurierten Kamerarelaisereignisse auf ihre korrekte Funktion überprüfen: Statusanzeige des Relaissymbols im logischen Baum, Ereignisse in der Alarmliste oder Ereignisprotokoll.

Aktivieren

Klicken Sie darauf, um das Relais in den konfigurierten Ruhezustand zu wechseln.

Deaktivieren

Klicken Sie darauf, um das Relais in den konfigurierten aktiven Zustand zu wechseln.

15.5 Seite "ONVIF-Ereignisquelle"

Hauptfenster > **Geräte** > Erweitern > Erweitern > Erweitern > Erweitern > Erweitern > > Registerkarte **ONVIF Ereignisquelle**

oder

Hauptfenster > **Geräte** > Erweitern > Erweitern > > Registerkarte **ONVIF Ereignisquelle**

oder

Hauptfenster > **Geräte** > Erweitern > Erweitern > Erweitern > Erweitern > Erweitern > > Registerkarte **ONVIF Ereignisquelle**

oder

Hauptfenster > **Geräte** > Erweitern > Erweitern > > Registerkarte **ONVIF Ereignisquelle**

oder

Hauptfenster > **Geräte** > Erweitern > Erweitern > Erweitern > Erweitern > Erweitern > > Registerkarte **ONVIF Ereignisquelle**

oder

Hauptfenster > **Geräte** > Erweitern > Erweitern > > Registerkarte **ONVIF Ereignisquelle**

Ereignisquelle

Sie können ONVIF-Ereignisse einer Quelle konfigurieren (Videokanal, Eingang oder Relais). Eine aktivierte Ereignisdefinition wird der Mapping-Tabelle des Encoders hinzugefügt.

Für Mehrkanal-Encoders können Sie beispielsweise konfigurieren, für welche Kamera ein **Bewegung erkannt** Ereignis ausgelöst wird.

Ereignis auslösen

Aktivieren Sie dieses Ereignis.

ONVIF Topic

Geben Sie einen String ein oder wählen Sie einen aus.

ONVIF Quellenname

Geben Sie einen String ein oder wählen Sie einen aus.

ONVIF Quellentyp

Geben Sie einen String ein oder wählen Sie einen aus.

ONVIF Quellenwert

Geben Sie einen String ein oder wählen Sie einen aus.

Siehe

- *ONVIF-Ereigniszuordnung, Seite 42*
- *Konfigurieren einer ONVIF-Mapping-Tabelle, Seite 243*

15.6 ONVIF-Profile zuweisen

Hauptfenster > **Kameras und Aufzeichnung** >

Sie können einer ONVIF-Kamera einen Codierschlüssel für das ONVIF-Medienprofil zuweisen.
Sie können diesen entweder für Live-Videos oder Aufzeichnungen zuweisen.

So weisen Sie einen Codierschlüssel für ein Live-Video zu:

- Wählen Sie in der Spalte **Live Video** - **Profil** den gewünschten Eintrag aus.

So weisen Sie einen Codierschlüssel für eine Aufzeichnung zu:

- Wählen Sie in der Spalte **Aufzeichnung** - **Profil** den gewünschten Eintrag aus.

Siehe

– *Seite Kameras, Seite 290*

16 Seite Nummernschild-Erkennung

Hauptfenster > **Geräte** > Erweitern Sie > Erweitern Sie > Erweitern Sie > > > **VCA** Registerkarte > **Nummernschild-Erkennung** Registerkarte

oder

Hauptfenster > **Geräte** > Erweitern Sie > Erweitern Sie > Erweitern Sie > > > **VCA** Registerkarte > **Nummernschild-Erkennung** Registerkarte

oder

Hauptfenster > **Geräte** > > > **VCA** Registerkarte > **Nummernschild-Erkennung**Registerkarte

oder

Hauptfenster > **Geräte** > > > **VCA** Registerkarte > **Nummernschild-Erkennung** Registerkarte

Auf der **Nummernschild-Erkennung** Seite werden die folgenden Informationen angezeigt:

- Datum und Zeitstempel, an dem ein Nummernschild erkannt wurde,
- Bild des Nummernschildes,
- Nummernschildkette,
- das Herkunftsland des Kennzeichens.

▸ Für weitere Details klicken Sie bitte auf **Mehr anzeigen**.

▸ Um eine weitere Fahrspur hinzuzufügen, klicken Sie auf **Fahrspur hinzufügen**.

Hinweis!
Um die LPR-Einstellungen zu konfigurieren, rufen Sie die Webseite der Kamera auf.

17 Seite „Karten und Struktur“

Hinweis!
BVMS Viewer bietet nur Grundfunktionen. Erweiterte Funktionen sind in BVMS Professional enthalten. Ausführliche Informationen zu den verschiedenen Versionen von BVMS finden Sie unter www.boschsecurity.com und in der BVMS Schnellauswahlhilfe: BVMS Schnellauswahlhilfe.

Die Anzahl der einem Eintrag untergeordneten Elemente wird in eckigen Klammern angezeigt.
Hauptfenster > **Karten und Struktur**
Berechtigungen können verloren gehen. Wenn Sie eine Gerätegruppe verschieben, verlieren diese Geräte ihre Berechtigungseinstellungen. Sie müssen die Berechtigungen auf der Seite **Benutzergruppen** neu einstellen.
Zeigt den Gerätebaum, den Logischen Baum und das Fenster **Globale Karte** an.
Dient zum Einrichten einer Struktur für alle im BVMS enthaltenen Geräte. Die Struktur wird im Logischen Baum abgebildet.
Dient zum Durchführen der folgenden Aufgaben:
- Konfigurieren des Vollständigen Logischen Baums
- Verwalten von Ressourcen
- Erstellen von Kommandoskripten
- Erstellen von Sequenzen
- Erstellen von Karten-Anzeigebereichen
- Erstellen von Störungsrelais
- Hinzufügen von Lageplänen und Erstellen von Hotspots

Die folgenden Elemente können Hotspots auf Karten sein:
- Kameras
- Eingänge
- Relais
- Kommandoskripte
- Sequenzen
- Dokumente
- Links zu anderen Lageplänen
- VRM
- iSCSI
- Leser eines Zutrittskontrollsystems
- Einbruchmeldezentralen
- Management-Server von Enterprise Systems

Beispiele für Ressourcen-Dateien:
- Karten-Dateien
- Dokumenten-Dateien
- Links zu externen URLs
- Audio-Dateien
- Links zu externen Anwendungen

Symbole

	Zeigt ein Dialogfeld zur Verwaltung von Ressourcen-Dateien an.
	Zeigt ein Dialogfeld zum Hinzufügen oder zur Verwaltung von Kommandoskripts zum Logischen Baum an.

	Zeigt ein Dialogfeld zum Hinzufügen oder Bearbeiten einer Kamerasequenz-Datei an.
	Erstellt einen Ordner im Logischen Baum.
	Zeigt ein Dialogfeld zum Hinzufügen von Kartenressourcen-Dateien an.
	Erstellt einen Karten-Anzeigebereich im Logischen Baum.
	Zeigt ein Dialogfeld zum Hinzufügen einer Dokument-Datei an.
	Zeigt ein Dialogfeld zum Hinzufügen eines Links zu einer externen Anwendung an.
	Zeigt ein Dialogfeld zum Hinzufügen eines Störungsrelais an.

Symbole

	Gerät wurde zum Logischen Baum hinzugefügt.

Um nach Elementen zu suchen:

- Tippen Sie im Suchfeld eine Zeichenfolge ein und drücken Sie auf den Schlüssel ENTER, um die angezeigten Elemente zu filtern.
  Nur Elemente mit der Zeichenfolge und ihre übergeordneten Elemente (nur in Bäumen) werden angezeigt. Die Anzahl der gefilterten Elemente und die gesamte Anzahl der Elemente wird angegeben.

Hinweis: Setzen Sie Zeichenfolgen zwischen doppelte Anführungszeichen, um genaue Treffer zu erhalten. Beispielsweise filtert "Camera 1" genau die Kameras mit diesem Namen, jedoch nicht camera 201.

18 Konfigurieren von Karten und dem Logischen Baum

Dieses Kapitel enthält Informationen zur Konfiguration des Logischen Baums und zur Verwaltung von Ressourcen-Dateien wie Karten.

Hinweis!
Wenn Sie eine Gerätegruppe im Logischen Baum verschieben, verlieren diese Geräte ihre Freigabeeinstellungen. Sie müssen die Freigaben auf der Seite **Benutzergruppen** neu festlegen.

– Klicken Sie auf , um die Einstellungen zu speichern.

– Klicken Sie auf , um die letzte Einstellung rückgängig zu machen.

– Klicken Sie auf , um die Konfiguration zu aktivieren.

Siehe
- *Dialogfeld Ressourcen-Manager, Seite 266*
- *Dialogfeld Ressource auswählen, Seite 267*
- *Dialogfeld Kamerasequenzen, Seite 269*
- *Dialogfeld Kamerasequenz hinzufügen, Seite 271*
- *Dialogfeld Sequenzschritt hinzufügen, Seite 272*
- *Dialogfeld URL hinzufügen, Seite 267*
- *Dialogfeld Karte für Link auswählen, Seite 273*
- *Dialogfeld „Störungsrelais“, Seite 280*
- *Dialogfeld „Link zu externer Anwendung“, Seite 268*

18.1 Konfigurieren des Logischen Baums

Hauptfenster > **Karten und Struktur** > **Logischer Baum** Registerkarte
Sie können Geräte, Ressourcen-Dateien, Karten-Anzeigebereiche, Sequenzen, Client-Kommandoskripts und Ordner zum Logischen Baum hinzufügen. Geräte werden im Gerätebaum aufgelistet. Sie können jede Ebene des Gerätebaums zum Logischen Baum ziehen.
Bei Ressourcen-Dateien kann es sich beispielsweise um Lagepläne, Dokumente, Web-Dateien, Audio-Dateien oder Kommandoskripte handeln.
- Ein Lageplan ist eine Datei, die Sie zum Logischen Baum hinzufügen können. Durch das Hinzufügen eines Lageplans zum Logischen Baum wird ein Kartenordner erstellt, in dem Sie die für die Karte spezifischen logischen Geräte strukturieren können.
- Ein Karten-Anzeigebereich ist ein Bereich einer globalen Karte mit festgelegter Mitte und Zoom-Stufe.
- Ordner ermöglichen Ihnen eine weitere Strukturierung der Geräte im Logischen Baum.

Wenn Sie den Configuration Client zum ersten Mal starten, ist der Logische Baum leer.
Wenn eine Benutzergruppe nicht über die Zugriffsberechtigung auf ein Gerät (z. B. eine Kamera) verfügt, wird das Gerät nicht auf dem Lageplan, im Karten-Anzeigebereich oder im Logischen Baum angezeigt.
Sie können die folgenden Elemente aus dem Gerätebaum oder dem Logischen Baum zu einem Lageplan hinzufügen:
- Kameras
- Eingänge
- Relais

- Kommandoskripte
- Sequenzen
- Dokumente
- Links zu anderen Lageplänen
- VRM
- iSCSI
- Leser eines Zutrittskontrollsystems
- Einbruchmeldezentralen
- Management-Server von Enterprise Systems

Durch das Hinzufügen eines Elements zu einem Lageplan wird ein Hotspot auf der Karte erstellt. Wenn Sie ein Element zu einem Kartenordner im Logischen Baum hinzufügen, wird es auch in der oberen linken Ecke der Karte angezeigt. Wenn Sie ein Element zu einer Karte hinzufügen, wird es auch unter dem entsprechenden Kartenknoten im Logischen Baum des Operator Client hinzugefügt. Sie können die folgenden Elemente aus dem Gerätebaum zur globalen Karte hinzufügen:

- Kameras

Führen Sie zum Konfigurieren des Logischen Baums einige oder alle der folgenden Schritte mehrmals durch.

So benennen Sie den Logischen Baum um:

1. Wählen Sie das Stammelement des Logischen Baums.
2. Klicken Sie auf .
3. Geben Sie einen neuen Namen ein.

Dieser Name ist für alle Benutzer im Logischen Baum des Operator Client sichtbar.

Siehe

- *Seite „Karten und Struktur", Seite 261*

18.2 Hinzufügen eines Geräts zum Logischen Baum

Hauptfenster > **Karten und Struktur** > Registerkarte **Logischer Baum**

So fügen Sie ein Gerät hinzu:

- Ziehen Sie ein Element aus dem Gerätebaum an den erforderlichen Ort im Logischen Baum. Sie können einen vollständigen Knoten mit allen Unterelementen aus dem Gerätebaum in den Logischen Baum ziehen. Sie können mehrere Geräte auswählen, indem Sie die STRG- oder die UMSCHALT-Taste drücken.

Siehe

- *Seite „Karten und Struktur", Seite 261*

18.3 Entfernen eines Baumelements

Hauptfenster > **Karten und Struktur** > Registerkarte **Logischer Baum**

So entfernen Sie ein Baumelement aus dem Logischen Baum:

- Klicken Sie mit der rechten Maustaste auf ein Element im Logischen Baum, und klicken Sie auf **Entfernen**. Wenn das ausgewählte Element über Unterelemente verfügt, wird ein Meldungsfeld angezeigt. Klicken Sie zum Bestätigen **OK**. Das Element wird entfernt.
  Wenn Sie ein Element aus einem Kartenordner des Logischen Baums entfernen, wird es auch aus der Karte entfernt.

Siehe

– *Seite „Karten und Struktur“, Seite 261*

18.4 Verwalten von Ressourcen-Dateien

Hauptfenster > **Karten und Struktur** > Registerkarte **Logischer Baum** >
oder

Hauptfenster > **Alarme** >

Sie können Ressourcen-Dateien folgender Formate importieren:

– DWF-Dateien (2 D, Kartenressourcen-Dateien)
– PDF-Dateien
– JPG-Dateien
– PNG-Dateien
– HTML-Dateien
– MP3-Dateien (Audiodatei)
– TXT-Dateien (Kommandoskripte oder Kamerasequenzen)
– MHT-Dateien (Webarchive)
– URL-Dateien (Links zu Webseiten)
– HTTPS-URL-Dateien (Links zu Intelligent Insights-Widgets)
– WAV-Dateien (Audiodatei)

Die importierten Ressourcen-Dateien werden zu einer Datenbank hinzugefügt. Sie werden nicht mit den ursprünglichen Dateien verknüpft.

Hinweis!
Nach jedem der folgenden Vorgänge:

Klicken Sie auf , um die Einstellungen zu speichern.

So importieren Sie eine Ressourcen-Datei:

1. Klicken Sie auf .
   Das Dialogfeld **Ressource importieren** wird angezeigt.
2. Wählen Sie eine oder mehrere Dateien aus.
3. Klicken Sie auf **öffnen**.
   Die ausgewählten Dateien werden der Liste hinzugefügt.
   Wurde bereits eine Datei importiert, wird ein Meldungsfeld angezeigt.
   Wenn Sie eine bereits importierte Datei erneut importieren möchten, wird der Liste ein neuer Eintrag hinzugefügt.

So entfernen Sie eine Ressourcen-Datei:

1. Wählen Sie eine Ressourcen-Datei aus.
2. Klicken Sie auf .
   Die ausgewählte Ressourcen-Datei wird aus der Liste entfernt.

So benennen Sie eine Ressourcen-Datei um:

1. Wählen Sie eine Ressourcen-Datei aus.
2. Klicken Sie auf .

3. Geben Sie einen neuen Namen ein.
   Der ursprüngliche Dateiname und das Erzeugungsdatum bleiben erhalten.

So ersetzen Sie den Inhalt einer Ressourcen-Datei:

1. Wählen Sie eine Ressourcen-Datei aus.
2. Klicken Sie auf .
   Das Dialogfeld **Ressource ersetzen** wird angezeigt.
3. Wählen Sie eine Datei mit dem entsprechenden Inhalt aus, und klicken Sie auf **Öffnen**.
   Der Ressourcen-Name bleibt erhalten, der ursprüngliche Dateiname wird durch den neuen Dateinamen ersetzt.

So exportieren Sie eine Ressourcen-Datei:

1. Wählen Sie eine Ressourcen-Datei aus.
2. Klicken Sie auf .
   Ein Dialogfeld zum Auswählen eines Verzeichnisses wird angezeigt.
3. Wählen Sie das entsprechende Verzeichnis aus und klicken Sie auf **OK**.
   Die Ursprungsdatei wird exportiert.

Siehe

– *Dialogfeld Ressource auswählen, Seite 267*

18.4.1 Dialogfeld Ressourcen-Manager

Hauptfenster > **Karten und Struktur** > > Dialogfeld **Ressourcen-Manager**

Erlaubt das Verwalten von Ressourcen-Dateien.

Sie können die folgenden Dateiformate verwalten:

– DWF-Dateien (Kartenressourcen-Dateien)
  Zur Verwendung im Operator Client werden diese Dateien in ein Bitmap-Format konvertiert.
– PDF-Dateien
– JPG-Dateien
– PNG-Dateien
– HTML-Dateien (HTML-Dokumente, z. B. Aktionspläne)
– MP3-Dateien (Audiodatei)
– TXT-Dateien (Textdateien)
– URL-Dateien (enthalten Links zu Webseiten oder Intelligent Insights-Widgets)
– MHT-Dateien (Webarchive)
– WAV-Dateien (Audiodatei)
– EXE

Klicken Sie hier, um ein Dialogfeld zum Importieren einer Ressourcen-Datei anzuzeigen.

Klicken Sie hier, um das Dialogfeld **URL hinzufügen** anzuzeigen.

Klicken Sie hier, um das Dialogfeld **Link zu einer externen Anwendung** anzuzeigen.

Klicken Sie hier, um die ausgewählte Ressourcen-Datei zu entfernen.

Klicken Sie hier, um die ausgewählte Ressourcen-Datei umzubenennen.

Klicken Sie hier, um ein Dialogfeld zum Ersetzen der ausgewählten Ressourcen-Datei durch eine andere anzuzeigen.

Klicken Sie hier, um ein Dialogfeld zum Exportieren der ausgewählten Ressourcen-Datei anzuzeigen.

18.4.2 Dialogfeld Ressource auswählen

Hauptfenster > **Karten und Struktur** >
Ermöglicht es Ihnen, eine Kartendatei im DWF-, PDF-, JPG- oder PNG-Format in den logischen Baum einzufügen.

Ressourcen-Datei auswählen:
Klicken Sie auf einen Dateinamen, um eine Kartendatei auszuwählen. Der Inhalt der ausgewählten Datei wird im Voransichtfenster angezeigt.

Verwalten...
Klicken Sie hier, um das Dialogfeld **Ressourcen-Manager** anzuzeigen.

Siehe
- *Hinzufügen einer Karte, Seite 272*
- *Zuordnen einer Karte zu einem Ordner, Seite 273*
- *Hinzufügen eines Dokuments, Seite 267*

18.5 Hinzufügen eines Dokuments

Hauptfenster > **Karten und Struktur** > Registerkarte **Logischer Baum**
Sie können Textdateien, HTML-Dateien (einschließlich MHT-Dateien), URL-Dateien (mit einer Internetadresse) oder HTTPS-URL-Dateien (z. B. mit einem enthaltenen Intelligent Insights-Widget) als Dokumente hinzufügen. Sie können auch einen Link zu einer anderen Anwendung hinzufügen. Bevor Sie ein Dokument hinzufügen können, müssen Sie zunächst Dokumentdateien importieren. Weitere Informationen zum Importieren von Dokumentdateien finden Sie unter *Verwalten von Ressourcen-Dateien, Seite 265*.
So fügen Sie eine Kartendokument-Datei/ein Intelligent Insights-**Widget hinzu:**
1. Stellen Sie sicher, dass die Dokumentdatei, die Sie hinzufügen möchten, bereits importiert wurde.
2. Wählen Sie einen Ordner aus, dem Sie das neue Dokument hinzufügen möchten.
3. Klicken Sie auf . Das Dialogfeld **Ressource auswählen** wird angezeigt.
4. Wählen Sie eine Datei in der Liste aus. Wenn die erforderlichen Dateien nicht in der Liste enthalten sind, klicken Sie auf **Verwalten...**, um das Dialogfeld **Ressourcen-Manager** für den Datei-Import anzuzeigen.
5. Klicken Sie auf **OK**. Ein neues Dokument wird dem ausgewählten Ordner hinzugefügt.

Siehe
- *Dialogfeld Ressource auswählen, Seite 267*
- *Verwalten von Ressourcen-Dateien, Seite 265*

18.5.1 Dialogfeld URL hinzufügen

Hauptfenster > **Karten und Struktur** > >

Dient zum Hinzufügen einer HTTP-Internetadresse (URL) oder einer HTTPS-Internetadresse (z. B. Intelligent Insights-Widgets) zum System. Sie können diese URL als Dokument in den Logischen Baum einfügen. Der Benutzer kann eine Internetseite oder ein Intelligent Insights-Widget im Operator Client anzeigen.

Name
Geben Sie einen Anzeigenamen für die URL ein.

URL
Geben Sie die URL ein.

Nur für sichere Verbindung
Benutzer
Geben Sie den Benutzernamen für die HTTPS-URL an.
Passwort:
Geben Sie das Passwort für die HTTPS-URL ein.

Passwort anzeigen
Klicken Sie hier, damit das eingegebene Passwort angezeigt wird. Achten Sie darauf, dass niemand das Passwort einsehen kann.

Siehe
– *Hinzufügen eines Dokuments, Seite 267*

18.6 Dialogfeld „Link zu externer Anwendung“

Hauptfenster > **Karten und Struktur** > Registerkarte **Logischer Baum** > > Dialogfeld **Ressourcen-Manager** > > Dialogfeld **Link zu einer externen Anwendung**
Damit können Sie einen Link zu einer externen Anwendung hinzufügen. Der Link muss auf der Arbeitsstation gültig sein, bei der dieser Link verwendet wird.

Hinweis!
Eine externe Anwendung, die mit einem Startbildschirm beginnt, wird nicht wie erwartet funktionieren.
Eine externe Anwendung, die Funktionen mit Operator Client teilt, funktioniert nicht wie erwartet und kann in seltenen Fällen zu einem Absturz des Operator Client führen.

Name
Geben Sie einen Namen für den Link ein, der in dem logischen Baum angezeigt wird.

Pfad
Geben Sie den Pfad zu der externen Anwendung ein oder suchen Sie ihn. Dieser Pfad muss auf der Arbeitsstation gültig sein, auf der der Benutzer Operator Client diesen Link verwendet.

Argumente
Falls erforderlich, geben Sie Argumente für den Befehl ein, der die externe Anwendung ausführt.

18.7 Hinzufügen eines Kommandoskripts

Hauptfenster > **Karten und Struktur** > Registerkarte **Logischer Baum**
Bevor Sie ein Kommandoskript hinzufügen können, müssen Sie zunächst Kommandoskript-Dateien importieren oder erstellen.
Weitere Informationen finden Sie unter *Konfigurieren von Kommandoskripten, Seite 89*.

So fügen Sie ein Kommandoskript hinzu:

1. Wählen Sie einen Ordner aus, dem Sie das neue Kommandoskript hinzufügen möchten.
2. Klicken Sie auf . Das Dialogfeld **Client-Skript auswählen** wird angezeigt.
3. Wählen Sie eine Datei in der Liste aus.
4. Klicken Sie auf **OK**.
   Ein neues Kommandoskript wird unter dem ausgewählten Ordner hinzugefügt.

Siehe

– *Dialogfeld Ressource auswählen, Seite 267*

18.8 Hinzufügen einer Kamerasequenz

Hauptfenster > **Karten und Struktur** > Registerkarte **Logischer Baum**
Eine Kamerasequenz wird zum Hauptverzeichnis oder zu einem Ordner des Logischen Baums hinzugefügt.

So fügen Sie eine Kamerasequenz hinzu:

1. Wählen Sie im Logischen Baum einen Ordner aus, dem Sie die neue Kamerasequenz hinzufügen möchten.
2. Klicken Sie auf . Das Dialogfeld **Kamerasequenzen** wird angezeigt.
3. Wählen Sie eine Kamerasequenz in der Liste aus.
4. Klicken Sie auf **Zum Logischen Baum hinzufügen**. Eine neue wird unter dem ausgewählten Ordner hinzugefügt.

Siehe

– *Dialogfeld Kamerasequenzen, Seite 269*

18.8.1 Dialogfeld Kamerasequenzen

Hauptfenster > **Karten und Struktur** >
Dient zum Verwalten von Kamerasequenzen.

Symbole

	Klicken Sie hier, um das Dialogfeld **Kamerasequenz hinzufügen** anzuzeigen.
	Klicken Sie hier, um eine Kamerasequenz umzubenennen.
	Klicken Sie hier, um die ausgewählte Kamerasequenz zu entfernen.

Schritt hinzufügen

Klicken Sie hier, um das Dialogfeld **Sequenzschritt hinzufügen** anzuzeigen.

Schritt entfernen

Klicken Sie darauf, um ausgewählte Schritte zu entfernen.

Schritt
Zeigt die Nummer des Schritts an. Alle Kameras eines bestimmten Schritts weisen die gleiche Verweilzeit auf.

Verweilzeit
Dient zum Ändern der Verweilzeit (Sekunden).

Kameranummer
Klicken Sie auf eine Zelle, um eine Kamera über ihre logische Nummer auszuwählen.

Kamera
Klicken Sie auf eine Zelle, um eine Kamera über ihren Namen auszuwählen.

Kamerafunktion
Klicken Sie auf eine Zelle, um die Kamerafunktion in dieser Zeile zu ändern.

Daten
Geben Sie die Dauer für die ausgewählte Kamerafunktion ein. Für diese Einstellung muss in der Spalte **Kamera** und in der Spalte **Kamerafunktion** jeweils ein Eintrag ausgewählt sein.

Datenmaßeinheit
Wählen Sie die Einheit für die ausgewählte Zeit aus, beispielsweise Sekunden. Für diese Einstellung muss in der Spalte **Kamera** und in der Spalte **Kamerafunktion** jeweils ein Eintrag ausgewählt sein.

Zum Logischen Baum hinzufügen
Klicken Sie darauf, um die ausgewählte Kamerasequenz dem Logischen Baum hinzuzufügen und das Dialogfeld zu schließen.

Siehe
– *Verwalten von vorkonfigurierten Kamerasequenzen, Seite 270*

18.9 Verwalten von vorkonfigurierten Kamerasequenzen

Hauptfenster > **Karten und Struktur** > Registerkarte **Logischer Baum**
Sie können folgende Aufgaben zum Verwalten von Kamerasequenzen durchführen:
– Erstellen einer Kamerasequenz
– Hinzufügen eines Schritts mit neuer Verweilzeit zu einer vorhandenen Kamerasequenz
– Entfernen eines Schritts aus der Kamerasequenz
– Löschen einer Kamerasequenz

Hinweis!
Wenn die Konfiguration geändert und aktiviert wurde, wird die (vorkonfigurierte oder automatische) Kamerasequenz normalerweise nach dem Neustart des Operator Clients fortgesetzt.
In den folgenden Fällen wird die Sequenz jedoch nicht fortgesetzt:
Ein Monitor wurde entfernt, auf dem die Sequenz gemäß Konfiguration angezeigt werden soll.
Der Modus eines Monitors (Einfach-Ansicht/Vierfach-Ansicht) wurde geändert, auf dem die Sequenz gemäß Konfiguration angezeigt werden soll.
Die logische Nummer eines Monitors wurde geändert, auf dem die Sequenz gemäß Konfiguration angezeigt werden soll.

Hinweis!
Nach jedem der folgenden Vorgänge:

Klicken Sie auf , um die Einstellungen zu speichern.

So erzeugen Sie eine Kamerasequenz:

1. Wählen Sie im Logischen Baum einen Ordner aus, in dem Sie die neue Kamerasequenz erzeugen möchten.
2. Klicken Sie auf .
   Das Dialogfeld **Kamerasequenzen** wird angezeigt.
3. Klicken Sie im Dialogfeld **Kamerasequenzen** auf .
   Das Dialogfeld **Kamerasequenz hinzufügen** wird angezeigt.
4. Geben Sie die erforderlichen Werte ein.
5. Klicken Sie auf **OK**.

   Eine neue Kamerasequenz wird hinzugefügt.

Detaillierte Informationen zu den verschiedenen Feldern finden Sie in der Online-Hilfe unter dem entsprechenden Anwendungsfenster.

So fügen Sie einen Schritt mit einer neuen Verweilzeit zu einer Kamerasequenz hinzu:

1. Wählen Sie die gewünschte Kamerasequenz aus.
2. Klicken Sie auf **Schritt hinzufügen**.
   Das Dialogfeld **Sequenzschritt hinzufügen** wird angezeigt.
3. Nehmen Sie die erforderlichen Einstellungen vor.
4. Klicken Sie auf **OK**.
   Ein neuer Schritt wird zur Kamerasequenz hinzugefügt.

So entfernen Sie einen Schritt aus einer Kamerasequenz:

- Klicken Sie mit der rechten Maustaste auf die gewünschte Kamerasequenz, und klicken Sie auf **Schritt entfernen**.
  Der Schritt mit der höchsten Zahl wird entfernt.

So löschen Sie eine Kamerasequenz:

1. Wählen Sie die gewünschte Kamerasequenz aus.
2. Klicken Sie auf . Die ausgewählte Kamerasequenz wird entfernt.

Siehe

– *Dialogfeld Kamerasequenzen, Seite 269*

18.9.1 Dialogfeld Kamerasequenz hinzufügen

Hauptfenster > **Karten und Struktur** > > Dialogfeld **Kamerasequenzen** >

Dient zum Konfigurieren der Eigenschaften einer Kamerasequenz.

Kamerasequenzname:

Geben Sie einen aussagekräftigen Namen für die neue Kamerasequenz ein.

Logische Nummer:

Geben Sie zur Verwendung mit einem Bosch IntuiKey Keyboard eine logische Nummer für die Sequenz ein.

Verweilzeit:

Geben Sie die Verweilzeit ein.

Kameras pro Schritt:

Geben Sie die Anzahl der Kameras in jedem Schritt ein.

Schritte:
Geben Sie die entsprechende Anzahl an Schritten ein.

18.9.2 Dialogfeld Sequenzschritt hinzufügen

Hauptfenster > **Karten und Struktur** > > Schaltfläche **Schritt hinzufügen**
Dient zum Hinzufügen eines Schritts mit einer neuen Verweilzeit zu einer vorhandenen Kamerasequenz.

Verweilzeit:
Geben Sie die Verweilzeit ein.

18.10 Hinzufügen eines Ordners

Hauptfenster > **Karten und Struktur** > Registerkarte **Logischer Baum**
So fügen Sie einen Ordner hinzu:

1. Wählen Sie einen Ordner aus, dem Sie den neuen Ordner hinzufügen möchten.
2. Klicken Sie auf . Ein neuer Ordner wird unter dem ausgewählten Ordner hinzugefügt.
3. Klicken Sie auf , um den Ordner umzubenennen.
4. Geben Sie den neuen Namen ein und drücken Sie die Eingabetaste.

Siehe
– *Seite „Karten und Struktur“, Seite 261*

18.11 Hinzufügen einer Karte

Hauptfenster > **Karten und Struktur** > Registerkarte **Logischer Baum**
Bevor Sie eine Karte hinzufügen können, müssen Sie zunächst Kartenressourcen-Dateien importieren. Weitere Informationen zum Importieren von Kartenressourcen-Dateien finden Sie unter *Verwalten von Ressourcen-Dateien, Seite 265*.
So fügen Sie eine Karte hinzu:

1. Stellen Sie sicher, dass die Kartenressourcen-Datei, die Sie hinzufügen möchten, bereits importiert wurde.
2. Wählen Sie einen Ordner aus, dem Sie die neue Karte hinzufügen möchten.
3. Klicken Sie auf . Das Dialogfeld **Ressource auswählen** wird angezeigt.
4. Wählen Sie eine Datei in der Liste aus.
   Wenn die erforderlichen Dateien nicht in der Liste enthalten sind, klicken Sie auf **Verwalten...**, um das Dialogfeld **Ressourcen-Manager** für den Datei-Import anzuzeigen.
5. Klicken Sie auf **OK**.
   Eine neue Karte wird unter dem ausgewählten Ordner hinzugefügt.
   Die Karte wird angezeigt.
   Alle Geräte in diesem Ordner werden im linken oberen Bereich der Karte angezeigt.

Siehe
– *Dialogfeld Ressource auswählen, Seite 267*

18.12 Hinzufügen eines Links zu einer anderen Karte

Hauptfenster > **Karten und Struktur** > Registerkarte **Logischer Baum**
Wenn mindestens zwei Karten vorhanden sind, können Sie einer Karte einen Link hinzufügen, der auf die andere Karte verweist, sodass der Benutzer mit einem Klick von einer Karte auf eine verknüpfte Karte gelangen kann.
So fügen Sie einen Link hinzu:

1. Klicken Sie im Logischen Baum auf einen Kartenordner .
2. Klicken Sie mit der rechten Maustaste auf die Karte und klicken Sie dann auf **Link erzeugen**. Das Dialogfeld **Karte für Link auswählen** wird angezeigt.
3. Klicken Sie im Dialogfeld auf eine Karte .
4. Klicken Sie auf **Auswählen**.
5. Ziehen Sie das Element an die gewünschte Stelle auf der Karte.

18.12.1 Dialogfeld Karte für Link auswählen

Hauptfenster > **Karten und Struktur** > Kartenordner im Logischen Baum auswählen > mit der rechten Maustaste auf die Karte klicken und auf **Link erzeugen** klicken.
Dient zum Auswählen einer Karte, um einen Link zu einer anderen Karte zu erzeugen.

Klicken Sie auf eine andere Karte, um diese auszuwählen.

Auswählen
Klicken Sie darauf, um den Link in die ausgewählte Karte einzufügen.

18.13 Zuordnen einer Karte zu einem Ordner

Hauptfenster > **Karten und Struktur** > Registerkarte **Logischer Baum**
Bevor Sie Karten zuweisen können, müssen Sie zunächst Kartenressourcen-Dateien importieren.
Weitere Informationen finden Sie unter *Verwalten von Ressourcen-Dateien, Seite 265*.
So weisen Sie eine Kartenressourcen-Datei zu:

1. Klicken Sie mit der rechten Maustaste auf einen Ordner, und klicken Sie auf **Karte zuordnen**. Das Dialogfeld **Ressource auswählen** wird angezeigt.
2. Wählen Sie eine Kartenressourcen-Datei in der Liste aus.
3. Klicken Sie auf **OK**. Der ausgewählte Ordner wird angezeigt als .
   Die Karte wird im Fenster „Karte" angezeigt.
   Alle Elemente in diesem Ordner werden im linken oberen Bereich der Karte angezeigt.

Siehe
- *Seite „Karten und Struktur", Seite 261*
- *Dialogfeld Ressource auswählen, Seite 267*

18.14 Verwalten von Geräten auf einem Lageplan

Hauptfenster > **Karten und Struktur** > Registerkarte **Logischer Baum**
Bevor Sie Geräte auf einem Lageplan verwalten können, müssen Sie zunächst eine Karte hinzufügen oder einem Ordner eine Karte zuweisen und diesem Ordner Geräte hinzufügen.

Hinweis!
Nach jedem der folgenden Vorgänge:

Klicken Sie auf , um die Einstellungen zu speichern.

So platzieren Sie Elemente auf einem Lageplan:

1. Wählen Sie einen Kartenordner aus.
2. Ziehen Sie Geräte vom Gerätebaum in den Kartenordner.
   Die Geräte eines Kartenordners befinden sich im linken oberen Bereich des Lageplans.
3. Ziehen Sie die Elemente an die gewünschten Stellen auf dem Lageplan.

So entfernen Sie ein Element des Logischen Baums nur vom Lageplan:

1. Klicken Sie mit der rechten Maustaste auf die Karte und klicken Sie auf **Unsichtbar**.
   Das Element wird aus dem Lageplan entfernt.
   Das Element bleibt im Logischen Baum.
2. Um das Gerät wieder sichtbar zu machen, klicken Sie im Logischen Baum mit der rechten Maustaste darauf und klicken Sie dann auf **Sichtbar auf einer Karte**.

So entfernen Sie ein Element vom Lageplan und aus dem Vollständigen Logischen Baum:

- Klicken Sie mit der rechten Maustaste auf das Element im Logischen Baum und klicken Sie dann auf **Entfernen**.
  Das Element wird vom Lageplan und aus dem Logischen Baum entfernt.

So ändern Sie das Symbol zur Ausrichtung einer Kamera:

- Klicken Sie mit der rechten Maustaste auf das Element, zeigen Sie mit dem Mauszeiger auf **Symbol ändern** und klicken Sie dann auf das gewünschte Symbol.
  Das Symbol ändert sich entsprechend.

So ändern Sie die Farbe eines Elements:

- Klicken Sie mit der rechten Maustaste auf das Element, und klicken Sie auf **Farbe ändern**.
  Wählen Sie die gewünschte Farbe aus.
  Das Symbol ändert sich entsprechend.

So umgehen Sie ein Gerät auf einem Lageplan bzw. heben die Umgehung auf:

1. Klicken Sie mit der rechten Maustaste auf das bestimmte Gerät auf dem Lageplan.
2. Klicken Sie auf **Umgehen/Umgehung aufheben**.

Hinweis!
Es ist möglich, umgangene Geräte über das Suchfeld zu filtern.

Siehe

- *Konfigurieren der Geräteumgehung, Seite 281*
- *Seite „Karten und Struktur“, Seite 261*

18.15 Konfigurieren der globalen Karte und der Karten-Anzeigebereiche

Hauptfenster > **Karten und Struktur** > Registerkarte **Globale Karte**
Damit Sie Online-Karten oder den Map-based tracking assistant im Operator Client verwenden können, müssen Sie Kameras zum Lageplan hinzufügen und konfigurieren.
Sie können Karten-Anzeigebereiche auf einer globalen Karte konfigurieren. Ein Karten-Anzeigebereich ist ein Bereich der globalen Karte mit festgelegter Mitte und Zoom-Stufe. Ein Karten-Anzeigebereich kann in einem Bildfenster des Operator Client angezeigt werden.

Wenn Sie einen Karten-Anzeigebereich erstellen oder den Map-based tracking assistant im Operator Client verwenden möchten, gehen Sie zunächst wie folgt vor:

1. Wählen Sie den Hintergrundkartentyp der globalen Karte aus.
2. Ziehen Sie Ihre Kameras auf die globale Karte.
3. Konfigurieren Sie die Richtung und den Bildwinkel Ihrer Kameras auf der globalen Karte.

Wenn Sie Map-Viewports erstellen möchten oder den Map-based tracking assistant in dem Operator Client **auf mehreren Etagenverwenden** möchten, gehen Sie zuerst wie folgt vor:

1. Wählen Sie den Hintergrundkartentyp der globalen Karte aus.
2. Fügen Sie eine Karte zur globalen Karte hinzu.
   Hinweis: Die erste Karte, die Sie hinzufügen, wird das Erdgeschoss sein. Wenn Sie den Typ Offline-Hintergrundkarte **Kein Eintrag** wählen, wird die erste Karte, die Sie hinzufügen, die Hintergrundkarte sein.
3. Fügen Sie Stockwerke zum Erdgeschoss oder zur Hintergrundkarte hinzu.
4. Wählen Sie die gewünschte Etage.
5. Ziehen Sie Ihre Kameras auf den Etagenplan.
6. Konfigurieren Sie die Richtung und den Sichtkegel Ihrer Kameras.

18.15.1 Konfigurieren der globalen Karte

Sie können die Hintergrundkartentypen für die globale Karte definieren und nach Kameras, Standorten und Adressen suchen.

So ändern Sie den Hintergrundkartentyp der globalen Karte:

1. Gehen Sie zum Hauptfenster und navigieren Sie zu Menü **Einstellungen** > Befehl **Optionen...**.
2. In dem Abschnitt **Systemfunktionen** Wählen Sie **Karten**.
3. In der **Art der Hintergrundkarte** list, select the desired option.
   Hinweis: Wenn Sie Zugang zum Internet haben, können Sie einen Online-Hintergrundkartentyp auswählen (**HERE** Karten). Wenn Sie keinen Zugang zum Internet haben, wählen Sie den Typ Offline-Hintergrundkarte **Kein Eintrag**.
   Für die Nutzung von Online-Karten müssen Sie eine Lizenz erwerben.
4. Klicken Sie auf **OK**.

Hinweis!
Wenn Sie den Typ der Hintergrundkarte von offline auf (**Kein Eintrag**) zu online (**HERE** Maps), überprüfen Sie, ob die Position der Submaps und der Kamera-Hotspots noch korrekt ist.

So suchen Sie auf der globalen Karte nach Kameras oder Standorten:

1. Geben Sie den Namen einer Kamera, eines Standorts oder einer Adresse in das Suchfeld ein.
   Sobald Sie mit dem Tippen begonnen haben, wird ein Dropdown-Menü mit einer Liste relevanter Optionen angezeigt.
2. Wählen Sie die entsprechende Option aus der Liste aus.
   Die Kamera, der Standort oder die Adresse wird angezeigt und einige Sekunden lang mit einer Fahne markiert.

Siehe

– *Dialogfeld „Optionen“ (Menü „Einstellungen“), Seite 121*

18.15.2 Konfigurieren von Kameras auf der globalen Karte

So konfigurieren Sie eine Kamera auf der globalen Karte:

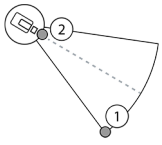
Hinweis: Wenn Sie mehrere Stockwerke auf Karten konfiguriert haben, stellen Sie sicher, dass Sie das richtige Stockwerk auswählen, in dem Sie Ihre Kameras konfigurieren möchten.

1. Öffnen Sie die Registerkarte **Globale Karte**.
2. Geben Sie im Suchfeld eine Adresse oder einen Standort ein, um zur Position zu wechseln, an der Sie Ihre Kamera platzieren möchten.

   Mit den Schaltflächen + und − oder dem Mausrad können Sie heran- oder herauszoomen.
3. Ziehen Sie eine Kamera aus dem Gerätebaum in den entsprechenden Bereich der globalen Karte.
4. Klicken Sie auf die Kamera, um sie auszuwählen.
5. Konfigurieren Sie die Richtung und den Bildwinkel der Kamera.
   Hinweis: Bei Auswahl einer Domekamera werden der erreichbare und der tatsächliche Bildwinkel angezeigt. Ein Warnsymbol weist darauf hin, dass der tatsächliche Bildwinkel der Domekamera in der horizontalen und vertikalen Ebene kalibriert werden muss. Öffnen Sie das Vorschaubild des Live-Videos, um die Domekamera zu kalibrieren.
6. Klicken Sie auf , um ein Vorschaubild des Live-Videos der ausgewählten Kamera anzuzeigen.
   Die Videovorschau kann hilfreich bei der Konfiguration von Richtung und Bildwinkel sein.
7. Klicken Sie auf , um die Videovorschau der ausgewählten Kamera auszublenden.

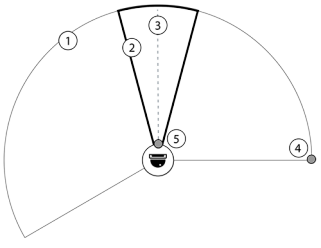
Hinweis: Wenn Sie eine Kamera zur globalen Karte hinzufügen, diese Kamera aber noch nicht zum Logischen Baum hinzugefügt haben, wird sie am Ende automatisch zum Logischen Baum hinzugefügt.

So konfigurieren Sie Richtung und Bildwinkel einer Kamera:



1. Ziehen Sie den Mauszeiger, um den Bildwinkel zu konfigurieren.
2. Ziehen Sie den Mauszeiger zum Rotieren und Konfigurieren der Richtung.

So konfigurieren Sie die horizontale Richtung und den Bildwinkel einer PTZ-Kamera (Plattform CPP4 oder höher):



1. Der erreichbare Bildwinkel gibt den theoretisch erreichbaren Ansichtsbereich an.
2. Der tatsächliche Bildwinkel gibt die tatsächliche PTZ-Position der PTZ-Kamera an.
3. Schwenkwinkel 0.
4. Ziehen Sie den Mauszeiger, um den Bildwinkel zu konfigurieren.
5. Ziehen Sie den Mauszeiger zum Rotieren und Konfigurieren der Richtung.

Hinweis!
Für eine optimale Nutzung des Map-based tracking assistant müssen Sie auch die vertikale Position der PTZ-Kamera anpassen. Wir empfehlen, die vertikale Position im Vorschaubild des Live-Videos anhand einer bekannten Position in der Umgebung festzulegen, beispielsweise mithilfe eines unverwechselbaren Gebäudes. Der Map-based tracking assistant wird später immer diese konfigurierte vertikale Position verwenden.

Zum Anzeigen oder Ausblenden von Kameravorschauen:

1. Klicken Sie auf , um ein Vorschaubild des Live-Videos der ausgewählten Kamera anzuzeigen.
   Oder
   klicken Sie mit der rechten Maustaste auf die Kamera und wählen Sie **Vorschau zeigen**.
   Die Videovorschau kann Ihnen helfen, die Richtung und den Sichtkegel zu konfigurieren.
2. Klicken Sie auf , um die Videovorschau der ausgewählten Kamera auszublenden.
   Oder
   klicken Sie mit der rechten Maustaste auf die Kamera und wählen Sie **Vorschau verbergen**.

So entfernen Sie eine Kamera aus der globalen Karte:

- Klicken Sie mit der rechten Maustaste auf die Kamera und wählen Sie **Entfernen**.

So machen Sie eine Kamera auf allen Etagen sichtbar:

- Klicken Sie mit der rechten Maustaste auf den Kamera-Hotspot und wählen Sie **Sichtbar auf allen Ebenen**.
  Die Kamera ist jetzt immer sichtbar, wenn Sie eine andere Etage auswählen.

So bearbeiten Sie die Geolokalisierung einer Kamera

1. Klicken Sie mit der rechten Maustaste auf die Kamera und wählen Sie **Standort bearbeiten**.
   Die **Standort bearbeiten** Dialogfeld wird angezeigt.
2. Geben Sie den Breitengrad und den Längengrad ein und klicken Sie dann auf **OK**.
   Hinweis: Sie können die Werte für den Breiten- und Längengrad auch aus einer externen Quelle kopieren, anstatt sie einzugeben. Wenn Sie in diesem Fall die Werte in das Feld Breitengrad einfügen, wird das Feld Längengrad automatisch ausgefüllt.

So aktivieren Sie die Objektverfolgung für eine Kamera:

- Klicken Sie mit der rechten Maustaste auf die Kamera, und wählen Sie aus **Objektverfolgung (wenn zum logischen Baum hinzugefügt)** aus.
  Die Objektverfolgung ist für diese Kamera aktiviert.
  Hinweis: Die Objektverfolgung ist nur für Kameras mit CPP6 oder höher verfügbar, die dem logischen Baum hinzugefügt werden.

Gruppieren von Kamera-Hotspots

Wenn Sie bereits mehrere Kameras auf der globalen Karte konfiguriert haben und herauszoomen, werden die Kamera-Hotspots zu Hotspot-Gruppen zusammengefasst. Die Anzahl der einzelnen Hotspots in einer Hotspot-Gruppe wird angezeigt. Eine ausgewählte Kamera wird nicht als Teil einer Gruppe angezeigt.

Siehe

– *Hinzufügen eines Bosch Encoders mit vorkonfigurierten Geolokalisierungseinstellungen, Seite 223*

18.15.3 Hinzufügen von Karten auf der globalen Karte

Sie können Karten-Dateien Ihres eigenen Gebäudes zur globalen Karte hinzufügen.
Die BVMS Bediener können dann eine detailliertere Ansicht bestimmter Kamerastandorte erhalten.

So fügen Sie eine Karte auf der globalen Karte hinzu:

1. Öffnen Sie die Registerkarte **Globale Karte**.
2. Geben Sie im Suchfeld eine Adresse oder einen Standort ein, um zur Position zu wechseln, an der Sie Ihren Lageplan platzieren möchten.

   Mit den Schaltflächen + und − oder dem Mausrad können Sie heran- oder herauszoomen.
3. Klicken Sie auf .
   Das Fenster **Ressource auswählen** wird geöffnet.
4. Wählen Sie eine Karte aus und klicken Sie auf **OK**.
5. Klicken Sie auf ↻ und ziehen Sie die Maus, um die Karte zu drehen.
6. Klicken Sie auf + und ziehen Sie die Maus, um die Karte zu bewegen.
7. Verwenden Sie die Ziehpunkte, um die Größe Ihrer Karte anzupassen.
8. Klicken Sie auf ×, um die Karte zu entfernen.

Hinweis: Wenn Sie mehrere Etagen hinzufügen möchten, wird die erste Karte, die Sie hinzufügen, das Erdgeschoss sein. Das Erdgeschoss wird durch die Zahl 0 im Feld

angezeigt.

Das Erdgeschoss um weitere Stockwerke zu erweitern:

1. Klicken Sie im Feld

auf die Zahl 0.

   Das Feld öffnet sich.
2. Wählen Sie die Etage aus, zu der Sie eine Karte hinzufügen möchten.
3. **Hinweis:** Sie können nur die nächsthöhere oder -tiefere Etage auswählen, um eine Karte hinzuzufügen.
4. Klicken Sie auf .
   Das Fenster **Ressource auswählen** wird geöffnet.
5. Wählen Sie eine Karte aus und klicken Sie auf **OK**.
6. Ändern Sie die hinzugefügte Bodenkarte, um die Position an die Position der Erdgeschosskarte anzupassen.

Um eine Etage auf allen Etagen sichtbar zu machen:

1. Klicken Sie mit der rechten Maustaste auf eines der Anpassungssymbole der jeweiligen Etagenkarte, ↻, + oder ×.
2. Wählen Sie **Sichtbar auf allen Ebenen**.
   Diese Etage ist jetzt immer sichtbar, wenn Sie eine andere Etage auswählen.

Hinweis: Wenn Sie keinen Zugang zum Internet haben und den Typ Offline-Hintergrundkarte **Kein Eintrag** gewählt haben, können Sie eine Karte als Hintergrundkarte hinzufügen. Wir empfehlen, diese Hintergrundkarte auf allen Etagen sichtbar zu machen. Die Hintergrundkarte wird dann immer sichtbar sein, wenn Sie eine andere Etage auswählen.

So legen Sie die Geolokalisierung einer Karte fest

1. Klicken Sie mit der rechten Maustaste auf eines der Einstellungssymbole des jeweiligen Etagenplans, ↻, +, × oder auf einen der Ziehpunkte auf der Karte und wählen Sie dann **Standort festlegen**.
   Die**Standort festlegen** Dialogfeld wird angezeigt.
   Hinweis: Für eine bessere Sichtbarkeit können Sie das Dialogfeld maximieren, indem Sie auf die Schaltfläche Maximieren in der oberen rechten Ecke klicken.
2. Ziehen Sie die Markierungen A und B zu den gewünschten Positionen auf der Karte.
3. Geben Sie den genauen Breiten- und Längengrad für jeden Marker in die vorgesehenen Felder ein und klicken Sie dann auf **OK**.
   Hinweis: Anstatt die Werte für Breiten- und Längengrad einzugeben, können Sie sie auch aus einer externen Quelle kopieren. Wenn Sie in diesem Fall die Werte in das Feld Breitengrad einfügen, wird das Feld Längengrad automatisch ausgefüllt.

18.16 Hinzufügen eines Karten-Anzeigebereichs

Hauptfenster > **Karten und Struktur** > Registerkarte **Logischer Baum**

So fügen Sie einen Karten-Anzeigebereich **hinzu:**

1. Klicken Sie auf , um einen Karten-Anzeigebereich hinzuzufügen.
2. Geben Sie den Namen Ihres Karten-Anzeigebereichs ein.
3. Geben Sie im Suchfeld der globalen Karte eine Adresse oder einen Standort ein, um zur Position zu wechseln, an der Sie Ihren Karten-Anzeigebereich erstellen möchten.

   Wenn Sie die Adresse oder den Standort nicht kennen, können Sie mit den Schaltflächen + und — oder dem Mausrad heran- oder herauszoomen.
4. Klicken Sie auf , um Ihre Konfiguration zu speichern.

Hinweis!
Wenn ein Kartenfenster verschiedene Stockwerke enthält, ist das Stockwerk, das beim Speichern der Konfiguration ausgewählt wurde, dasjenige, das im Fenster Operator Client angezeigt wird, wenn der Bediener das Kartenfenster öffnet. Der Operator kann den Boden des Kartenfensters im Bildfenster nachträglich ändern.

18.17 Aktivierung des Map-based Tracking Assistant

Der Map-based tracking assistant unterstützt Sie dabei, sich bewegende Objekte über mehrere Kameras hinweg zu verfolgen. Die entsprechenden Kameras müssen auf der globalen Karte konfiguriert werden. Wenn Benutzer ein sich bewegendes Objekt in einem Live-Video, in der Wiedergabe oder in einem Alarmfenster sehen, können Sie den Map-based tracking assistant starten, der automatisch alle Kameras in der Nähe des Objekts anzeigt.

So aktivieren Sie den Map-based tracking assistant:

1. Gehen Sie zum Hauptfenster und navigieren Sie zu Menü **Einstellungen** > Befehl **Optionen...**.
2. Aktivieren Sie das Kontrollkästchen **Systemfunktion aktivieren**.
3. Klicken Sie auf **OK**.

18.18 Ein Störungsrelais hinzufügen

Hauptfenster > **Karten und Struktur** > Registerkarte **Logischer Baum** > > Dialogfeld **Störungsrelais**

Vorgesehene Verwendung

Ein Störungsrelais dient dazu, im Falle eines schwerwiegenden Systemfehlers einen externen Alarm (Blitzlicht, Sirene usw.) auszulösen.

Der Benutzer muss das Relais manuell zurücksetzen.

Dabei kann es sich um eines der folgenden Störungsrelais handeln:

- BVIP-Encoder- oder -Decoder-Relais
- ADAM-Relais
- Ausgabe der Einbruchmeldezentrale

Beispiel

Tritt ein Ereignis ein, das schwerwiegende Auswirkungen auf den Systembetrieb hat (bspw. ein Festplattenausfall) oder die Sicherheit eines Standorts bedroht (bspw. eine fehlgeschlagene Referenzbildprüfung), wird das Störungsrelais aktiviert. Dies kann bspw. einen akustischen Alarm auslösen oder die Türen automatisch verschließen.

Funktionsbeschreibung

Sie können ein einzelnes Relais so konfigurieren, dass es als Störungsrelais fungiert. Das Störungsrelais wird automatisch aktiviert, sobald ein Ereignis aus einer Reihe benutzerdefinierter Ereignisse ausgelöst wird. Die Aktivierung eines Relais bedeutet, dass ein Schließbefehl an das Relais gesendet wird. Das anschließend als „Relais geschlossen“ bezeichnete Ereignis wird vom Befehl getrennt und nur erzeugt bzw. empfangen, wenn der Status des Relais physisch geändert wird! Bspw. wird dieses Ereignis nicht bei einem zuvor geschlossenen Relais gesendet.

Abgesehen von der automatischen Auslösung durch eine Reihe benutzerdefinierter Ereignisse wird das Störungsrelais wie jedes andere Relais behandelt. Daher ist der Benutzer in der Lage, das Störungsrelais im Operator Client zu deaktivieren. Auch der Web Client ermöglicht die Deaktivierung des Störungsrelais. Da die regulären Zugriffsberechtigungen auch für das Störungsrelais gelten, müssen alle Clients die Berechtigungen des angemeldeten Benutzers berücksichtigen.

So führen Sie das Hinzufügen aus:

1. Wählen Sie aus der Liste **Störungsrelais** das gewünschte Relais aus.
2. Klicken Sie auf **Ereignisse...**
   Das Dialogfeld **Ereignisauswahl für Störungsrelais** wird angezeigt.
3. Wählen Sie die gewünschten Ereignisse, die das Störungsrelais auslösen können, durch Anklicken aus.
4. Klicken Sie auf **OK**.
   Das Störungsrelais wird dem System hinzugefügt.

18.18.1 Dialogfeld „Störungsrelais“

Hauptfenster > **Karten und Struktur** > Registerkarte **Logischer Baum** > > Dialogfeld **Störungsrelais**

Sie können Ihrem System ein Störungsrelais hinzufügen. Sie definieren das als Störungsrelais zu verwendende Relais und konfigurieren die Ereignisse, die das Störungsrelais auslösen können.

Das Relais muss bereits im Logischen Baum konfiguriert sein.

Störungsrelais

Wählen Sie das gewünschte Relais aus der Liste aus.

Ereignisse...
Klicken Sie hier, um das Dialogfeld **Ereignisauswahl für Störungsrelais** anzuzeigen.

18.19 Konfigurieren der Geräteumgehung

Hauptfenster > **Karten und Struktur** > Registerkarte **Logischer Baum**
Es ist möglich, bestimmte Encoder, Kameras, Eingänge und Relais zu umgehen, z. B. bei Bauarbeiten. Wenn ein Encoder, eine Kamera, ein Eingang oder ein Relais umgangen wird, wird die Aufzeichnung gestoppt, der BVMS Operator Client zeigt keine Ereignisse oder Alarme an und Alarme werden nicht im Logbuch aufgezeichnet.
Die umgangenen Kameras zeigen weiterhin Live-Videos im Operator Client an und der Bediener hat weiterhin Zugriff auf ältere Aufzeichnungen.

Hinweis!
Wenn der Encoder umgangen wird, werden für alle Kameras, Relais und Eingänge dieses Encoders keine Alarme und Ereignisse mehr ausgelöst. Wenn eine bestimmte Kamera, ein bestimmtes Relais oder ein bestimmter Eingang separat umgangen wird und das bestimmte Gerät vom Encoder getrennt wird, werden diese Alarme weiterhin ausgelöst.

So umgehen Sie ein Gerät im Logischen Baum oder Gerätebaum bzw. heben die Umgehung auf:
1. Klicken Sie im Logischen Baum oder Gerätebaum mit der rechten Maustaste auf ein bestimmtes Gerät.
2. Klicken Sie auf **Umgehen/Umgehung aufheben**.

So umgehen Sie ein Gerät auf einer Karte bzw. heben die Umgehung auf:
Siehe *Verwalten von Geräten auf einem Lageplan, Seite 273*

Hinweis!
Es ist möglich, umgangene Geräte über das Suchfeld zu filtern.

Siehe
– *Verwalten von Geräten auf einem Lageplan, Seite 273*

19 Seite Zeitpläne

Hauptfenster > **Zeitpläne**
Dient zum Konfigurieren von Aufzeichnungszeitplänen und Aktionszeitplänen.

Klicken Sie hier, um den ausgewählten Aufzeichnungs- oder Aktionszeitplan umzubenennen.

Aufzeichnungszeitpläne
Zeigt den Baum Aufzeichnungszeitpläne an. Wählen Sie einen Eintrag für die Konfiguration aus.

Aktionszeitpläne
Zeigt den Baum Aktionszeitpläne an. Wählen Sie einen Eintrag für die Konfiguration aus.

Hinzufügen
Klicken Sie darauf, um einen neuen Aktionszeitplan hinzuzufügen.

Löschen
Klicken Sie darauf, um den ausgewählten Aktionszeitplan zu löschen.

Siehe
– *Konfigurieren von Zeitplänen, Seite 284*

19.1 Seite Aufzeichnungszeitpläne

Hauptfenster > > Eintrag im Baum Aufzeichnungszeitpläne auswählen
Dient zum Konfigurieren von Aufzeichnungszeitplänen.

Wochentage
Klicken Sie darauf, um die Zeitplantabelle für Wochentage anzuzeigen. Die Zeitbereiche aller konfigurierten Aufzeichnungszeitpläne werden angezeigt.
Ziehen Sie den Mauszeiger, um die Zeitbereiche für den ausgewählten Zeitplan auszuwählen. Alle ausgewählten Zellen werden in der gleichen Farbe wie der ausgewählte Zeitplan dargestellt.
Die 24 Stunden eines Tages werden horizontal angezeigt. Jede Stunde ist in 4 Zellen unterteilt. Eine Zelle stellt 15 Minuten dar.

Feiertage
Klicken Sie darauf, um die Zeitplantabelle für Feiertage anzuzeigen.

Besondere Tage
Klicken Sie darauf, um die Zeitplantabelle für besondere Tage anzuzeigen.

Hinzufügen
Klicken Sie darauf, um ein Dialogfeld zum Hinzufügen der erforderlichen Feiertage oder besonderen Tage anzuzeigen.

Löschen
Klicken Sie darauf, um ein Dialogfeld zum Entfernen von Feiertagen oder besonderen Tagen anzuzeigen.

Siehe
– *Konfigurieren eines Aufzeichnungszeitplans, Seite 284*
– *Hinzufügen von Feiertagen und besonderen Tagen, Seite 286*
– *Entfernen von Feiertagen und besonderen Tagen, Seite 287*
– *Umbenennen eines Zeitplans, Seite 287*

19.2 Seite Aktionszeitpläne

Hauptfenster > > Eintrag im Baum Aktionszeitpläne auswählen

Dient zum Konfigurieren verfügbarer Aktionszeitpläne. Sie können ein Standardmuster und ein wiederkehrendes Muster konfigurieren.

Standard
Klicken Sie darauf, um die Zeitplantabelle anzuzeigen und Standard-Aktionszeitpläne zu konfigurieren. Bei Konfiguration eines Standardmusters gilt für den ausgewählten Zeitplan kein wiederkehrendes Muster.

Wiederkehrend
Klicken Sie darauf, um die Zeitplantabelle anzuzeigen und ein wiederkehrendes Muster für den ausgewählten Aktionszeitplan zu konfigurieren. Beispiel: Sie können einen Zeitplan für jeden zweiten Dienstag eines Monats oder für den 4. Juli eines Jahres konfigurieren. Bei Konfiguration eines wiederkehrenden Musters gilt für den ausgewählten Aktionszeitplan kein Standardmuster.

Wochentage
Klicken Sie darauf, um die Zeitplantabelle für Wochentage anzuzeigen.
Ziehen Sie den Mauszeiger, um die Zeitbereiche für den ausgewählten Zeitplan auszuwählen. Die ausgewählten Zellen werden in der gleichen Farbe wie der ausgewählte Zeitplan dargestellt.
Die 24 Stunden eines Tages werden horizontal angezeigt. Jede Stunde ist in 4 Zellen unterteilt. Eine Zelle stellt 15 Minuten dar.

Feiertage
Klicken Sie darauf, um die Zeitplantabelle für Feiertage anzuzeigen.

Besondere Tage
Klicken Sie darauf, um die Zeitplantabelle für besondere Tage anzuzeigen.

Alle löschen
Klicken Sie darauf, um die Auswahl der Zeitbereiche aller verfügbaren Tage (Wochentage, Feiertage, besondere Tage) aufzuheben.

Alles auswählen
Klicken Sie darauf, um die Zeitbereiche aller verfügbaren Tage (Wochentage, Feiertage, besondere Tage) auszuwählen.

Hinzufügen...
Klicken Sie darauf, um ein Dialogfeld zum Hinzufügen der erforderlichen Feiertage oder besonderen Tage anzuzeigen.

Löschen...
Klicken Sie darauf, um ein Dialogfeld zum Löschen von Feiertagen oder besonderen Tagen anzuzeigen.

Wiederkehrendes Muster
Wählen Sie aus, wie häufig der Aktionszeitplan wiederholt werden soll (Täglich, Wöchentlich, Monatlich, Jährlich), und aktivieren Sie anschließend die entsprechenden Optionen.

Tagesmuster
Ziehen Sie den Mauszeiger, um die Zeitbereiche für das wiederkehrende Muster auszuwählen.

Siehe
- *Hinzufügen eines Aktionszeitplans, Seite 285*
- *Konfigurieren eines Standard-Aktionszeitplans, Seite 285*
- *Konfigurieren eines wiederkehrenden Aktionszeitplans, Seite 285*
- *Entfernen eines Aktionszeitplans, Seite 286*
- *Hinzufügen von Feiertagen und besonderen Tagen, Seite 286*
- *Entfernen von Feiertagen und besonderen Tagen, Seite 287*
- *Umbenennen eines Zeitplans, Seite 287*

20 Konfigurieren von Zeitplänen

Hauptfenster > **Zeitpläne**

Zwei Zeitplantypen sind verfügbar:

- Aufzeichnungszeitpläne
- Aktionszeitpläne

Sie können maximal 10 verschiedene Aufzeichnungszeitpläne in der Aufzeichnungszeitplan-Tabelle konfigurieren. In diesen Abschnitten können sich die Kameras unterschiedlich verhalten. Beispielsweise können sie verschiedene Bildraten und Auflösungseinstellungen haben (Konfiguration auf der Seite **Kameras und Aufzeichnung**). Zu jedem Zeitpunkt ist genau ein Aufzeichnungszeitplan gültig. Es gibt weder Lücken noch Überschneidungen.

Aktionszeitpläne werden zur Planung verschiedener Ereignisse konfiguriert, die in Ihrem System auftreten können (Konfiguration auf der Seite **Ereignisse**).

Definitionen zu Aufzeichnungszeitplänen und Aktionszeitplänen finden Sie im Glossar.

Die Zeitpläne werden auf anderen Seiten des Configuration Client verwendet:

- Seite **Kameras und Aufzeichnung**
  Zum Konfigurieren von Aufzeichnungen.
- Seite **Ereignisse**
  Zum Festlegen, wann Ereignisse Protokollierung, Alarme oder die Ausführung von Kommandoskripten auslösen sollen.
- Seite **Benutzergruppen**
  Zum Festlegen, wann sich die Mitglieder einer Benutzergruppe anmelden können.

- Klicken Sie auf , um die Einstellungen zu speichern.
- Klicken Sie auf , um die letzte Einstellung rückgängig zu machen.
- Klicken Sie auf , um die Konfiguration zu aktivieren.

Siehe

- *Seite Aufzeichnungszeitpläne, Seite 282*
- *Seite Aktionszeitpläne, Seite 282*

20.1 Konfigurieren eines Aufzeichnungszeitplans

Hauptfenster > **Zeitpläne**

Sie können jedem Aufzeichnungszeitplan besondere Tage und Feiertage hinzufügen. Diese Einstellungen setzen die normalen wöchentlichen Einstellungen außer Kraft.

Die Reihenfolge bei abnehmender Priorität lautet: besondere Tage, Feiertage, Wochentage.

Die maximale Anzahl der Aufzeichnungspläne ist 10. Die ersten drei Einträge werden standardmäßig konfiguriert. Sie können diese Einstellungen ändern. Bei Einträgen mit dem grauen Symbol ist kein Zeitbereich konfiguriert.

Aufzeichnungszeitpläne haben dieselben Wochentage.

Jeder Standard-Aktionszeitplan verfügt über eigene Wochentagsanordnungen.

So konfigurieren Sie einen Aufzeichnungszeitplan:

1. Wählen Sie im Baum **Aufzeichnungszeitpläne** einen Zeitplan aus.
2. Klicken Sie auf die Registerkarte **Wochentage**.

3. Ziehen Sie im Feld **Zeitplantabelle** den Mauszeiger, um die Zeitbereiche für den ausgewählten Zeitplan auszuwählen. Die ausgewählten Zellen werden in der gleichen Farbe wie der ausgewählte Zeitplan dargestellt.

Hinweise:

– Sie können einen Zeitbereich für den Wochentag eines Aufzeichnungszeitplans mit der Farbe eines anderen Aufzeichnungszeitplans markieren.

Siehe

– *Seite Aufzeichnungszeitpläne, Seite 282*

20.2 Hinzufügen eines Aktionszeitplans

Hauptfenster > **Zeitpläne**

So fügen Sie einen Aktionszeitplan hinzu:

1. Klicken Sie auf **Hinzufügen**.
   Ein neuer Eintrag wird hinzugefügt.
2. Geben Sie einen Namen ein.
3. Klicken Sie auf **Standard**, um einen Standard-Aktionszeitplan hinzuzufügen, oder auf **Wiederkehrend**, um einen wiederkehrenden Aktionszeitplan hinzuzufügen.
   Wenn Sie eine Einstellung ändern, wird ein Meldungsfeld angezeigt. Klicken Sie auf **OK**, wenn Sie den Zeitplantyp ändern möchten.
   Ein Standard-Aktionszeitplan mit dem Symbol gekennzeichnet und ein wiederkehrender Aktionszeitplan mit dem Symbol .
4. Nehmen Sie die erforderlichen Einstellungen für den ausgewählten Zeitplan vor.

Siehe

– *Seite Aktionszeitpläne, Seite 282*

20.3 Konfigurieren eines Standard-Aktionszeitplans

Hauptfenster > **Zeitpläne**

Jeder Standard-Aktionszeitplan verfügt über eigene Wochentagsanordnungen.

So konfigurieren Sie einen Standard-Aktionszeitplan:

1. Wählen Sie in der Struktur **Aktionszeitpläne** einen Standard-Aktionszeitplan aus.
2. Klicken Sie auf die Registerkarte **Wochentage**.
3. Ziehen Sie im Feld **Zeitplantabelle** den Mauszeiger, um die Zeitbereiche für den ausgewählten Zeitplan auszuwählen.

Siehe

– *Seite Aktionszeitpläne, Seite 282*

20.4 Konfigurieren eines wiederkehrenden Aktionszeitplans

Hauptfenster > **Zeitpläne**

Jeder Standard-Aktionszeitplan verfügt über eigene Wochentagsanordnungen.

So konfigurieren Sie einen wiederkehrenden Aktionszeitplan:

1. Wählen Sie im Baum **Aktionszeitpläne** einen wiederkehrenden Aktionszeitplan aus.

2. Wählen Sie im Feld **Wiederkehrendes Muster** aus, wie häufig der Aktionszeitplan wiederholt werden soll (**Täglich**, **Wöchentlich**, **Monatlich**, **Jährlich**), und nehmen Sie anschließend die entsprechenden Einstellungen vor.
3. Wählen Sie in der Liste **Startdatum:** das gewünschte Startdatum aus.
4. Ziehen Sie im Feld **Tagesmuster** den Mauszeiger, um den gewünschten Zeitbereich auszuwählen.

Siehe

– *Seite Aktionszeitpläne, Seite 282*

20.5 Entfernen eines Aktionszeitplans

Hauptfenster > > Eintrag im Baum **Aktionszeitpläne** auswählen

So entfernen Sie einen Aktionszeitplan:

1. Wählen Sie im Baum **Aktionszeitpläne** einen Eintrag aus.
2. Klicken Sie auf **Löschen**.
   Der Aktionszeitplan wird gelöscht. Für die Einträge, die diesem Zeitplan zugeordnet sind, erfolgt keine Planung mehr.

Siehe

– *Seite Aktionszeitpläne, Seite 282*

20.6 Hinzufügen von Feiertagen und besonderen Tagen

Hauptfenster > **Zeitpläne**

Hinweis!
Sie können leere besondere Tage und Feiertage konfigurieren. Besondere Tage und Feiertage ersetzen den Zeitplan des entsprechenden Wochentags.
Beispiel:
Alte Konfiguration:
Konfigurierter Wochentagszeitplan ist aktiv von 9:00 bis 10:00 Uhr.
Konfigurierter Zeitplan für besondere Tage ist aktiv von 10:00 bis 11:00 Uhr.
Ergebnis: Aktivität von 10:00 bis 11:00 Uhr.
Das gleiche Verhalten gilt für Feiertage.

Sie können einem Aufzeichnungszeitplan oder einem Aktionszeitplan Feiertage und besondere Tage hinzufügen.
Aufzeichnungszeitpläne haben dieselben Feiertage und besonderen Tage.
Jeder Standard-Aktionszeitplan verfügt über eigene Anordnungen für Feiertage und besondere Tage.

So fügen Sie einem Zeitplan Feiertage und besondere Tage hinzu:

1. Wählen Sie im Baum **Aufzeichnungszeitpläne** oder **Aktionszeitpläne** einen Zeitplan aus.
2. Klicken Sie auf die Registerkarte **Feiertage**.
3. Klicken Sie auf **Hinzufügen**.
   Das Dialogfeld **Feiertag(e) hinzufügen** wird angezeigt.
4. Wählen Sie einen oder mehrere Feiertage aus, und klicken Sie auf **OK**.
   Die ausgewählten Feiertage werden der Zeitplantabelle hinzugefügt.
5. Ziehen Sie den Mauszeiger, um den gewünschten Zeitbereich auszuwählen. (Für Aufzeichnungszeitpläne ist dies nicht möglich.)
   Die Auswahl von ausgewählten Zellen wird aufgehoben, nicht ausgewählte Zellen werden ausgewählt.

6. Klicken Sie auf die Registerkarte **Besondere Tage**.
7. Klicken Sie auf **Hinzufügen**.
   Das Dialogfeld **Besondere Tage hinzufügen** wird angezeigt.
8. Wählen Sie einen oder mehrere besondere Tage aus, und klicken Sie auf **OK**.
   Die ausgewählten besonderen Tage werden der Zeitplantabelle hinzugefügt.
9. Ziehen Sie den Mauszeiger, um den gewünschten Zeitbereich auszuwählen. (Für Aufzeichnungszeitpläne ist dies nicht möglich.)
   Die Auswahl ausgewählter Zellen wird aufgehoben, nicht ausgewählte Zellen werden ausgewählt.
   Die hinzugefügten Feiertage und besonderen Tage werden chronologisch sortiert.

Hinweise:

– Sie können einen Zeitbereich für den Feiertag oder besonderen Tag eines Aufzeichnungszeitplans mit der Farbe eines anderen Aufzeichnungszeitplans markieren.

Siehe

– *Seite Aufzeichnungszeitpläne, Seite 282*
– *Seite Aktionszeitpläne, Seite 282*

20.7 Entfernen von Feiertagen und besonderen Tagen

Hauptfenster > **Zeitpläne**

Sie können Feiertage und besondere Tage aus einem Aufzeichnungszeitplan oder einem Aktionszeitplan entfernen.

So entfernen Sie Feiertage und besondere Tage aus einem Aktionszeitplan:

1. Wählen Sie im Baum **Aufzeichnungszeitpläne** oder **Aktionszeitpläne** einen Zeitplan aus.
2. Klicken Sie auf die Registerkarte **Feiertage**.
3. Klicken Sie auf **Löschen**.
   Das Dialogfeld **Wählen Sie Feiertage zum Löschen.** wird angezeigt.
4. Wählen Sie einen oder mehrere Feiertage aus, und klicken Sie auf **OK**.
   Die ausgewählten Feiertage werden aus der Zeitplantabelle entfernt.
5. Klicken Sie auf die Registerkarte **Besondere Tage**.
6. Klicken Sie auf **Löschen**.
   Das Dialogfeld **Wählen Sie besonderen Tage zum Löschen.** wird angezeigt.
7. Wählen Sie einen oder mehrere besondere Tage aus, und klicken Sie auf **OK**.
   Die ausgewählten besonderen Tage werden aus der Zeitplantabelle entfernt.

Siehe

– *Seite Aufzeichnungszeitpläne, Seite 282*
– *Seite Aktionszeitpläne, Seite 282*

20.8 Umbenennen eines Zeitplans

Hauptfenster >

So benennen Sie einen Zeitplan um:

1. Wählen Sie im Baum **Aufzeichnungszeitpläne** oder **Aktionszeitpläne** einen Eintrag aus.
2. Klicken Sie auf .
3. Geben Sie den neuen Namen ein, und drücken Sie die Eingabetaste. Der Eintrag wird umbenannt.

Siehe

- *Seite Aufzeichnungszeitpläne, Seite 282*
- *Seite Aktionszeitpläne, Seite 282*

21 Seite Kameras und Aufzeichnung

Hinweis!
BVMS Viewer bietet nur Grundfunktionen. Erweiterte Funktionen sind in BVMS Professional enthalten. Ausführliche Informationen zu den verschiedenen Versionen von BVMS finden Sie unter www.boschsecurity.com und in der BVMS Schnellauswahlhilfe: BVMS Schnellauswahlhilfe.

Hauptfenster > **Kameras und Aufzeichnung**
Zeigt die Seite „Kameratabelle“ oder die Seite „Aufzeichnungstabelle“ an.
Dient zum Konfigurieren von Kameraeigenschaften und Aufzeichnungseinstellungen.
Dient zum Filtern der angezeigten Kameras nach Typ.

Symbole

	Klicken Sie hier, um Aufzeichnungseinstellungen von einem Aufzeichnungszeitplan in einen anderen zu kopieren.
	Klicken Sie hier, um das Dialogfeld **Stream-Qualitätseinstellungen** anzuzeigen.
	Klicken Sie hier, um das Dialogfeld **Geplante Aufzeichnungseinstellungen** anzuzeigen.
	Klicken Sie hier, um das Dialogfeld zum Konfigurieren einer ausgewählten PTZ-Kamera anzuzeigen.
	Zeigt alle verfügbaren Kameras unabhängig von ihrem Archivierungsgerät an.
	Klicken Sie hier, um die Kameratabelle gemäß dem ausgewählten Speichergerät zu ändern.
	Zeigt die entsprechende Kameratabelle an. Es sind keine Aufzeichnungseinstellungen verfügbar, da diese Kameras nicht im BVMS aufgezeichnet werden.
	Klicken Sie, um die Spalten auszuwählen, die in der **Kameras** Tabelle angezeigt werden sollen.

Um nach Elementen zu suchen:

- Tippen Sie im Suchfeld eine Zeichenfolge ein und drücken Sie auf den Schlüssel ENTER, um die angezeigten Elemente zu filtern.
  Nur Elemente mit der Zeichenfolge und ihre übergeordneten Elemente (nur in Bäumen) werden angezeigt. Die Anzahl der gefilterten Elemente und die gesamte Anzahl der Elemente wird angegeben.

Hinweis: Setzen Sie Zeichenfolgen zwischen doppelte Anführungszeichen, um genaue Treffer zu erhalten. Beispielsweise filtert "Camera 1" genau die Kameras mit diesem Namen, jedoch nicht camera 201.

21.1 Seite Kameras

Hauptfenster > **Kameras und Aufzeichnung** > Klicken Sie auf ein Symbol, um die Seite Kameras entsprechend dem gewünschten Speichergerät zu ändern, zum Beispiel

Zeigt verschiedene Informationen zu den Kameras an, die im BVMS zur Verfügung stehen.

Dient zum Ändern der folgenden Kameraeigenschaften:

- Kameraname
- Zuordnung einer Audioquelle
- Logische Nummer
- PTZ-Steuerung, sofern verfügbar
- Livequalität (VRM und Live-/Lokale Archivierung)
- Profil der Aufzeichnungseinstellungen
- Minimale und maximale Aufzeichnungsdauer
- Region of Interest (RoI)
- Automated Network Replenishment
- Duale Aufzeichnung

So passen Sie die Kameras Tabelle an:

1. Klicken Sie auf , um die Spalten auszuwählen, die in der **Kameras** Tabelle angezeigt werden sollen.
2. Klicken Sie auf eine Spaltenüberschrift, um die Tabelle nach dieser Spalte zu sortieren.

Kamera - Encoder

Zeigt den Gerätetyp an.

Kamera - Kamera

Zeigt den Namen der Kamera an.

Kamera - Netzwerkadresse

Zeigt die IP-Adresse der Kamera an.

Kamera - Ort

Zeigt den Ort der Kamera an. Wenn die Kamera noch keinem Logischen Baum zugeordnet wurde, wird **Nicht-zugeordneter Ort** angezeigt.

Kamera - Gerätefamilie

Zeigt den Namen der Gerätefamilie an, zu der die ausgewählte Kamera gehört.

Kamera - Nummer

Klicken Sie auf eine Zelle, um die logische Nummer zu bearbeiten, die die Kamera bei der Erkennung automatisch erhalten hat. Wenn Sie eine bereits vergebene Nummer eingeben, wird eine entsprechende Fehlermeldung angezeigt.

Die logische Nummer ist wieder „frei“, wenn die Kamera entfernt wird.

Audio

Klicken Sie auf eine Zelle, um der Kamera eine Audioquelle zuzuweisen.

Wenn ein Alarm mit niedriger Priorität auftritt und bei der entsprechenden Kamera Audio konfiguriert ist, wird dieses Audiosignal wiedergegeben, selbst wenn gleichzeitig ein Alarm mit höherer Priorität angezeigt wird. Dies gilt jedoch nur, wenn für den Alarm mit hoher Priorität kein Audio konfiguriert ist.

Audioverknüpfung zwischen Kameras

Durch die Audio-Verknüpfung kann ein Konfigurator jeder Kamera den Audioeingang und -ausgang einer anderen Kamera zuweisen.

Diese Funktion ist beispielsweise vorteilhaft für Szenarien, in denen einer Kamera ohne Mikrofon und Lautsprecher der Audioeingang und -ausgang einer anderen Kamera zugewiesen werden kann. Dadurch können Bediener mit Personen in der Nähe einer der zwei Kameras kommunizieren, während sie den Live-Stream einer beliebigen Kamera ansehen.
Die Optionen für die geräteübergreifende Verknüpfung von Audio werden in der folgenden Reihenfolge angezeigt:

1. **<Kein Audio>**
2. Audio des ausgewählten Geräts
3. Audio von Geräten, die sich an der gleichen Stelle in der Gerätestruktur befinden
4. Audio von allen anderen verfügbaren Geräten

Streams / Stream Grenzwerte
Diese Spalte ist schreibgeschützt und zeigt die Streamgrenzen der jeweiligen Kamera an.
Hinweis: Die Stream-Grenzwerte werden nur für CPP13-, CPP14- und CPP16-Kameras angezeigt.

Hinweis!
Sie können die Streamgrenzen nicht in BVMS bearbeiten. Sie können sie auf der Website des Encoders oder in dem Configuration Manager bearbeiten. Nachdem Sie die Streamgrenzen auf der Website oder in dem Configuration Manager geändert haben, müssen Sie die Gerätefunktionen in BVMS aktualisieren. Wenn Sie die Gerätefunktionen nicht aktualisieren, überschreibt BVMS die aktualisierten Stream-Grenzwerte mit den alten Einstellungen, die angezeigt wurden, als Sie die Gerätefunktionen das letzte Mal aktualisiert haben.

Stream 1 / Stream 2 / Stream 3 Einstellungen

Hinweis!
Nur CPP13-, CPP14- und CPP16-Kameras unterstützen einen dritten Stream.

Hinweis!
Sie können Stream 3 nur für die Live-Anzeige verwenden. Eine Aufzeichnung ist nicht möglich.

Stream 1 - Codec / Stream 2 - Codec / Stream 3 - Codec (nur verfügbar für VRM, Nur Live-Kameras und Kameras mit lokaler Speicherung)
Klicken Sie auf eine Zelle, um die gewünschte Videoauflösung auszuwählen.
Die Werte für die Videoauflösung werden vom Encoder geladen. Die Anzeige dieser Werte kann eine Weile dauern.
Hinweis: Diese Spalte wird nur angezeigt, wenn Sie mindestens eine Kamera konfiguriert haben, die einen dritten Stream unterstützt.

Stream 1 - Qualität / Stream 2 - Qualität / Stream 3 - Qualität (nur verfügbar für VRM, Nur Live-Kameras und Kameras mit lokaler Speicherung)
Wählen Sie die gewünschte Streamqualität für die Live-Anzeige oder Aufzeichnung aus. Sie konfigurieren die Qualitätseinstellungen in der **Stream-Qualitätseinstellungen** Dialogfeld.
Hinweis: Diese Spalte wird nur angezeigt, wenn Sie mindestens eine Kamera konfiguriert haben, die einen dritten Stream unterstützt.

Stream 1 - Aktive Plattform / Stream 2 - Aktive Plattform / Stream 3 - Aktive Plattform (nur verfügbar für VRM, Nur Live-Kameras und Kameras mit lokaler Speicherung)
Zeigt den Namen der Plattformeinstellungen im Dialogfeld **Stream-Qualitätseinstellungen** an. Only live cameras and cameras with local storage)
Note: Diese Spalte wird nur angezeigt, wenn Sie mindestens eine Kamera konfiguriert haben, die einen dritten Stream unterstützt.

Stream 1/Profil, Stream 2/Profil (nur verfügbar für ONVIF cameras)
Klicken Sie auf eine Zelle, um nach den verfügbaren Profil-Token für diese Zelle zu suchen ONVIF Kamera.
Wenn Sie den Eintrag **<Automatisch>** auswählen, wird automatisch der Stream mit der höchsten Qualität verwendet.
Hinweis: Wenn Sie eine ältere VSG Version, die keine zwei Streams unterstützt, dann wird automatisch die Option **<Stream 1 verwenden>** ist eingestellt für **Stream 2/Profil**.
Stellen Sie sicher, dass Sie die neuesteVSGVersion.

Stream 1/Bildauflösung, Stream 2/Bildauflösung (nur verfügbar fürONVIF Kameras)
Diese Spalte ist schreibgeschützt und gibt die Bildauflösung des ausgewählten Stream-Profils an.

Live Video - Stream (nur verfügbar für VRM,Nur Live-Kameras und Kameras mit lokaler Speicherung)
Klicken Sie auf eine Zelle, um den Stream für eineVRM , oder ein lokaler Speicher, oder ein reiner Live-Speicher Geber.

Live Video - ROI (nur verfügbar für VRM, Nur Live-Kameras und Kameras mit lokaler Speicherung)
Klicken Sie hier, um Region of Interest (ROI) zu aktivieren. Dies ist nur möglich, wenn in der Spalte **Qualität** das Element H.264 MP SD ROI oder H.265 MP SD ROI für Stream 2 ausgewählt ist und Stream 2 dem Live-Video zugeordnet wurde.
Hinweis: Wenn Stream 1 für eine bestimmte Arbeitsstation im Live-Modus verwendet wird, kann der auf dieser Arbeitsstation ausgeführte Operator Client nicht die ROI-Funktion für diese Kamera aktivieren.

wird in der Tabelle automatisch aktiviert.

Live Video - Live-Stream (nur verfügbar für Kameras, die über eine VSG)
Klicken Sie auf eine Zelle, um den gewünschten Live-Stream für die jeweilige Kamera auszuwählen.
Für ONVIF Kameras sind die folgenden Optionen verfügbar:
- **Direkt (von der Kamera)**
- **Stream 1 (über VSG)**
- **Stream 2 (über VSG)**

Für Bosch Kameras sind die folgenden Optionen verfügbar:
- **Stream 1**
- **Stream 2**

Hinweis: Wenn Sie eine Video Streaming Gateway Gerät zum Abrufen des Live-Videos an einem Arbeitsplatz, wird das Live-Video nur abgerufen, wenn Sie die Option **Direkt (von der Kamera)** für den Live-Stream.

Live Video - Profil (nur verfügbar für ONVIF Kameras, die über ein VSG)
Klicken Sie auf eine Zelle, um nach den verfügbaren Live-Profil-Token dieser Zelle zu suchen ONVIF Kamera.
Hinweis: Sie können nur dann ein Live-Video-Profil auswählen, wenn Sie die Option **Direkt (von der Kamera)** für den Live-Stream. Wenn Sie wählen **Stream 1 (über VSG)** or **Stream 2 (über VSG)** für den Live-Stream, dann wird das Live-Videoprofil automatisch auf **<Automatisch>**.

Aufzeichnung - Einstellung
Klicken Sie auf eine Zelle, um die erforderliche Aufzeichnungseinstellung auszuwählen. Sie konfigurieren die verfügbaren Aufzeichnungseinstellungen im Dialogfeld **Geplante Aufzeichnungseinstellungen**.

Aufzeichnung - ANR
Aktivieren Sie ein Kontrollkästchen, um die Funktion ANR zu aktivieren. Sie können diese Funktion nur aktivieren, wenn der Encoder über eine entsprechende Firmware-Version sowie über einen entsprechenden Gerätetyp verfügt.

Aufzeichnung - Max. Voralarmdauer
Zeigt die berechnete maximale Dauer des Voralarms dieser Kamera an. Dieser Wert kann Sie bei der Berechnung der erforderlichen Speicherkapazität des lokalen Speichermediums unterstützen.

Hinweis!
Wenn eine gespiegelte VRM bereits für einen Encoder konfiguriert wurde, können Sie die Einstellungen dieses Encoders nicht in den Spalten **Sekundäre Aufzeichnung** ändern.

Sekundäre Aufzeichnung – Einstellung (nur verfügbar, wenn ein Sekundärer VRM konfiguriert ist)
Klicken Sie auf eine Zelle, um der dualen Aufzeichnung dieses Encoders eine geplante Aufzeichnungseinstellung zuzuordnen.
In Abhängigkeit Ihrer Konfiguration kann es passieren, dass die konfigurierte Streamqualität für die sekundäre Aufzeichnung nicht gültig ist. In diesem Fall wird die für die primäre Aufzeichnung konfigurierte Streamqualität verwendet.

Sekundäre Aufzeichnung - Profil (nur für ONVIF-Kameras verfügbar)
Klicken Sie auf eine Zelle, um nach verfügbaren Tokens für Aufzeichnungsprofile dieser ONVIF-Kamera zu suchen.

(Nur sichtbar, wenn Sie auf **Alle** klicken)
Aktivieren Sie ein Kontrollkästchen, um die PTZ-Kamerasteuerung zu aktivieren.

Hinweis:
Weitere Informationen zu Port-Einstellungen finden Sie in COM1.

Port (Nur sichtbar, wenn Sie auf **Alle** klicken)
Klicken Sie auf eine Zelle, um den seriellen Encoder-Port für die PTZ-Kamerasteuerung anzugeben. Für eine an ein Bosch Allegiant System angeschlossene PTZ-Kamera können Sie **Allegiant** auswählen. Für eine solche Kamera benötigen Sie keine Trunkline.

Protokoll (Nur sichtbar, wenn Sie auf **Alle** klicken)
Klicken Sie auf eine Zelle, um ein Protokoll für die PTZ-Kamerasteuerung auszuwählen.

PTZ-Adresse (Nur sichtbar, wenn Sie auf **Alle** klicken)
Geben Sie die Adressnummer für die PTZ-Kamerasteuerung ein.

Objektverfolgung (Nur sichtbar, wenn Sie auf klicken und die Funktion **Objektvisualisierung auf der Karte** aktiviert ist (Menü **Einstellungen** > **Optionen...** > **Metadaten-Verarbeitung**))
Hier können Sie die Objektverfolgung für die gewünschten Kameras aktivieren/deaktivieren.

Hinweis!
Objektverfolgung ist nur für Kameras mit CPP6 oder höher verfügbar, die dem logischen Baum und der globalen Karte hinzugefügt werden.

Aufzeichnung - Archivierung Min Zeit [Tage]
Sekundäre Aufzeichnung - Archivierung Min Zeit [Tage] (nur VRM und Lokale Aufzeichnung)
Klicken Sie auf eine Zelle, um die Anzahl der Tage zu bearbeiten, die die Videodaten dieser Kamera mindestens gespeichert werden sollen. Aufzeichnungen, deren Speicherzeit unter diesem Wert liegt, werden nicht automatisch gelöscht.

Aufzeichnung - Archivierung Max Zeit [Tage]
Sekundäre Aufzeichnung - Archivierung Max Zeit [Tage] (nur VRM und Lokale Aufzeichnung)
Klicken Sie auf eine Zelle, um die Anzahl der Tage zu bearbeiten, die die Videodaten dieser Kamera maximal gespeichert werden sollen. Nur Aufzeichnungen, deren Speicherzeit über diesem Wert liegt, werden automatisch gelöscht; 0 = unbegrenzt.

Siehe
- *Duale Aufzeichnung in der Kameratabelle konfigurieren, Seite 308*
- *Konfigurieren von voreingestellten Positionen und AUX-Kommandos, Seite 305*
- *Konfigurieren von PTZ Port-Einstellungen, Seite 305*
- *Konfigurieren von Stream-Qualitätseinstellungen, Seite 298*
- *Kopieren und Einfügen in Tabellen, Seite 296*
- *ANR-Funktion konfigurieren, Seite 308*
- *Kameratabelle exportieren, Seite 297*
- *ONVIF-Profile zuweisen, Seite 309*
- *ROI-Funktion konfigurieren, Seite 307*

21.2 Seiten für Aufzeichnungseinstellungen

Hauptfenster > **Kameras und Aufzeichnung** > > auf eine Registerkarte für einen Aufzeichnungszeitplan klicken (z. B. **Tag**)
Dient zum Konfigurieren der Aufzeichnungseinstellungen.
Die angezeigten Aufzeichnungszeitpläne werden in **Zeitpläne** konfiguriert.
Es werden nur die Spalten beschrieben, die nicht Teil einer Kameratabelle sind.

- Klicken Sie auf eine Spaltenüberschrift, um die Tabelle nach dieser Spalte zu sortieren.

Daueraufzeichnung
Klicken Sie in der Spalte **Qualität** auf eine Zelle, um die Aufzeichnung zu deaktivieren oder die Streamqualität von Stream 1 auszuwählen.

Aktivieren Sie in der Spalte ein Kontrollkästchen, um Audio zu aktivieren.

Live-/Vorereignisaufzeichnung
Klicken Sie in der Spalte **Qualität** auf eine Zelle, um die Stream-Qualität des Live-Anzeigemodus (erforderlich bei zeitversetzter Wiedergabe) und des Vorereignis-Aufzeichnungsmodus (erforderlich bei Bewegungs- und Alarmaufzeichnung) von Stream 2 auszuwählen. Falls Dual Streaming für diesen Encoder aktiviert ist, können Sie Stream 1 zur Live- oder Vorereignisaufzeichnung auswählen.

Aktivieren Sie in der Spalte ein Kontrollkästchen, um Audio zu aktivieren.

Bewegungsaufzeichnung
Klicken Sie in der Spalte **Qualität** auf eine Zelle, um die Aufzeichnung zu deaktivieren oder die Streamqualität von Stream 1 auszuwählen.

Klicken Sie in der Spalte auf eine Zelle, um Audio zu aktivieren.
Klicken Sie in der Spalte **Vorereignis [s]** auf eine Zelle, um die Aufzeichnungszeit vor dem Bewegungsereignis in Sekunden auszuwählen.

Klicken Sie in der Spalte **Nachereignis [s]** auf eine Zelle, um die Aufzeichnungszeit nach dem Bewegungsereignis in Sekunden auszuwählen.

Alarmaufzeichnung

Klicken Sie in der Spalte **Qualität** auf eine Zelle, um die Streamqualität von Stream 1 auszuwählen.
Konfigurieren Sie zur Alarmaufzeichnung einen entsprechenden Alarm.

Aktivieren Sie in der Spalte ein Kontrollkästchen, um Audio zu aktivieren.
Klicken Sie in der Spalte **Vorereignis [s]** auf eine Zelle, um die Zeit vor dem Alarm in Sekunden auszuwählen.
Klicken Sie in der Spalte **Nachereignis [s]** auf eine Zelle, um die Zeit nach dem Alarm in Sekunden auszuwählen.

Siehe

– *Kopieren und Einfügen in Tabellen, Seite 296*

22 Konfigurieren von Kameras und Aufzeichnungseinstellungen

Hinweis!
In diesem Dokument werden einige Funktionen beschrieben, die nicht für BVMS Viewer verfügbar sind.
Ausführliche Informationen zu den verschiedenen Versionen von BVMS finden Sie unter www.boschsecurity.com und in der BVMS Schnellauswahlhilfe: BVMS Schnellauswahlhilfe.

Hauptfenster > **Kameras und Aufzeichnung**
Dieses Kapitel enthält Informationen zur Konfiguration der Kameras in Ihrem BVMS.
Sie können verschiedene Kameraeigenschaften und die Aufzeichnungseinstellungen konfigurieren.

- Klicken Sie auf , um die Einstellungen zu speichern.
- Klicken Sie auf , um die letzte Einstellung rückgängig zu machen.
- Klicken Sie auf , um die Konfiguration zu aktivieren.

Siehe
- *Seite Kameras, Seite 290*
- *Dialogfeld Geplante Aufzeichnungseinstellungen (nur VRM und Lokale Archivierung), Seite 302*
- *Dialogfeld Stream-Qualitätseinstellungen, Seite 298*
- *Dialogfeld „Voreingestellte Positionen und AUX-Kommandos“, Seite 306*

22.1 Kopieren und Einfügen in Tabellen

Sie können in einer Kameratabelle, Ereigniskonfigurations-Tabelle oder Alarmkonfigurations-Tabelle viele Objekte gleichzeitig konfigurieren.
Sie können die konfigurierbaren Werte einer Tabellenzeile in andere Zeilen kopieren:
- Kopieren aller Werte einer Zeile in andere Zeilen
- Kopieren eines Werts einer Zeile in eine andere Zeile
- Kopieren eines Werts einer Zelle in eine ganze Spalte

Sie können die Werte auf zwei verschiedene Weisen kopieren:
- Kopieren in die Zwischenablage und anschließendes Einfügen
- Direktes Kopieren und Einfügen

Sie können bestimmen, in welchen Zeilen die Einfügung erfolgen soll:
- Kopieren in alle Zeilen
- Kopieren in ausgewählte Zeilen

So kopieren Sie alle konfigurierbaren Werte einer Zeile und fügen sie in eine andere Zeile ein:
1. Klicken Sie mit der rechten Maustaste auf die Zeile mit den gewünschten Werten, und klicken Sie auf **Zeile kopieren**.
2. Klicken Sie auf die Überschrift der Zeile, die Sie ändern möchten.
   Um mehrere Zeilen auszuwählen, drücken Sie die STRG-Taste, und zeigen Sie mit dem Mauszeiger auf die anderen Zeilenüberschriften.
3. Klicken Sie mit der rechten Maustaste auf die Tabelle, und klicken Sie auf **Einfügen**.
   Die Werte werden kopiert.

So kopieren Sie einen Wert einer Zeile und fügen ihn in eine andere Zeile ein:
1. Klicken Sie mit der rechten Maustaste auf die Zeile mit den gewünschten Werten, und klicken Sie auf **Zeile kopieren**.

2. Klicken Sie mit der rechten Maustaste auf die zu ändernde Zelle, zeigen Sie auf **Zelle einfügen in**, und klicken Sie auf **Aktuelle Zelle**.
   Der Wert wird kopiert.

So kopieren Sie alle konfigurierbaren Werte direkt:

1. Klicken Sie auf die Überschrift der Zeile, die Sie ändern möchten.
   Um mehrere Zeilen auszuwählen, drücken Sie die STRG-Taste, und zeigen Sie mit dem Mauszeiger auf die anderen Zeilenüberschriften.
2. Klicken Sie mit der rechten Maustaste auf die Zeile mit den gewünschten Werten, zeigen Sie auf **Kopiere Zeileninhalt nach**, und klicken Sie auf **Ausgewählte Zeilen**.
   Die Werte werden kopiert.

So kopieren Sie einen Wert direkt:

1. Klicken Sie auf die Überschrift der Zeile, die Sie ändern möchten.
   Um mehrere Zeilen auszuwählen, drücken Sie die STRG-Taste, und zeigen Sie mit dem Mauszeiger auf die anderen Zeilenüberschriften.
2. Klicken Sie mit der rechten Maustaste auf die Zelle mit dem gewünschten Wert, zeigen Sie auf **Kopiere Zellinhalt nach**, und klicken Sie auf **Auswahl in Spalte** .
   Der Wert wird kopiert.

So kopieren Sie einen Zellenwert in alle anderen Zellen dieser Spalte:

- Klicken Sie mit der rechten Maustaste auf die Zelle mit dem gewünschten Wert, zeigen Sie auf **Kopiere Zellinhalt nach**, und klicken Sie auf **Ganze Spalte**.
  Der Wert wird kopiert.

So duplizieren Sie eine Zeile:

- Klicken Sie mit der rechten Maustaste auf die Zeile, und klicken Sie auf **Duplizierte Reihe hinzufügen**.
  Die Zeile wird mit einem neuen Namen unterhalb dieser Zeile eingefügt.

Siehe

- *Seite Kameras, Seite 290*
- *Dialogfeld Geplante Aufzeichnungseinstellungen (nur VRM und Lokale Archivierung), Seite 302*
- *Seite Ereignisse, Seite 310*
- *Seite Alarme, Seite 315*

22.2 Kameratabelle exportieren

Hauptfenster > **Kameras und Aufzeichnung**
Oder
Hauptfenster > **Kameras und Aufzeichnung** > auf ein Symbol klicken, um die Seite der Kamera entsprechend dem gewünschten Speichergerät zu ändern, wie z. B.
Zeigt verschiedene Informationen zu den Kameras an, die im BVMS zur Verfügung stehen.
Sie können die Kameratabelle in eine CSV-Datei exportieren.

So führen Sie einen Export durch:

1. Klicken Sie mit der rechten Maustaste an eine beliebige Stelle in der Kameratabelle und anschließend auf **Tabelle exportieren...**
2. Geben Sie im Dialogfeld einen entsprechenden Dateinamen ein.
3. Klicken Sie auf **Speichern**.
   Die gewünschte Kameratabelle wird in eine CSV-Datei exportiert.

22.3 Konfigurieren von Stream-Qualitätseinstellungen

So fügen Sie einen Eintrag mit Einstellungen für die Streamqualität hinzu:

1. Klicken Sie auf , um einen neuen Eintrag zur Liste hinzuzufügen.
2. Geben Sie einen Namen ein.

So entfernen Sie einen Eintrag mit Einstellungen für die Streamqualität:

- Wählen Sie einen Eintrag in der Liste aus, und klicken Sie auf , um den Eintrag zu löschen.
  Standardeinträge können nicht gelöscht werden.

So benennen Sie einen Eintrag mit Einstellungen für die Streamqualität um:

1. Wählen Sie einen Eintrag in der Liste aus.
2. Geben Sie den neuen Namen in das Feld **Name** ein.
   Standardeinträge können nicht umbenannt werden.
3. Klicken Sie auf **OK**.

So konfigurieren Sie Einstellungen für die Streamqualität:

1. Wählen Sie einen Eintrag in der Liste aus.
2. Nehmen Sie die erforderlichen Einstellungen vor.

22.3.1 Dialogfeld Stream-Qualitätseinstellungen

Hauptfenster > **Kameras und Aufzeichnung** >

Ermöglicht Ihnen das Konfigurieren von Profilen für die Streamqualität, die Sie später auf der Seite **Kameras und Aufzeichnung** oder im Dialogfeld **Geplante Aufzeichnungseinstellungen** Kameras zuordnen können.

Die Streamqualität umfasst Videoauflösung, Bildfrequenz, maximale Bandbreite und Videokomprimierung.

Stream-Qualitäten

Wählen Sie eine vordefinierte Streamqualität aus und klicken Sie auf , um eine neue Streamqualität auf Basis der vordefinierten Streamqualität hinzuzufügen. Wenn Sie einen einzelnen Stream auswählen und auf klicken, wird die Einstellung dieser Streamqualität als Knoten der obersten Ebene ohne untergeordnete Elemente kopiert.

Klicken Sie hier, um eine ausgewählte Streamqualität zu löschen. Sie können die Einstellungen der Streamqualität nicht löschen.

Die Liste zeigt alle verfügbaren vordefinierten Einstellungen der Streamqualität an. Wir empfehlen, eine Streamqualität mit demselben Namen wie die Plattform der Kamera zuzuordnen.

Die folgenden Profile für Streamqualitäten stehen zur Auswahl:

Image optimized: Die Einstellungen sind für die Bildqualität optimiert. Dies kann das Netzwerk überlasten.

Bit rate optimized: Die Einstellungen sind für geringe Bandbreite optimiert. Dadurch wird die Bildqualität reduziert.

Balanced: Die Einstellungen bieten einen Kompromiss zwischen optimaler Bildqualität und optimaler Bandbreitennutzung.

Die folgenden Profile für Streamqualitäten sind seit BVMS 9.0 verfügbar, um die Intelligent Streaming-Funktion von Bosch Kameras zu unterstützen:

Cloud optimized 1/8 FR: Die Einstellungen sind für geringe Bandbreite und für alle Kameratypen identisch optimiert.
PTZ optimized: Die Einstellungen sind für PTZ-Kameras optimiert.
Image optimized quiet / standard / busy
Bit rate optimized quiet / standard / busy
Balanced quiet / standard / busy

Szenetypkategorien:
quiet: Die Einstellungen sind für Bilder mit geringer Aktivität optimiert. 89 % statische Szene, 10 % normale Szene, 1 % belebte Szene.
standard: Die Einstellungen sind für Bilder mit mittlerer Aktivität optimiert. 54 % statische Szene, 35 % normale Szene, 11 % belebte Szene.
busy: Die Einstellungen sind für Bilder mit hoher Aktivität optimiert. 30 % statische Szene, 55 % belebte Szene, 15 % sehr belebte Szene.
Die Prozentwerte beziehen sich auf die Verteilung während eines Tages.

Standardmäßig ist das Profil Balanced standard zugewiesen.

Hinweis!
Für jede Kombination der Kameraplattform (CPP3-CPP7.3) und für jede der verfügbaren Auflösungen steht eine bestimmte Einstellung zur Verfügung, damit die richtigen Bitraten für die Kameras festgelegt werden können.
Das Profil muss manuell mit dem entsprechenden Szenetypen für jede Kamera ausgewählt werden.

Hinweis!
Nachdem eine Aktualisierung installiert wurde, müssen die neuen Profile manuell ausgewählt werden, damit sie aktiv werden. Die alten Profile bleiben hiervon unberührt.

Name
Zeigt den Namen der Streamqualität an. Wenn Sie eine neue Streamqualität hinzufügen, können Sie den Namen ändern.

SD Videoauflösung
Diese Einstellung ist nur gültig, wenn der Codec des Streams auf SD-Auflösung gesetzt ist.

Wählen Sie die gewünschte Videoauflösung aus. Für HD-Qualität konfigurieren Sie die SD-Qualität für Stream 2.

Hinweis: Wenn der Codec als HD- oder UHD-Auflösung konfiguriert ist (höher als der SD-Codec), hat dies keine Auswirkungen auf die Auflösung. Die Auflösung einer HD-Kamera kann mit dieser Einstellung z. B. nicht auf SD reduziert werden.

Encoding-Intervall
Verschieben Sie den Schieberegler, oder geben Sie einen Wert ein.
Das System hilft Ihnen bei der Berechnung des entsprechenden Werts für IPS.
Mit dem **Encoding-Intervall** wird das Intervall konfiguriert, in dem Bilder codiert und übertragen werden. Bei der Eingabe 1 werden alle Bilder codiert. Bei dem Wert 4 wird nur jedes vierte Bild codiert, die folgenden drei Bilder werden übersprungen. Dies kann besonders bei niedrigen Bandbreiten von Vorteil sein. Je niedriger die Bandbreite, desto höher sollte dieser Wert sein, um eine hochwertige Videoqualität zu erzielen.

Das Codierungsmodul erhält z. B. 30 Frames vom Sensor als Eingang. Der erforderliche Ausgang für die Liveansicht oder Aufzeichnung beträgt 15 Frames.

Um dies zu erreichen:

- Setzen Sie das **Encoding-Intervall** Parameter auf 2.
  Der Encoder überspringt jeden zweiten Frame vom Sensor und liefert einen H.264-codierten Stream mit nur 15 Frames.

Encoding-Intervall:

– 1 = vollständige Bildfrequenz wie in Codec-Einstellungen angegeben
– 2 = 50 % der Fps in Codec-Einstellungen

Für die Berechnung der Bildfrequenz lautet die Formel: IPS = Sensormodus/Bildcodierungsintervall

GOP-Struktur

Wählen Sie die Struktur aus, die Sie für die Bildgruppe (GOP; Group-of-Pictures) benötigen. Je nachdem, ob eine möglichst geringe Verzögerung (nur IP-Frames) oder eine möglichst geringe Bandbreite Vorrang hat, können Sie zwischen IP, IBP oder IBBP wählen. (GOP-Auswahl ist auf einigen Kameras nicht verfügbar.)

Hinweis:

B-Frames werden nur von Kameras bis zu einer Auflösung von 1080 p und von Firmware 6.40 unterstützt.

Vermeiden Sie B-Frames in der Liveansicht und bei PTZ, da dies zu Livevideo-Latenzzeit führt.

Bitraten-Optimierung

Die Bitratenoptimierung bezieht sich auf die Priorität, die der Bildqualität oder der Bitratenreduzierung eingeräumt wird.

Die **Hohe Qualität** oder **Maximale Qualität** bietet weniger oder keine Bitrateneinsparung, aber ein gutes bis ausgezeichnetes Bild. Die

Niedrige Bitrate und **Medium** Bitrate spart mehr Bandbreite, aber das resultierende Bild liefert möglicherweise weniger Details.

Wenn die Bitratenoptimierung deaktiviert ist, wird eine durchschnittliche Bitrate von 24 h erwartet (höher als die Zielbitrate).

Ziel-Bitrate [Kbps]

Verschieben Sie den Schieberegler, oder geben Sie einen Wert ein.

Sie können die Datenrate für den encoder begrenzen, um die Auslastung der Bandbreite in Ihrem Netzwerk zu reduzieren. Die Ziel-Datenrate sollte entsprechend der gewünschten Bildqualität für typische Szenen ohne übermäßige Bewegung eingestellt werden.

Bei komplexen Bildern oder häufigem Wechsel des Bildinhaltes durch viele Bewegungen kann diese Grenze zeitweise bis zu dem Wert überschritten werden, der im Feld **Maximale Bitrate [Kbps]** angegeben ist.

Maximale Bitrate [Kbps]

Verschieben Sie den Schieberegler, oder geben Sie einen Wert ein.

Mit der maximalen Datenrate wird die maximale Übertragungsgeschwindigkeit konfiguriert, die nicht überschritten werden darf.

Durch Beschränken der Bitrate können Sie zuverlässig den Festplattenspeicher zum Speichern der Videodaten bestimmen.

Dies kann je nach den Einstellungen für die Videoqualität der I- und P-Frames zum Überspringen einzelner Bilder führen.

Der hier eingegebene Wert muss mindestens 10 % höher liegen als der im Feld **Ziel-Bitrate [Kbps]** eingegebene Wert. Wenn der hier eingegebene Wert zu klein ist, wird er automatisch angepasst.

I-Frame Distanz
Dieser Parameter ermöglicht die Einstellung der Intervalle, in denen die I-Frames codiert werden. 1 bedeutet, dass I-Frames kontinuierlich generiert werden. Der Eintrag 10 gibt an, dass nur jedes zehnte Bild ein I-Frame ist, und 60 gibt an, dass nur jedes sechzigste Bild ein I-Frame ist, usw. Die dazwischenliegenden Frames werden als P-Frames codiert.
Hinweis: Bei Verwendung eines sehr langen GOP (bis zu 255) und einer niedrigen Bildfrequenz (1 fps) ist der Zeitabstand zwischen den I-Frames zu groß, und die Wiedergabe kann nicht angezeigt werden. Wir empfehlen, die GOP-Länge auf 30 zu reduzieren.

Frame-Qualitätsstufe
In diesem Dialogfeld können Sie für I-Frames und P-Frames einen Wert zwischen 0 und 100 einstellen. Der niedrigste Wert bewirkt höchste Qualität und niedrigste Bildwiederholfrequenz. Der höchste Wert bewirkt höchste Bildwiederholfrequenz und niedrigste Bildqualität.
Je niedriger die verfügbare Übertragungsbandbreite, desto höher sollte die Qualitätsstufe eingestellt werden, um eine hohe Videoqualität aufrechtzuerhalten.

Hinweis:
Sollten die Kontrollkästchen nicht durch den technischen Support angewiesen werden, empfiehlt es sich, die Kontrollkästchen **Automatisch** auszuwählen. Das optimale Verhältnis zwischen Bewegungs- und Bilddefinition wird dann automatisch eingestellt.

VIP X1600 XFM4-Einstellungen
Ermöglicht Ihnen die Konfiguration der folgenden H.264-Einstellungen für das VIP X 1600 XFM4 Encoder-Modul.
H.264-Anti-Blocking-Filter: Wählen Sie diese Option, um die optische Qualität und Vorhersageleistung durch Glätten scharfer Kanten zu verbessern.
CABAC: Wählen Sie diese Option, um eine sehr effiziente Komprimierung zu aktivieren. Diese Option benötigt eine hohe Verarbeitungsleistung.

Siehe
– *Konfigurieren von Stream-Qualitätseinstellungen, Seite 298*

22.4 Konfigurieren der Kameraeigenschaften

Hauptfenster > **Kameras und Aufzeichnung** >

So ändern Sie die Kameraeigenschaften:
1. Klicken Sie in der Spalte **Kamera** auf eine Zelle und geben Sie einen neuen Namen für die Kamera ein.
   Dieser Name wird an allen Stellen angezeigt, an denen Kameras aufgelistet sind.
2. Nehmen Sie in den anderen Spalten die erforderlichen Einstellungen vor.

Detaillierte Informationen zu den verschiedenen Feldern erhalten Sie, wenn Sie unten auf den Link des entsprechenden Anwendungsfensters klicken.

Siehe
– *Seite Kameras, Seite 290*

22.5 Konfigurieren von Aufzeichnungseinstellungen (nur VRM und Lokale Archivierung)

Hauptfenster > > **Kameras und Aufzeichnung**

Sie können die Aufzeichnungseinstellungen aller Geräte konfigurieren, die dem VRM-Geräteelement im Gerätebaum hinzugefügt werden.
Hinweis: Zur Aufzeichnung muss der entsprechende VRM oder die lokale Archivierung ordnungsgemäß konfiguriert sein.

VRM: **Geräte** > erweitern >

Lokale Archivierung: **Geräte** > erweitern >

So fügen Sie einen Eintrag für die Aufzeichungseinstellungen hinzu:

1. Klicken Sie auf , um einen neuen Eintrag zur Liste hinzuzufügen.
2. Geben Sie einen Namen ein.

So entfernen Sie einen Eintrag für die Aufzeichnungseinstellungen:

- Wählen Sie einen Eintrag in der Liste aus, und klicken Sie auf , um den Eintrag zu löschen. Standardeinträge können nicht gelöscht werden.

So benennen Sie einen Eintrag für die Aufzeichungseinstellungen um:

1. Wählen Sie einen Eintrag in der Liste aus.
2. Geben Sie den neuen Namen in das Feld **Name:** ein. Standardeinträge können nicht umbenannt werden.
3. Klicken Sie auf **OK**.

So konfigurieren Sie Aufzeichnungseinstellungen:

1. Wählen Sie einen Eintrag in der Liste aus.
2. Nehmen Sie die erforderlichen Einstellungen vor, und klicken Sie auf **OK**.
3. Klicken Sie auf oder .
4. Wählen Sie in der Spalte **Aufzeichnung** die gewünschte Aufzeichnungseinstellung für jeden Encoder aus.

Detaillierte Informationen zu den verschiedenen Feldern finden Sie in der Online-Hilfe unter dem entsprechenden Anwendungsfenster.

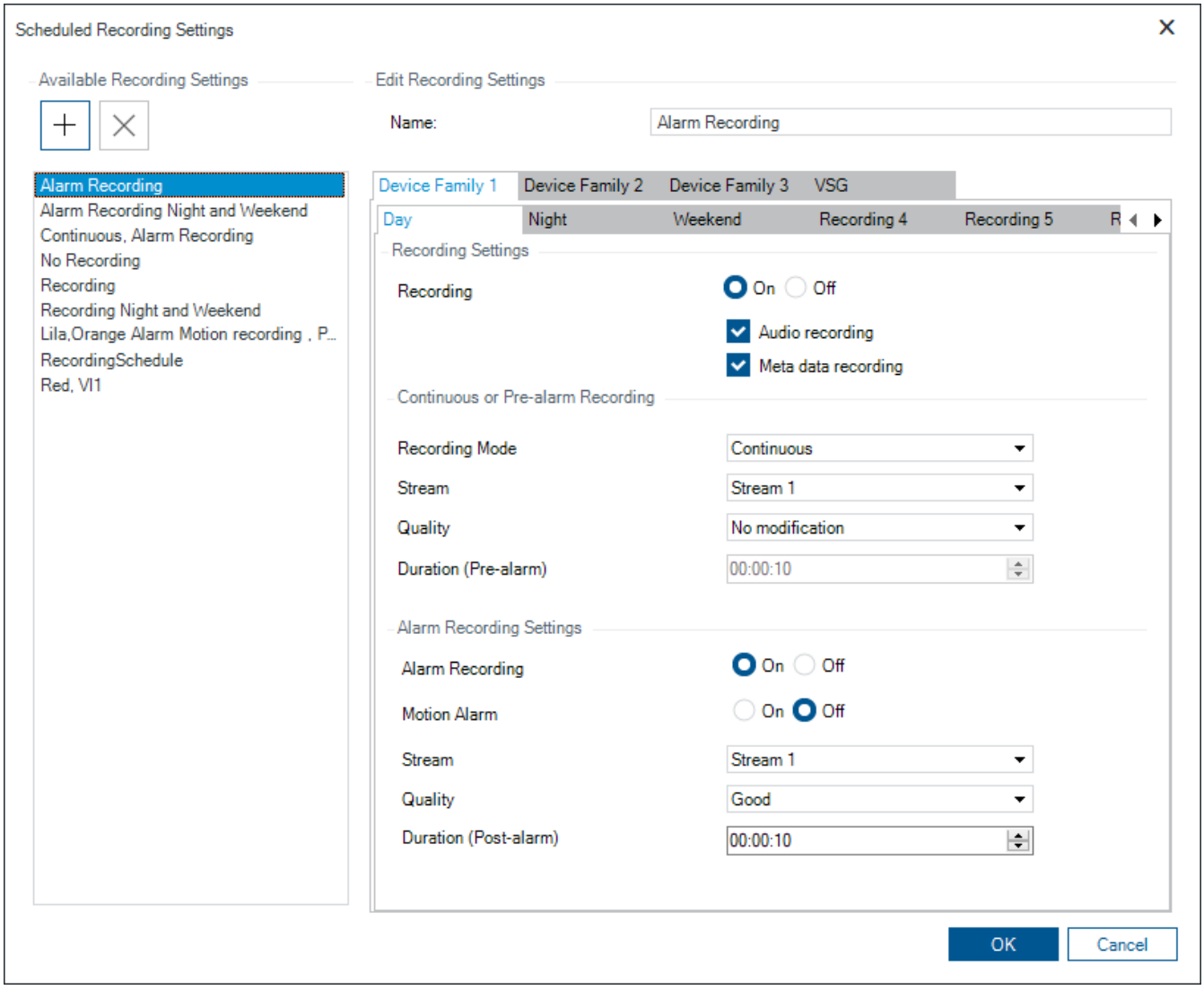
Siehe

– *Dialogfeld Geplante Aufzeichnungseinstellungen (nur VRM und Lokale Archivierung), Seite 302*

22.6 Dialogfeld Geplante Aufzeichnungseinstellungen (nur VRM und Lokale Archivierung)

Hauptfenster > **Kameras und Aufzeichnung** >

Dient zum Konfigurieren zeitplanabhängiger Aufzeichnungseinstellungen für jede verfügbare Gerätefamilie. Eine Gerätefamilie ist verfügbar, wenn mindestens ein Encoder dieser Gerätefamilie zum Gerätebaum hinzugefügt wurde. In der Tabelle **Kameras** weisen Sie jeder Kamera eine solche Aufnahmeeinstellung zu.
Verwenden Sie dazu die Aufzeichnungszeitpläne, die auf der Seite **Zeitpläne** konfiguriert wurden.
Hinweis: Das Ein- oder Ausschalten der normalen Aufzeichnung gilt für alle Gerätefamilien.



Verfügbare Aufzeichnungseinstellungen
Wählen Sie eine vordefinierte Aufzeichnungseinstellung aus, um deren Eigenschaften zu ändern. Sie können eine benutzerdefinierte Einstellung hinzufügen oder löschen.

Name:
Geben Sie einen Namen für die neue Aufzeichnungseinstellung ein.

Registerkarte Gerätefamilie
Wählen Sie die gewünschte Gerätefamilie aus, um die für diese Gerätefamilie gültigen Aufzeichnungseinstellungen zu konfigurieren.

Registerkarte Aufzeichnungsplan
Wählen Sie für die ausgewählte Gerätefamilie einen Aufzeichnungsplan, um die Aufzeichnungseinstellungen zu konfigurieren.

Aufzeichnung
Schalten Sie die normale Aufzeichnung ein oder aus (Daueraufzeichnung oder Voralarmaufzeichnung)

Audioaufzeichnung
Wählen Sie diese Option aus, wenn Sie Audio aufzeichnen möchten.

Metadaten-Aufzeichnung
Wählen Sie diese Option aus, wenn Sie Metadaten aufzeichnen möchten.

Aufzeichnungsmodus
Wählen Sie den gewünschten Aufzeichnungsmodus aus.
Die folgenden Elemente stehen zur Auswahl:
– **Dauer**
– **Voralarm**

Stream
Wählen Sie den gewünschten Stream für die normale Aufzeichnung aus.
Hinweis: Es hängt von der Gerätefamilie ab, welche Streams verfügbar sind.

Qualität
Wählen Sie die gewünschte Streamqualität für die normale Aufzeichnung aus. Die verfügbaren Qualitätseinstellungen werden im Dialogfeld **Stream-Qualitätseinstellungen** konfiguriert.

Dauer (Voralarm)
Geben Sie die gewünschte Aufzeichnungszeit vor einem Alarm ein. Geben Sie die Uhrzeit im Format HH:MM:SS ein.
Hinweis: Nur aktiviert, wenn**Voralarm** ausgewählt ist.

Hinweis!
Für Voralarmeinstellungen zwischen 1 und 10 wird der Voralarm automatisch auf dem RAM des Encoders gespeichert, wenn ausreichend RAM-Platz verfügbar ist, sonst werden sie gespeichert. Voralarmeinstellungen, die größer als 10 s sind, werden die Voralarme im Speicher gespeichert. Die Speicherung der Voralarme auf dem RAM des Encoders ist nur für Firmware-Version 5.0 oder höher möglich.

Einstellungen Alarmaufzeichnung
Dient zum Ein- und Ausschalten der Alarmaufzeichnung für diese Kamera.

Bewegungsalarm
Dient zum Ein- und Ausschalten der Alarmaufzeichnung, die durch eine Bewegung ausgelöst wird.

Stream
Wählen Sie den Stream aus, der für die Alarmaufzeichnung verwendet werden soll.
Hinweis: Es hängt von der Gerätefamilie ab, welche Streams verfügbar sind.

Qualität
Wählen Sie die gewünschte Streamqualität für die Aufzeichnung aus. Die verfügbaren Qualitätseinstellungen werden im Dialogfeld **Stream-Qualitätseinstellungen** konfiguriert.
Nur für Geräte der Gerätefamilie 2 oder 3: Wenn Sie den Eintrag **Keine Änderung** auswählen, wird für die Alarmaufzeichnung die gleiche Qualität wie für die Daueraufzeichnung/Voralarmaufzeichnung verwendet. Es wird empfohlen, den Eintrag **Keine Änderung** zu verwenden. Wenn Sie eine Streamqualität für die Alarmaufzeichnung auswählen, werden nur die Werte für das Encoding-Intervall und die Ziel-Bitrate entsprechend den Einstellungen in dieser Streamqualität geändert. Die anderen Qualitätseinstellungen entsprechen den Qualitätseinstellungen der jeweiligen Daueraufzeichnung/Voralarmaufzeichnung.

Dauer (Nachalarm)
Geben Sie die gewünschte Alarmaufzeichnungszeit ein. Geben Sie die Uhrzeit im Format HH:MM:SS ein.

Siehe
– *Kopieren und Einfügen in Tabellen, Seite 296*
– *Konfigurieren von Aufzeichnungseinstellungen (nur VRM und Lokale Archivierung), Seite 301*

22.7 Konfigurieren von PTZ Port-Einstellungen

Hauptfenster > **Geräte** > erweitern > erweitern > > Registerkarte **Schnittstellen** > Registerkarte **Peripherie**

Hauptfenster > **Geräte** > > > Registerkarte **Schnittstellen** > Registerkarte **Peripherie**

Sie können Port-Einstellungen für einen Encoder nur konfigurieren, wenn die Steuerung der Kamera verfügbar und aktiviert ist.

Wenn der Encoder oder die PTZ-Kamera ausgetauscht wird, gehen die Port-Einstellungen verloren. Sie müssen sie erneut konfigurieren.

Nachdem die Firmware aktualisiert wurde, überprüfen Sie die Port-Einstellungen.

So konfigurieren Sie die Port-Einstellungen eines Encoders:

- Nehmen Sie die erforderlichen Einstellungen vor.
  Die Einstellungen sind sofort wirksam, nachdem sie gespeichert wurden. Sie brauchen die Konfiguration nicht zu aktivieren.

Detaillierte Informationen zu den verschiedenen Feldern finden Sie in der Online-Hilfe unter dem entsprechenden Anwendungsfenster.

22.8 Konfigurieren von voreingestellten Positionen und AUX-Kommandos

Hauptmenü > **Kameras und Aufzeichnung** >

Sie können Kamerapositionen für PTZ-, ROI- und Panoramakameras voreinstellen und speichern. Für PTZ-Kameras können Sie auch AUX-Kommandos definieren.

Hinweis: Konfigurieren Sie zunächst die Port-Einstellungen der PTZ-Kamera. Anschließend können Sie die PTZ-Kameraeinstellungen konfigurieren. Anderenfalls funktioniert die PTZ-Steuerung in diesem Dialogfeld nicht.

So konfigurieren Sie eine voreingestellte Position:

1. Wählen Sie in der Tabelle **Kameras** den erforderlichen Encoder aus.
2. Nur für PTZ-Kameras: Aktivieren Sie das Kontrollkästchen in der Spalte , um die Steuerung einer PTZ-Kamera zu aktivieren.
3. Klicken Sie auf die Schaltfläche .
   Das Dialogfeld **Voreingestellte Positionen und AUX-Befehle** wird angezeigt.
4. Sie können die Anzahl der voreingestellten Positionen definieren, die Sie verwenden möchten.
5. Wählen Sie die Position aus, die Sie einstellen möchten.
6. Navigieren Sie im Vorschaufenster per Maussteuerung zu der Position, die Sie konfigurieren möchten.
   Verwenden Sie das Mausrad zum Heran- und Herauszoomen und verschieben Sie den Bildausschnitt durch Klicken und Ziehen.
7. Geben Sie ggf. einen Namen für die konfigurierte Position ein.
8. Klicken Sie auf , um die voreingestellte Position zu speichern.

   Hinweis: Sie müssen für jede voreingestellte Position auf klicken. Andernfalls wird die Position nicht gespeichert.
9. Klicken Sie auf **OK**.

So zeigen Sie bereits konfigurierte voreingestellte Positionen an:

1. Wählen Sie in der Tabelle **Kameras** den erforderlichen Encoder aus.
2. Klicken Sie auf die Schaltfläche .
   Das Dialogfeld **Voreingestellte Positionen und AUX-Befehle** wird angezeigt.
3. Wählen Sie die gewünschte Position aus.
4. Klicken Sie auf .
   Die voreingestellte Kameraposition wird im Vorschaufenster angezeigt.

Hinweis:
Voreingestellte Positionen für PTZ- und ROI-Kameras werden direkt in der Kamera gespeichert.
Voreingestellte Positionen für Panoramakameras werden in BVMS gespeichert.
PTZ-Kameras bewegen sich physisch in die voreingestellte Position. Panorama- und ROI-Kameras zeigen nur einen Ausschnitt des gesamten Bildbereichs der Kamera an.

So konfigurieren Sie AUX-Kommandos für PTZ-Kameras:

1. Wählen Sie in der Tabelle **Kameras** den erforderlichen Encoder aus.
2. Klicken Sie auf die Schaltfläche .
   Das Dialogfeld **Voreingestellte Positionen und AUX-Befehle** wird angezeigt.
3. Öffnen Sie die Registerkarte **AUX-Befehle**.
4. Nehmen Sie die erforderlichen Einstellungen vor.
5. Klicken Sie auf , um die voreingestellten Kommandos zu speichern.

Detaillierte Informationen zu den verschiedenen Feldern finden Sie in der Online-Hilfe unter dem entsprechenden Anwendungsfenster.

Siehe

- *Dialogfeld „Voreingestellte Positionen und AUX-Kommandos“, Seite 306*
- *Konfigurieren von PTZ Port-Einstellungen, Seite 305*
- *Konfigurieren eines Alarms, Seite 327*
- *Dialogfeld Bildfensterinhalt auswählen, Seite 317*
- *Dialogfeld Alarmoptionen, Seite 318*
- *Dialogfeld „Bildfensterinhalt auswählen“ (MG), Seite 318*

22.9 Dialogfeld „Voreingestellte Positionen und AUX-Kommandos“

Hauptfenster > **Kameras und Aufzeichnung** > > PTZ-, ROI- oder Panoramakamera auswählen >

Dient zum Konfigurieren einer PTZ-, ROI- oder Panoramakamera.
Für ROI- und Panoramakameras sind keine AUX-Kommandos verfügbar.
Hinweis: Konfigurieren Sie zunächst die Port-Einstellungen der PTZ-Kamera. Anschließend können Sie die PTZ-Kameraeinstellungen konfigurieren. Anderenfalls funktioniert die PTZ-Steuerung in diesem Dialogfeld nicht.

Symbole

	Klicken Sie hier, um die Kamera in die voreingestellte Position zu bringen oder das Kommando auszuführen.

	Klicken Sie hier, um die voreingestellte Position oder das Kommando zu speichern.

Registerkarte Voreingestellte Positionen
Klicken Sie darauf, um die Tabelle mit den voreingestellten Positionen anzuzeigen.

Nr
Zeigt die Nummer der voreingestellten Position an.

Name
Klicken Sie auf eine Zelle, um den Namen der voreingestellten Position zu bearbeiten.

AUX-Befehle Registerkarte (nur für PTZ-Kameras)
Klicken Sie darauf, um die Tabelle mit den AUX-Kommandos anzuzeigen.
Hinweis: Wenn ein ONVIF-Encoder AUX-Kommandos unterstützt, werden die AUX-Kommandos direkt vom ONVIF-Encoder bereitgestellt.

Nr
Zeigt die Nummer des AUX-Kommandos an.

Name
Klicken Sie auf eine Zelle, um den Namen des Kommandos zu bearbeiten.
Code
Klicken Sie auf eine Zelle, um den Kommando-Code zu bearbeiten.

Siehe
- *Konfigurieren von PTZ Port-Einstellungen, Seite 305*
- *Konfigurieren von voreingestellten Positionen und AUX-Kommandos, Seite 305*

22.10 ROI-Funktion konfigurieren

Hauptfenster > **Kameras und Aufzeichnung** >
Sie können die ROI-Funktion für eine feststehende HD-Kamera aktivieren.
Sie müssen Stream 2 für Live-Video und den H.264 MP SD ROI- oder H.265 MP SD ROI-Codec für Stream 2 konfigurieren.
Stellen Sie sicher, dass Stream 2 für Live-Video auf jeder Arbeitsstation, auf der die ROI-Funktion genutzt wird, verwendet wird.

So aktivieren Sie die ROI-Funktion:
1. Wählen Sie in der Spalte **Stream 2** – **Codec** den H.264 MP SD ROI- oder H.265 MP SD ROI-Codec.
2. Wählen Sie in der Spalte **Live Video** – **Stream** den **Stream 2** aus.
3. Aktivieren Sie mit einem Klick in der Spalte **Live Video** – **ROI** das Kontrollkästchen.

So deaktivieren Sie die ROI-Funktion:
1. Deaktivieren Sie mit einem Klick in der Spalte **Live Video** - **ROI** das Kontrollkästchen.
2. Wählen Sie in der Spalte **Stream 2** - **Codec** den gewünschten Codec.

Siehe
- *Seite Kameras, Seite 290*

22.11 ANR-Funktion konfigurieren

Hauptfenster > **Kameras und Aufzeichnung** >

Bevor Sie die ANR-Funktion aktivieren können, müssen Sie die Speichermedien eines Encoders dem gewünschten Encoder hinzufügen und diese Speichermedien konfigurieren.

Sie müssen die duale Aufzeichnung für den Encoder deaktivieren, um ANR konfigurieren zu können.

Die ANR-Funktion ist nur zusammen mit Encodern möglich, die über eine Firmware-Version 5.90 oder höher verfügen. Nicht alle Encoder-Typen unterstützen die ANR-Funktion, selbst wenn die korrekte Firmware-Version installiert ist.

So gehen Sie zur Aktivierung vor:

- Aktivieren Sie in der Zeile der gewünschten Kamera bzw. in der Spalte **ANR** das Kontrollkästchen.

Siehe

- *Duale Aufzeichnung in der Kameratabelle konfigurieren, Seite 308*
- *Seite Kameras, Seite 290*
- *Speichermedien eines Encoders konfigurieren, Seite 232*

22.12 Duale Aufzeichnung in der Kameratabelle konfigurieren

Hauptfenster > **Kameras und Aufzeichnung** >

Um die duale Aufzeichnung konfigurieren zu können, muss die ANR-Funktion deaktiviert werden.

Wenn Sie die duale Aufzeichnung für eine Kamera eines Mehrkanal-Encoders konfigurieren, stellt das System sicher, dass für alle Kameras dieses Encoders dasselbe Aufzeichnungsziel konfiguriert wird.

So führen Sie die Konfiguration durch:

1. Klicken Sie in der Spalte **Sekundäre Aufzeichnung** - **Ziel** auf eine Zelle des gewünschten Encoders und anschließend auf den gewünschten Pool eines Sekundären VRM.
   Alle Kameras des betreffenden Encoders werden automatisch so konfiguriert, dass sie im ausgewählten Sekundären VRM aufgezeichnet werden.
2. Wählen Sie in der Spalte **Einstellung** eine geplante Aufzeichnungseinstellung.

Siehe

- *Duale Aufzeichnung im Gerätebaum konfigurieren, Seite 189*
- *ANR-Funktion konfigurieren, Seite 308*
- *Duale/Failover-Aufzeichnung, Seite 31*
- *Seite Kameras, Seite 290*

22.13 Verwalten von Video-Streaming-Gateways

Siehe

- *Seite „Video Streaming Gateway-Gerät“, Seite 200*
- *Dialogfeld „Bosch Encoder hinzufügen/bearbeiten“, Seite 203*
- *Dialogfeld „ONVIF-Encoder hinzufügen/bearbeiten“, Seite 204*
- *Dialogfeld „JPEG-Kamera hinzufügen/bearbeiten“, Seite 206*
- *Dialogfeld „RTSP-Encoder hinzufügen/bearbeiten“, Seite 207*

22.13.1 ONVIF-Profile zuweisen

Hauptfenster > **Kameras und Aufzeichnung** >

Sie können einer ONVIF-Kamera einen Codierschlüssel für das ONVIF-Medienprofil zuweisen.
Sie können diesen entweder für Live-Videos oder Aufzeichnungen zuweisen.

So weisen Sie einen Codierschlüssel für ein Live-Video zu:

- Wählen Sie in der Spalte **Live Video** - **Profil** den gewünschten Eintrag aus.

So weisen Sie einen Codierschlüssel für eine Aufzeichnung zu:

- Wählen Sie in der Spalte **Aufzeichnung** - **Profil** den gewünschten Eintrag aus.

Siehe

– *Seite Kameras, Seite 290*

23 Seite Ereignisse

Hauptfenster> **Ereignisse**

Zeigt den Ereignisbaum mit allen verfügbaren Ereignissen sowie eine Ereigniskonfigurations-Tabelle für jedes Ereignis an. Die Ereignisse sind nach Typ gruppiert. Beispielsweise sind alle Kamera-Aufzeichnungsereignisse wie Daueraufzeichnung oder Alarmaufzeichnung unter „Aufzeichnungsmodus“ gruppiert.

Die verfügbaren Ereignisse werden unter den entsprechenden Geräten gruppiert. Die Statusänderung eines Geräts wird unter als angezeigt. Alle anderen Ereignisse werden unter den geräteabhängigen Gruppen als angezeigt.

Für jedes Ereignis können Sie Folgendes konfigurieren:

- Auslösen eines Alarms gemäß einem Zeitplan (nicht für alle Ereignisse verfügbar)
- Protokollieren des Ereignisses gemäß einem Zeitplan. Ein protokolliertes Ereignis wird im Operator Client in der Ereignisliste angezeigt.
- Ausführen eines Kommandoskripts gemäß einem Zeitplan (nicht für alle Ereignisse verfügbar)
- Für Ereignisse des Typs : Hinzufügen von Textdaten zu Aufzeichnungen.

Bei Eintreten des Ereignisses werden die Einstellungen ausgeführt.

Sie können ein Zusammengesetztes Ereignis erstellen, das mehrere Ereignisse mit Hilfe von booleschen Ausdrücken kombiniert.

- Klicken Sie auf ein Baumelement, um die entsprechende Ereigniskonfigurations-Tabelle anzuzeigen.

Klicken Sie hier, um ein Ereignis zu duplizieren. Dient zum Erzeugen mehrerer Alarme für ein bestimmtes Ereignis.

Klicken Sie hier, um ein dupliziertes Ereignis oder Zusammengesetztes Ereignis zu löschen.

Klicken Sie hier, um das ausgewählte Zusammengesetzte Ereignis umzubenennen.

Klicken Sie hier, um ein Dialogfeld zum Erzeugen von Zusammengesetzten Ereignissen mit Hilfe von booleschen Ausdrücken anderer Ereignisse (maximal 10) anzuzeigen.

Zusammengesetzte Ereignisse werden der Ereigniskonfigurations-Tabelle hinzugefügt.

Klicken Sie hier, um das ausgewählte Zusammengesetzte Ereignis zu bearbeiten.

Klicken Sie hier, um ein Dialogfeld zum Erzeugen und Bearbeiten von Kommandoskripten anzuzeigen.

Um nach Elementen zu suchen:

- Tippen Sie im Suchfeld eine Zeichenfolge ein und drücken Sie auf den Schlüssel ENTER, um die angezeigten Elemente zu filtern.
  Nur Elemente mit der Zeichenfolge und ihre übergeordneten Elemente (nur in Bäumen) werden angezeigt. Die Anzahl der gefilterten Elemente und die gesamte Anzahl der Elemente wird angegeben.

Hinweis: Setzen Sie Zeichenfolgen zwischen doppelte Anführungszeichen, um genaue Treffer zu erhalten. Beispielsweise filtert "Camera 1" genau die Kameras mit diesem Namen, jedoch nicht camera 201.

Siehe

- *Konfigurieren von Ereignissen und Alarmen, Seite 323*
- *Konfigurieren von Kommandoskripten, Seite 89*
- *Dialogfeld „Optionen“ (Menü „Einstellungen“), Seite 121*
- *Konfigurieren der blinkenden Hotspots, Seite 330*

23.1 Registerkarte „Entprelleinstellungen“

Hinweis: Bei einigen Ereignissen ist die Registerkarte "Debounce Settings" (Entprelleinstellungen) aufgrund von technischen Einschränkungen nicht verfügbar.
Dient zum Konfigurieren der Entprelleinstellungen für das ausgewählte Ereignis.

Entprellzeit
Während des eingegebenen Zeitraums werden alle weiteren Ereignisse ignoriert.

Priorität für Ereignisstatus
Für einen Ereignis-Status können Sie eine Prioritätseinstellung zuordnen.

Prioritäten bearbeiten
Klicken Sie hier, um das Dialogfeld zum Konfigurieren einer Prioritätseinstellung anzuzeigen.

Einstellung hinzufügen
Klicken Sie hier, um eine Zeile zum Konfigurieren einer Entprelleinstellung zu konfigurieren, die sich von den Entprelleinstellungen für alle Geräte unterscheidet.

Einstellung entfernen
Klicken Sie hier, um die ausgewählte Zeile zu entfernen. Klicken Sie zur Auswahl einer Zeile auf die linke Zeilenüberschrift.

23.2 Registerkarte „Einstellungen” für die erweiterte Anzeige der Karte

Die Konfiguration der Farbzustände auf den Karten ist nur möglich, wenn Sie auf das Kontrollkästchen **Erweiterte Statusanzeige aktiviert (Hot-Spot-Färbung in Karten in abhängig von Status)**oder die **Erweiterte Statusanzeige aktiviert (Hot-Spot-Färbung in Karten in abhängig von Alarm)** Option im **Optionen** Dialogfeld wählen.

Für jedes -Ereignis bzw. jeden -Alarm können Sie die Hintergrundfarbe und das Verhalten (blinkend oder nicht blinkend) für Hotspots konfigurieren. Beispielsweise können Sie ein -Ereignis bzw. einen -Alarm eines Geräts konfigurieren, sodass das Gerätesymbol auf einer Karte zu blinken anfängt, wenn sich der Status des Geräts ändert.
Darüber hinaus können Sie die Anzeigepriorität für alle Hotspots konfigurieren. Dies ist erforderlich, wenn verschiedene Ereignisse für dasselbe Gerät auftreten. (1 = höchste Priorität)
Die konfigurierte Farbe gilt für alle Hotspots mit derselben Anzeigepriorität. Sie können Farbe, Verhalten und Priorität bei jedem -Ereignis/-Alarm ändern: Die veränderte Farbe und das Verhalten werden für alle Hotspots aller anderen -Ereignisse/-Alarme mit derselben Priorität verwendet.

Färben von Zuständen auf Karten aktivieren
Klicken Sie, damit die Hotspots der Geräte zu diesem Ereignis mit farbigen Hintergrund und blinkender Funktion auf Karten angezeigt werden können.

Anzeigepriorität auf Karte:
Klicken Sie auf die Pfeile, um die Priorität für die Hotspots der Geräte zu ändern, die zu diesem Ereignis gehören.

Hintergrundfarbe auf Karte:
Klicken Sie auf das Farbfeld, um die für die Hotspots verwendete Hintergrundfarbe der Geräte auszuwählen, die zu diesem Ereignis gehören.
Hinweis: Alle Statusereignisse aller Geräte mit derselben Priorität besitzen dieselbe Farbe.

Blinken
Klicken Sie, um die Hotspots der Geräte zu aktivieren, die zu diesem Ereignis gehören.

23.3 Registerkarte „Einstellungen” für die Ereigniskonfiguration

Gerät
Zeigt den Namen eines Geräts oder Zeitplans an.

Netzwerk
Zeigt die IP-Adresse des entsprechenden IP-Geräts an.

Alarm auslösen
Klicken Sie auf eine Zelle, um einen Aufzeichnungs- oder Aktionszeitplan zum Auslösen eines Alarms auszuwählen.
Wählen Sie **Immer** aus, wenn der Alarm unabhängig vom Zeitpunkt ausgelöst werden soll.
Wählen Sie **Nie** aus, wenn der Alarm nicht ausgelöst werden soll.

Protokoll
Klicken Sie in der Spalte **Zeitplan** auf eine Zelle, um einen Aufzeichnungs- oder Aktionszeitplan für die Protokollierung auszuwählen.
Wählen Sie **Immer** aus, wenn das Ereignis unabhängig vom Zeitpunkt protokolliert werden soll.
Wählen Sie **Nie** aus, wenn das Ereignis nicht protokolliert werden soll.

Skript
Klicken Sie in der Spalte **Skript** auf eine Zelle, um ein Kommandoskript auszuwählen.
Klicken Sie in der Spalte **Zeitplan** auf eine Zelle, um einen Aufzeichnungs- oder Aktionszeitplan für die Ausführung eines Kommandoskripts auszuwählen.
Wählen Sie **Immer** aus, wenn das Kommandoskript unabhängig vom Zeitpunkt ausgeführt werden soll.
Wählen Sie **Nie** aus, wenn das Kommandoskript nicht ausgeführt werden soll.

Aufzeichnung von Textdaten
Sie können konfigurieren, dass Textdaten zur Daueraufzeichnung einer Kamera hinzugefügt werden.
Hinweis: Diese Spalte ist nur für Ereignisse mit Textdaten verfügbar. Beispiel: **ATM/POS-Geräte** > **ATM-Eingang** > **Daten-Input**

23.4 Dialogfeld Kommandoskript-Editor

Hauptfenster > **Ereignisse** >
Dient zum Erzeugen und Bearbeiten von Kommandoskripten.

Klicken Sie hier, um die geänderten Einstellungen zu speichern.

Klicken Sie hier, um die gespeicherten Einstellungen wiederherzustellen.

Klicken Sie hier, um den Code eines Skripts zu prüfen.

Klicken Sie hier, um eine Scriptlet-Datei zu erzeugen.

Klicken Sie hier, um eine Scriptlet-Datei zu löschen.

Klicken Sie hier, um ein Dialogfeld zum Importieren einer Skriptdatei anzuzeigen.

Klicken Sie hier, um ein Dialogfeld zum Exportieren einer Skriptdatei anzuzeigen.

Klicken Sie hier, um ein vorhandenes Skript in die andere verfügbare Skriptsprache umzuwandeln. Der gesamte vorhandene Skripttext wird gelöscht.

Klicken Sie hier, um die Online-Hilfe für BVMS Script API anzuzeigen.

Klicken Sie hier, um die Online-Hilfe für das BVMS anzuzeigen.

Klicken Sie hier, um das Dialogfeld **Kommandoskript-Editor** zu schließen.

Siehe

– *Konfigurieren von Kommandoskripten, Seite 89*

23.5 Zusammengesetztes Ereignis erzeugen / Dialogfeld Zusammengesetztes Ereignis bearbeiten

Hauptfenster > **Ereignisse** >

Dient zum Erzeugen bzw. Ändern eines Zusammengesetzten Ereignisses.

Um nach Elementen zu suchen:

- Tippen Sie im Suchfeld eine Zeichenfolge ein und drücken Sie auf den Schlüssel ENTER, um die angezeigten Elemente zu filtern.
  Nur Elemente mit der Zeichenfolge und ihre übergeordneten Elemente (nur in Bäumen) werden angezeigt. Die Anzahl der gefilterten Elemente und die gesamte Anzahl der Elemente wird angegeben.

Hinweis: Setzen Sie Zeichenfolgen zwischen doppelte Anführungszeichen, um genaue Treffer zu erhalten. Beispielsweise filtert "Camera 1" genau die Kameras mit diesem Namen, jedoch nicht camera 201.

Ereignisname:
Geben Sie den Namen für das Zusammengesetzte Ereignis ein.

Ereigniszustände:
Wählen Sie die Statusänderung aus, die Teil eines Zusammengesetzten Ereignisses sein soll.

Objekte:
Wählen Sie eines oder mehrere der verfügbaren Objekte des gewählten Ereignisstatus aus. Dieser Status und das gewählte Objekt werden im zusammengesetzten Ereignisbaum dem Root-Operator unmittelbar untergeordnet angezeigt.

Zusammengesetzte Ereignisse:
Ermöglicht Ihnen die Erstellung zusammengesetzter Ereignisse im zusammengesetzten Ereignisbaum. Alle unmittelbar untergeordneten Elemente eines booleschen Operators (AND, OR) werden von diesem Operator kombiniert.

Siehe

– *Erzeugen eines Zusammengesetzten Ereignisses, Seite 326*

– *Bearbeiten eines Zusammengesetzten Ereignisses, Seite 327*

23.6 Dialogfeld Skriptsprache auswählen

Hauptfenster > **Ereignisse** >
Dient zum Festlegen der Skriptsprache für Ihre Kommandoskripte.
Für bereits vorhandene Kommandoskripte kann die Skriptsprache nicht geändert werden.

Skriptsprache:
Wählen Sie die Skriptsprache aus.

Siehe
– *Konfigurieren von Kommandoskripten, Seite 89*

23.7 Prioritäten des Dialogfelds „Ereignistyp“ bearbeiten

Hauptfenster > **Ereignisse** > Registerkarte **Debounce Settings** (Entprelleinstellungen) > Schaltfläche **Prioritäten bearbeiten**
Sie können bei Bedarf Prioritäten für die verschiedenen Zustandsänderungen eines Ereignisses konfigurieren, zum Beispiel „virtueller Eingang geschlossen“ und „virtueller Eingang geöffnet“. Eine Zustandsänderung mit höherer Priorität ersetzt die Entprellzeit einer anderen Zustandsänderung mit niedrigerer Priorität.

Name der Priorität:
Geben Sie einen Namen für die Priorisierungseinstellung ein.

State-Wert
Zeigt die Namen der Ereigniszustände für das ausgewählte Ereignis an.

Status-Priorität
Geben Sie die gewünschte Priorität ein. 1 = höchste Priorität, 10 = niedrigste Priorität.

23.8 Dialogfeld Geräte auswählen

Hauptfenster > **Ereignisse** > oder > Registerkarte **Entprelleinstellungen** > Schaltfläche **Einstellung hinzufügen**

Auswählen
Aktivieren Sie das Kontrollkästchen für den gewünschten Eintrag, und klicken Sie auf **OK**, um der Tabelle **Geräte mit abweichenden Entprelleinstellungen** eine Zeile hinzuzufügen.

23.9 Dialogfeld „Textatenaufzeichnung“

Hauptfenster > **Ereignisse** > im Ereignisbaum **Daten-Input** wählen (es müssen Textdaten vorhanden sein, beispielsweise: **Foyerkartenleser-Geräte** > **Foyerkartenleser** > **Karte abgewiesen**) > Spalte **Aufzeichnung von Textdaten** > ...
Sie können die Kameras konfigurieren, denen Zusatzdaten für die Daueraufzeichnung hinzugefügt werden sollen.

Siehe
– *Alarmaufzeichnung mit Textdaten auslösen, Seite 329*

24 Seite Alarme

Hauptfenster > **Alarme**

Zeigt den Ereignisbaum sowie eine Alarmkonfigurations-Tabelle für jedes Ereignis an. Nur die auf der Seite **Ereignisse** konfigurierten Ereignisse werden angezeigt.

In den Tabellen können Sie für jedes Ereignis konfigurieren, wie ein durch dieses Ereignis ausgelöster Alarm angezeigt wird und von welchen Kameras Bilder aufgezeichnet und angezeigt werden, wenn dieser Alarm auftritt.

Einige Ereignisse werden standardmäßig als Alarm konfiguriert, z. B. Systemfehler.

Für die folgenden Ereignisse kann kein Alarm konfiguriert werden:

- Änderung eines Aufzeichnungsmodus
- Änderung eines Alarmzustands
- Die meisten Benutzeraktionen, z. B. PTZ-Aktion

Klicken Sie hier, um das Dialogfeld **Ressourcen-Manager** anzuzeigen.

Anzeige eines Dialogfelds zum Festlegen von für diesen Management Server gültigen Alarmeinstellungen.

Um nach Elementen zu suchen:

- Tippen Sie im Suchfeld eine Zeichenfolge ein und drücken Sie auf den Schlüssel ENTER, um die angezeigten Elemente zu filtern.
  Nur Elemente mit der Zeichenfolge und ihre übergeordneten Elemente (nur in Bäumen) werden angezeigt. Die Anzahl der gefilterten Elemente und die gesamte Anzahl der Elemente wird angegeben.

Hinweis: Setzen Sie Zeichenfolgen zwischen doppelte Anführungszeichen, um genaue Treffer zu erhalten. Beispielsweise filtert "Camera 1" genau die Kameras mit diesem Namen, jedoch nicht camera 201.

- Klicken Sie auf ein Baumelement, um die entsprechende Alarmkonfigurations-Tabelle anzuzeigen.

Gerät

Zeigt das Gerät der im Ereignisbaum ausgewählten Ereignisbedingung an.

Netzwerkadresse

Zeigt die IP-Adresse des entsprechenden IP-Geräts an.

Alarm Identität

Klicken Sie in der Spalte **Priorität** auf eine Zelle, um die Alarmpriorität für den ausgewählten Alarm einzugeben (**100** bedeutet geringe Priorität, **1** hohe Priorität). In der Spalte **Titel** klicken Sie in eine Zelle, um den Titel des Alarms einzugeben, der in BVMS angezeigt werden soll, zum Beispiel in der Alarmliste. In der Spalte **Farbe** klicken Sie in eine Zelle, um ein Dialogfeld zur Auswahl einer Farbe für den Alarm anzuzeigen, der in der Operator Client angezeigt werden soll, zum Beispiel in der Alarmliste.

Alarmfenster

Klicken Sie in einer der Spalten **1-5** in einer Zelle auf ..., um ein Dialogfeld zum Auswählen einer Kamera anzuzeigen.

Sie können eine Kamera nur auswählen, wenn sie in **Karten und Struktur** dem Logischen Baum hinzugefügt wurde.

Die Anzahl der verfügbaren Alarmfenster können Sie im Dialogfeld **Alarmeinstellungen** konfigurieren.

Klicken Sie in der Spalte **Audiodatei** in einer Zelle auf ..., um ein Dialogfeld zum Auswählen einer Audiodatei anzuzeigen, die bei Alarm wiedergegeben werden soll.

Alarmoptionen
Klicken Sie in einer Zelle auf ..., um das Dialogfeld **Alarmoptionen** anzuzeigen.

Siehe
– *Alarmbearbeitung, Seite 39*

24.1 Dialogfeld „Alarmeinstellungen“

Hauptfenster > **Alarme**>

Registerkarte Alarmeinstellungen

Max. Bildfenster pro Alarm:
Geben Sie die maximale Anzahl der bei Alarm anzuzeigenden Alarmfenster ein.
Hinweis: Beim Betrieb eines Enterprise System gilt die höchste maximale Anzahl, die im Online-Betrieb Management Servers konfiguriert ist.

Zeit für Auto-Löschen:
Geben Sie die Zeit in Sekunden ein, nach der ein Alarm automatisch gelöscht wird.
Dies gilt nur für Alarme, für die auf der Seite **Alarm wird nach einer konfigurierten Zeit gelöscht ('Alarmeinstellungen' Dialogfeld)** die Option **Alarme** eingestellt ist.

Mehrreihige-Alarm-Anzeige in Alarm-Bildfensterbereich
Aktivieren Sie das Kontrollkästchen, um die mehrzeilige Alarmanzeige des Alarmfensterbereichs zu aktivieren.

Hinweis!
Für bestehende Alarmkonfigurationen ist die mehrzeilige Alarmanzeige aktiviert, für neue Alarmkonfigurationen ist sie deaktiviert und die Einfachanzeige ist aktiv.

Zeitlimit für Aufzeichnungen, die durch einen Status ausgelöst wurden, festlegen:
Aktivieren Sie das Kontrollkästchen, um eine zeitliche Begrenzung für von einem Status ausgelöste Alarmaufzeichnungen zu aktivieren. Geben Sie die Anzahl der Minuten für die Dauer der Alarmaufzeichnung ein. Die Alarmaufzeichnung hält nach der konfigurierten Dauer automatisch an. Der Benutzer kann eine Dauer zwischen 1 und 1440 Minuten eingeben.
Wenn ein Alarm eine Aufzeichnung mit einem konfigurierten zeitlichen Begrenzung auslöst:
– Wenn der Alarm ausgelöst wird, bevor das Timeout erreicht ist, wird die Aufzeichnung fortgesetzt und das Timeout startet wieder von 0.
– Wenn der Alarm abgebrochen wird, bevor das Timeout erreicht ist, wird die Aufzeichnung bis zum konfigurierten Nachalarm-Timeout fortgesetzt.

Registerkarte Monitorgruppen

Anzeigereihenfolge bei gleicher Alarmpriorität
Wählen Sie den gewünschten Eintrag aus, um Alarme der gleichen Priorität entsprechend ihrer Zeitstempel zu sortieren.

Leeren Bildschirm anzeigen
Klicken Sie darauf, um zu konfigurieren, dass auf einem nicht für die Alarmanzeige verwendeten Monitor nichts angezeigt wird.

Live-Display fortsetzen
Klicken Sie darauf, um zu konfigurieren, dass auf einem nicht für die Alarmanzeige verwendeten Monitor die Live-Anzeige fortgesetzt wird.

Siehe

– *Konfigurieren der Einstellungen aller Alarme, Seite 328*

24.2 Dialogfeld Bildfensterinhalt auswählen

Hauptfenster > **Alarme** > oder > **Spalte Alarmbildfenster** > Klicken Sie auf ... in einer der Spalten **1-5**

Ermöglicht es Ihnen, das Element des Logischen Baums auszuwählen, das bei einem ausgewählten Alarm angezeigt und aufgezeichnet wird (sofern das Element eine Kamera ist).

Hinweis!
Ein im Alarmfenster angezeigter Lageplan wird für die Anzeige optimiert und enthält nur die Ausgangsansicht der originalen Karten-Datei.

Suche nach
Geben Sie Text ein, um ein Element im Logischen Baum zu suchen.

Suche
Klicken Sie darauf, um nach der Kamera mit dem eingegebenen Suchtext in der Beschreibung zu suchen.

Live
Klicken Sie hier, um festzulegen, dass bei Alarm das Live-Bild der Kamera angezeigt wird.

Zeitversetzte Wiedergabe
Klicken Sie hier, um festzulegen, dass die zeitversetzte Wiedergabe der Kamera angezeigt wird. Die Rückspulzeit für zeitversetzte Alarmwiedergabe wird auf der Seite **Bediener Funktionen** konfiguriert (siehe *Seite mit den Bedienereigenschaften, Seite 342*).

Wiedergabe pausieren
Aktivieren Sie das Kontrollkästchen, um die Kamera für zeitversetzte Alarmwiedergabe mit angehaltener zeitversetzter Wiedergabe anzuzeigen. Der Benutzer kann die zeitversetzte Wiedergabe bei Bedarf starten.

Loop-Wiedergabe
Aktivieren Sie das Kontrollkästchen, um die Kamera für zeitversetzte Alarmwiedergabe mit sich wiederholender zeitversetzter Wiedergabe anzuzeigen.
Die Dauer der sich wiederholenden zeitversetzten Wiedergabe im Alarmfenster entspricht der Rückspulzeit zuzüglich der Dauer des Alarmzustands zuzüglich der Rückspulzeit.

Diese Kamera aufzeichnen
Aktivieren Sie das Kontrollkästchen, um die Alarmaufzeichnung für diese Kamera bei Alarm zu aktivieren. Wird ein Alarm ausgelöst, erfolgt die Aufzeichnung dieser Kamera in Alarmaufzeichnungsqualität. Die Aufzeichnungsdauer entspricht der Dauer des Alarmzustands zuzüglich der Vor- und Nachalarmdauer. Diese Einstellung bewirkt eine direkte Änderung der Alarmaufzeichnungseinstellung im Dialogfeld **Alarmoptionen** und umgekehrt.
Hinweis: Wenn für eine Panoramakamera eine voreingestellte Position ausgewählt ist, wird nicht nur dieser Bildausschnitt, sondern die vollständige Kreisansicht gespeichert.

Voreingestellte Panorama-Position
Wenn Sie eine Panoramakamera ausgewählt haben, können Sie eine voreingestellte Kameraposition auswählen. Wenn ein Benutzer des Operator Client diesen Alarm akzeptiert, wird das Alarmbild an der voreingestellten Position in der zugeschnittenen Ansicht angezeigt.
Wenn **<kein Eintrag>** ausgewählt ist, wird das Alarmbild in der Panoramaansicht angezeigt.

Siehe

- *Seite mit den Bedienereigenschaften, Seite 342*
- *Konfigurieren eines Alarms, Seite 327*

24.3 Dialogfeld „Bildfensterinhalt auswählen“ (MG)

Hauptfenster >

Alarme > oder > Spalte **Alarmoptionen** > auf ... klicken > Dialogfeld **Alarmoptionen** > Registerkarte **Monitorgruppe** > in einer der 1-10 Spalten auf ... klicken

Dient zum Auswählen einer Kamera aus dem Logischen Baum. Diese Kamera wird beim ausgewählten Alarm auf dem zugeordneten Monitor angezeigt.

Suche nach

Geben Sie Text ein, um ein Element im Logischen Baum zu suchen.

Suche

Klicken Sie darauf, um nach der Kamera mit dem eingegebenen Suchtext in der Beschreibung zu suchen.

Voreingestellte Panorama-Position

Wenn Sie eine Panoramakamera ausgewählt haben, können Sie eine voreingestellte Kameraposition auswählen. Wenn ein Benutzer des Operator Client diesen Alarm akzeptiert, wird das Alarmbild an der voreingestellten Position in der zugeschnittenen Ansicht angezeigt.

Wenn Sie **<kein Eintrag>** auswählen, zeigt der Decoder das Alarmbild in der Kreisansicht an.

Keine Kamera

Klicken Sie hier, um eine Kamera aus der Spalte „Monitorgruppe“ zu löschen.

Hinweis:

Das Blickfeld einer voreingestellten Panoramakameraposition unterscheidet sich bei Operator oder Configuration Client und Decoder.

Hinweis!

Um konfigurierte voreingestellten Positionen für Panoramakameras verwenden zu können, muss die **Einbauposition** der Panoramakamera **Wand** oder **Decke** sein.

24.4 Dialogfeld Alarmoptionen

Hauptfenster > **Alarme** > oder > **Alarmoptionen** Spalte > ...

Dient zum Konfigurieren der folgenden Alarmeinstellungen:

- Kameras, die bei einem Alarm die Aufzeichnung starten.
- Aktivieren des Schutzes für diese Alarmaufzeichnungen.
- Aktivieren und Konfigurieren abweichender Einstellungen für die Alarmdauer.
- Auslösen von PTZ-Kommandos im Falle eines Alarms.
- Benachrichtigungen, die im Falle eines Alarms gesendet werden.
- Workflow, der bei einem Alarm ausgeführt werden muss.
- Zuweisen von Kameras, die bei Alarm in Monitorgruppen angezeigt werden

Registerkarte Kameras

Nr	Zeigt die auf der Seite **Kameras und Aufzeichnung** festgelegte Kameranummer an.
Name	Zeigt den auf der Seite **Kameras und Aufzeichnung** festgelegten Kameranamen an.
Ort	Zeigt den auf der Seite **Karten und Struktur** konfigurierten Ort an.
Aufzeichnen	Aktivieren Sie ein Kontrollkästchen, um die Alarmaufzeichnung für diese Kamera bei Alarm zu aktivieren. Wird ein Alarm ausgelöst, erfolgt die Aufzeichnung dieser Kamera in Alarmaufzeichnungsqualität. Die Aufzeichnungsdauer entspricht der Dauer des Alarmzustands zuzüglich der Vor- und Nachalarmdauer. Diese Einstellung bewirkt eine direkte Änderung der Alarmaufzeichnungseinstellung im Dialogfeld **Bildfensterinhalt auswählen** und umgekehrt.
Aufzeichnung schützen	Aktivieren Sie ein Kontrollkästchen, um die Alarmaufzeichnung dieser Kamera zu schützen. **Hinweis:** Die geschützten Videodaten werden niemals automatisch von VRM gelöscht. Berücksichtigen Sie, dass zu viele geschützte Blöcke den Speicher füllen können und die Kamera dadurch ggf. nicht mehr aufzeichnet.
Abweichende Alarmdauer-Einstellungen	Das Kontrollkästchen wird automatisch aktiviert, wenn Sie das Kontrollkästchen **Aufzeichnen** aktivieren und die Kamera ANR unterstützt.
AUX-Befehle	Klicken Sie auf eine Zelle, um ein AUX-Kommando auszuwählen, das bei Alarm ausgeführt werden soll. Die Einträge in dieser Liste sind nur für PTZ-Kameras verfügbar.
Voreingestellte Position	Klicken Sie auf eine Zelle, um eine voreingestellte Position auszuwählen, die bei Alarm eingestellt werden soll. Die Einträge in dieser Liste sind nur für PTZ-Kameras verfügbar.

Hinweis: Sie können nicht beides konfigurieren, **AUX-Befehle** und **Voreingestellte Position**, für dieselbe Kamera und denselben Alarm.

Registerkarte Benachrichtigungen

E-Mail	Aktivieren Sie das Kontrollkästchen, um bei Alarm eine E-Mail zu senden.
Server	Wählen Sie einen E-Mail-Server aus.
Empfänger:	Geben Sie die E-Mail-Adresse der Empfänger - durch Kommas getrennt - ein (Beispiel: name@provider.com).
Text:	Geben Sie den Text der Benachrichtigung ein.

Information:	Aktivieren Sie das Kontrollkästchen, um dem Benachrichtigungstext die entsprechenden Informationen hinzuzufügen. **Hinweis:** Für E-Mails wird das Datum der Zeitzone des Management Server verwendet.

Registerkarte Workflow

Nur-Aufzeichnung Alarm	Aktivieren Sie das Kontrollkästchen, damit die Kamera bei diesem Alarm nur aufgezeichnet, nicht aber angezeigt wird. Dieses Kontrollkästchen ist nur verfügbar, wenn das Kontrollkästchen **Aufzeichnen** auf der Registerkarte **Kameras** aktiviert ist.
Alarm wird nach einer konfigurierten Zeit gelöscht ('Alarmeinstellungen' Dialogfeld)	Aktivieren Sie das Kontrollkästchen, damit dieser Alarm automatisch gelöscht wird.
Alarm wird gelöscht, sobald der Ereignisstatus zu Normal zurückwechselt	Aktivieren Sie das Kontrollkästchen, damit dieser Alarm automatisch gelöscht wird, wenn sich der Status des alarmauslösenden Ereignisses ändert. Der Alarm wird nicht automatisch gelöscht, wenn er angenommen und zurückgegeben wurde.
Löschen des Alarmes für die Dauer des alarmauslösenden Zustands verweigern	Aktivieren Sie das Kontrollkästchen, um zu verhindern, dass dieser Alarm gelöscht wird, solange die Alarmursache noch vorhanden ist.
Doppelte Alarme in der Alarmliste unterdrücken	Aktivieren Sie das Kontrollkästchen, um zu verhindern, dass Alarme für denselben Ereignistyp und dasselbe Gerät doppelt in der Alarmliste von BVMS Operator Client auftreten. Solange ein Alarm aktiv ist (im Alarmzustand **Aktiv** oder **Angenommen**), werden keine weiteren Alarme für denselben Ereignistyp und dasselbe Gerät in der Alarmliste angezeigt. **Hinweis:** – Ereignisse werden weiterhin im Logbuch protokolliert. – Bitte beachten Sie, dass alle von diesem Alarm ausgelösten Alarmaktionen (z. B. Start der Alarmaufzeichnung usw.) nicht erneut ausgelöst werden. Nachdem der Alarm gelöscht wurde und für dasselbe Gerät und vom selben Ereignistyp ein neuer Alarm ausgelöst wurde, erscheint der neue Alarm wieder in der Alarmliste und alle für diesen Alarm festgelegten Alarmaktionen werden erneut ausgelöst. – Dieses Kontrollkästchen ist für Person Identification-Alarme bereits aktiviert.
Aktionsplan anzeigen	Aktivieren Sie mit diesem Kontrollkästchen den Workflow, der bei Alarm ausgeführt werden muss.

Ressourcen...	Klicken Sie hier, um das Dialogfeld **Ressourcen-Manager** anzuzeigen. Wählen Sie ein Dokument mit einer Beschreibung des entsprechenden Workflows aus.
Kommentarfeld anzeigen	Aktivieren Sie das Kontrollkästchen, damit bei Alarm ein Kommentarfeld angezeigt wird. Bei Alarm kann der Benutzer Kommentare in dieses Kommentarfeld eingeben.
Workflow für Benutzer erforderlich	Aktivieren Sie das Kontrollkästchen, um den Benutzer zur Ausführung des Workflows zu zwingen. Bei aktiviertem Kontrollkästchen kann der Benutzer den Alarm erst löschen, wenn er einen Kommentar zu dem Alarm eingegeben hat.
Folgendes Client-Skript ausführen, wenn der Alarm angenommen worden ist:	Wählen Sie ein Client-Kommandoskript aus, das automatisch ausgeführt wird, wenn der Benutzer einen Alarm annimmt.

Registerkarte Monitorgruppe

1...10	Klicken Sie in einer nummerierten Spalte auf eine Zelle. Das Dialogfeld **Bildfensterinhalt auswählen** wird angezeigt. Wählen Sie eine Kamera aus dem Logischen Baum aus. Diese Kamera wird bei Alarm auf dem zugeordneten Monitor angezeigt. Wählen Sie voreingestellte Kamerapositionen aus (sofern konfiguriert). Weitere Informationen finden Sie in der Online-Hilfe für das Dialogfeld **Bildfensterinhalt auswählen** (MG).
Tabelle löschen	Klicken Sie hier, um alle Kamerazuordnungen zu Monitorgruppen zu entfernen.
Bildschirmanzeige (OSD) (**OSD**) Einstellungen	
Alarmtitel als OSD	Aktivieren Sie das Kontrollkästchen, damit der Alarmtitel auf den Monitoren als Bildschirmtext angezeigt wird.
Alarmzeit	Aktivieren Sie das Kontrollkästchen, damit die Alarmzeit auf den Monitoren als Bildschirmtext angezeigt wird.
Alarmdatum	Aktivieren Sie das Kontrollkästchen, damit das Alarmdatum auf den Monitoren als Bildschirmtext angezeigt wird.
Alarmkameraname	Aktivieren Sie das Kontrollkästchen, damit der Name der Alarmkamera auf den Monitoren als Bildschirmtext angezeigt wird.
Alarmkameranummer	Aktivieren Sie das Kontrollkästchen, damit die Nummer der Alarmkamera auf den Monitoren als Bildschirmtext angezeigt wird.
Nur erster Monitor	Aktivieren Sie das Kontrollkästchen, damit der Alarmtitel und die Alarmzeit nur auf dem ersten Monitor der Monitorgruppe als Bildschirmtext angezeigt werden.

Registerkarte Abweichende Alarmdauer-Einstellungen
Die Einstellungen auf dieser Registerkarte stehen nur zur Verfügung, wenn ANR für diese Kamera aktiviert ist.

Profileinstellungen verwenden	Klicken Sie, um die Einstellung zu aktivieren. Für diese Kamera werden die Einstellungen für die Vor- und Nachalarmdauer verwendet, die im Dialogfeld **Geplante Aufzeichnungseinstellungen** konfiguriert sind.
Einstellungen überschreiben	Klicken Sie, um die folgenden Einstellungen für die Vor- und Nachalarmdauer zu aktivieren.
Dauer (Voralarm)	Für alle Ereignisse verfügbar.
Dauer (Nachalarm)	Nur für Ereignisse verfügbar.

Registerkarte **Bedrohungsstufe**

Erhöhen Sie die Gefahrenstufe auf	Wählen Sie die Bedrohungsstufe aus, die durch diesen Alarm ausgelöst wird. Wählen Sie den **Bedrohungsstufe zurücksetzen** Eintrag, wenn dieser Alarm eine aktive Gefahrenstufe beenden soll. Der Operator Client melden Sie sich ab, und der Benutzer kann sich erneut anmelden.

Siehe
- *Konfigurieren von Decodern für das On-Screen-Display (OSD), Seite 235*
- *Dialogfeld „Bildfensterinhalt auswählen“ (MG), Seite 318*
- *Alarmaufzeichnung mit Textdaten auslösen, Seite 329*
- *Konfigurieren eines Alarms, Seite 327*
- *Vor- und Nachalarmdauer bei einem Alarm konfigurieren, Seite 328*

24.5 Dialogfeld Ressource auswählen

Hauptfenster > **Alarme** > oder > **Alarmidentitätsspalte** > **Audiodatei** spalte > Klicken ...
Dient zum Auswählen einer Audiodatei, die bei Alarm wiedergegeben werden soll.

Wiedergabe
Klicken Sie darauf, um die ausgewählte Audiodatei wiederzugeben.

Pause
Klicken Sie darauf, um die Wiedergabe der ausgewählten Audiodatei vorübergehend anzuhalten.

Stop
Klicken Sie darauf, um die Wiedergabe der ausgewählten Audiodatei zu stoppen.

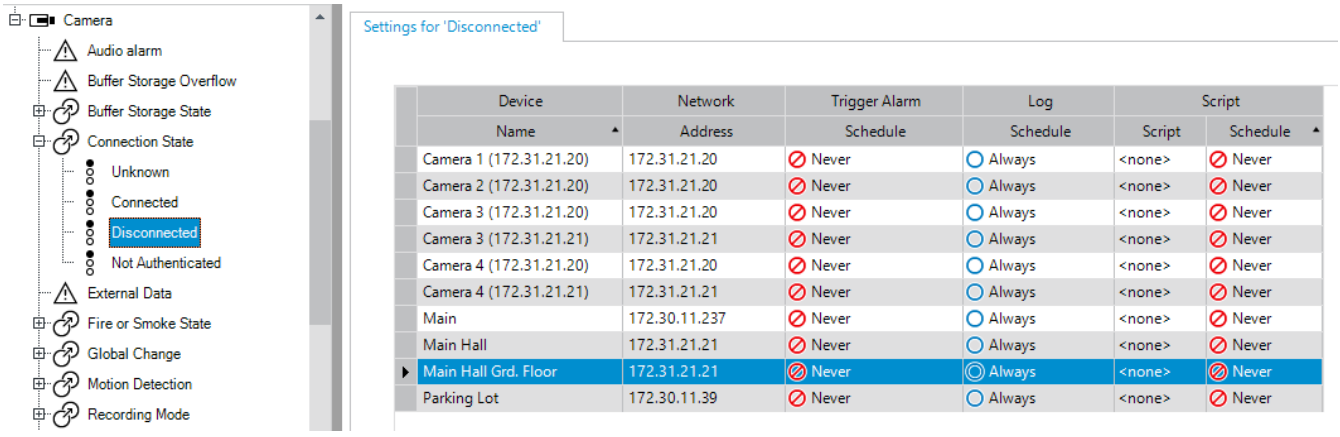
Verwalten...
Klicken Sie hier, um das Dialogfeld **Ressourcen-Manager** anzuzeigen.

Siehe
- *Konfigurieren eines Alarms, Seite 327*
- *Verwalten von Ressourcen-Dateien, Seite 324*

25 Konfigurieren von Ereignissen und Alarmen

Hauptfenster > **Ereignisse**
oder
Hauptfenster > **Alarme**

Dieses Kapitel enthält Informationen zur Konfiguration von Ereignissen und Alarmen in Ihrem System.
Die verfügbaren Ereignisse werden unter den entsprechenden Geräten gruppiert.
Auf der Seite **Ereignisse** konfigurieren Sie, wann ein Ereignis in Ihrem BVMS einen Alarm auslösen, ein Kommandoskript ausführen und protokolliert werden soll.
Beispiel (Teil einer Ereigniskonfigurations-Tabelle):



Dieses Beispiel bedeutet:
Wenn das Videosignal der ausgewählten Kamera verloren geht, wird ein Alarm ausgelöst, das Ereignis protokolliert und kein Skript ausgeführt.
Auf der Seite **Alarme** definieren Sie, wie ein Alarm angezeigt wird und welche Kameras bei Alarm angezeigt und aufgezeichnet werden.
Einige Systemereignisse werden standardmäßig als Alarme konfiguriert.

- Klicken Sie auf , um die Einstellungen zu speichern.
- Klicken Sie auf , um die letzte Einstellung rückgängig zu machen.
- Klicken Sie auf , um die Konfiguration zu aktivieren.

Siehe

- *Registerkarte „Entprelleinstellungen“, Seite 311*
- *Registerkarte „Einstellungen” für die erweiterte Anzeige der Karte, Seite 311*
- *Registerkarte „Einstellungen” für die Ereigniskonfiguration, Seite 312*
- *Dialogfeld Kommandoskript-Editor, Seite 312*
- *Zusammengesetztes Ereignis erzeugen / Dialogfeld Zusammengesetztes Ereignis bearbeiten, Seite 313*
- *Dialogfeld Skriptsprache auswählen, Seite 314*
- *Prioritäten des Dialogfelds „Ereignistyp“ bearbeiten, Seite 314*
- *Dialogfeld Geräte auswählen, Seite 314*
- *Dialogfeld „Textatenaufzeichnung“, Seite 314*
- *Dialogfeld „Alarmeinstellungen“, Seite 316*
- *Dialogfeld Bildfensterinhalt auswählen, Seite 317*
- *Dialogfeld Alarmoptionen, Seite 318*

25.1 Kopieren und Einfügen in Tabellen

Sie können in einer Kameratabelle, Ereigniskonfigurations-Tabelle oder Alarmkonfigurations-Tabelle mit wenigen Mausklicks viele Objekte gleichzeitig konfigurieren.
Ausführliche Informationen finden Sie im *Kopieren und Einfügen in Tabellen, Seite 296*.

25.2 Entfernen einer Tabellenzeile

Hauptfenster > **Alarme**
Sie können nur Tabellenzeilen entfernen, die von Ihnen oder einem anderen Benutzer hinzugefügt wurden, d. h. Sie können duplizierte Ereignisse und Zusammengesetzte Ereignisse löschen.
Zusammengesetzte Ereignisse befinden sich im Ereignisbaum unter **Systemgeräte** > **Zusammengesetzte Ereignisse**.
So entfernen Sie eine Tabellenzeile:

1. Wählen Sie die Zeile aus.
2. Klicken Sie auf .

Siehe

– *Seite Ereignisse, Seite 310*

25.3 Verwalten von Ressourcen-Dateien

Ausführliche Informationen finden Sie im:

– *Verwalten von Ressourcen-Dateien, Seite 265*.

25.4 Konfigurieren eines Ereignisses

Hauptfenster > **Ereignisse**
So konfigurieren Sie ein Ereignis:

1. Wählen Sie im Baum ein Ereignis oder einen Ereignisstatus, zum Beispiel **Systemgeräte** > **Authentifizierung** > **Benutzeranmeldung zurückgewiesen**.
   Die entsprechende Ereigniskonfigurations-Tabelle wird angezeigt.
2. Klicken Sie in der Spalte **Alarm auslösen** – **Zeitplan** auf eine Zelle, und wählen Sie einen Zeitplan aus.
   Der Zeitplan bestimmt, wann der Alarm ausgelöst wird.
   Wählen Sie einen der Aufzeichnungszeitpläne oder Aktionszeitpläne aus, die Sie auf der Seite **Zeitpläne** konfiguriert haben.
3. Klicken Sie in der Spalte **Protokoll** - **Zeitplan** auf eine Zelle, und wählen Sie einen Zeitplan aus.
   Der Zeitplan bestimmt, wann das Ereignis protokolliert wird.
4. Klicken Sie in der Spalte **Skript** - **Skript** auf eine Zelle, und wählen Sie ein entsprechendes Kommandoskript aus.
5. Klicken Sie in der Spalte **Skript** – **Zeitplan** auf eine Zelle, und wählen Sie den entsprechenden Zeitplan aus.
   Der Zeitplan bestimmt, wann das Ereignis den Start des Kommandoskripts auslöst.

Siehe

– *Seite Ereignisse, Seite 310*

25.5 Duplizieren eines Ereignisses

Hauptfenster > **Ereignisse**

Sie können ein Ereignis duplizieren, um verschiedene Alarme für ein bestimmtes Ereignis auszulösen.

So duplizieren Sie ein Ereignis:

1. Wählen Sie im Baum eine Ereignisbedingung aus. Die entsprechende Ereigniskonfigurations-Tabelle wird angezeigt.
2. Wählen Sie eine Tabellenzeile aus.
3. Klicken Sie auf . Unterhalb der ausgewählten Tabellenzeile wird eine neue Zeile eingefügt. Sie verfügt über die Standardeinstellungen.

Siehe

– *Seite Ereignisse, Seite 310*

25.6 Protokollieren von Benutzerereignissen

Hauptfenster > **Ereignisse** > **Systemgeräte** erweitern > **Benutzeraktionen**

Sie können das Protokollierungsverhalten verschiedener Benutzeraktionen für jede verfügbare Benutzergruppe einzeln konfigurieren.

Beispiel:

So protokollieren Sie Benutzerereignisse:

1. Wählen Sie ein Benutzerereignis, um sein Protokollierungsverhalten zu konfigurieren, z. B. **Benutzeranmeldung**.
   Die entsprechende Ereigniskonfigurations-Tabelle wird angezeigt.
   Jede Benutzergruppe wird in der Spalte **Gerät** angezeigt.
2. Sofern verfügbar, klicken Sie in der Spalte **Alarm auslösen** - **Zeitplan** auf eine Zelle, und wählen Sie den passenden Zeitplan.
   Der Zeitplan bestimmt, wann der Alarm ausgelöst wird, der den Benutzer benachrichtigen soll.
   Sie können einen der Aufzeichnungszeitpläne oder Aktionszeitpläne wählen, die Sie im Abschnitt **Zeitpläne** konfiguriert haben.
3. Klicken Sie in der Spalte **Protokoll** - **Zeitplan** auf eine Zelle, und wählen Sie einen Zeitplan aus.
   Der Zeitplan bestimmt, wann das Ereignis ausgelöst wird.
   Im Beispiel wird die Bedieneranmeldung der Admin-Gruppe und der Power-Benutzergruppe nicht protokolliert, während die Bedieneranmeldung der Live-Benutzergruppe während des Zeitplans **Tag** protokolliert wird.

Siehe

– *Seite Ereignisse, Seite 310*

25.7 Konfigurieren von Benutzerereignisschaltflächen

Hauptfenster > **Ereignisse**

Sie können die im Operator Client verfügbaren Benutzerereignisschaltflächen konfigurieren. Sie können konfigurieren, dass eine oder mehrere Benutzerereignisschaltflächen im Operator Client nicht angezeigt werden.

Auf der Seite **Benutzergruppen** wird konfiguriert, dass die Benutzerereignisschaltflächen nur für die betreffende Benutzergruppe im Operator Client verfügbar sind.

So konfigurieren Sie Benutzerereignisschaltflächen:

1. Wählen Sie im Baum **Systemgeräte** > **Operator Client Ereignisschaltflächen** > **Benutzerereignisschaltfläche geklickt** aus.
   Die entsprechende Ereigniskonfigurations-Tabelle wird angezeigt.
2. Wählen Sie eine Benutzerereignisschaltfläche aus, um ihr Verhalten zu konfigurieren.

3. Sofern verfügbar: Klicken Sie in der Spalte **Alarm auslösen** - **Zeitplan** auf eine Zelle und wählen Sie einen Zeitplan aus.
   Der Zeitplan bestimmt, wann der Alarm ausgelöst wird, mit dem der Benutzer benachrichtigt werden soll.
4. Klicken Sie in der Spalte **Protokoll** - **Zeitplan** auf eine Zelle, und wählen Sie einen Zeitplan aus.
   Der Zeitplan bestimmt, wann das Ereignis protokolliert wird.
   Bei der Auswahl von **Nie** ist die Benutzerereignisschaltfläche für alle Benutzergruppen, für die Benutzerereignisschaltflächen freigegeben sind, nicht im Operator Client verfügbar.
5. Klicken Sie in der Spalte **Skript** - **Skript** auf eine Zelle, und wählen Sie ein Kommandoskript aus.
6. Klicken Sie in der Spalte **Skript** - **Zeitplan** auf eine Zelle und wählen Sie einen Zeitplan aus.
   Der Zeitplan bestimmt, wann das Kommandoskript ausgeführt wird.

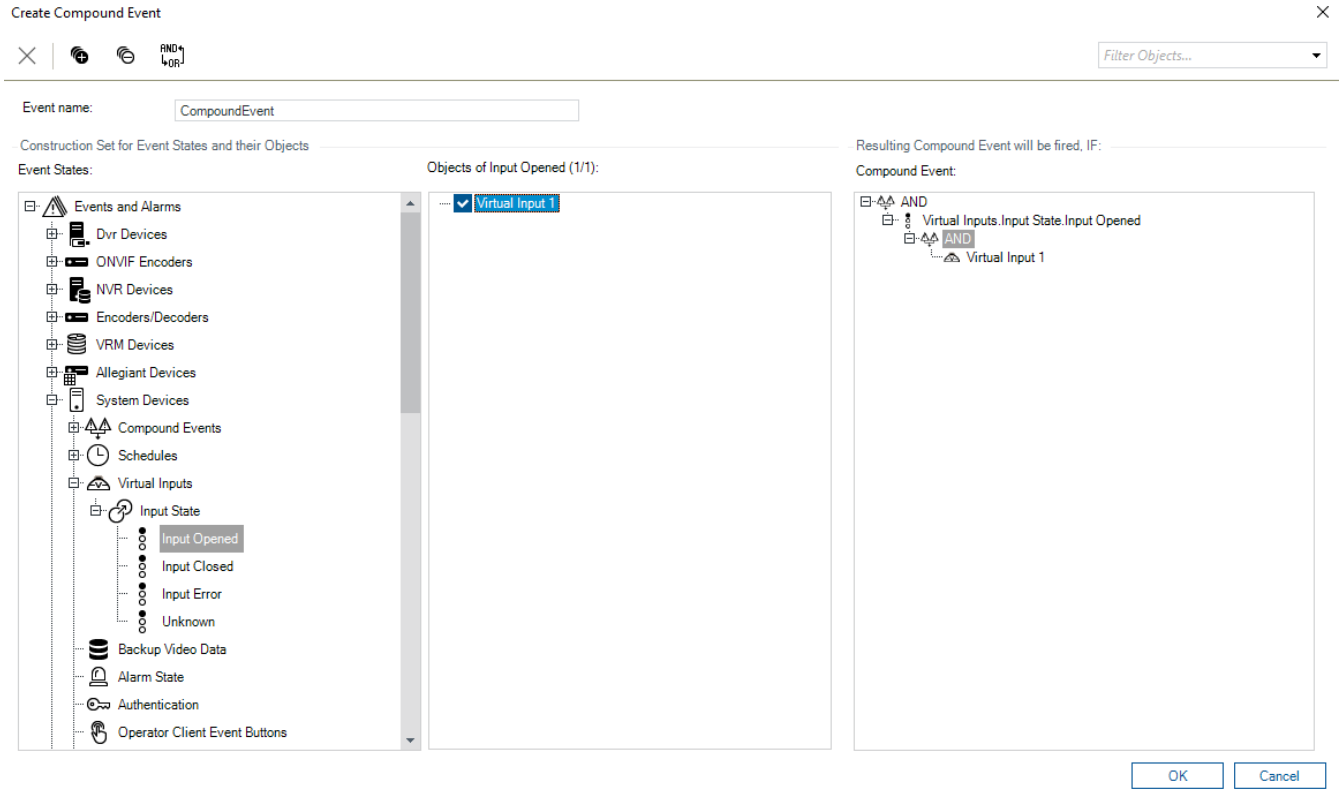
Siehe

– *Seite Ereignisse, Seite 310*

25.8 Erzeugen eines Zusammengesetzten Ereignisses

Hauptfenster > **Ereignisse** >

Sie erstellen ein Zusammengesetztes Ereignis. Sie können nur Statusänderungen und ihre Objekte kombinieren. Objekte können z. B. Zeitpläne oder Geräte sein. Sie können die Statusänderungen und ihre Objekte mit den booleschen Ausdrücken UND und ODER kombinieren.
Beispiel: Sie kombinieren die Verbindungszustände einer IP-Kamera und eines Decoders. Das zusammengesetzte Ereignis soll nur auftreten, wenn die Verbindung beider Geräte unterbrochen wird. In diesem Fall verwenden Sie für die zwei Objekte (IP-Kamera und Decoder) und für die zwei Verbindungszustände **Videosignal verloren** und **Verbindung unterbrochen** den Operator UND.



So erzeugen Sie ein zusammengesetztes Ereignis:

1. Geben Sie im Feld **Ereignisname:** einen Namen für das zusammengesetzte Ereignis ein.
2. Wählen Sie im Feld **Ereigniszustände:** einen Ereignisstatus aus.
   Die verfügbaren Objekte werden im Feld **Objekte:** angezeigt.
3. Wählen Sie im Feld **Objekte:** bei Bedarf das entsprechende Gerät aus.
   Das entsprechende Ereignis und die ausgewählten Geräte werden dem Fenster „Zusammengesetztes Ereignis" hinzugefügt.
4. Klicken Sie im Feld **Zusammengesetzte Ereignisse:** mit der rechten Maustaste auf eine boolesche Operation und ändern Sie diese gegebenenfalls.
   Eine boolesche Operation definiert die Verknüpfung der ihr direkt untergeordneten Elemente.
5. Klicken Sie auf **OK**.
   Das neue zusammengesetzte Ereignis wird der Ereigniskonfigurations-Tabelle hinzugefügt. Es ist im Ereignisbaum unter **Systemgeräte** zu finden.

Siehe

– *Seite Ereignisse, Seite 310*

25.9 Bearbeiten eines Zusammengesetzten Ereignisses

Hauptfenster > **Ereignisse**

Sie können ein zuvor erzeugtes zusammengesetztes Ereignis ändern.

So bearbeiten Sie ein zusammengesetztes Ereignis:

1. Erweitern Sie im Ereignisbaum **Systemgeräte** > **Status des zusammengesetzten Ereignisses** > **Zusammengesetztes Ereignis ist Wahr**.
2. Klicken Sie in der Ereigniskonfigurations-Tabelle in der Spalte **Gerät** mit der rechten Maustaste auf das erforderliche zusammengesetzte Ereignis, und klicken Sie auf **Bearbeiten**.
   Das Dialogfeld **Zusammengesetztes Ereignis bearbeiten** wird angezeigt.
3. Nehmen Sie die erforderlichen Änderungen vor.
4. Klicken Sie auf **OK**.
   Das zusammengesetzte Ereignis wird geändert.

Siehe

– *Seite Ereignisse, Seite 310*

25.10 Konfigurieren eines Alarms

Hauptfenster > **Alarme**

Bevor Sie einen Alarm konfigurieren können, müssen Sie zunächst den Auslöser in **Ereignisse** konfigurieren.

So konfigurieren Sie einen Alarm:

1. Wählen Sie im Baum einen Alarm aus, z. B. **Systemgeräte** > **Authentifizierung** > **Benutzeranmeldung zurückgewiesen**.
   Die entsprechende Alarmkonfigurations-Tabelle wird angezeigt.
2. Klicken Sie in der Spalte **Priorität** in einer Zelle auf ..., um die Alarmpriorität für den ausgewählten Alarm einzugeben (100 bedeutet geringe Priorität, 1 hohe Priorität).
   Klicken Sie in der Spalte **Titel** in einer Zelle auf ..., um den Alarmtitel einzugeben, der im BVMS angezeigt werden soll, beispielsweise in der Alarmliste.
   Klicken Sie in der Spalte **Farbe** in einer Zelle auf ..., um ein Dialogfeld zum Auswählen einer Farbe für den Alarm anzuzeigen, die im Operator Client angezeigt werden soll, beispielsweise in der Alarmliste.

3. Klicken Sie in den Spalten 1-5 in einer Zelle auf ..., um das Dialogfeld **Bildfensterinhalt auswählen** anzuzeigen.
   Nehmen Sie die erforderlichen Einstellungen vor.
4. Klicken Sie in der Spalte **Audiodatei** in einer Zelle auf ..., um ein Dialogfeld zum Auswählen einer Audiodatei anzuzeigen, die bei Alarm wiedergegeben werden soll.
5. Klicken Sie in der Spalte **Alarmoptionen** in einer Zelle auf ..., um das Dialogfeld **Alarmoptionen** anzuzeigen.
6. Nehmen Sie die erforderlichen Einstellungen vor.

Detaillierte Informationen zu den verschiedenen Feldern finden Sie in der Online-Hilfe unter dem entsprechenden Anwendungsfenster.

Siehe
- *Konfigurieren eines Ereignisses, Seite 324*
- *Seite Alarme, Seite 315*
- *Dialogfeld Bildfensterinhalt auswählen, Seite 317*
- *Dialogfeld Alarmoptionen, Seite 318*

25.11 Konfigurieren der Einstellungen aller Alarme

Hauptfenster > **Alarme**

Sie können die folgenden Alarmeinstellungen festlegen, die für diesen Management Server gültig sind:
- Anzahl der Bildfenster je Alarm
- Zeit für Auto-Löschen
- Zeit der manuellen Alarmaufzeichnung
- Mehrzeilige Alarmanzeige im Alarmfensterbereich
- Zeitliche Begrenzung für von einem Status ausgelöste Alarmaufzeichnungen
- Konfiguration des Verhaltens aller Monitorgruppen

So konfigurieren Sie alle Alarme:

1. Klicken Sie auf .
   Das Dialogfeld **Alarmeinstellungen** wird angezeigt.
2. Nehmen Sie die erforderlichen Einstellungen vor.

▸ Klicken Sie auf **OK**.

Detaillierte Informationen zu den verschiedenen Feldern finden Sie in der Online-Hilfe unter dem entsprechenden Anwendungsfenster.

Siehe
- *Dialogfeld „Alarmeinstellungen“, Seite 316*

25.12 Vor- und Nachalarmdauer bei einem Alarm konfigurieren

Zur Konfiguration der Einstellungen für die Dauer des Vor- und Nachalarms benötigen Sie eine Kamera, die ANR unterstützt und bei der die Firmware-Version 5.90 oder höher installiert ist.

Hauptfenster > **Kameras und Aufzeichnung** >

▸ Klicken Sie bei der gewünschten Kamera zur Aktivierung auf **ANR**.

Hauptfenster > **Ereignisse**

▸ Konfigurieren Sie das gewünschte Ereignis für die Kamera, bei der die ANR-Funktion aktiviert ist.

Hauptfenster > **Alarme**

1. Konfigurieren Sie einen Alarm für dieses Ereignis.

2. Wählen Sie bzw.
3. Klicken Sie in der Spalte **Alarmoptionen** auf ...
   Das Dialogfeld **Alarmoptionen** wird angezeigt.
4. Aktivieren Sie in der Spalte **Aufzeichnen** das Kontrollkästchen der Kamera, bei der die ANR-Funktion aktiviert ist, um die Alarmaufzeichnung zu aktivieren.
   Das Kontrollkästchen in der Spalte **Abweichende Alarmdauer-Einstellungen** wird automatisch ausgewählt.
5. Klicken Sie auf die Registerkarte **Abweichende Alarmdauer-Einstellungen**.
6. Konfigurieren Sie die Einstellungen für die Alarmdauer nach Bedarf.

Siehe

– *Dialogfeld Alarmoptionen, Seite 318*

25.13 Alarmaufzeichnung mit Textdaten auslösen

Hauptfenster > **Alarme**

Sie können eine Alarmaufzeichnung mit Textdaten auslösen.

Bevor Sie einen Alarm konfigurieren können, müssen Sie ein Ereignis konfigurieren, das Textdaten enthält.

Beispiel: **Ereignisse** > im Ereignisbaum wählen (es müssen Textdaten vorhanden sein, beispielsweise: **Foyerkartenleser-Geräte** > **Foyerkartenleser** > **Karte abgewiesen**)

Hinweis!

Konfigurieren Sie die Entprellzeit für das ausgewählte Ereignis auf 0.

Damit wird sichergestellt, dass keine Textdaten verloren gehen.

So konfigurieren Sie eine Alarmaufzeichnung:

1. Wählen Sie im Baum einen Alarm aus, z. B. **ATM/POS-Geräte** > **ATM-Eingang** > **Daten-Input**.
   Die entsprechende Alarmkonfigurations-Tabelle wird angezeigt.
2. Nehmen Sie die erforderlichen Einstellungen vor.
3. Klicken Sie in der Spalte **Alarmoptionen** in einer Zelle auf ..., um das Dialogfeld **Alarmoptionen** anzuzeigen.
4. Klicken Sie auf die Registerkarte **Kameras** und aktivieren Sie das Kontrollkästchen **Aufzeichnen**.

Siehe

– *Dialogfeld Alarmoptionen, Seite 318*
– *Dialogfeld „Textatenaufzeichnung“, Seite 314*

25.14 Textdaten einer Daueraufzeichnung hinzufügen

Hauptfenster > **Ereignisse** > im Ereignisbaum **Daten-Input** wählen (es müssen Textdaten vorhanden sein, beispielsweise: **Foyerkartenleser-Geräte** > **Foyerkartenleser** > **Karte abgewiesen**) > Spalte **Aufzeichnung von Textdaten** > ...

Sie können einer Daueraufzeichnung Textdaten hinzufügen.

25.15 Alarmaufzeichnung schützen

Hauptfenster > **Alarme**
Bevor Sie einen Alarm konfigurieren können, müssen Sie unter **Ereignisse** ein Ereignis konfigurieren.

Hinweis!
Wenn Sie die Alarmaufzeichnung einer Kamera schützen, werden die geschützten Videodaten niemals automatisch von VRM gelöscht. Berücksichtigen Sie, dass zu viele geschützte Blöcke den Speicher füllen können und die Kamera dadurch ggf. nicht mehr aufzeichnet. Sie müssen den Schutz der Videodaten manuell im Operator Client aufheben.

So konfigurieren Sie eine Alarmaufzeichnung:

1. Wählen Sie im Baum einen Alarm aus, z. B. **ATM/POS-Geräte** > **ATM-Eingang** > **Daten-Input**. Die entsprechende Alarmkonfigurations-Tabelle wird angezeigt.
2. Nehmen Sie die erforderlichen Einstellungen vor.
3. Klicken Sie in der Spalte **Alarmoptionen** in einer Zelle auf ..., um das Dialogfeld **Alarmoptionen** anzuzeigen.
4. Klicken Sie auf die Registerkarte **Kameras** und aktivieren Sie das Kontrollkästchen **Aufzeichnen**.
1. Aktivieren Sie das Kontrollkästchen **Aufzeichnung schützen**.

Siehe

– *Dialogfeld Alarmoptionen, Seite 318*

25.16 Konfigurieren der blinkenden Hotspots

Hinweis!
Ein blinkender Hotspot kann nur für ein Ereignis oder einen Alarm konfiguriert werden.

Hauptfenster > **Ereignisse**
oder
Hauptfenster > **Alarme**

Für jedes -Ereignis bzw. jeden -Alarm können Sie die Hintergrundfarbe und das Verhalten (blinkend oder nicht blinkend) für Hotspots konfigurieren. Beispielsweise können Sie ein -Ereignis bzw. einen -Alarm eines Geräts konfigurieren, sodass das Gerätesymbol auf einer Karte zu blinken anfängt, wenn sich der Status des Geräts ändert.
Darüber hinaus können Sie die Anzeigepriorität für alle Hotspots konfigurieren. Dies ist erforderlich, wenn verschiedene Ereignisse für dasselbe Gerät auftreten. (1 = höchste Priorität)
Die konfigurierte Farbe gilt für alle Hotspots mit derselben Anzeigepriorität. Sie können Farbe, Verhalten und Priorität bei jedem -Ereignis/-Alarm ändern: Die veränderte Farbe und das Verhalten werden für alle Hotspots aller anderen -Ereignisse/-Alarme mit derselben Priorität verwendet.
Die Konfiguration der Farbzustände auf den Karten ist nur möglich, wenn Sie auf das Kontrollkästchen **Erweiterte Statusanzeige aktiviert (Hot-Spot-Färbung in Karten in abhängig von Status)** oder die **Erweiterte Statusanzeige aktiviert (Hot-Spot-Färbung in Karten in abhängig von Alarm)** Option im **Optionen** Dialogfeld wählen.

So konfigurieren Sie einen blinkenden Hotspot für ein Ereignis:

1. Wählen Sie im Baum einen Ereignisstatus ( ), zum Beispiel **Encoder/Decoder** > **Encoder-Relais** > **Relais-Status** > **Relais offen**.
   Die entsprechende Ereigniskonfigurations-Tabelle wird angezeigt.
2. Klicken Sie auf **Färben von Zuständen auf Karten aktivieren**.
3. Geben Sie im Feld **Anzeigepriorität auf Karte:** die gewünschte Priorität ein.
4. Klicken Sie auf das Feld **Hintergrundfarbe auf Karte:**, um die gewünschte Farbe wählen.
5. Wenn gewünscht, klicken Sie zum Aktivieren auf **Blinken**.

So konfigurieren Sie einen blinkenden Hotspot für einen Alarm:
Siehe Kapitel *Alarm Identität , Seite 315* auf der *Seite Alarme, Seite 315*.

Hinweis!
Der Hotspot blinkt nur, wenn der Alarm in der Alarmliste ist.

Die Gerätesymbole auf einer Karte blinken in derselben Farbe, die für den Alarm oder das Ereignis konfiguriert ist.

Siehe
- *Seite Ereignisse, Seite 310*
- *Dialogfeld „Optionen“ (Menü „Einstellungen“), Seite 121*

25.17 Ereignisse und Alarme für Zutrittskontrollsysteme

Zusätzliche Informationen zu Ereignissen und Alarmen für Zutrittskontrollsysteme.

Ereignis „Zutritt angefordert“
Dieses Ereignis erlaubt einem BVMS Bediener, einer Person über ein Zutrittskontrollsystem manuell Zutritt zu gewähren oder zu verweigern. Sie können Alarmaufzeichnung, Textdatenaufzeichnung oder weitere Informationen für dieses Ereignis konfigurieren.
„Zutritt angefordert“-Ereignisse werden nur an BVMS gesendet, wenn die Option **Zusätzliche Überprüfung** bei jedem Leser des Zutrittskontrollsystems aktiviert ist. In der BVMS Ereigniskonfiguration lösen von Lesern gesendete **Zutritt angefordert**-Ereignisse immer einen Alarm in BVMS aus.

Hinweis!
Es wird empfohlen, die höchste Priorität (1) für die **Zutritt angefordert**-Alarme festzulegen. Dadurch wird sichergestellt, dass die Alarme automatisch als Popup angezeigt werden und die notwendige Aufmerksamkeit des Bedieners erhalten.

25.18 Ereignisse und Alarme zur Person Identification

Hauptfenster > **Ereignisse**
Zusätzliche Informationen über Ereignisse und Alarme für Person Identification.

Unbefugte Person erkannt
Für jede Kamera können Sie konfigurieren, welche Personengruppe zum Zugriff auf einen bestimmten Bereich berechtigt oder nicht berechtigt ist.

Hinweis: Die Konfiguration von nicht autorisierten und autorisierten Personengruppen ist nur möglich, wenn Sie die **Ereigniseinstellungen ändern** Berechtigung haben.

Zum Konfigurieren von Unbefugte Person erkannt

1. Wählen Sie die entsprechende Kamera unter **Video Analytics**.
2. Wählen Sie das **Unbefugte Person erkannt** Ereignis.
3. Öffnen Sie die Registerkarte **Unbefugte Person erkannt**.
4. Klicken Sie auf ... in der **Unbefugt** oder der **Befugt** Zelle.
   Das Dialogfeld **Berechtigung für Kamera** wird angezeigt.
5. Setzen Sie die konfigurierten Personengruppen per Drag-and-Drop in das jeweilige Feld.
6. Klicken Sie auf **OK**.
   Für die jeweilige Kamera sind die konfigurierten Personengruppen nun als autorisiert oder nicht autorisiert eingestellt.

26 Seite Benutzergruppen

Hinweis!
BVMS Viewer bietet nur Grundfunktionen. Erweiterte Funktionen sind in BVMS Professional enthalten. Ausführliche Informationen zu den verschiedenen Versionen von BVMS finden Sie unter www.boschsecurity.com und in der BVMS Schnellauswahlhilfe: BVMS Schnellauswahlhilfe.

Hauptfenster > **Benutzergruppen**
Dient zum Konfigurieren von Benutzergruppen, Enterprise User Groups und Enterprise Access.
Die folgende Benutzergruppe ist standardmäßig verfügbar:

– **Admin Gruppe** (mit einem Admin-Benutzer).

Zuordnung des Identity provider (IdP)
Ermöglicht Ihnen die Zuordnung Ihrer IdP Gruppen zu BVMS Benutzergruppen.
Doppelte Berechtigungsgruppen und Benutzergruppen, die Anmeldepaaren zugewiesen sind, sind von der Zuordnung ausgeschlossen.
Hinweis: Das gleiche IdP Gruppe kann nicht mehrfach abgebildet werden.

Zur Abbildung Ihrer IdP Gruppen zu BVMS Benutzergruppen:

1. Klicken Sie auf **Hinzufügen**.
   Das Dialogfeld **Zugeordnete IdP-Gruppen hinzufügen/bearbeiten** wird angezeigt.
2. Geben Sie den Namen des Anspruchs und den Wert des Anspruchs ein, und klicken Sie dann auf **Hinzufügen**.

   Hinweis: Die ***Anspruchsname** Feld und das ***Anspruchswert** wird zwischen Groß- und Kleinschreibung unterschieden.
3. Klicken Sie auf **OK**, um die Änderungen zu speichern.
4. Wenn ein Benutzer zu mehr als einer zugeordneten Gruppe gehört, legt die Listenreihenfolge die Priorität fest, in der die BVMS Benutzergruppe gewählt wird. Sie können die Reihenfolge mit den Auf- und Ab-Schaltflächen anpassen.
5. Klicken Sie auf , um die Konfiguration zu aktivieren.

Registerkarte Benutzergruppen
Klicken Sie darauf, um die Seiten für die Konfiguration der Rechte der Standardbenutzergruppe anzuzeigen.

Registerkarte Enterprise User Groups
Klicken Sie hier, um die Seiten für die Konfiguration der Berechtigungen einer Enterprise User Group anzuzeigen.

Registerkarte Enterprise Access
Klicken Sie darauf, um die Seiten zum Hinzufügen und Konfigurieren von Enterprise Access anzuzeigen.

Optionen für Benutzer/Benutzergruppen

Symbol	Beschreibung
	Klicken Sie darauf, um einen gewählten Eintrag zu löschen.

Symbol	Beschreibung
	Klicken Sie darauf, um eine neue Gruppe oder ein neues Konto hinzuzufügen.
	Klicken Sie darauf, um der gewählten Benutzergruppe einen neuen Benutzer hinzuzufügen. Ändern Sie gegebenenfalls den Standardbenutzernamen.
	Klicken Sie hier, um eine neue 4-Augen-Gruppe hinzuzufügen.
	Klicken Sie darauf, um ein neues Anmeldungspaar für das 4-Augen-Prinzip hinzuzufügen.
	Zeigt ein Dialogfeld an, um Freigaben von einer ausgewählten Benutzergruppe in eine andere Benutzergruppe zu kopieren.
	Klicken Sie darauf, um die Seiten für die Konfiguration der Benutzereigenschaften anzuzeigen.
	Klicken Sie hier, um die Seite für die Konfiguration der Anmeldungspaareigenschaften anzuzeigen.
	Klicken Sie hier, um die Seiten für die Konfiguration der Berechtigungen dieser 4-Augen-Gruppe anzuzeigen.

Aktivieren von Änderungen beim Benutzernamen und Passwort

Klicken Sie darauf, um Änderungen beim Passwort zu aktivieren.

Klicken Sie darauf, um Änderungen beim Benutzernamen zu aktivieren.

Hinweis!
Änderungen beim Benutzernamen und Passwort werden nach einem Rollback auf eine frühere Konfiguration wiederhergestellt.

Berechtigungen auf einem Enterprise System

Für ein Enterprise System können Sie die folgenden Berechtigungen konfigurieren:

- Bedienberechtigungen für den Operator Client, die die Benutzeroberfläche zur Arbeit mit dem konfigurierten Enterprise System bestimmen (z. B. Benutzeroberfläche für den Alarmmonitor). Verwenden Sie eine Enterprise User Group. Konfigurieren Sie sie auf dem Enterprise Management Server.
- Geräteberechtigungen, die für die Arbeit mit einem Enterprise Management Server zur Verfügung stehen sollen, sind auf jedem Management Server definiert. Verwenden Sie Enterprise Accounts. Konfigurieren Sie es auf jedem Management Server.

Berechtigungen auf einem einzelnen Management Server

Für die Verwaltung des Zugangs zu einem der Management Servers verwenden Sie die Standardbenutzergruppe. Sie können alle Berechtigungen auf diesem Management Server in dieser Benutzergruppe konfigurieren.

Sie können 4-Augen-Gruppen für Standardbenutzergruppen und Enterprise User Groups konfigurieren.

Typ	Enthält	Verfügbare Konfigurationseinstellungen	Wo wird konfiguriert?
Benutzergruppe	Benutzer	– Bedien- und Geräteberechtigungen	– Management Server
Enterprise User Group	Benutzer	– Bedienberechtigungen – Je Management Server: Name der entsprechenden Enterprise Access Accounts mit Zugangsdaten für die Anmeldung	– Enterprise Management Server
Enterprise Account	-	– Geräteberechtigungen – Kontoschlüssel	– Management Server
4-Augen-Benutzergruppe	Benutzergruppen	– Siehe Benutzergruppen	– Siehe Benutzergruppen
Enterprise 4-Augen-Prinzip	Enterprise User Groups	– Siehe Enterprise User Groups	– Siehe Enterprise User Groups

Um nach Elementen zu suchen:

- Tippen Sie im Suchfeld eine Zeichenfolge ein und drücken Sie auf den Schlüssel ENTER, um die angezeigten Elemente zu filtern.
  Nur Elemente mit der Zeichenfolge und ihre übergeordneten Elemente (nur in Bäumen) werden angezeigt. Die Anzahl der gefilterten Elemente und die gesamte Anzahl der Elemente wird angegeben.

Hinweis: Setzen Sie Zeichenfolgen zwischen doppelte Anführungszeichen, um genaue Treffer zu erhalten. Beispielsweise filtert "Camera 1" genau die Kameras mit diesem Namen, jedoch nicht camera 201.

26.1 Seite Eigenschaften der Benutzergruppen

Hauptfenster> **Benutzergruppen** > Registerkarte **Benutzergruppen** > > Registerkarte **Bedienberechtigungen** > Registerkarte **Eigenschaften der Benutzergruppen**
oder

Hauptfenster> **Benutzergruppen** > Registerkarte **Enterprise User Groups** > > Registerkarte **Bedienberechtigungen** > Registerkarte **Eigenschaften der Benutzergruppen**
Dient zum Konfigurieren der folgenden Einstellungen für die ausgewählte Benutzergruppe:

– Zeitplan für Anmeldung
– Auswahl einer zugeordneten LDAP-Benutzergruppe

Eigenschaften der Benutzergruppen

Beschreibung:
Geben Sie eine aussagekräftige Beschreibung für die Benutzergruppe ein.

Sprache
Sprache des Operator Client wählen.

Zeitplan für Anmeldung
Wählen Sie einen Aktions- oder Aufzeichnungszeitplan aus. Die Benutzer der ausgewählten Gruppe können sich nur zu den in diesem Zeitplan definierten Zeiten beim System anmelden.

LDAP-Eigenschaften

Suche nach Gruppen
Klicken Sie hier, um die verfügbaren zugeordneten LDAP-Gruppen in der Liste **Zugeordnete LDAP-Gruppe** anzuzeigen. Zur Auswahl einer zugeordneten LDAP-Gruppe müssen Sie im Dialogfeld **LDAP Server-Einstellungen** die entsprechenden Einstellungen vornehmen.

Zugeordnete LDAP-Gruppe
Wählen Sie eine LDAP-Gruppe in der Liste **Zugeordnete LDAP-Gruppe** aus, die Sie für Ihr System verwenden möchten.

Siehe
- *Auswählen einer zugeordneten LDAP-Gruppe, Seite 363*
- *Zuordnen einer LDAP-Gruppe, Seite 118*
- *Festlegen eines Freigabezeitplans für Benutzeranmeldungen, Seite 363*

26.2 Seite Benutzereigenschaften

Hauptfenster > **Benutzergruppen** > **Benutzergruppen** Registerkarte >
oder

Hauptfenster > **Benutzergruppen** > Registerkarte **Enterprise User Groups** > >
Dient zum Konfigurieren eines neuen Benutzers in einer Standardbenutzergruppe oder Enterprise User Group.
Wenn Sie das Passwort für einen Benutzer ändern oder einen Benutzer löschen, während er angemeldet ist, kann dieser Benutzer auch nach der Änderung oder Löschung noch mit dem Operator Client arbeiten. Wenn nach der Änderung oder dem Löschen des Passworts die Verbindung zum Management Server unterbrochen ist (z. B. nach der Aktivierung der Konfiguration), kann sich der Benutzer automatisch ohne Abmeldung/Anmeldung beim Operator Client erneut wieder mit dem Management Server verbinden.

Konto ist aktiviert
Aktivieren Sie das Kontrollkästchen, um ein Benutzerkonto zu aktivieren.
Hinweis: Jedes neue Benutzerkonto ist standardmäßig deaktiviert. Sie müssen zunächst ein Passwort setzen und dann das Benutzerkonto aktivieren.

Vollständiger Name
Geben Sie den vollständigen Namen des Benutzers ein.

Beschreibung
Geben Sie eine aussagekräftige Beschreibung für den Benutzer ein.

Benutzer muss Passwort bei nächster Anmeldung ändern
Aktivieren Sie das Kontrollkästchen, um Benutzer zum Festlegen eines neuen Passworts bei der nächsten Anmeldung zu zwingen.

Neues Passwort eingeben
Geben Sie das Passwort für den neuen Benutzer ein.

Passwort bestätigen
Geben Sie das neue Passwort erneut ein.

Hinweis!
Um die Änderungen in diesem Dialog zu aktivieren, klicken Sie auf .

Hinweis!
Es wird dringend empfohlen, ein bestimmtes Passwort für alle neuen Benutzer zuzuweisen und diese bei der Anmeldung zum Ändern ihres Passworts anzuhalten.

Hinweis!
Kunden von Web Client, Bosch iOS App und SDK Die Clients können das Passwort bei der Anmeldung nicht ändern.

Übernehmen
Klicken Sie darauf, um die Einstellungen zu übernehmen.

Klicken Sie auf , um das Passwort zu aktivieren.

Zusatzinformationen
Nach der Aktualisierung auf BVMS 9.0.0.x sind die folgenden **Benutzereigenschaften**-Einstellungen festgelegt:
- **Konto ist aktiviert** ist festgelegt.
- **Benutzer muss Passwort bei nächster Anmeldung ändern** ist nicht festgelegt.

26.3 Seite Eigenschaften des Anmeldungspaares

Hauptfenster > **Benutzergruppen** > Registerkarte **Benutzergruppen** > **Neue 4-Augen-Gruppe** >

oder

Hauptfenster > **Benutzergruppen** > Registerkarte **Enterprise User Groups** > **Neue Enterprise 4-Augen-Gruppe** >

Dient zum Ändern zweier Benutzergruppen in eine 4-Augen-Gruppe. Die Benutzer der ersten Benutzergruppe sind die Benutzer, die sich im ersten Anmeldedialogfeld anmelden müssen. Die Benutzer der zweiten Benutzergruppe bestätigen die Anmeldung.

Benutzergruppe auswählen
Wählen Sie in jeder Liste eine Benutzergruppe aus.

4-Augen-Prinzip erforderlich
Aktivieren Sie das Kontrollkästchen, damit sich ein Benutzer nur zusammen mit einem Benutzer der zweiten Benutzergruppe anmelden kann.

Hinweis!
Benutzer, die Mitglieder einer Gruppe mit doppelter Berechtigung sind, können sich nicht bei Operator Client mit Single Sign-On.

Siehe
– *Hinzufügen eines Anmeldungspaars zu einer 4-Augen-Gruppe, Seite 361*

26.4 Seite Kamerafreigaben

Hinweis!
BVMS Viewer bietet nur Grundfunktionen. Erweiterte Funktionen sind in BVMS Professional enthalten. Ausführliche Informationen zu den verschiedenen Versionen von BVMS finden Sie unter www.boschsecurity.com und in der BVMS Schnellauswahlhilfe: BVMS Schnellauswahlhilfe.

Hauptfenster> **Benutzergruppen** > Registerkarte **Benutzergruppen** > > Registerkarte **Geräteberechtigungen** > Registerkarte **Kameraberechtigungen**
oder

Hauptfenster> **Benutzergruppen** > Registerkarte **Enterprise Access** > > Registerkarte **Geräteberechtigungen** > Registerkarte **Kameraberechtigungen**

Dient zum Konfigurieren der Zugriffsrechte auf die Funktionen einer ausgewählten Kamera oder Kameragruppe für die ausgewählte Benutzergruppe.
Werden neue Komponenten hinzugefügt, müssen die Kameraberechtigungen anschließend konfiguriert werden.
Den Zugriff auf eine Kamera können Sie auf der Seite **Kamera** entziehen.

Kamera
Zeigt den auf der Seite **Kameras und Aufzeichnung** festgelegten Kameranamen an.

Ort
Zeigt den auf der Seite **Karten und Struktur** konfigurierten Ort der Kamera an.

Zugriff
Aktivieren Sie ein Kontrollkästchen, um den Zugriff auf diese Kamera freizugeben.

Live Video
Aktivieren Sie ein Kontrollkästchen, um die Verwendung von Live Video freizugeben.

Live Audio
Aktivieren Sie ein Kontrollkästchen, um die Verwendung von Live Audio freizugeben.

Manuelle Aufzeichnung
Aktivieren Sie ein Kontrollkästchen, um die manuelle Aufzeichnung (Alarmaufzeichnung) freizugeben. Sie können dieses Kontrollkästchen nur aktivieren oder deaktivieren, wenn die manuelle Alarmaufzeichnung auf der Seite **Bediener Funktionen** freigegeben ist.

Video-Playback
Aktivieren Sie ein Kontrollkästchen, um die Verwendung der Video-Wiedergabe freizugeben.
Sie können dieses Kontrollkästchen nur aktivieren oder deaktivieren, wenn die Wiedergabe auf der Seite **Bediener Funktionen** freigegeben ist.

Audio-Playback
Aktivieren Sie ein Kontrollkästchen, um die Verwendung der Audio-Wiedergabe freizugeben.
Sie können dieses Kontrollkästchen nur aktivieren oder deaktivieren, wenn die Wiedergabe auf der Seite **Bediener Funktionen** freigegeben ist.

Textdaten
Aktivieren Sie ein Kontrollkästchen, um die Anzeige von Textdaten freizugeben.
Sie können dieses Kontrollkästchen nur aktivieren oder deaktivieren, wenn die Anzeige von Textdaten auf der Seite **Bediener Funktionen** freigegeben ist.

Export
Aktivieren Sie ein Kontrollkästchen, um den Export von Videodaten freizugeben.
Sie können dieses Kontrollkästchen nur aktivieren oder deaktivieren, wenn der Export von Videodaten auf der Seite **Bediener Funktionen** freigegeben ist.

PTZ/ROI
Aktivieren Sie ein Kontrollkästchen, um die Verwendung der PTZ-Steuerung oder der ROI dieser Kamera zu erlauben.
Sie können dieses Kontrollkästchen nur aktivieren oder deaktivieren, wenn die PTZ-Steuerung oder die ROI-Funktion einer Kamera auf der Seite **Bediener Funktionen** freigegeben ist. Darüber hinaus müssen Sie PTZ oder ROI in der Kameratabelle konfigurieren.

Aux
Aktivieren Sie ein Kontrollkästchen, um die Ausführung von AUX-Kommandos freizugeben.
Sie können dieses Kontrollkästchen nur aktivieren oder deaktivieren, wenn die PTZ-Steuerung einer Kamera auf der Seite **Bediener Funktionen** freigegeben ist.

Voreingestellte Positionen setzen
Aktivieren Sie ein Kontrollkästchen, um dem Benutzer die Festlegung voreingestellter Positionen für diese PTZ-Kamera zu erlauben.
Sie können ebenfalls Vorpositionen für die Zielregion-Funktion „ROI“ festlegen, falls diese aktiviert und autorisiert ist.
Sie können dieses Kontrollkästchen nur aktivieren oder deaktivieren, wenn die PTZ-Steuerung einer Kamera auf der Seite **Bediener Funktionen** freigegeben ist.

Referenzbild
Aktivieren Sie das Kontrollkästchen, um die Aktualisierung des Referenzbilds dieser Kamera zu ermöglichen.

Privacy overlay
Aktivieren Sie ein Kontrollkästchen, um Privacy overlay für diese Kamera im Live- und Wiedergabemodus zu aktivieren.

26.5 Seite „Prioritäten für Steuerungen“

Hauptfenster > **Benutzergruppen** > Registerkarte **Benutzergruppen** > > Registerkarte **Geräteberechtigungen** > Registerkarte **Prioritäten für Steuerungen**
oder

Hauptfenster > **Benutzergruppen** > Registerkarte **Enterprise Access** > > Registerkarte **Geräteberechtigungen** > Registerkarte **Prioritäten für Steuerungen**

Prioritäten für Steuerungen
Bewegen Sie den entsprechenden Schieberegler nach rechts, um die Priorität für die Übernahme von PTZ-Kamerasteuerungen und Bosch Allegiant Trunklines zu verringern. Ein Benutzer mit hoher Priorität kann die PTZ-Kamerasteuerungen oder die Steuerung einer Trunkline für Benutzer mit niedrigeren Prioritäten sperren. Der Timeout zum Sperren der PTZ-Kamerasteuerung wird im Feld **Timeout [min]** eingestellt. Die Standardeinstellung ist 1 Minute.

Timeout [min]
Geben Sie den Zeitraum in Minuten ein.

Siehe
– *Konfigurieren verschiedener Prioritäten, Seite 365*

26.6 Dialogfeld Freigaben für Benutzergruppen kopieren

Hauptfenster > **Benutzergruppen** > Registerkarte **Benutzergruppen** > >
oder

Hauptfenster > **Benutzergruppen** > Registerkarte **Enterprise User Groups** > >
Dient zum Wählen der Berechtigungen für eine Benutzergruppe und zum Kopieren dieser Berechtigungen in die gewählten Benutzergruppen.

Kopieren von:
Zeigt die ausgewählte Benutzergruppe an. Ihre Berechtigungen werden in eine andere Benutzergruppe kopiert.

Einstellungen zum Kopieren
Aktivieren Sie ein Kontrollkästchen, um die gewünschten Berechtigungen der Benutzergruppen für den Kopiervorgang auszuwählen.

Kopieren nach:
Aktivieren Sie ein Kontrollkästchen, um die Benutzergruppe festzulegen, in die die ausgewählten Berechtigungen der Benutzergruppen kopiert werden sollen.

Siehe
– *Kopieren von Freigaben für Benutzergruppen, Seite 368*

26.7 Seite Decoder-Freigaben

Hauptfenster> **Benutzergruppen** > Registerkarte **Benutzergruppen** > > Registerkarte **Geräteberechtigungen** > Registerkarte **Decoderberechtigungen**
oder

Hauptfenster > **Benutzergruppen** > Registerkarte **Enterprise Access** > > Registerkarte **Geräteberechtigungen** > Registerkarte **Decoderberechtigungen**
Dient zum Konfigurieren der Decoder, auf die die Benutzer dieser Gruppe Zugriff haben.

Decoder
Zeigt die verfügbaren Decoder an.
Klicken Sie auf das Kontrollkästchen, um der Benutzergruppe Zugriff auf diesen Decoder zu gewähren.

Monitorgruppe
Aktivieren Sie das Kontrollkästchen, um den Benutzern der ausgewählten Benutzergruppe Zugriff auf diese Monitorgruppe zu gewähren.

26.8 Seite Ereignisse und Alarme

Hauptfenster> **Benutzergruppen** > Registerkarte **Benutzergruppen** > > Registerkarte **Geräteberechtigungen** > Registerkarte **Ereignisse und Alarme**
oder

Hauptfenster > **Benutzergruppen** > Registerkarte **Enterprise Access** > > Registerkarte **Geräteberechtigungen** > Registerkarte **Ereignisse und Alarme**
Dient zum Konfigurieren der Berechtigungen für den Ereignisbaum, z. B. legen Sie die Ereignisse fest, die die Benutzergruppe verwenden bzw. nicht verwenden darf.
Für die Standardbenutzergruppen können diese Einstellungen nicht geändert werden.
Für jedes Ereignis gibt es mindestens ein Gerät. Beispiele: Die Geräte für das Ereignis **Videosignalverlust** sind die verfügbaren Kameras. Das entsprechende Gerät für ein Ereignis wie **Sicherung beendet** ist die **Zeitgesteuerte Sicherung**. Bei dem Gerät kann es sich also auch um einen Software-Prozess handeln.

1. Erweitern Sie ein Baumelement, und klicken Sie zum Aktivieren der Ereignisse auf die entsprechenden Kontrollkästchen. Aktivieren Sie in der Spalte **Zugriff** das Kontrollkästchen eines Geräts, um die Ereignisse dieses verfügbaren Geräts zu aktivieren. Der Zugriff auf die Geräte wird auf der Seite **Kamera** und auf der Seite **Kameraberechtigungen** konfiguriert.
2. Mit dem Kontrollkästchen **Ereignisse und Alarme** können Sie sämtliche Ereignisse in einem einzigen Schritt aktivieren bzw. deaktivieren.

26.9 Seite „Zugangsberechtigungen“

Hauptfenster> **Benutzergruppen** > Registerkarte **Enterprise Access** > > Registerkarte **Geräteberechtigungen** > Registerkarte **Anmeldeinformationen**
Konfigurieren Sie die Anmeldedaten eines Enterprise Accounts auf einem Management Server.
Sie können den Enterprise Access auf jedem Management Server konfigurieren, der Ihrem Enterprise System angehört. Anhand dieser Berechtigung erteilt der Enterprise Management Server den Geräten dieses Management Servers Zugriff auf den Operator Client, der sich als Benutzer einer Enterprise User Group anmeldet.

Beschreibung:
Geben Sie eine Beschreibung für den gewünschten Enterprise Account ein.
Sichere Schlüssel Richtlinie
Das Kontrollkästchen **Sichere Schlüssel Richtlinie** ist bereits für alle neu erstellten Benutzergruppen aktiviert.
Es wird dringend empfohlen, diese Einstellung beizubehalten, um Ihren Computer besser vor unbefugtem Zugriff zu schützen.
Es gelten die folgenden Regeln:

- Mindestlänge des Schlüssels gemäß den Angaben auf der Seite **Kontorichtlinien** für die entsprechende Benutzergruppe.
- Verwenden Sie keinen der vorher verwendeten Schlüssel.
- Verwenden Sie mindestens einen Großbuchstaben (A bis Z).
- Verwenden Sie mindestens eine Ziffer (0 bis 9).

– Verwenden Sie mindestens ein Sonderzeichen (z. B.: ! $ # %).

Neuen Schlüssel eingeben: / Schlüssel bestätigen:
Geben Sie den Schlüssel für diesen Management Server ein und bestätigen Sie ihn.

Siehe
– *Erstellen eines Enterprise Accounts, Seite 359*

26.10 Seite Logischer Baum

Hauptfenster > **Benutzergruppen** > Registerkarte **Benutzergruppen** > > Registerkarte **Geräteberechtigungen** > Registerkarte **Logischer Baum**
oder

Hauptfenster > **Benutzergruppen** > Registerkarte **Enterprise Access** > > Registerkarte **Geräteberechtigungen** > Registerkarte **Logischer Baum**
Dient zum Konfigurieren des Logischen Baums für die einzelnen Benutzergruppen.
So konfigurieren Sie Berechtigungen:

- Aktivieren oder deaktivieren Sie die Kontrollkästchen nach Bedarf.
  Durch die Auswahl eines Elements unter einem Knoten wird der Knoten automatisch ausgewählt.
  Durch die Auswahl eines Knotens werden alle untergeordneten Elemente automatisch ausgewählt.

Kamera
Aktivieren Sie ein Kontrollkästchen, um den Benutzern der ausgewählten Benutzergruppe Zugriff auf die entsprechenden Geräte zu gewähren.
Den Zugriff auf eine Kamera können Sie auf der Seite **Kameraberechtigungen** entziehen.

Monitorgruppe
Aktivieren Sie das Kontrollkästchen, um den Benutzern der ausgewählten Benutzergruppe Zugriff auf diese Monitorgruppe zu gewähren.

Siehe
– *Konfigurieren von Geräteberechtigungen, Seite 364*

26.11 Seite mit den Bedienereigenschaften

Hauptfenster> **Benutzergruppen** > Registerkarte **Benutzergruppen** > > Registerkarte **Bedienberechtigungen** > Registerkarte **Bediener Funktionen**
oder

Hauptfenster> **Benutzergruppen** > Registerkarte **Enterprise User Groups** > > Registerkarte **Bedienberechtigungen** > Registerkarte **Bediener Funktionen**

Dient zum Konfigurieren verschiedener Berechtigungen für die ausgewählte Benutzergruppe.

Steuerung von PTZ-Kameras
Aktivieren Sie das Kontrollkästchen, um die Steuerung einer Kamera freizugeben.
Seite **Prioritäten für Steuerungen**: Im Feld **Prioritäten für Steuerungen** können Sie die Priorität für die Übernahme der Steuerung einer Kamera einstellen.

Allegiant-Trunklines
Aktivieren Sie das Kontrollkästchen, um den Zugriff auf Bosch Allegiant Trunklines freizugeben.
Seite **Prioritäten für Steuerungen**: Im Feld **Prioritäten für Steuerungen** können Sie die Priorität für die Übernahme von Bosch Allegiant Trunklines einstellen.

Drucken und Speichern von Video
Aktivieren Sie das Kontrollkästchen, um das Drucken und Speichern von Videodaten, Karten und Dokumenten zuzulassen.

Alarmanzeige
Aktivieren Sie das Kontrollkästchen, um die Alarmanzeige freizugeben. Wenn Sie diese Option aktivieren, wird gleichzeitig die Option **Alarmverarbeitung** deaktiviert.

Alarmverarbeitung
Aktivieren Sie das Kontrollkästchen, um die Alarmverarbeitung freizugeben.

Windows Bildschirmschoner für eingehende Alarme unterbrechen
Aktivieren Sie das Kontrollkästchen, damit ein eingehender Alarm auch bei aktivem Bildschirmschoner angezeigt wird. Wenn zur Unterbrechung des Bildschirmschoners Benutzername und Passwort erforderlich sind, ist diese Einstellung wirkungslos.

Videoanalyse aktivieren bzw. deaktivieren
Aktivieren Sie das Kontrollkästchen, damit die Benutzer der ausgewählten Benutzergruppe die Videoanalyse aktivieren bzw. deaktivieren können.

Playback
Aktivieren Sie das Kontrollkästchen, um verschiedene Wiedergabefunktionen zu aktivieren.

Video exportieren
Aktivieren Sie das Kontrollkästchen, um den Export von Videodaten zuzulassen.

In nicht-natives Format exportieren
Aktivieren Sie das Kontrollkästchen, um den Export von Videodaten in ein nicht natives Format freizugeben.

Video schützen
Aktivieren Sie das Kontrollkästchen, um den Schutz von Videodaten freizugeben.

Videoschutz aufheben
Aktivieren Sie das Kontrollkästchen, um den Schutz und das Aufheben des Schutzes der Videodaten zu ermöglichen.

Video sperren (gesperrtes Video kann nur von Benutzern mit der entsprechenden Berechtigung gesehen werden)
Aktivieren Sie das Kontrollkästchen, um die Beschränkung von Videodaten zuzulassen.

Videosperrung aufheben
Wählen Sie das Kontrollkästchen aus, um eine Beschränkung und Freigabe der Videodaten zu ermöglichen.

Hinweis!
VRM
Bei Bedarf können Sie die Benutzerberechtigungen für die Beschränkung und Freigabe der Videodaten manuell in BVMS konfigurieren.
Nur ein Benutzer mit der Berechtigung **Video sperren (gesperrtes Video kann nur von Benutzern mit der entsprechenden Berechtigung gesehen werden)** kann ein eingeschränktes Video auf der Timeline von Operator Client anzeigen. Andernfalls wird beim eingeschränkten Zeitraum **Keine Aufzeichnung** angezeigt.

Hinweis!
DIVAR AN
Bei Bedarf können Sie die Benutzerberechtigungen für die Beschränkung und Freigabe der Videodaten manuell auf Ihrem DIVAR AN Gerät konfigurieren. Erstellen Sie einen Benutzer in BVMS mit denselben Anmeldeinformationen und konfigurieren Sie die Berechtigungen für die Beschränkungen und Freigaben der Videodaten entsprechend.
Die Anzeige von beschränkten Videos wird dabei nicht beeinflusst und muss separat auf dem DIVAR AN Gerät konfiguriert werden.

Aufzeichnung löschen
Aktivieren Sie das Kontrollkästchen, um das Löschen von Videodaten freizugeben.

Zugriff auf Video, die in Zeitbereichen aufgenommen wurden, in denen die Benutzergruppe sich nicht anmelden durfte
Aktivieren Sie das Kontrollkästchen, um den Zugriff auf die beschriebenen Videodaten freizugeben.

Logbuchzugriff
Aktivieren Sie das Kontrollkästchen, um den Zugriff auf das Logbuch freizugeben.

Textdaten aus den Logbucheinträgen entfernen (um personenbezogene Daten zu entfernen)
Aktivieren Sie das Kontrollkästchen, um das Löschen von Textdaten aus Logbucheinträgen zu ermöglichen.

Benutzerereignisschaltflächen
Aktivieren Sie das Kontrollkästchen, um Benutzerereignisschaltflächen im Operator Client freizugeben.

Operator Client schließen
Aktivieren Sie das Kontrollkästchen, um das Schließen des Operator Client freizugeben.

Operator Client minimieren
Aktivieren Sie das Kontrollkästchen, um das Minimieren des Operator Client freizugeben.

Audio Intercom
Aktivieren Sie das Kontrollkästchen, um dem Benutzer zu erlauben, über die Lautsprecher eines Encoders zu sprechen, der mit einem Audioeingang und -ausgang ausgestattet ist.

Manuelle Alarmaufzeichnung
Aktivieren Sie das Kontrollkästchen, um die manuelle Alarmaufzeichnung freizugeben.

Referenzbildabgleich
Aktivieren Sie das Kontrollkästchen, um die Aktualisierung des Referenzbilds im Operator Client freizugeben.

Bereichsauswahl für Referenzbild
Aktivieren Sie das Kontrollkästchen, damit der Bereich des Kamerabilds zum Aktualisieren des Referenzbilds in Operator Client ausgewählt werden kann.

Passwort ändern
Aktivieren Sie das Kontrollkästchen, um einen Benutzer von Operator Client zu ermöglichen, das Kennwort für die Anmeldung zu ändern.

Bereiche der Einbruchmeldezentrale scharfschalten
Aktivieren Sie das Kontrollkästchen, um einem Benutzer des Operator Client zu erlauben, Bereiche, die in einer Einbruchmeldezentrale Ihrer BVMS Konfiguration konfiguriert sind, scharfzuschalten.

Scharfschalten der Einbruchmeldezentralenbereiche erzwingen
Durch die Aktivierung des Kontrollkästchens erlauben Sie einem Benutzer des Operator Client das Scharfschalten von Bereichen durchzusetzen, die in einer Einbruchmeldezentrale konfiguriert sind, die wiederum Teil Ihrer BVMS Konfiguration ist.

Bereiche der Einbruchmeldezentrale unscharfschalten
Durch die Aktivierung des Kontrollkästchens erlauben Sie einem Benutzer des Operator Client, Bereiche unscharfzuschalten, die in einer Einbruchmeldezentrale konfiguriert sind, die wiederum Teil Ihrer BVMS Konfiguration ist.

Signalgeber stummschalten für Bereiche der Einbruchmeldezentrale
Aktivieren Sie das Kontrollkästchen, um einem Benutzer des Operator Client das Ausschalten der Alarmsirenen von Bereichen zu erlauben, die in einer Einbruchmeldezentrale konfiguriert sind, die wiederum Teil Ihrer BVMS Konfiguration ist.

Melder einer Einbruchmeldezetrale umgehen
Aktivieren Sie das Kontrollkästchen, um einem Benutzer des Operator Client zu erlauben, den Status eines Melders zu ändern, der in einer Einbruchmeldezentrale zum **Melder umgangen**-Status konfiguriert wurde. Ein umgangener Melder kann keinen Alarm senden. Wenn der Status zurück in **Melder-Umgehung aufgehoben** geändert wird, kann ein anstehender Alarm, falls verfügbar, gesendet werden.

Entsperren von Türen einer Einbruchmeldezentrale
Aktivieren Sie das Kontrollkästchen, um einem Benutzer des Operator Client zu erlauben, eine in einer Einbruchmeldezentrale konfigurierte Tür zu entsperren.

Sichern und entsichern von Türen einer Einbruchmeldezentrale
Aktivieren Sie das Kontrollkästchen, um einem Benutzer des Operator Client zu erlauben, eine in einer Einbruchmeldezentrale konfigurierte Tür zu sichern und zu entsichern.

Türen einer Einbruchmeldezentrale kurzzeitig entsperren
Aktivieren Sie das Kontrollkästchen, um einem Benutzer des Operator Client zu erlauben, den Türöffner für eine in einer Einbruchmeldezentrale konfigurierte Tür zu betätigen.

Zutritts-Türen bedienen
Aktivieren Sie das Kontrollkästchen, damit ein Benutzer von Operator Client den Zutritts- und Türzustand ändern kann (sichern, verriegeln, entriegeln).

Entscheidung für Zutritt treffen
Aktivieren Sie das Kontrollkästchen, um einem Benutzer von Operator Client zu erlauben, eine Zugriffsentscheidung zu treffen.

Personenverwaltung
Aktivieren Sie das Kontrollkästchen, um dem Benutzer von Operator Client zu ermöglichen, Personen für Person Identification-Alarme zu verwalten.

Bedrohungsstufe zurücksetzen
Aktivieren Sie das Kontrollkästchen, um einem Benutzer von Operator Client zu erlauben, die Bedrohungsstufe zurückzusetzen, wenn der Operator Client sich im Bedrohungsstufenmodus befindet.

Favoriten und Lesezeichen importieren/exportieren
Aktivieren Sie das Kontrollkästchen, um einem Benutzer von Operator Client zu erlauben, Favoriten oder Lesezeichen zu importieren oder zu exportieren.

Anzeigereihenfolge bei gleicher Alarmpriorität
Wählen Sie einen Wert aus, um die Reihenfolge der Alarmfenster in der Alarmanzeige des Operator Client zu konfigurieren.

Rückspulzeit für zeitversetzte Wiedergabe:
Geben Sie die Anzahl der Sekunden für die Alarmdauer der zeitversetzten Wiedergabe ein.

Alarmaudio wiederholen:
Aktivieren Sie das Kontrollkästchen, und geben Sie die Zeit in Sekunden ein, nach der ein Alarmton wiederholt wird.

Zugriff begrenzen auf Aufzeichnungen bis zu den letzten n Minuten:
Aktivieren Sie das Kontrollkästchen, um den Zugriff auf aufgezeichnete Videos einzuschränken. Geben Sie in der Liste die Zeit in Minuten ein.

Automatische Bedienerabmeldung nach dieser Zeit der Inaktivität erzwingen:
Aktivieren Sie das Kontrollkästchen, um die automatische Abmeldung von Operator Client nach dem konfigurierten Zeitraum zu aktivieren.

Siehe
– *Abmeldung bei Inaktivität, Seite 43*

26.12 Seite Prioritäten

Hauptfenster> **Benutzergruppen** > Registerkarte **Benutzergruppen** > > Registerkarte **Bedienberechtigungen** > Registerkarte **Prioritäten**
oder

Hauptfenster> **Benutzergruppen** > Registerkarte **Enterprise User Groups** > > Registerkarte **Bedienberechtigungen** > Registerkarte **Prioritäten**
Dient zum Konfigurieren eines Timeouts für explizites Sperren der PTZ-Steuerung. Sie können Prioritäten für die PTZ-Steuerung und die Anzeige eingehender Alarme einstellen.

Automatisches Popup-Verhalten
Verschieben Sie den Schieberegler, um den Prioritätswert für den Live-Bildfensterbereich oder Wiedergabe-Bildfensterbereich einzustellen. Dieser Wert ist für die Entscheidung erforderlich, ob eingehende Alarme automatisch im Alarmfensterbereich angezeigt werden.
Beispiel: Wenn Sie den Schieberegler für den Live-Bildfensterbereich auf 50 und für die Wiedergabeanzeige auf 70 setzen und ein Alarm mit der Priorität 60 eingeht, wird der Alarm nur dann automatisch angezeigt, wenn die Wiedergabeanzeige aktiv ist. Der Alarm wird nicht automatisch angezeigt, wenn die Live-Anzeige aktiv ist.

Siehe
– *Konfigurieren verschiedener Prioritäten, Seite 365*

26.13 Seite Benutzeroberfläche

Hauptfenster> **Benutzergruppen** > Registerkarte **Benutzergruppen** > > Registerkarte **Bedienberechtigungen** > Registerkarte **Benutzeroberfläche**
oder

Hauptfenster> **Benutzergruppen** > Registerkarte **Enterprise User Groups** > > Registerkarte **Bedienberechtigungen** > Registerkarte **Benutzeroberfläche**
Dient zum Konfigurieren der Benutzeroberfläche für 4 Monitore, die vom Operator Client verwendet werden.

Sie können einen Multimonitorbetrieb mit bis zu 4 Monitoren konfigurieren. Sie können für jeden Monitor einstellen, was angezeigt werden soll. Beispielsweise können Sie angeben, dass Monitor 2 nur Live-Bildfenster anzeigen soll oder dass Monitor 1 und Monitor 2 das Bildformat 16:9 für HD-Kameras verwenden sollen.

Hauptmonitor
Wählen Sie den Monitor aus, der als ein Hauptmonitor verwendet werden soll.

Max. Bildfenster in Wiedergabe
Wählen Sie die Höchstzahl der Bildfensterzeilen aus, die im Wiedergabe-Bildfensterbereich auf dem Hauptmonitor angezeigt werden sollen.

Alarm Monitor
Wählen Sie den Alarmmonitor aus, der entweder den Live- und Alarminhalt oder nur den Alarminhalt anzeigen kann.

Monitor 1-4
Wählen Sie in der jeweiligen Liste jedes Monitors den gewünschten Eintrag aus.
- Für den Hauptmonitor ist der Eintrag **Steuerung** voreingestellt und kann nicht geändert werden.
- Für den Alarmmonitor können Sie einen der folgenden Einträge auswählen:
  - **Live- und Alarm-Bildfensterbereich**
  - **Nur Alarm-Bildfensterbereich**
- Für die übrigen Monitore können Sie einen der folgenden Einträge auswählen:
  - **Nur Live-Bildfensterbereich**
  - **Karten- und Dokumentfenster**
  - **Zwei Karten- und Dokumentfenster**
  - **Live Bildfensterbereich auf ganzem Bildschirm**
  - **Vierfach Livebildbereich**

Max. Reihen von Bildfenstern
Wählen Sie die Höchstzahl der Bildfensterzeilen aus, die im Bildfensterbereich auf dem entsprechenden Monitor angezeigt werden sollen.
Hinweis: Diese Option ist nur für die folgenden Ansichten verfügbar:
- **Steuerung**
- **Nur Alarm-Bildfensterbereich**
- **Live- und Alarm-Bildfensterbereich**
- **Nur Live-Bildfensterbereich**

Die verbleibenden Ansichten haben eine feste Anordnung mit einer festgelegten Anzahl von Bildfensterzeilen und können nicht geändert werden.

Seitenverhältnis der Bildfenster
Wählen Sie für jeden Monitor das erforderliche Bildformat für den ersten Start des Operator Client aus. Verwenden Sie 16:9 für HD-Kameras.

Standardwert wiederherstellen
Klicken Sie darauf, um die Standardeinstellungen dieser Seite wiederherzustellen. Alle Listeneinträge werden auf ihre Standardeinstellungen zurückgesetzt.

26.14 Seite „Server-Zugriff“

Hauptfenster > **Benutzergruppen** > Registerkarte **Enterprise User Groups** > > Registerkarte **Serverzugriff**
Dient zum Konfigurieren des Server-Zugriffs auf einem Enterprise Management Server.

Geben Sie den Namen des Enterprise Accounts und das Passwort für jeden Management Server Ihres Enterprise System ein. Dieses Konto ist auf jedem Management Server konfiguriert.

Management Server
Zeigt den Namen des Management Server an, der auf diesem Enterprise Management Server konfiguriert wurde.

Netzwerkadresse
Anzeige der privaten IP-Adresse oder des DNS-Namen des Management Server.

Server-Nummer
Anzeige der Nummer des Management Servers. Diese Nummer wird von einem Bosch IntuiKey Keyboard zur Auswahl des gewünschten Management Servers verwendet.

Zugriff
Aktivieren Sie das Kontrollkästchen, wenn Sie den Zugriff auf den Management Server gewähren. Dieser Management Server ist nun ein Enterprise Management Server.

Enterprise Konto
Geben Sie den Namen des Enterprise Accounts ein, der auf dem Management Server konfiguriert wurde.

Authentifizierung
Wählen Sie die entsprechende Authentifizierungsoption im Dialogfeld **Authentifizierungseinstellungen**.

Konfig-API
Aktivieren Sie das Kontrollkästchen, wenn das Zugriffstoken den Zugriff auf den Config API-Dienst des Management Server.

Server-Beschreibung
Zeigt den Beschreibungstext für diesen Server an.
Weitere Spalten werden angezeigt, wenn sie zur Server-Liste hinzugefügt wurden.

Siehe
- *Erstellen einer Gruppe oder eines Kontos, Seite 358*
- *Erstellung eines Enterprise Systems, Seite 85*
- *Konfigurieren der Serverliste für Enterprise System, Seite 85*
- *Tokenbasierte Authentifizierung, Seite 87*

26.15 Seite „Konfigurationsberechtigungen“

Hinweis!
In diesem Dokument werden einige Funktionen beschrieben, die nicht für BVMS Viewer verfügbar sind.
Ausführliche Informationen zu den verschiedenen Versionen von BVMS finden Sie unter www.boschsecurity.com und in der BVMS Schnellauswahlhilfe: BVMS Schnellauswahlhilfe.

Hauptfenster > **Benutzergruppen** > Registerkarte **Benutzergruppen** > > Registerkarte **Bedienberechtigungen** > Registerkarte **Konfigurationsberechtigungen**
oder

Hauptfenster> **Benutzergruppen** > Registerkarte **Enterprise User Groups** > > Registerkarte **Bedienberechtigungen** > Registerkarte **Konfigurationsberechtigungen**

Dient zum Konfigurieren verschiedener Benutzerberechtigungen für den Configuration Client.

Gerätebaum
In diesem Abschnitt können Sie die Berechtigungen auf der Seite **Geräte** angeben. Aktivieren Sie das Kontrollkästchen für die entsprechende Berechtigung.

Karten und Struktur
In diesem Abschnitt können Sie die Berechtigungen auf der Seite **Karten und Struktur** angeben. Aktivieren Sie das Kontrollkästchen der entsprechenden Berechtigung.

Zeitpläne
In diesem Abschnitt können Sie die Berechtigungen auf der Seite **Zeitpläne** angeben. Aktivieren Sie das Kontrollkästchen der entsprechenden Berechtigung.

Kameras und Aufzeichnung
In diesem Abschnitt können Sie die Berechtigungen auf der Seite **Kameras und Aufzeichnung** angeben. Aktivieren Sie das Kontrollkästchen der entsprechenden Berechtigung.

Ereignisse
In diesem Abschnitt können Sie die Berechtigungen auf der Seite **Ereignisse** angeben. Aktivieren Sie das Kontrollkästchen der entsprechenden Berechtigung.

Alarme
In diesem Abschnitt können Sie die Berechtigungen auf der Seite **Alarme** angeben. Aktivieren Sie das Kontrollkästchen der entsprechenden Berechtigung.

Benutzergruppen
In diesem Abschnitt können Sie die Berechtigungen für die Konfiguration von Benutzergruppen angeben. Aktivieren Sie das Kontrollkästchen der entsprechenden Berechtigung.

Hinweis!
Das gleichzeitige Aktivieren des Kontrollkästchens **Benutzergruppen/Enterprise Accounts konfigurieren** und der Kontrollkästchen **Benutzer konfigurieren** und **Enterprise-Benutzer konfigurieren** ist aus Sicherheitsgründen ausgeschlossen.

Hinweis!
Nachdem Sie die Berechtigungen **Benutzer konfigurieren** und **Enterprise-Benutzer konfigurieren** zugewiesen haben, müssen Sie auf der Seite **Berechtigungen der Benutzergruppen** die Benutzergruppen zuweisen, in denen neue Benutzer hinzugefügt und konfiguriert werden können.

Audit Trail
In diesem Abschnitt können Sie angeben, ob ein Benutzer die Audit Trail-Funktion nutzen und Audit Trail-Daten exportieren kann.
Aktivieren Sie das Kontrollkästchen der entsprechenden Berechtigung.

Menübefehle
In diesem Abschnitt können Sie die Berechtigungen für die Konfiguration von Menübefehlen angeben. Aktivieren Sie das Kontrollkästchen der entsprechenden Berechtigung.

Auswertungen
In diesem Abschnitt können Sie die Berechtigungen für die Konfiguration von Auswertungen angeben. Aktivieren Sie das Kontrollkästchen der entsprechenden Berechtigung.

Hinweis!
Wenn Sie den Konfigurations-API-Dienst des Management Server verwenden möchten, müssen Sie Folgendes auswählen: **Konfigurationsberechtigungen**:
- **Geräte-Eigenschaften ändern**
- **Aktivierungs-Manager aufrufen**

Hinweis!
Wenn Sie die Option **Einstellungen für vertrauenswürdige Zertifikate** konfigurieren wollen, müssen Sie die **Benutzergruppen konfigurieren/Enterprise Accounts** Berechtigung wählen.

26.16 Seite „Berechtigungen für Benutzergruppen“

Hauptfenster > **Benutzergruppen** > Registerkarte **Benutzergruppen** > > Registerkarte **Bedienberechtigungen** > Registerkarte **Berechtigungen der Benutzergruppen**
oder

Hauptfenster > **Benutzergruppen** > Registerkarte **Enterprise User Groups** > > Registerkarte **Bedienberechtigungen** > Registerkarte **Berechtigungen der Benutzergruppen**
Hier können Sie zuweisen, zu welchen Benutzergruppen die Benutzer einer bestimmten Benutzergruppe neue Benutzer hinzufügen können.

Hinweis!
Sie können Benutzergruppenberechtigungen nur einer Benutzergruppe zuweisen, der Sie zuvor die Berechtigung zum Konfigurieren von Benutzern zugewiesen haben. Diese Berechtigung können Sie auf der Seite **Konfigurationsberechtigungen** zuweisen.

Hinweis!
Die Benutzer einer Standardbenutzergruppe haben keine Berechtigung, um neue Benutzer zur Admin-Gruppe hinzuzufügen. Dieses Kontrollkästchen ist nicht aktiv.

Siehe
– *Seite „Konfigurationsberechtigungen“, Seite 348*

26.17 Seite „Kontorichtlinien“

Hauptfenster > **Benutzergruppen** > Registerkarte **Benutzergruppen** > > Registerkarte **Sicherheit** > Registerkarte **Kontorichtlinien**
oder

Hauptfenster > **Benutzergruppen** > Registerkarte **Enterprise User Groups** > > Registerkarte **Sicherheit** > Registerkarte **Kontorichtlinien**

Dient zum Konfigurieren der Einstellungen für Benutzer und Passwörter.

Richtlinie für sichere Passwörter
Wählen Sie das Kontrollkästchen aus, um die Passwortrichtlinie zu aktivieren.

Weitere Informationen siehe: *Konfigurieren von Benutzern, Berechtigungen und Enterprise Access, Seite 357*

Hinweis!
Die Einstellung **Richtlinie für sichere Passwörter** wird für die Benutzer nur angewendet, wenn das Kontrollkästchen in der entsprechenden Benutzergruppe aktiviert ist.
Es wird dringend empfohlen, diese Einstellung beizubehalten, um Ihren Computer besser vor unbefugtem Zugriff zu schützen.

Mindestlänge des Passworts
Diese Einstellung legt die Mindestzahl der Zeichen fest, aus denen ein Passwort für ein Benutzerkonto bestehen muss.
Aktivieren Sie das Kontrollkästchen, um die Einstellung zu aktivieren, und geben Sie die minimale Zeichenanzahl ein.

Maximales Passwortalter in Tagen
Diese Einstellung legt den Zeitraum (in Tagen) fest, in dem ein Passwort verwendet werden kann, bevor das System den Benutzer zur Änderung auffordert.
Aktivieren Sie das Kontrollkästchen, um die Einstellung zu aktivieren, und geben Sie die maximale Anzahl von Tagen ein.

Anzahl verwendeter Passwörter in Historie
Diese Einstellung bestimmt die Anzahl der einzigartigen neuen Passwörter, die für ein Benutzerkonto festgelegt werden müssen, bevor ein altes Passwort erneut verwendet werden kann.
Aktivieren Sie das Kontrollkästchen, um die Einstellung zu aktivieren, und geben Sie die minimale Anzahl von Passwörtern ein.

Maximale ungültige Anmeldeversuche
Diese Einstellung legt die Deaktivierung eines Kontos nach einer bestimmten Anzahl ungültiger Anmeldeversuche fest.
Aktivieren Sie das Kontrollkästchen, um die Einstellung zu aktivieren, und geben Sie die maximale Anzahl von Versuchen ein.
Wenn das Kontrollkästchen **Maximale ungültige Anmeldeversuche** aktiviert ist, können Sie die folgenden zwei Einstellungen festlegen:

Kontosperrdauer
Diese Einstellung legt die Anzahl der Minuten fest, für die ein deaktiviertes Konto deaktiviert bleibt, bevor es automatisch wieder aktiviert wird.
Aktivieren Sie das Kontrollkästchen, um die Einstellung zu aktivieren, und geben Sie die Anzahl von Minuten ein.

Kontosperrungszähler zurücksetzen nach
Diese Einstellung legt die Anzahl der Minuten fest, die ab dem Zeitpunkt einer fehlgeschlagenen Anmeldung vergehen müssen, bevor der Zähler für fehlgeschlagene Anmeldeversuche auf Null zurückgesetzt wird.
Aktivieren Sie das Kontrollkästchen, um die Einstellung zu aktivieren, und geben Sie die Anzahl von Minuten ein.

Hinweis!
Wenn die maximale Anzahl ungültiger Anmeldeversuche überschritten wird, wird das Konto deaktiviert.
Wenn das Kontrollkästchen **Kontosperrdauer** nicht aktiviert ist, muss das Konto manuell aktiviert werden.
Wenn das Kontrollkästchen **Kontosperrdauer** aktiviert ist, wird das Konto nach dem definierten Zeitraum automatisch aktiviert.

Hinweis!
Der Zähler für ungültige Anmeldeversuche wird auf Null zurückgesetzt:
nach einer erfolgreichen Anmeldung
nach der angegebenen Dauer, wenn das Kontrollkästchen **Kontosperrungszähler zurücksetzen nach** aktiviert ist

Offline Client deaktivieren
Aktivieren Sie das Kontrollkästchen, um die Anmeldung bei einem Offline-Client zu deaktivieren.

Zusatzinformationen
Ab BVMS 9.0 sind die folgenden Einstellungen zu **Kontorichtlinien** standardmäßig aktiviert:
- Das Kontrollkästchen **Richtlinie für sichere Passwörter** ist bereits aktiviert.
- Das Kontrollkästchen **Mindestlänge des Passworts** ist bereits aktiviert. Der Standardwert ist 10.
- Das Kontrollkästchen **Maximales Passwortalter in Tagen** ist nicht aktiviert. Der Standardwert ist 90.
- Das Kontrollkästchen **Anzahl verwendeter Passwörter in Historie** ist nicht aktiviert. Der Standardwert ist 10.
- Das Kontrollkästchen **Maximale ungültige Anmeldeversuche** ist nicht aktiviert. Der Standardwert ist 1.
- Das Kontrollkästchen **Offline Client deaktivieren** ist nicht aktiviert.

Seit BVMS 10.0.1 sind die folgenden **Kontorichtlinien**-Einstellungen standardmäßig für alle Benutzergruppen ausgewählt:
- **Maximale ungültige Anmeldeversuche**
- **Kontosperrdauer**
- **Kontosperrungszähler zurücksetzen nach**

26.17.1 Offline Operator Client

Mit der Funktion des Offline Operator Client sind folgende Fälle möglich:
- Operator Client Unterbrechungsfreier Betrieb für Live-Aufzeichnung, Wiedergabe und Export ohne Verbindung zum Management Server Computer.
- Wenn eine Arbeitsstation einmal mit dem Management Server Computer verbunden war, kann sie sich jederzeit offline mit einem beliebigen Benutzer verbinden.

Für Offline-Modus BVMS ist Version 3.0 oder höher erforderlich.
Wenn eine Operator Client Arbeitsstation vom Management Server Computer getrennt wird, ist es möglich, trotzdem weiterzuarbeiten. Gewisse Hauptfunktionen wie beispielsweise Live und Videowiedergabe sind immer noch möglich.
Ab BVMS V5.5 kann eine Operator Client Arbeitsstation offline mit einer Konfiguration von BVMS V5.0.5 betrieben werden.

Hinweis!
Wenn auf dem Management Server eine Passwortänderung vorgenommen wird, während Operator Client offline ist, wird diese Passwortänderung nicht an diesen Operator Client übertragen. Wenn Operator Client online ist, muss der Benutzer sich mit dem neuen Passwort anmelden. Wenn Operator Client offline ist, muss der Benutzer sich mit dem alten Passwort anmelden. Es wird nicht geändert, bis eine neue Konfiguration aktiviert und an die Operator Client-Arbeitsstation übertragen wurde.

Hinweis!
Wenn eine Kamera zur Anzeige in einer Monitorgruppe mit einer Arbeitsstation aufgerufen wird, die mit dem Bosch IntuiKey Keyboard verbunden und offline ist, gibt das Keyboard keinen Fehlerton aus.

26.17.1.1 Im Offline-Modus arbeiten

Wenn Operator Client von einem Management Server getrennt ist, wird das jeweilige Overlay-Symbol im Logischen Baum auf dem getrennten Management Server angezeigt. Sie können weiterhin mit Operator Client arbeiten, selbst wenn die Unterbrechung länger dauert, jedoch sind einige Funktionen dann nicht verfügbar.
Wenn die Verbindung mit dem Management Server wiederhergestellt wird, wird ein entsprechendes Symbol eingeblendet.
Wenn eine neue Konfiguration auf einem Management Server aktiviert wurde, wird im Logischen Baum auf dem Symbol des betroffenen Management Servers ein entsprechendes Symbol angezeigt, und ein Dialogfeld wird einige Sekunden lang eingeblendet. Akzeptieren Sie die neue Konfiguration, oder lehnen Sie sie ab.
Wenn Ihre Operator Client-Instanz laut Zeitplan zu einem bestimmten Zeitpunkt abgemeldet werden soll, erfolgt diese Abmeldung auch dann, wenn die Verbindung mit dem Management Server zu diesem Zeitpunkt nicht wiederhergestellt ist.
Wenn ein Benutzer von Operator Client nach der Anmeldung Server Lookup im Offline-Status verwendet, wird die Serverliste der letzten erfolgreichen Anmeldung angezeigt. Offline-Status bedeutet hier, dass die Operator Client Arbeitsstation, an der sich der Benutzer anmeldet, keine Netzwerkverbindung zum Server mit der Server-Liste hat.

Funktion während dem Trennen der Verbindung nicht verfügbar.
Beim Trennen vom Management Server sind einige der folgenden Symbole nicht im Operator Client verfügbar:

- Alarmliste:
  Dies umfasst das Bearbeiten von Alarmen, Die Alarmliste ist leer und wird beim Wiederverbinden automatisch ergänzt.
- Allegiant:
  Die Bearbeitung der Trunklinie ist nicht verfügbar. In einer früheren Version wurden Allegiant-Kameras automatisch mit einem Meldungsfeld geschlossen, wenn eine Trunklinienbearbeitung nicht verfügbar war. Mit dem BVMS V3.0 bieten wir benutzerfreundlichere Bildfenster an, die den Benutzer über die Unmöglichkeit informieren, diese Kamera gerade jetzt anzuzeigen.
- MG:
  Es ist nicht möglich, die Kameras in die MG-Steuerung zu ziehen. Die Steuerung ist deaktiviert und wird beim Wiederverbinden automatisch aktiviert.
- PTZ-Prioritäten

Ohne eine Verbindung zum Management Server , kann ein Offline Operator Client eine PTZ-Kamera verbinden, solange die PTZ-Kamera selber nicht gesperrt ist. Die Dome-Prioritäten werden beim Wiederverbinden automatisch aktualisiert.

- Eingang:
  Der Eingang kann nicht geändert werden.
- Logbuch:
  Das Logbuch ist nicht verfügbar und kann nicht geöffnet werden. Ein geöffnetes Logbuchsuchfenster wird nicht automatisch geschlossen. Bestehende Suchergebnisse können verwendet und exportiert werden.
- Operator Client SDK:
  Operator Client-SDK-Funktionen mit IServerApi können nicht verarbeitet werden.
  Das Erstellen einer RemoteClientApi ist nicht möglich.
  Gewisse Methoden, die nur im API-Client verfügbar sind, funktionieren nicht, beispielsweise ApplicationManager (versuchen Sie es mit GetUserName()).
- Passwortänderung:
  Der Bediener kann sein Passwort nicht ändern.
- Relais:
  Relais können nicht geändert werden.
- Server-Script:
  Die Servermethoden auf dem IServerApi werden verarbeitet, können aber nicht an den Client gesendet werden, nämlich:
  - AlarmManager
  - AnalogMonitorManager
  - CameraManager
  - CompoundEventManager
  - DecoderManager
  - DeviceManager
  - DomeCameraManager
  - EventManager
  - InputManager
  - LicenseManager
  - Logbuch
  - MatrixManager
  - RecorderManager
  - RelayManager
  - ScheduleManager
  - SendManager
  - SequenceManager
  - VirtualInputManager
- Status-Einblendungen:
  Keine Status-Einblendungen von Kameras, Eingängen oder Relais verfügbar.

Status-Einblendungen des Geräts:
Die Gerätestatus (Aufzeichnungspunkt, zu laut, zu dunkel...) werden vom Management Server verarbeitet. Beim Trennen der Verbindung zwischen dem Client und dem Server können die Status im Client nicht aktualisiert werden. Eine Statuseinblendung gibt Ihnen ein visuelles Feedback, dass alle Gerätestatus im Moment nicht verfügbar sind. Wenn der Client wieder eine Verbindung zum Server aufgebaut hat, wird die Statuseinblendung automatisch aktualisiert.

- Status unbekannt

Die Statusanzeige eine Geräts im logischen Baum oder auf einer Karte, wenn der Client vom Management Server Computer getrennt wird.

Gründe für die Trennung der Verbindung
Mögliche Gründe für die Trennung der Verbindung Operator Client und Management Server können sein

- Physische Verbindung ist unterbrochen
- Passwort des angemeldeten Benutzers wurde während der Offline-Zeit geändert.
- Management Server hat fließende Workstation-Lizenzen an einen anderen online Operator Client vergeben, während der jetzt getrennte Operator Client offline war.
- Operator Client und Management Server haben unterschiedliche Versionen (Management Server vor Version 5.5).

26.18 Berechtigungen für die Anmeldung pro Anwendungstypseite

Hauptfenster > **Benutzergruppen** > Registerkarte **Benutzergruppen** > > Registerkarte **Berechtigungen für Anwendungen** > Registerkarte **Berechtigungen für die Anmeldung je Anwendungsart**
oder

Hauptfenster > **Benutzergruppen** > Registerkarte **Enterprise User Groups** > > Registerkarte **Berechtigungen für Anwendungen** > Registerkarte **Berechtigungen für die Anmeldung je Anwendungsart**

Dient zum Konfigurieren verschiedener Benutzerberechtigungen für die verschiedenen Anwendungen.

Operator Client oder Cameo SDK (direkt zu Management Server)
Wählen Sie das Kontrollkästchen, um sich direkt im Management Server vom Operator Client oder der Cameo SDK-Anwendung anzumelden.

Operator Client (zu Unmanaged Site)
Wählen Sie das Kontrollkästchen, um die Anmeldung bei der Anwendung Operator Client zu ermöglichen, indem Sie eine Verbindung zu einer unmanaged site herstellen.

Configuration Client
Aktivieren Sie das Kontrollkästchen, um eine Anmeldung beim Configuration Client zuzulassen.

Konfigurations-API
Wählen Sie das Kontrollkästchen, um eine Anmeldung bei **Konfigurations-API** zuzulassen.

Mobiler Zugang via Video Security Client
Aktivieren Sie das Kontrollkästchen, um mobile Zugriffe vom Video Security Client zuzulassen.

BVMS Server SDK/Server API
Aktivieren Sie das Kontrollkästchen, um eine Anmeldung bei der BVMS Server SDK-Anwendung zuzulassen.

BVMS Client SDK (erlaubt Verbindung zu Operator Client)

Aktivieren Sie das Kontrollkästchen, um die Anmeldung bei der Client-SDK-Anwendung für bestimmte Benutzergruppen zu ermöglichen.

26.19 Seite mit den Einstellungen für das Bedrohungsmanagement

Hauptfenster > **Benutzergruppen** > **Benutzergruppen** Registerkarte > > **Bedrohungsstufenverwaltung** Registerkarte > **Einstellungen** Registerkarte

Hier können Sie konfigurieren, ob sich eine Gruppe aufgrund verschiedener Gefahrenstufen ändern soll.
Hinweis: Im Falle eines Alarms mit Bedrohungslevel wird der Operator Client-Benutzer abgemeldet und der Operator Client startet neu. Der Benutzer muss sich erneut im Bedrohungsmodus Operator Client anmelden. Abhängig von der Konfiguration der Benutzergruppe bekommt der entsprechende Benutzer dann die Berechtigungen der konfigurierten Benutzergruppe für die aktive Gefahrenstufe.

So konfigurieren Sie eine Gefahrenstufe für eine Benutzergruppe:
1. Wählen Sie jeweilige Benutzergruppe aus.
2. Wählen Sie im Dropdown-Menü der jeweiligen Gefahrenstufe die Benutzergruppe aus, die in dieser Gefahrenstufe aktiv sein soll.

27 Konfigurieren von Benutzern, Berechtigungen und Enterprise Access

Hinweis!
BVMS Viewer bietet nur Grundfunktionen. Erweiterte Funktionen sind in BVMS Professional enthalten. Ausführliche Informationen zu den verschiedenen Versionen von BVMS finden Sie unter www.boschsecurity.com und in der BVMS Schnellauswahlhilfe: BVMS Schnellauswahlhilfe.

Hauptfenster > **Benutzergruppen**
Dieses Kapitel enthält Informationen zur Konfiguration von Benutzergruppen, Enterprise User Groups und Enterprise Access.
Sie konfigurieren alle Gerätefreigaben und Bedienberechtigungen pro Benutzergruppe und nicht pro Benutzer.
Es gelten die folgenden Regeln:
- Ein BVMS Benutzer kann nur einer BVMS-Benutzergruppe oder Enterprise User Group angehören. Ein LDAP-Benutzer kann Mitglied mehrerer LDAP-Benutzergruppen sein.
- Die Einstellungen einer Standardbenutzergruppe können nicht geändert werden.
- Diese Benutzergruppe hat Zugriff auf alle Geräte des Vollständigen Logischen Baums. Ihr wird der Zeitplan **Immer** zugewiesen.
- Für den Zugriff auf Windows-Benutzergruppen einer Domäne werden LDAP-Benutzergruppen genutzt.
- Klicken Sie auf , um die Einstellungen zu speichern.
- Klicken Sie auf , um die letzte Einstellung rückgängig zu machen.
- Klicken Sie auf , um die Konfiguration zu aktivieren.

Richtlinie für sichere Passwörter
Für einen besseren Schutz Ihres Computers vor unbefugtem Zugriff wird empfohlen, Benutzerkonten mit starken Passwörtern zu verwenden.
Daher ist standardmäßig eine Richtlinie für sichere Passwörter für alle neu erstellten Benutzergruppen aktiviert. Dies umfasst die Admin-Benutzergruppe und auch Standard-Benutzergruppen, Enterprise User Groups und Enterprise Access.
Es gelten die folgenden Regeln:
- Mindestlänge des Passworts gemäß den Angaben auf der Seite **Kontorichtlinien** für die entsprechende Benutzergruppe.
- Verwenden Sie keines der vorherigen Passwörter.
- Verwenden Sie mindestens einen Großbuchstaben (A bis Z).
- Verwenden Sie mindestens eine Ziffer (0 bis 9).
- Verwenden Sie mindestens ein Sonderzeichen (z. B.: ! $ # %).

Wenn der Admin-Benutzer Configuration Client zum ersten Mal startet, wird das Dialogfeld **Passwortrichtlinie verletzt** angezeigt, in dem er aufgefordert wird, ein Passwort für das Admin-Benutzerkonto festzulegen. Es wird dringend empfohlen, diese Einstellung beizubehalten und für das Admin-Benutzerkonto ein starkes Passwort entsprechend der Passwortrichtlinie festzulegen.

Beim Anlegen neuer Benutzergruppen im Configuration Client ist die Richtlinie für sichere Passwörter standardmäßig aktiviert. Wenn Sie keine Passwörter für die neuen Benutzerkonten der entsprechenden Benutzergruppe festlegen, können Sie die Konfiguration nicht aktivieren. Das Dialogfeld **Passwortrichtlinie verletzt** wird angezeigt, in dem alle Benutzer aufgelistet sind, für die kein Passwort festgelegt wurde.
Um die Konfiguration zu aktivieren, legen Sie die fehlenden Passwörter fest.

Siehe
- *Seite „Kontorichtlinien“, Seite 350*
- *Seite Eigenschaften der Benutzergruppen, Seite 335*
- *Seite Benutzereigenschaften, Seite 336*
- *Seite Eigenschaften des Anmeldungspaares, Seite 337*
- *Seite Kamerafreigaben, Seite 338*
- *Seite „Prioritäten für Steuerungen“, Seite 339*
- *Dialogfeld Freigaben für Benutzergruppen kopieren, Seite 340*
- *Seite Decoder-Freigaben, Seite 340*
- *Seite Ereignisse und Alarme, Seite 341*
- *Dialogfeld „LDAP-Server-Einstellungen“ (Menü „Einstellungen“), Seite 116*
- *Seite „Zugangsberechtigungen“, Seite 341*
- *Seite Logischer Baum, Seite 342*
- *Seite mit den Bedienereigenschaften, Seite 342*
- *Seite Prioritäten, Seite 346*
- *Seite Benutzeroberfläche, Seite 346*
- *Seite „Server-Zugriff“, Seite 347*

27.1 Erstellen einer Gruppe oder eines Kontos

Hauptfenster > **Benutzergruppen**
Sie können eine Standardbenutzergruppe, eine Enterprise User Group oder ein Enterprise Account erstellen.
Zur Anpassung der Berechtigungen für Benutzergruppen an Ihre Anforderungen erstellen Sie eine neue Benutzergruppe und ändern deren Einstellungen.

27.1.1 Erstellen einer Standard-Benutzergruppe

Hauptfenster > **Benutzergruppen**

So erstellen Sie eine Standard-Benutzergruppe:
1. Klicken Sie auf die Registerkarte **Benutzergruppen**.
2. Klicken Sie auf .
   Das Dialogfeld **Neue Benutzergruppe** wird angezeigt.
3. Geben Sie den Namen und eine Beschreibung ein.
4. Klicken Sie auf **OK**.
   Eine neue Gruppe wird dem entsprechenden Baum hinzugefügt.
5. Klicken Sie mit der rechten Maustaste auf die neue Benutzergruppe, und klicken Sie auf **Umbenennen**.
6. Geben Sie den gewünschten Namen ein, und drücken Sie die Eingabetaste.

Siehe
- *Seite Eigenschaften der Benutzergruppen, Seite 335*
- *Seite mit den Bedienereigenschaften, Seite 342*

– *Seite Prioritäten, Seite 346*
– *Seite Benutzeroberfläche, Seite 346*

27.1.2 Erstellen einer Enterprise User Group

Hauptfenster > **Benutzergruppen**

Die Aufgabe zum Erstellen einer Enterprise User Group für ein Enterprise System führen Sie auf einem Enterprise Management Server aus.
Erstellen Sie eine Enterprise User Group mit Benutzern, um deren Bedienberechtigungen zu konfigurieren. Diese Bedienberechtigungen sind auf einem Operator Client verfügbar, der mit dem Enterprise Management Server verbunden ist. Ein Beispiel für eine Bedienberechtigung ist die Benutzeroberfläche für den Alarmmonitor.

So erstellen Sie eine Enterprise User Group:

1. Klicken Sie auf die Registerkarte **Enterprise User Groups**.
   Hinweis: Die Registerkarte **Enterprise User Groups** ist nur verfügbar, wenn die entsprechende Lizenz verfügbar ist und wenn ein oder mehrere Management Server-Computer in **Geräte** > **Enterprise System** > **Serverliste / Adressbuch** konfiguriert sind.
2. Klicken Sie auf .
   Das Dialogfeld **Neue Enterprise Benutzergruppe** wird angezeigt.
3. Geben Sie den Namen und eine Beschreibung ein.
4. Klicken Sie auf **OK**.
   Die Enterprise User Group wird dem entsprechenden Baum hinzugefügt.
5. Klicken Sie mit der rechten Maustaste auf die neue Enterprise User Group, und klicken Sie auf **Umbenennen**.
6. Geben Sie den gewünschten Namen ein, und drücken Sie die Eingabetaste.
7. Konfigurieren Sie auf der Seite **Bedienberechtigungen** die Bedienberechtigungen und den Server-Zugriff für die konfigurierten Management Server-Computer nach Bedarf.

Siehe

– *Seite Eigenschaften der Benutzergruppen, Seite 335*
– *Seite mit den Bedienereigenschaften, Seite 342*
– *Seite Prioritäten, Seite 346*
– *Seite Benutzeroberfläche, Seite 346*
– *Seite „Server-Zugriff“, Seite 347*

27.1.3 Erstellen eines Enterprise Accounts

Hauptfenster > **Benutzergruppen**

Hinweis!
Im Gerätebaum muss mindestens ein Gerät konfiguriert sein, damit Sie einen Enterprise Account hinzufügen können.

Die Aufgabe zum Erstellen eines Enterprise Accounts führen Sie auf einem Management Server aus. Wiederholen Sie diese Aufgabe auf jedem Management Server, der Ihrem Enterprise System angehört.
Erstellen Sie einen Enterprise Account, um die Geräteberechtigungen für einen Operator Client mit einem Enterprise System zu konfigurieren.

So erstellen Sie einen Enterprise Account:

1. Klicken Sie auf die Registerkarte **Enterprise Access**.

2. Klicken Sie auf .
   Das Dialogfeld **Neuer Enterprise Account** wird angezeigt.
3. Geben Sie den Namen und eine Beschreibung ein.
4. Das Kontrollkästchen **Benutzer muss Passwort bei nächster Anmeldung ändern** ist bereits für alle neu erstellten Benutzerkonten aktiviert.
   Geben Sie den Schlüssel entsprechend der Schlüsselrichtlinie ein und bestätigen Sie ihn.
5. Klicken Sie auf **OK**.
   Ein neuer Enterprise Account wird zum entsprechenden Baum hinzugefügt.
6. Klicken Sie mit der rechten Maustaste auf den neuen Enterprise Account und klicken Sie auf **Umbenennen**.
7. Geben Sie den gewünschten Namen ein, und drücken Sie die Eingabetaste.
8. Konfigurieren Sie auf der Seite **Geräteberechtigungen** die Zugangs- und Geräteberechtigungen nach Bedarf.

Siehe

- *Richtlinie für sichere Passwörter , Seite 357*
- *Seite „Zugangsberechtigungen“, Seite 341*
- *Seite Logischer Baum, Seite 342*
- *Seite Ereignisse und Alarme, Seite 341*
- *Seite „Prioritäten für Steuerungen“, Seite 339*
- *Seite Kamerafreigaben, Seite 338*
- *Seite Decoder-Freigaben, Seite 340*

27.2 Erzeugen eines Benutzers

Hauptfenster > **Benutzergruppen** > **Benutzergruppen** Registerkarte
oder
Hauptfenster > **Benutzergruppen** > Registerkarte **Enterprise User Groups**
Ein Benutzer wird als neues Mitglied einer bestehenden Standard-Benutzergruppe oder Enterprise User Group erstellt.

Hinweis!
Zur Bedienung von Bosch IntuiKey Keyboards, die mit einem Decoder verbunden sind, müssen die jeweiligen Benutzer über Benutzernamen und Passwörter verfügen, die ausschließlich aus Ziffern bestehen. Der Benutzername kann aus maximal 3 Ziffern, das Passwort aus maximal 6 Ziffern bestehen.

So erzeugen Sie einen Benutzer:

1. Wählen Sie eine Gruppe aus und klicken Sie auf oder klicken Sie mit der rechten Maustaste auf die gewünschte Gruppe und klicken Sie auf **Neuer Benutzer**.
   Ein neuer Benutzer wird zum **Benutzergruppen**-Baum hinzugefügt.
2. Klicken Sie mit der rechten Maustaste auf den neuen Benutzer, und klicken Sie auf **Umbenennen**.
3. Geben Sie den gewünschten Namen ein, und drücken Sie die Eingabetaste.
4. Geben Sie auf der Seite **Benutzereigenschaften** den Benutzernamen und eine Beschreibung ein.
5. Das Kontrollkästchen **Benutzer muss Passwort bei nächster Anmeldung ändern** ist bereits für alle neu erstellten Benutzerkonten aktiviert.
   Geben Sie das Passwort entsprechend der Passwortrichtlinie ein und bestätigen Sie es.
6. Klicken Sie auf **Übernehmen**, um die Einstellungen zu übernehmen.
7. Aktivieren Sie das Kontrollkästchen **Konto ist aktiviert**, um das Benutzerkonto zu aktivieren.

8. Klicken Sie auf , um das Passwort zu aktivieren.
9. Klicken Sie auf , um die Konfiguration zu aktivieren.

Hinweis: Nachdem Sie einen neuen Benutzer hinzugefügt haben, müssen Sie die Konfiguration immer aktivieren.

Siehe
- *Seite Benutzereigenschaften, Seite 336*
- *Richtlinie für sichere Passwörter , Seite 357*
- *Seite Benutzergruppen, Seite 333*

27.3 Erzeugen einer 4-Augen-Gruppe

Hauptfenster > **Benutzergruppen** > **Benutzergruppen** Registerkarte
oder
Hauptfenster > **Benutzergruppen** > Registerkarte **Enterprise User Groups**
Sie können das 4-Augen-Prinzip für eine Standard-Benutzergruppe oder Enterprise User Group festlegen.
Für Enterprise Access ist das 4-Augen-Prinzip nicht verfügbar.
Sie wählen zwei Benutzergruppen aus. Die Mitglieder dieser Benutzergruppen sind Mitglieder der neuen 4-Augen-Gruppe.

So erzeugen Sie eine 4-Augen-Gruppe:

1. Klicken Sie auf .
   Das Dialogfeld **Neue 4-Augen-Gruppe** bzw. **Neue Enterprise 4-Augen-Gruppe** wird angezeigt.
2. Geben Sie einen Namen und eine Beschreibung ein.
3. Klicken Sie auf **OK**.
   Eine neue 4-Augen-Gruppe wird dem entsprechenden Baum hinzugefügt.
4. Klicken Sie mit der rechten Maustaste auf die neue 4-Augen-Gruppe und klicken Sie dann auf **Umbenennen**.
5. Geben Sie den gewünschten Namen ein und drücken Sie die Eingabetaste.

Hinweis!
Benutzer, die Mitglieder einer Gruppe mit doppelter Berechtigung sind, können sich nicht bei Operator Client mit Single Sign-On.

Siehe
- *Hinzufügen eines Anmeldungspaars zu einer 4-Augen-Gruppe, Seite 361*
- *Seite Eigenschaften der Benutzergruppen, Seite 335*
- *Seite mit den Bedienereigenschaften, Seite 342*
- *Seite Prioritäten, Seite 346*
- *Seite Benutzeroberfläche, Seite 346*

27.4 Hinzufügen eines Anmeldungspaars zu einer 4-Augen-Gruppe

Hauptfenster > **Benutzergruppen** > **Benutzergruppen** Registerkarte > **Neue 4-Augen-Gruppe**

Hauptfenster > **Benutzergruppen** > Registerkarte **Enterprise User Groups** > **Neue Enterprise 4-Augen-Gruppe**

So fügen Sie ein Anmeldungspaar zu einer 4-Augen-Gruppe hinzu:

1. Wählen Sie die gewünschte 4-Augen-Gruppe aus und klicken Sie auf oder klicken Sie mit der rechten Maustaste auf die Gruppe und klicken Sie auf **Neues Anmeldungspaar**.
   Das entsprechende Dialogfeld wird angezeigt.
2. Wählen Sie in jeder Liste eine Benutzergruppe aus.
   Die Benutzer der ersten Benutzergruppe sind die Benutzer, die sich im ersten Anmeldedialogfeld anmelden müssen. Die Benutzer der zweiten Benutzergruppe bestätigen die Anmeldung.
   Es ist möglich, dieselbe Gruppe in beiden Listen auszuwählen.
3. Bei Bedarf können Sie für jede Gruppe **4-Augen-Prinzip erforderlich** auswählen.
   Wenn dieses Kontrollkästchen aktiviert ist, können sich die Benutzer der ersten Gruppe nur zusammen mit einem Benutzer der zweiten Gruppe anmelden.
   Wenn dieses Kontrollkästchen deaktiviert ist, können sich die Benutzer der ersten Gruppe alleine anmelden, haben jedoch nur die Zugriffsrechte dieser Gruppe.
4. Klicken Sie auf **OK**.
   Ein neues Anmeldungspaar wird der entsprechenden 4-Augen-Gruppe hinzugefügt.
5. Klicken Sie mit der rechten Maustaste auf das neue Anmeldungspaar, und klicken Sie auf **Umbenennen**.
6. Geben Sie den gewünschten Namen ein, und drücken Sie die Eingabetaste.

Hinweis!
Benutzer, die Mitglieder einer Gruppe mit doppelter Berechtigung sind, können sich nicht bei Operator Client mit Single Sign-On.

Siehe
- *Erzeugen einer 4-Augen-Gruppe, Seite 361*
- *Seite Eigenschaften des Anmeldungspaares, Seite 337*

27.5 Konfigurieren der Admin-Gruppe

Hauptfenster > **Benutzergruppen** > Registerkarte **Benutzergruppen** > Admin-Gruppe
Dient zum Hinzufügen neuer Admin-Benutzer zur Admin-Gruppe, Umbenennen von Admin-Benutzern und Entfernen aus der Admin-Gruppe.

So fügen Sie einen neuen Admin-Benutzer zur Admin-Gruppe hinzu:

1. Klicken Sie auf oder klicken Sie mit der rechten Maustaste auf die Admin-Gruppe und klicken Sie auf **Neuen Benutzer hinzufügen**.
   Ein neuer Admin-Benutzer wird zur Admin-Gruppe hinzugefügt.
2. Geben Sie auf der Seite **Benutzereigenschaften** den Benutzernamen und eine Beschreibung ein.
3. Das Kontrollkästchen **Benutzer muss Passwort bei nächster Anmeldung ändern** ist bereits für alle neu erstellten Benutzerkonten aktiviert.
   Geben Sie das Passwort entsprechend der Passwortrichtlinie ein und bestätigen Sie es.
4. Klicken Sie auf **Übernehmen**, um die Einstellungen zu übernehmen.

5. Klicken Sie auf , um das Passwort zu aktivieren.

So benennen Sie einen Admin-Benutzer um:

1. Klicken Sie mit der rechten Maustaste auf den gewünschten Admin-Benutzer, und klicken Sie auf **Umbenennen**.
2. Geben Sie den gewünschten Namen ein, und drücken Sie die Eingabetaste.
3. Klicken Sie auf , um die Änderungen beim Benutzernamen zu aktivieren.

So entfernen einen Admin-Benutzer aus der Admin-Gruppe:

- Klicken Sie mit der rechten Maustaste auf den gewünschten Admin-Benutzer, und klicken Sie auf **Entfernen**.
  Der Admin-Benutzer wird aus der Admin-Gruppe entfernt.

Hinweis:

Sie können einen Admin-Benutzer nur dann aus der Admin-Gruppe entfernen, wenn andere Admin-Benutzer vorhanden sind.
Wenn sich nur ein Admin-Benutzer in der Admin-Gruppe befindet, kann er nicht entfernt werden.

Siehe

- *Seite Benutzergruppen, Seite 333*
- *Seite Benutzereigenschaften, Seite 336*
- *Richtlinie für sichere Passwörter , Seite 357*

27.6 Auswählen einer zugeordneten LDAP-Gruppe

Hauptfenster > **Benutzergruppen** > Registerkarte **Benutzergruppen** > > Registerkarte **Bedienberechtigungen** > Registerkarte **Eigenschaften der Benutzergruppen**
oder

Hauptfenster> **Benutzergruppen** > Registerkarte **Enterprise User Groups** > > Registerkarte **Bedienberechtigungen** > Registerkarte **Eigenschaften der Enterprise Benutzergruppen**
Sie können LDAP-Gruppen in Standardbenutzergruppen oder in Enterprise User Groups konfigurieren.

So wählen Sie eine zugeordnete LDAP-Gruppe aus:

1. Klicken Sie auf die Schaltfläche **Suche nach Gruppen**.
2. Wählen Sie in der Liste **Zugeordnete LDAP-Gruppe** die entsprechende LDAP-Gruppe aus.

Detaillierte Informationen zu den verschiedenen Feldern erhalten Sie, wenn Sie unten auf den Link des entsprechenden Anwendungsfensters klicken.

Siehe

- *Dialogfeld „LDAP-Server-Einstellungen“ (Menü „Einstellungen“), Seite 116*
- *Seite Eigenschaften der Benutzergruppen, Seite 335*

27.7 Festlegen eines Freigabezeitplans für Benutzeranmeldungen

Hauptfenster > **Benutzergruppen** > Registerkarte **Benutzergruppen** > > Registerkarte **Bedienberechtigungen** > Registerkarte **Eigenschaften der Benutzergruppen**
oder

Hauptfenster> **Benutzergruppen** > Registerkarte **Enterprise User Groups** > > Registerkarte **Bedienberechtigungen** > Registerkarte **Eigenschaften der Enterprise Benutzergruppen**

Sie können festlegen, dass sich die Mitglieder einer Benutzergruppe oder Enterprise User Group nur während bestimmter Zeiträume auf ihren Computern anmelden dürfen.

Für die Standardbenutzergruppen können diese Einstellungen nicht geändert werden.

So legen Sie einen Anmeldezeitplan fest:

1. Klicken Sie auf die Registerkarte **Eigenschaften der Benutzergruppen**.
2. Wählen Sie in der Liste **Zeitplan für Anmeldung** einen Zeitplan aus.

27.8 Konfigurieren von Bedienberechtigungen

Hauptfenster > **Benutzergruppen** > Registerkarte **Benutzergruppen** > > Registerkarte **Bedienberechtigungen** > Registerkarte **Eigenschaften der Benutzergruppen**

oder

Hauptfenster> **Benutzergruppen** > Registerkarte **Enterprise User Groups** > > Registerkarte **Bedienberechtigungen** > Registerkarte **Eigenschaften der Enterprise Benutzergruppen**

- Sie können Bedienberechtigungen wie Logbuch-Zugang oder Benutzeroberflächeneinstellungen konfigurieren.
- Für die Standardbenutzergruppen können diese Einstellungen nicht geändert werden.
- Sie können Bedienberechtigungen in Standardbenutzergruppen oder in Enterprise User Groups konfigurieren.

Detaillierte Informationen zu den verschiedenen Feldern finden Sie in der Online-Hilfe unter dem entsprechenden Anwendungsfenster.

Detaillierte Informationen zu den verschiedenen Feldern erhalten Sie, wenn Sie unten auf den Link des entsprechenden Anwendungsfensters klicken.

Siehe

- *Seite Eigenschaften der Benutzergruppen, Seite 335*
- *Seite mit den Bedienereigenschaften, Seite 342*
- *Seite Prioritäten, Seite 346*
- *Seite Benutzeroberfläche, Seite 346*
- *Seite „Server-Zugriff“, Seite 347*

27.9 Konfigurieren von Geräteberechtigungen

Hauptfenster > **Benutzergruppen** > Registerkarte **Benutzergruppen** > Registerkarte **Geräteberechtigungen**

oder

Hauptfenster > **Benutzergruppen** > Registerkarte **Enterprise Access** > Registerkarte **Geräteberechtigungen**

Sie können die Berechtigungen für alle Geräte des Logischen Baums unabhängig voneinander einstellen.

Wenn Sie freigegebene Geräte in einen Ordner verschieben, der für diese Benutzergruppe nicht freigegeben ist, müssen Sie die Berechtigungen für den Ordner einstellen, um Zugriff auf die darin enthaltenen Geräte zu gewähren.

- Für die Standardbenutzergruppen können diese Einstellungen nicht geändert werden.

– Sie können Geräteberechtigungen in Standardbenutzergruppen oder Enterprise Accounts konfigurieren.

Detaillierte Informationen zu den verschiedenen Feldern finden Sie in der Online-Hilfe unter dem entsprechenden Anwendungsfenster.
Detaillierte Informationen zu den verschiedenen Feldern erhalten Sie, wenn Sie unten auf den Link des entsprechenden Anwendungsfensters klicken.

Siehe

– *Seite Logischer Baum, Seite 342*
– *Seite Ereignisse und Alarme, Seite 341*
– *Seite „Prioritäten für Steuerungen“, Seite 339*
– *Seite Kamerafreigaben, Seite 338*
– *Seite Decoder-Freigaben, Seite 340*

27.10 Konfigurieren verschiedener Prioritäten

Problem	Mögliche Ursache	Aktion
1. Kein Ton	Verstärker	Überprüfen Sie, ob alle elektronischen Komponenten eingeschaltet sind, das Signalrouting korrekt ist, die Quelle aktiv ist, die Lautstärke aufgedreht ist, kein Kanal stummgeschaltet ist usw. Korrigieren/reparieren/ersetzen Sie nach Bedarf. Kommt weiterhin kein Ton, kann es an der Verkabelung liegen.
	Verkabelung	Überprüfen Sie, ob die korrekten Kabel am Verstärker angeschlossen sind. Spielen Sie mit dem Verstärker Audio in geringer Lautstärke ab. Verbinden Sie einen Testlautsprecher parallel mit der nicht funktionierenden Leitung. Ist kein Schallpegel oder nur ein sehr leiser Schallpegel vorhanden, liegt im Signalweg ein Kurzschluss vor (möglicherweise durch einen Riss, ein eingeklemmtes Kabel oder eine fehlende Verbindung verursacht). Überprüfen Sie mit dem Testlautsprecher jeden Anschluss und jede Verbindung im Signalweg, bis Sie das Problem gefunden und behoben haben. Achten Sie auf eine korrekte Polung.
2. Audioausgabe ist unterbrochen, verzerrt, oder es rauscht	Fehlerhafte Verbindung	Überprüfen Sie alle Verbindungen am Verstärker und an den Lautsprechern. Tritt das Problem weiterhin auf, überprüfen Sie die Verkabelung. Siehe Problem 1.
3. Dauerhafte Störgeräusche wie Brummen und Rauschen	Fehlerhafte Audioquelle oder fehlerhaftes anderes Gerät	Treten Störgeräusche auf, ohne dass Audio wiedergegeben wird, überprüfen Sie jede Komponente, um das Problem zu isolieren. Wahrscheinlich ist der Signalweg unterbrochen.

Problem	Mögliche Ursache	Aktion
	Schlechte Erdung	Überprüfen und korrigieren Sie die Systemerdung nach Bedarf.
4. Mit dem an INPUTS 1-2 angeschlossenen Mikrofon ist kein Signal hörbar.	Das Mikrofon erfordert eine Phantomspeisung.	Vergewissern Sie sich, dass das Mikrofon an die INPUTS 1-2 angeschlossen ist. Vergewissern Sie sich, dass PHANTOM für diesen Kanal eingeschaltet (**ON**) ist. Für INPUT 3–6 ist keine Phantomspeisung verfügbar.
	Der Eingangskanal ist stumm geschaltet (Mute) oder LEVEL ist zu niedrig.	Wählen Sie den Kanal aus, und stellen Sie sicher, dass er nicht stummgeschaltet ist. Wenn er nicht stummgeschaltet ist, erhöhen Sie LEVEL für den Kanal langsam, bis der Ton erzeugt wird.
5. Ton ist verzerrt, vordere LED ist aus, auf LCD-Display erscheint LIMIT.	Eingangssignal ist zu hoch	Reduzieren Sie den Eingangspegel oder die Lautsprecherlautstärke, um die Übersteuerung zu verhindern.
	Falsche Gain-Struktur, oder der Audioeingang (Mischpult/ Vorverstärker) ist übersteuert.	Überprüfen Sie mit dem VU-Meter auf dem LCD-Display, ob die Pegelregler der Audioquelle korrekt eingestellt sind. Bleibt der Balken des VU-Meters unverändert, oder signalisiert das System CLIP oder LIMIT, ist das Eingangssignal oder der Ausgangspegel zu hoch.
6. Das Mikrofon erzeugt ein akustisches Feedback (akustische Rückkopplung), wenn der Eingangspegel verstärkt wird.	Falsche Gain-Struktur (Verstärkungsstruktur)	Reduzieren Sie das Mikrofonsignal, indem Sie den INPUT-Pegel verringern. Das Positionieren des Mikrofons nahe an der Audioquelle erhöht den Gain (Verstärkung) vor einem Feedback (akustische Rückkopplung).
	MODE ist auf MUSIC eingestellt.	Ändern Sie MODE zu LIVE oder SPEECH.
	Die Mikrofonposition ist zu nahe vor dem Lautsprecher.	Stellen Sie die Lautsprecher möglichst so auf, dass sich das Mikrofon dahinter befindet. Wird ein separater Lautsprecher an einer Monitorposition verwendet, stellen Sie ihn in Richtung Mikrofonrückseite auf.
7. DSP-Steuerungsmenü ist gesperrt	Die **Menü-Sperrfunktion LOCK** wurde aktiviert. Auf dem LCD-Display erscheint ein Schlosssymbol.	Drücken Sie den Regler **MASTER VOLUME** oder die Softkeys für die Eingangsauswahl zum Entsperren.
8. Die QuickSmart Mobile App erkennt den Lautsprecher nicht	Bluetooth® aktivieren	Vergewissern Sie sich, dass am Lautsprecher Bluetooth® aktiviert ist. Für Android: Stellen Sie sicher, dass die Ortungsdienste aktiviert sind. Entfernen Sie den Lautsprecher von iOS/Android in den Einheitseinstellungen (manchmal auch „FORGET“ genannt).

Problem	Mögliche Ursache	Aktion
		Starten Sie die Kopplung neu. Stellen Sie sicher, dass das Telefon/Tablet die erforderliche Betriebssystemversion und die neuesten Updates installiert hat. Stellen Sie sicher, dass die neueste QuickSmart Mobile App installiert ist. Stellen Sie sicher, dass kein anderes Telefon/ Tablet mit demselben Lautsprecher verbunden ist.
9. PIN-Code konnte nicht entsperrt werden	Falscher PIN-Code eingegeben	PIN-Code-Eingabe wiederholen oder Halten Sie den Softkey **INPUT 2** und und den Regler **MASTER VOLUME** Taste mindestens 15 Sekunden lang gedrückt, um den Lautsprecher auf die Voreinstellungen zurückzusetzen.
10. Bei Verwendung von QuickSmart Link ist der Ton verzerrt oder unterbrochen	Ungeeignetes oder zu langes Kabel	Verwenden Sie geschirmte CAT5-Kabel (oder besser), die nicht länger als 100 m sind.
	Netzwerk-Hardware (Switches/Router) angeschlossen	Nur eine direkte Verbindung zwischen maximal zwei EKX Systemen darf korrekt funktionieren.

Hauptfenster > **Benutzergruppen** > Registerkarte **Benutzergruppen**
oder
Hauptfenster > **Benutzergruppen** > Registerkarte **Enterprise User Groups**
oder
Hauptfenster > **Benutzergruppen** > Registerkarte **Enterprise Access**
PTZ-SteuerungSie können die folgenden Prioritäten konfigurieren:

- Für Standardbenutzergruppen und **Enterprise User Groups**: Sie können die Alarmprioritäten für den Live Modus und den Playback Modus konfigurieren.
- Für Standardbenutzergruppen und **Enterprise Access**: Sie können die Prioritäten für die Übernahme von PTZ-Steuerungen und Bosch Allegiant Trunklines konfigurieren.
  Sie können eine PTZ-Sperrzeit konfigurieren, sodass ein Benutzer mit höherer Priorität die Kamerasteuerung von einem Benutzer mit niedrigerer Priorität übernehmen und für diesen Zeitbereich sperren kann.

So konfigurieren Sie Live- und Wiedergabe-Prioritäten:

1. Wählen Sie eine Standardbenutzergruppe oder eine Enterprise User Group aus.
2. Klicken Sie auf **Bedienberechtigungen**.
3. Klicken Sie auf die Registerkarte **Prioritäten**.
4. Verschieben Sie die Schieberegler im Feld **Automatisches Popup-Verhalten** nach Bedarf.

So konfigurieren Sie Prioritäten für PTZ und Bosch Allegiant Trunklines:

1. Wählen Sie eine Standardbenutzergruppe oder ein Enterprise Account aus.
2. Klicken Sie auf die Registerkarte **Geräteberechtigungen**.
3. Klicken Sie auf die Registerkarte **Prioritäten für Steuerungen**.
4. Verschieben Sie die Schieberegler im Feld **Prioritäten für Steuerungen** nach Bedarf.
5. Wählen Sie in der Liste **Timeout [min]** den erforderlichen Eintrag aus.

Siehe

- *Seite „Prioritäten für Steuerungen“, Seite 339*

– *Seite Prioritäten, Seite 346*

27.11 Kopieren von Freigaben für Benutzergruppen

Hauptfenster > **Benutzergruppen** > Registerkarte **Benutzergruppen**
oder
Hauptfenster > **Benutzergruppen** > Registerkarte **Enterprise User Groups**
oder
Hauptfenster > **Benutzergruppen** > Registerkarte **Enterprise Access**

Sie können Berechtigungen von einer Gruppe in eine andere bzw. von einem Konto in ein anderes kopieren. Sie müssen mindestens 2 Gruppen bzw. Konten konfiguriert haben.

So kopieren Sie Berechtigungen:

1. Wählen Sie im Benutzergruppen-Baum eine Gruppe oder ein Konto aus.
2. Klicken Sie auf .
   Das Dialogfeld **Benutzergruppen-Berechtigungen kopieren** wird angezeigt.
3. Wählen Sie die geeigneten Berechtigungen und eine Zielgruppe bzw. ein Zielkonto aus.
4. Klicken Sie auf **OK**. Die Gruppenberechtigungen dieser Gruppe werden in die andere Gruppe bzw. das andere Konto kopiert. Das Dialogfeld wird geschlossen.

28 Audit Trail-Seite

Hinweis!
BVMS Viewer bietet nur Grundfunktionen. Erweiterte Funktionen sind in BVMS Professional enthalten. Ausführliche Informationen zu den verschiedenen Versionen von BVMS finden Sie unter www.boschsecurity.com und in der BVMS Schnellauswahlhilfe: BVMS Schnellauswahlhilfe.

Hauptfenster > **Audit Trail**

Mit der Audit Trail-Funktion können Sie alle Änderungen an der Systemkonfiguration nachverfolgen und die Daten in eine CSV-Datei exportieren.

Voraussetzungen:
1. Installieren Sie die Audit Trail-Datenbank, indem Sie sie in der BVMS-Einrichtung auswählen (optionale Konfigurationsfunktion).
2. Sie verfügen über die folgende Berechtigung: **Audit Trail-Seite anzeigen**.
3. Unter **Einstellungen** > **Optionen...** > **Audit Trail** ist Audit Trail aktiviert.

Empfehlungen:
- Aktivieren Sie die Funktion Audit Trail nicht von Beginn an, da die Protokollierung umfangreich ist.
- Nehmen Sie stattdessen die Erstkonfiguration des Systems vor, erstellen Sie Auswertungen für die Inbetriebnahme, und aktivieren Sie anschließend die Audit Trail-Funktion, um weitere Änderungen zu protokollieren.
- Deaktivieren Sie die Audit Trail-Funktion außerdem beim Importieren von Konfigurationen.

So erweitern Sie Audit Trail-Daten oder blenden sie aus

1. Klicken Sie auf , um einen Datenknoten zu erweitern.
2. Klicken Sie auf , um einen Datenknoten auszublenden.
3. Klicken Sie auf **Alle erweitern/Alle schließen**, um alle geladenen Datenknoten zu erweitern oder auszublenden.

So laden Sie Audit Trail-Daten

▸ Klicken Sie auf **Mehr laden**.

Hinweis: Durch Klicken auf die Schaltfläche **Mehr laden** werden nur zehn Datenknoten gleichzeitig geladen.

So exportieren Sie Audit Trail-Daten

▸ Klicken Sie auf **Export**, um die geladenen Daten als CSV-Datei zu speichern.

Hinweis: Es werden nur die geladenen Daten exportiert.

Siehe
- *Dialogfeld „Optionen“ (Menü „Einstellungen“), Seite 121*
- *Seite „Konfigurationsberechtigungen“, Seite 348*

28.1 Audit Trail-Protokollierungsdetails

Hinweis: Wenn nicht genügend Speicherplatz in der Datenbank zur Verfügung steht, werden die ältesten Einträge automatisch gelöscht. Wenn die Speicherzeit abläuft, werden diese Einträge automatisch gelöscht.

Die Audit Trail-Tabelle enthält folgende Spalten:

Aktion	Die vom Benutzer ausgelöste Änderung.
Erstellt	Der BVMS-Konfiguration wurde ein neues Objekt hinzugefügt, z. B. eine Kamera oder ein Benutzer.
Modifiziert	Ein bereits vorhandenes Objekt in der Konfiguration wurde geändert, z. B. der Anzeigename einer Kamera.
Gelöscht	Ein vorhandenes Objekt in der Konfiguration wurde gelöscht.
Listeneintrag hinzugefügt	Ein Objekt wurde einer Liste hinzugefügt, z. B. eine Kamera einem VRM-Pool hinzugefügt.
Listenelement entfernt	Ein Objekt wurde aus einer Liste entfernt, z. B. eine Kamera aus einem VRM-Pool oder einem VSG
Objekttyp	Der Typ des Konfigurationsobjekts, das geändert wurde.
Objekt	Das geänderte Objekt, z. B. eine Kamera, ein Benutzer oder ein Zeitplan.
Netzwerkadresse	Die Netzwerkadresse des Objekts, falls vorhanden.
Objekt-Kontext 1 / **Objekt-Kontext 2**	Ein Kontext des geänderten Elements, in der Regel ein Vorgänger des Objekts. Beispiel: Einem iSCSI-Gerät wird ein Target hinzugefügt. Der Gerätekontext 1 ist das übergeordnete iSCSI-Gerät, Kontext 2 der VRM, zum dem das iSCSI-Gerät gehört.
Eigenschaft	Der Name der Eigenschaft, die geändert wurde.
Alter Wert	Der alte Wert, bevor die Änderung ausgelöst wurde.
Neuer Wert	Der neue Wert, der bei der Änderung festgelegt wurde.
Kontext 1 / **Kontext 2**	Zusätzlicher Kontext, in dem die Änderung beschrieben wird. Beispiel: Wenn Sie die Einstellungen einer Kamera in den Alarmoptionen eines Alarms ändern, wird diese Kamera als Kontext hinzugefügt.

28.2 Audit Trail-Dialogfeld zum Filtern

Im Dialogfeld zum Filtern können Sie Informationen in der Audit Trail-Datenbank filtern oder nach bestimmten Informationen suchen.
Das Dialogfeld enthält folgende vordefinierte Filter:

- Kategorie
- Aktion
- Zeitbereich

Wenn Sie im Filterdialogfeld mehrere Kategorien oder Aktionen auswählen, sind alle diese Abschnitte in der Suche enthalten.

Zusätzlich können Sie Zeichenfolgen im Feld „Freie Textsuche“ eingeben, mit denen Sie z. B. nach bestimmten Benutzern, Geräten oder Einstellungen filtern können. Wenn Sie mehrere Suchbegriffe eingeben, muss das Ergebnis alle im Suchfeld eingegebenen Worte enthalten.
Für Begriffe, die ein Leerzeichen enthalten, können Sie Anführungszeichen verwenden. Beispiel: "Camera 1".

Beispiel:
Sie wählen die Kategorien **Geräte** und **Karten und Struktur** aus, und geben im Freitextfeld den Kameranamen “Cam1” und den Benutzernamen “X” ein.
Ergebnis: In der Audit Trail-Datenbank werden alle Änderungen gefunden, die der Benutzer “X” an den Konfigurationsobjekten für die Kamera “Cam1” vorgenommen hat und die entweder in **Geräte** oder **Karten und Struktur** enthalten sind.

So verwenden Sie den Audit Trail-Filter

1. Klicken Sie auf **Filter**.
   Das Audit Trail-Dialogfeld zum Filtern wird geöffnet.
2. Klicken Sie nach der Filterkonfiguration auf **Übernehmen**.
3. Klicken Sie auf , um einzelne Filterobjekte zu löschen.
4. Klicken Sie auf **Alle Filter zurücksetzen**, um Ihre gesamte Filterkonfiguration zurückzusetzen.

29 Konfigurieren der videobasierten Brandmeldeanlage

Für die Konfiguration einer videobasierten Brandmeldung müssen Sie die folgenden Schritte durchführen:

1. Konfigurieren Sie eine Branderkennung auf Ihrer Branderkennungskamera.
   Verwenden Sie die Webseite der Kamera für diese Konfiguration.
   Detaillierte Informationen zum Konfigurieren einer Branderkennungskamera finden Sie unter
   – *Konfigurieren einer Branderkennungskamera, Seite 372*
2. Fügen Sie diese Branderkennungskamera zum System hinzu. Sie können die Branderkennungskamera zu einem VRM-Pool als nur Live-Encoder oder als Encoder mit lokaler Archivierung hinzufügen.
   Detaillierte Informationen zum Hinzufügen einer Kamera finden Sie unter
   – *Hinzufügen eines Encoders zu einem VRM-Pool, Seite 220*
   – *Hinzufügen eines Nur-Live-Encoders, Seite 220*
   – *Hinzufügen eines Encoders mit lokaler Archivierung, Seite 220*
3. Konfigurieren Sie ein Brandereignis für diese Kamera.
   – *Konfigurieren eines Brandereignisses, Seite 374*
4. Konfigurieren Sie den Alarm für das Brandereignis.
   – *Konfigurieren eines Feueralarms, Seite 375*

Siehe

– *Hinzufügen eines Encoders zu einem VRM-Pool, Seite 373*
– *Hinzufügen eines Nur-Live-Encoders, Seite 220*
– *Hinzufügen eines Encoders mit lokaler Archivierung, Seite 220*
– *Konfigurieren eines Brandereignisses, Seite 374*
– *Konfigurieren eines Feueralarms, Seite 375*

29.1 Konfigurieren einer Branderkennungskamera

Hauptfenster > **Geräte** > erweitern > erweitern > erweitern >
oder
Hauptfenster > **Geräte** > erweitern > erweitern > erweitern >
oder
Hauptfenster > **Geräte** > >
oder
Hauptfenster > **Geräte** > >

Zum Konfigurieren einer videobasierten Brandmeldung müssen Sie zunächst die Branderkennung auf der Branderkennungskamera konfigurieren.
Einzelheiten finden Sie im Benutzerhandbuch der Branderkennungskamera.

So führen Sie die Konfiguration durch:

1. Klicken Sie mit der rechten Maustaste auf das Gerätesymbol, und klicken Sie auf **Webseite im Browser anzeigen**.

2. Klicken Sie auf **Konfiguration**.
3. Erweitern Sie im Navigationsbereich **Alarm**, und klicken Sie auf **Feuerdetektion**.
4. Führen Sie die gewünschten Einstellungen durch.

29.2 Hinzufügen eines Encoders zu einem VRM-Pool

Informationen zum Hinzufügen eines Encoders zu einem VRM-Pool finden Sie unter *Hinzufügen von Encodern per Suchvorgang, Seite 179*.

Siehe

– *Hinzufügen eines Geräts, Seite 126*

29.3 Hinzufügen von Encodern per Suchvorgang

So fügen Sie Encoder per Suchvorgang hinzu:

1. Klicken Sie mit der rechten Maustaste auf und klicken Sie auf **Nach Encodern scannen**.
   Das Dialogfeld **BVMS Scan Wizard** wird angezeigt.
2. Wählen Sie die erforderlichen Encoder sowie den gewünschten VRM-Pool aus und klicken Sie auf **Zuordnen**, um diese dem VRM-Pool zuzuweisen.
3. Klicken Sie auf **Weiter >>**.
   Das Dialogfeld des Assistenten für die **Authentifizierung der Geräte** wird angezeigt.
4. Geben Sie das Passwort für jedes Gerät ein, das von einem Passwort geschützt ist.
   Passwortüberprüfungen erfolgen automatisch, wenn Sie während ein paar Sekunden keine weiteren Zeichen im Passwortfeld eingeben oder außerhalb des Passwortfelds klicken.
   Wenn die Passwörter aller Geräte identisch sind, können Sie es im ersten Feld **Passwort** eingeben. Machen Sie mit der Maus einen Rechtsklick und klicke Sie dann auf **Zellinhalt in Spalte kopieren**.
   In der **Status** Spalte wird die erfolgreiche Anmeldung mit angezeigt. Fehlgeschlagene Anmeldungen werden mithilfe von angezeigt.
5. Klicken Sie auf **Fertig stellen**.
   Das Gerät wird zum Gerätebaum hinzugefügt.

Das ⚠ Symbol weist auf einen Fehler hin, um den Sie sich kümmern müssen. In der QuickInfo finden Sie weitere Informationen zu dem jeweiligen Fehler.

29.4 Hinzufügen von Nur-Live-Geräten per Suchvorgang

So fügen Sie Nur-Live-Geräte von Bosch per Suchvorgang hinzu:

1. Klicken Sie mit der rechten Maustaste auf und klicken Sie auf **Nach Nur Live-Encodern scannen**.
   Das Dialogfeld **BVMS Scan Wizard** wird angezeigt.
2. Aktivieren Sie die Kontrollkästchen der Geräte, die hinzugefügt werden sollen.
3. Klicken Sie auf **Weiter >>**.
   Das Dialogfeld des Assistenten für die **Authentifizierung der Geräte** wird angezeigt.

4. Geben Sie das Passwort für jedes Gerät ein, das von einem Passwort geschützt ist.
   Passwortüberprüfungen erfolgen automatisch, wenn Sie während ein paar Sekunden keine weiteren Zeichen im Passwortfeld eingeben oder außerhalb des Passwortfelds klicken.
   Wenn die Passwörter aller Geräte identisch sind, können Sie es im ersten Feld **Passwort** eingeben. Machen Sie mit der Maus einen Rechtsklick und klicke Sie dann auf **Zellinhalt in Spalte kopieren**.
   In der **Status** Spalte wird die erfolgreiche Anmeldung mit .
   angezeigt. Fehlgeschlagene Anmeldungen werden mithilfe von angezeigt.
5. Klicken Sie auf **Fertig stellen**.
   Das Gerät wird zum Gerätebaum hinzugefügt.

Das Symbol weist auf einen Fehler hin, um den Sie sich kümmern müssen. In der QuickInfo finden Sie weitere Informationen zu dem jeweiligen Fehler.

29.5 Hinzufügen von Encodern mit lokaler Archivierung per Suchvorgang

Hauptfenster > **Geräte** > Erweitern >
Ermöglicht es Ihnen, Encoder mit lokaler Archivierung hinzuzufügen und zu konfigurieren.

So fügen Sie Encoder mit lokaler Archivierung per Suchvorgang hinzu:

1. Klicken Sie im Gerätebaum mit der rechten Maustaste auf und klicken Sie anschließend auf **Nach Encodern mit lokaler Archivierung scannen**.
   Das Dialogfeld **BVMS Scan Wizard** wird angezeigt.
2. Aktivieren Sie die Kontrollkästchen der Geräte, die hinzugefügt werden sollen.
3. Klicken Sie auf **Weiter >>**.
   Das Dialogfeld des Assistenten für die **Authentifizierung der Geräte** wird angezeigt.
4. Geben Sie das Passwort für jedes Gerät ein, das von einem Passwort geschützt ist.
   Passwortüberprüfungen erfolgen automatisch, wenn Sie während ein paar Sekunden keine weiteren Zeichen im Passwortfeld eingeben oder außerhalb des Passwortfelds klicken.
   Wenn die Passwörter aller Geräte identisch sind, können Sie es im ersten Feld **Passwort** eingeben. Machen Sie mit der Maus einen Rechtsklick und klicke Sie dann auf **Zellinhalt in Spalte kopieren**.
   In der **Status** Spalte wird die erfolgreiche Anmeldung mit .
   angezeigt. Fehlgeschlagene Anmeldungen werden mithilfe von angezeigt.
5. Klicken Sie auf **Fertig stellen**.
   Das Gerät wird zum Gerätebaum hinzugefügt.

29.6 Konfigurieren eines Brandereignisses

Hauptfenster > **Ereignisse**

So führen Sie die Konfiguration durch:

1. Wählen Sie im Baum **Encoder/Decoder > Kamera > Brand- oder Rauch-Status** > **Brand oder Rauch gemeldet** aus.
   Die entsprechende Ereigniskonfigurations-Tabelle wird angezeigt.
2. Klicken Sie in der Spalte **Alarm auslösen** – **Zeitplan** auf eine Zelle, und wählen Sie einen Zeitplan aus.
   Der Zeitplan bestimmt, wann der Alarm ausgelöst wird.
   Wählen Sie einen der Aufzeichnungszeitpläne oder Aktionszeitpläne aus, die Sie auf der Seite **Zeitpläne** konfiguriert haben.
3. Nehmen Sie die erforderlichen Einstellungen vor.

Hinweis: Sie können dasselbe Verfahren für die anderen verfügbaren Brandereignisse verwenden.

29.7 Konfigurieren eines Feueralarms

Hauptfenster > **Alarme**

So führen Sie die Konfiguration durch:

1. Wählen Sie im Baum **Encoder/Decoder > Kamera > Brand- oder Rauch-Status** > **Brand oder Rauch gemeldet** aus.
   Die entsprechende Alarmkonfigurations-Tabelle wird angezeigt.
2. Nehmen Sie die erforderlichen Einstellungen vor.

30 Konfigurieren der MIC IP 7000, die mit einem VIDEOJET 7000 connect verbunden ist

Für den Betrieb einer MIC IP 7000-Kamera, die mit einem VIDEOJET 7000 connect verbunden ist, müssen Sie für eine ordnungsgemäße Funktion die folgende Konfiguration durchführen.

Bevor Sie die MIC IP-Kamera zu BVMS hinzufügen, müssen Sie die folgenden Aufgaben durchführen:

1. Setzen Sie die MIC IP 7000-Kamera und das VIDEOJET 7000 connect-Gerät auf der Webseite des jeweiligen Geräts auf die Werkseinstellungen zurück.
2. Legen Sie für die MIC IP 7000-Kamera die **MIC IP Starlight 7000 HD-VJC-7000**-Variante fest.
3. Konfigurieren Sie die MIC IP 7000-Kamera und das VIDEOJET 7000 connect-Gerät gemäß der Dokumentation, die im Lieferumfang der Geräte enthalten ist.
4. Wenn Sie ANR verwenden möchten, führen Sie das ANR-Setup-Dienstprogramm für das VIDEOJET 7000 connect-Gerät aus.
   Führen Sie diese Aufgabe auf einem Computer aus, der sich im gleichen Netzwerk wie das VIDEOJET 7000 connect-Gerät befindet.
   Sie finden das ANR-Setup-Dienstprogramm auf der Produktkatalogseite für das VIDEOJET 7000 connect-Gerät.

Führen Sie folgende Schritte zum Hinzufügen und Konfigurieren der MIC IP 7000-Kamera in BVMS durch:

1. Fügen Sie im Gerätebaum nur die MIC IP 7000-Kamera hinzu.
   Sie können das VIDEOJET 7000 connect-Gerät nicht zu BVMS hinzufügen.
2. Klicken Sie mit der rechten Maustaste auf die gerade hinzugefügte Kamera und dann auf **Encoder bearbeiten**.
   Das Dialogfeld **Encoder bearbeiten** wird angezeigt.
   Die Gerätefunktionen werden automatisch entsprechend der oben konfigurierten Variante abgerufen.
3. Konfigurieren Sie bei Bedarf ANR auf der Seite **Kameras und Aufzeichnung**.

31 Problembehandlung

Dieses Kapitel enthält Informationen zur Behebung bekannter Probleme im BVMS Configuration Client.

Probleme während der Installation

Problem	Ursache	Lösung
Setup zeigt falsche Zeichen an.	Die Windows-Spracheinstellungen sind nicht korrekt.	*Konfigurieren der gewünschten Sprache in Windows, Seite 379*
Setup stoppt und zeigt die Meldung an, dass OPC-Server nicht installiert werden kann.	OPC-Server-Dateien können nicht überschrieben werden.	Deinstallieren Sie OPC Core Components Redistributable, und starten Sie BVMS Setup neu.
Die Software kann nicht durch Ausführen des Setup deinstalliert werden.		Navigieren Sie zu Control Panel > Add/Remove Programs, und deinstallieren Sie BVMS.

Probleme unmittelbar nach dem Starten der Anwendung

Problem	Ursache	Lösung
BVMS zeigt die falsche Sprache an.	In Windows wurde nicht die gewünschte Sprache eingestellt.	*Konfigurieren der Sprache des Configuration Client, Seite 72* oder *Konfigurieren der Sprache des Operator Client, Seite 72*
Das Anmeldedialogfeld des Operator Client wird in der falschen Sprache angezeigt.	Sie haben zwar die Sprache für den Operator Client im Configuration Client geändert, die Sprache für das Anmeldedialogfeld des Operator Client hängt jedoch von der Spracheinstellung in Windows ab.	*Konfigurieren der gewünschten Sprache in Windows, Seite 379*

Probleme mit der Anzeigesprache

Problem	Ursache	Lösung
Einige Anzeigetexte im Configuration Client oder Operator Client erscheinen in einer Fremdsprache (meist Englisch).	Auf dem Computer, auf dem der Management Server installiert ist, wird das Betriebssystem häufig in Englisch ausgeführt. Wenn die BVMS Datenbank auf diesem Computer generiert wird, werden daher viele Anzeigetexte auf Englisch erzeugt. Die auf einem Operator Client Computer	Nehmen Sie keine Änderung vor.

Problem	Ursache	Lösung
	konfigurierte Windows Sprache hat darauf keine Auswirkung. Zur Vermeidung solcher Sprachdiskrepanzen installieren Sie die Management Server Software auf einem Computer, der die gewünschte Sprache für die Windows Benutzeroberfläche aufweist.	

Probleme mit dem Bosch IntuiKey Keyboard

Problem	Ursache	Lösung
Das Bosch IntuiKey Keyboard löst einen Alarm aus, und die Softkey-Anzeige zeigt Off Line an.	Die Verbindung zur Arbeitsstation ist unterbrochen. Das Kabel wurde beschädigt/ entfernt, oder die Arbeitsstation wurde zurückgesetzt.	*Wiederherstellen der Verbindung mit einem Bosch IntuiKey Keyboard, Seite 379*

Probleme mit den Einstellungen in der Aufzeichnungssteuerung der Sound-Karte

Problem	Ursache	Lösung
Bei Einsatz eines Mikrofons für die Intercom-Funktion treten Rückkopplungen auf.	In der Aufzeichnungssteuerung der Sound-Karte muss Mikrofon (nicht Stereo-Mix oder Ähnliches) ausgewählt sein. Beim Starten prüft der Operator Client die Konfigurationsdatei und gleicht die Einstellungen in der Aufzeichnungssteuerung entsprechend ab. Die Konfigurationsdatei enthält einen Standardeintrag, der möglicherweise nicht mit Ihrer Systemkonfiguration übereinstimmt. Diese Einstellung wird bei jedem Start des Operator Client wiederhergestellt.	Ändern Sie die Einstellung in der Konfigurationsdatei des Operator Client in Mikrofon.

Abstürzen des Configuration Client

Problem	Ursache	Lösung
Configuration Client stürzt ab.	Wenn in einer Allegiant Datei viele Kameras konfiguriert sind, die nicht mit dem Bosch Video	Siehe *Reduzieren der Anzahl der Allegiant Kameras, Seite 379*.

Problem	Ursache	Lösung
	Management System verbunden sind, können Sie die Anzahl reduzieren. Dadurch werden unnötige Systemlasten vermieden.	

31.1 Konfigurieren der gewünschten Sprache in Windows

Wenn Sie die Anzeigesprache für die Einrichtung des BVMS ändern möchten, müssen Sie die Sprache unter Windows ändern. Nachdem Sie die folgenden Schritte durchgeführt haben, wird der Computer zur Aktivierung der Spracheinstellungen neu gestartet.

So konfigurierten Sie die gewünschte Sprache:

1. Klicken Sie auf **Start** und **Systemsteuerung**, und doppelklicken Sie anschließend auf **Regions- und Sprachoptionen**.
2. Klicken Sie auf die Registerkarte **Erweitert**, und wählen Sie unter **Sprache für Programme, die Unicode nicht unterstützen** die gewünschte Sprache aus.
3. Klicken Sie auf **OK.**
4. Klicken Sie in den nächsten Meldungsfeldern jeweils auf **Ja**.
   Der Computer wird neu gestartet.

31.2 Wiederherstellen der Verbindung mit einem Bosch IntuiKey Keyboard

1. Schließen Sie das Kabel wieder an, oder warten Sie, bis die Arbeitsstation online ist.
   Die Meldung Off Line wird nicht mehr angezeigt.
2. Drücken Sie den Softkey Terminal, um das BVMS aufzurufen.

31.3 Reduzieren der Anzahl der Allegiant Kameras

Zur Bearbeitung der Allegiant Datei benötigen Sie die Allegiant Master Control Software.

So reduzieren Sie die Anzahl der Allegiant Kameras:

1. Starten Sie die Master Control Software.
2. Öffnen Sie die Allegiant Datei.
3. Klicken Sie auf die Registerkarte Camera.
4. Markieren Sie die Kameras, die nicht benötigt werden.
5. Klicken Sie im Menü Edit auf Delete.
6. Speichern Sie die Datei. Die Dateigröße bleibt unverändert.
7. Wiederholen Sie den letzten Schritt für Monitore, die Sie nicht benötigen. Klicken Sie auf die Registerkarte Monitors.
8. Importieren Sie diese Datei in das Bosch Video Management System (siehe *Hinzufügen eines Geräts, Seite 126*).

31.4 Verwendete Ports

In diesem Abschnitt werden alle Ports aufgeführt, die für Komponenten von BVMS innerhalb eines LANs offen sein müssen. Geben Sie diese Ports nicht für das Internet frei! Verwenden Sie für den Betrieb über das Internet sichere Verbindungen wie VPN.

In jeder Tabelle werden die lokalen Ports aufgeführt, die auf dem Computer offen sein müssen, auf dem der Server installiert ist bzw. die für den Router/Ebene-3-Switch freigegeben wurden, der mit der Hardware verbunden ist.
Konfigurieren Sie in einer Windows-Firewall eine eingehende Regel für jeden offenen Port.
Lassen Sie alle ausgehenden Verbindungen für alle BVMS Softwareanwendungen zu.

Management Server-/Enterprise Management Server-Ports

Server (Listener)	Protokoll	Eingehende Ports	Client (Requester)	Bemerkung
Management Server	UDP	123	Encoder	TimeServer NTP
Management Server	TCP	5322	Operator Client	SSH-Verbindung
Management Server	TCP	5422	Operator Client	Berechtigungsanbieter-Dienst
Management Server	TCP	5389	ONVIF-Gerät	ONVIF-Proxy, Ereignisbenachrichtigung
Management Server	TCP	5390	Operator Client, Configuration Client	.NET Remoting
Management Server	TCP	5391	Operator Client, Configuration Client, NVR Clients	Remoting-Port für alle NVR Services
Management Server	TCP	5392	Operator Client, Configuration Client, BVMS SDK-Anwendung	WCF, gateway.push.apple.com
Management Server	TCP	5393	Operator Client, VRM	Data-Access-Service
Management Server	TCP	5394	Operator Client	Remoting-Port für Operator Client
Management Server	TCP	5395	Configuration Client, Operator Client	Benutzereinstellungen, Datenübertragung
Management Server	TCP	5396	Configuration Client, WCF Clients	Mex Eingangspunkt (normalerweise ausgeschaltet)
Management Server	TCP	5397	Operator Client für NoTouchDeployment	NoTouchDeployment-Port
Management Server	TCP	5398	Configuration-API-Client	Interne Kommunikation zwischen AKKA.Net Komponente und CS
Management Server	UDP	12544	SNMP-Client	BVMS SNMP-Port für GET-Abfragen
Management Server	TCP	162	SNMP	

Server (Listener)	Protokoll	Eingehende Ports	Client (Requester)	Bemerkung
Management Server	TCP	5389 - 5396	BVMS-Ports	
Management Server	TCP, UDP	135	BRS DCOM	BRS
Management Server	TCP	808	BRS WebService (DIBOS)	Zentraler Server, der an diesem Port mit DiBos verbunden ist, wenn WCF verbunden ist
Management Server	TCP	1756 / 1757	RCP	1757 für sekundäre VRM

Zusätzliche Zentralkomponenten

Server (Listener)	Protokoll	Eingehende Ports	Client (Requester)	Bemerkung
Configuration Client	UDP	1024 - 65535	Encoder, VRM	Video-Streaming
Konfiguration API	TCP	5399	REST-API Client	Konfiguration API
Management Server	TCP	5443	PID	PID-Verbindung, Zugriff über HTTPS
Arbeitsstationsüberwachung	TCP	5410	Operator Client, Management Server	
Arbeitsstationsüberwachung	TCP	5411	GRPC-Dienst	
Metadaten-Dienst	TCP	5460	GRPC-Dienst	

Video Recording Manager-Ports

Server (Listener)	Protokoll	Eingehende Ports	Client (Requester)	Bemerkung
VRM	TCP	554 / 555	RTSP-Client	Primären / sekundären RTSP Stream abrufen
VRM	TCP	40023	Telnet-Client	Telnet (nur lokaler Host von VRM 4.x)
VRM	TCP	40080 / 40081	VRM Client	HTTP port vj_generic.dll
VRM	TCP	41080 / 41081	VRM Client	HTTP vj_generic.dll (nur lokaler Host)
VRM	TCP	1756 / 1757	Management Server, Configuration Client	über RCP+, (1757 für sekundären VRM RCP+ Client)

Server (Listener)	Protokoll	Eingehende Ports	Client (Requester)	Bemerkung
VRM	UDP	1757	Management Server, Operator Client	Scan-Zielübermittlung
VRM	UDP	1758	Management Server, Configuration Client	Scan-Reaktion
VRM	UDP	1759	Management Server, Configuration Client	Netzwerkentdeckung, Scan-Ziel Multicast
VRM	UDP	1760		
VRM	UDP	1800 / 1900	Management Server, Operator Client	Scan-Ziel für Multicast
VRM	TCP	80	Operator Client	Primäre VRM-Wiedergabe über http
VRM	TCP	443	Operator Client	Primäre VRM-Wiedergabe über https
VRM	TCP	81	Operator Client	Sekundäre VRM-Wiedergabe über http
VRM	TCP	444	Operator Client	Sekundäre VRM-Wiedergabe über https

Bosch Video Streaming Gateway-Ports

Server (Listener)	Protokoll	Eingehende Ports	Client (Requester)	Bemerkung
Bosch Video Streaming Gateway	TCP	8080 - 8086	VRM, Management Server, Configuration Client, Operator Client	HTTP
Bosch Video Streaming Gateway	TCP	8443 - 8449	VRM, Management Server, Configuration Client, Operator Client	HTTPS
Bosch Video Streaming Gateway	TCP	8756 - 8762	VRM, Management Server, Configuration Client	RCP+
Bosch Video Streaming Gateway	TCP	8443-8449	VRM, Management Server, Configuration Client, Operator Client	HTTPS
Bosch Video Streaming Gateway	UDP	1757	VRM-Client	Scan-Zielübermittlung
Bosch Video Streaming Gateway	UDP	1758	VRM-Client	Scan-Reaktion
Bosch Video Streaming Gateway	UDP	1759	VRM-Client	Netzwerkentdeckung, Scan-Ziel Multicast

Server (Listener)	Protokoll	Eingehende Ports	Client (Requester)	Bemerkung
Bosch Video Streaming Gateway	UDP	1800, 1900	VRM Configuration Client	Netzwerkentdeckung, Scan-Ziel Multicast
Bosch Video Streaming Gateway	UDP	1064-65535	Encoder, VRM	Video-Streaming

iSCSI-Speichersystemports

Konfigurieren Sie die Portweiterleitung am angeschlossenen Router für dieses Gerät.

Server (Listener)	Protokoll	Eingehende Ports	Client (Requester)	Bemerkung
iSCSI Speichersystem	TCP	3260	Encoder, VRM, Configuration Client, Operator Client	iSCSI Speichersystem

DVR-Ports

Konfigurieren Sie die Portweiterleitung am angeschlossenen Router für dieses Gerät.

Server (Listener)	Protokoll	Eingehende Ports	Client (Requester)	Bemerkung
DVR	TCP	80	Management Server, Configuration Client, Operator Client	Zugriff über HTTP
DVR	TCP	443	Management Server, Configuration Client, Operator Client	Zugriff über HTTPS

ONVIF-Kamera-/Kamera-/Encoderports

Konfigurieren Sie die Portweiterleitung am angeschlossenen Router für dieses Gerät.

Server (Listener)	Protokoll	Eingehende Ports	Client (Requester)	Bemerkung
Encoder	TCP	80	Management Server, VSG, Configuration Client, Operator Client	Zugriff über HTTP
Encoder	TCP	443	Management Server, VSG, Configuration Client, Operator Client	Zugriff über HTTPS
Encoder	UDP	123	Management Server, VRM	SNTP
Encoder	UDP	161	Management Server, VRM	SNMP
Encoder	TCP	554	Operator Client, BVMS SDK Anwendung, VSG	RTSP-Streaming
Encoder	TCP	3260	Encoder (ausgehend)	iSCSI-Aufzeichnung
Encoder	TCP	1756	Decoder, Management Server, Operator Client	Ausgehende Verbindung für die Bosch-Kameras

Server (Listener)	Protokoll	Eingehende Ports	Client (Requester)	Bemerkung
Encoder	UDP	1757	Decoder, Management Server, Operator Client	Scan-Zielübermittlung
Encoder	UDP	1758	Decoder, Management Server, Operator Client	Scan-Reaktion
Encoder	UDP	1800	Decoder, Management Server, Operator Client	Netzwerkentdeckung, Scan-Ziel Multicast
Encoder	UDP	1900		SSDP (optionaler Encoder-Port)
Encoder	TCP	21		FTP (optionaler Encoder-Port)
Encoder	UDP	3702		UPNP (optionaler Encoder-Port)
Encoder	UDP	9554		SRTSP (optionaler Encoder-Port)
Encoder	UDP	15344 / 15345		RTSP senden (optionaler Encoder-Port)

BVMS Decoder-Ports

Konfigurieren Sie die Portweiterleitung am angeschlossenen Router für dieses Gerät.

Server (Listener)	Protokoll	Eingehende Ports	Client (Requester)	Bemerkung
Decoder	TCP	1756	Management Server, Operator Client, Configuration Client, BVMS SDK Anwendung	Ausgehende Verbindung für die Bosch-Kameras
Decoder	UDP	1757	Management Server, Operator Client	Scan-Zielübermittlung
Decoder	UDP	1758	Management Server, Operator Client	Scan-Reaktion
Decoder	UDP	1800	Management Server, Operator Client	Netzwerkentdeckung, Scan-Ziel Multicast
Decoder	TCP	80	Operator Client	Zugriff über HTTP
Decoder	TCP	443	Operator Client	Zugriff über HTTPS
Decoder	UDP	1024-65535	Encoder	Streaming-Ports
Decoder	UDP	123	Management Server, VRM	SNTP
Decoder	UDP	161	Management Server, VRM	SNMP

BVMS Operator Client/Cameo SDK-Ports

Server (Listener)	Protokoll	Eingehende Ports	Client (Requester)	Bemerkung
Operator Client	TCP	5394	BVMS SDK-Anwendung, BIS	WCF
Operator Client	UDP	1024-65535	Encoder, VRM	Video-Streaming

Server (Listener)	Protokoll	Eingehende Ports	Client (Requester)	Bemerkung
Operator Client	TCP	40082		
Operator Client	TCP	41756		

LPR, BVMS Geräteadapter-Ports

Server (Listener)	Protokoll	Eingehende Ports	Client (Requester)	Bemerkung
BVMS Geräteadapter	TCP	31000	LPR Kamera-Client	VRC

AMS, Access Management System-Ports

Server (Listener)	Protokoll	Eingehende Ports	Client (Requester)	Bemerkung
AMS	TCP	62904	Management Server	Zugriff über HTTPS

Transcoder

Server (Listener)	Protokoll	Eingehende Ports	Client (Requester)	Bemerkung
	UDP	5080		
	UDP	5443		
	UDP	5756		

31.5 Ermöglicht die Protokollierung von ONVIF-Ereignissen

Hinweis!
Hinweis: Diese Funktion wird bald eingestellt.
Verwenden Sie das ONVIF Camera Event Driver Tool zur einfachen ONVIF-Ereigniszuordnung.
Siehe *Starten des ONVIF Camera Event Driver Tool aus dem Configuration Client, Seite 209*.

Sie können die Protokollierung für ONVIF Ereignisse aktivieren, zum Beispiel wenn Sie Probleme beim Empfang von BVMS Ereignissen haben. Die Protokollierung unterstützt Sie dabei, das Problem zu finden.

So aktivieren Sie die Protokollierung:

1. Öffnen Sie die Datei `%programfiles%\Bosch\VMS\AppData\Server\CentralServer\BVMSLogCfg.xml` in einem entsprechenden Editor, z. B. Notepad. Starten Sie die Notepad-Anwendung als Administrator.
2. Navigieren Sie zur Zeile mit der nachfolgenden Zeichenfolge:
   `Add logging for onvif events of a device by network address`
   Die kommentierte Zeile enthält eine kurze Erklärung.
3. Geben Sie als Protokollnamen `OnvifEvents.<Networkaddress>` ein.
   Geben Sie nur `OnvifEvents` ein, um die Ereignisse für alle ONVIF-Geräte zu protokollieren.
4. Geben Sie als Pegelwert `DEBUG` für alle eingehenden und ausgehenden Ereignisse ein.
   Geben Sie `INFO` für alle ausgehenden Ereignisse ein.
   Geben Sie `WARN` oder `ERROR` zum Deaktivieren ein.

Hinweis: Für die Aktivierung muss der zentrale Server ggf. neu gestartet werden.
Die folgenden Zeilen zeigen ein Beispiel für die Protokollierung der Ereignisse von Gerät 172.11.122.22 mit allen aus- und eingehenden Ereignissen:

```
<logger name="OnvifEvents.172.11.122.22" additivity="false">
<level value = "DEBUG"/>
<appender-ref ref="OnvifRollingFileAppender"/>
</logger>
```

Support

Supportdienstleistungen erhalten Sie unter www.boschsecurity.com/xc/en/support/.
Bosch Security and Safety Systems bietet Support in diesen Bereichen:

- Apps und Tools
- Building Information Modeling
- Garantie
- Problembehandlung
- Reparatur und Austausch
- Produktsicherheit

Bosch Building Technologies Academy

Besuchen Sie die Website der Bosch Building Technologies Academy und erhalten Sie Zugang zu **Schulungskursen, Videoanleitungen** und **Dokumenten**: www.boschsecurity.com/xc/en/support/training/

Siehe

- *Starten des ONVIF Camera Event Driver Tool aus dem Configuration Client, Seite 209*
- *Konfigurieren einer ONVIF-Mapping-Tabelle, Seite 243*
- *ONVIF-Ereigniszuordnung, Seite 42*

Glossar

4-Augen-Prinzip

Sicherheitsrichtlinie, die zwei verschiedene Benutzer für die Anmeldung am Operator Client erfordert. Beide Benutzer müssen Mitglied einer normalen Bosch Video Management System Benutzergruppe sein. Diese Benutzergruppe (oder diese Benutzergruppen, wenn die Benutzer Mitglieder verschiedener Benutzergruppen sind) muss zu einer 4-Augen-Gruppe gehören. Eine 4-Augen-Gruppe verfügt über eigene Zugriffsrechte im Bosch Video Management System. Diese 4-Augen-Gruppe sollte über mehr Zugriffsrechte verfügen als die normale Benutzergruppe, zu der die Benutzer gehören. Beispiel: Benutzer A ist Mitglied einer Benutzergruppe namens Gruppe A. Benutzer B ist Mitglied der Gruppe B. Zusätzlich wird eine 4-Augen-Gruppe konfiguriert, deren Mitglieder Gruppe A und Gruppe B sind. Für die Benutzer von Gruppe A ist das 4-Augen-Prinzip optional, für Benutzer von Gruppe B ist es obligatorisch. Wenn sich Benutzer A anmeldet, wird ein zweites Dialogfeld zur Anmeldebestätigung angezeigt. In diesem Dialogfeld kann sich ein zweiter Benutzer anmelden, wenn er verfügbar ist. Andernfalls kann Benutzer A fortfahren und den Operator Client starten. Er verfügt dann nur über die Zugriffsrechte von Gruppe A. Wenn sich Benutzer B anmeldet, wird ebenfalls ein zweites Anmeldedialogfeld angezeigt. In diesem Dialogfeld muss sich ein zweiter Benutzer anmelden. Andernfalls kann Benutzer B den Operator Client nicht starten.

Aktionszeitplan

Dient zur zeitlichen Planung von Ereignissen, die im Bosch Video Management System auftreten können, beispielsweise die Durchführung eines Kommandoskripts. In „Ereignisse“ werden den Ereignissen Aktionszeitpläne zugeordnet. Für die Planung von Ereignissen können Sie auch Aufzeichnungszeitpläne verwenden. Mit einem Standardaktionszeitplan können Sie Zeitbereiche für jeden Wochentag, Feiertage und besondere Tage konfigurieren. Mit einem wiederkehrenden Aktionszeitplan können Sie wiederkehrende Zeitbereiche konfigurieren. Sie können täglich, wöchentlich, monatlich oder jährlich wiederkehren.

Alarm

Ereignis, das zum Erstellen eines Alarms konfiguriert wird. Dabei handelt es sich um eine besondere Situation (erkannte Bewegung, Läuten der Türklingel, Signalverlust usw.), die eine sofortige Reaktion erfordert. Ein Alarm kann ein Video im Live Modus oder Playback Modus, einen Aktionsplan, eine Web-Seite oder eine Karte anzeigen.

Alarmfensterbereich

Bildfensterbereich zum Anzeigen eines oder mehrerer Alarmfenster.

Alarmliste

Fenster im Bosch Video Management System, in dem eine Liste aktiver Alarme angezeigt wird.

Allegiant

Bosch Produktfamilie analoger Kreuzschienensysteme.

ANR

Automated Network Replenishment. Ein integrierter Prozess, bei dem fehlende Videodaten nach einem Netzwerkfehler von einem Video-Transceiver auf den Netzwerk-Videorekorder kopiert werden. Die kopierten Videodaten füllen genau die nach dem Netzwerkfehler entstandene Lücke auf. Daher muss der Transceiver mit lokalen Speichermedien ausgestattet sein. Die Aufzeichnungskapazität der lokalen Speichermedien lässt sich mit folgender Formel berechnen: (Netzwerkbandbreite x geschätzte Netzwerkausfallzeit + Sicherheitspuffer) x (1 + 1/ Sicherungsgeschwindigkeit). Die resultierende Aufzeichnungskapazität ist erforderlich, da die Daueraufzeichnung während des Kopiervorgangs weiterläuft.

Arbeitsstation

In der BVMS Umgebung: Ein dedizierter Computer, auf dem Operator Client installiert ist. Dieser Computer ist als Arbeitsstation im Configuration Client zur Aktivierung bestimmter Funktionen konfiguriert.

ATM

Akronym für Automatic Teller Machine (Geldautomat).

Aufzeichnungszeitplan

Dient zur zeitlichen Planung der Aufzeichnung sowie einiger Ereignisse, wie Starten der Datensicherung oder Einschränken der Anmeldung. Lücken oder Überschneidungen in Aufzeichnungszeitplänen sind nicht möglich. Er gibt auch die Aufzeichnungsqualität für das Video an.

Benutzergruppe

Mit Benutzergruppen lassen sich gemeinsame Benutzerattribute definieren, wie Berechtigungen, Rechte und Prioritäten für die PTZ-Kamerasteuerung. Durch die Mitgliedschaft in einer Gruppe erbt ein Benutzer automatisch alle Attribute dieser Gruppe.

Bereich

Eine Gruppe von Erkennungsgeräten verbunden mit dem Sicherheitssystem

Bereiche

„Bereich“ ist ein Begriff aus dem Gebiet der ONVIF-Kameras. Es ist ein Parameter, der für die Prüfung von ONVIF-Geräten verwendet wird. In der Regel enthält der Parameter einen URI wie folgend: onvif://www.onvif.org/<path>. Der Parameter <Pfad> kann z. B. ein Video-Encoder oder ein Audio-Encoder sein. Ein ONVIF-Gerät kann mehrere Bereiche haben. Dieser URI bezeichnet den Aufgabenbereich des Geräts.

B-Frame

Bidirectional Frame. Teil eines Videokomprimierungsverfahrens.

Bildfenster

Wird zum Anzeigen von Live- oder aufgezeichneten Videobildern einer einzelnen Kamera, eines Lageplans, eines Dokuments, einer Sequenz, einer Monitorgruppe, einer externen Anwendung oder eines Karten-Anzeigebereichs verwendet.

Bildfensterbereich

Container für Bildfenster, strukturiert durch eine Bildfensteranordnung.

Bildfensterleiste

Symbolleiste eines Bildfensters.

BIS

Building Integration System

CCL-Emulation

Die Emulation der Command Console Language, die zur Steuerung der Allegiant Kreuzschiene verwendet wird. Sie können diesen Satz an Befehlen nutzen, um eine BVMS IP-Kamera oder einen Encoder auf einen BVMS IP-Decoder umzuschalten. Sie können keine alten Analogkameras oder die Allegiant Kreuzschiene selbst direkt steuern.

Decoder

Wandelt einen digitalen Stream in einen analogen Stream um.

DNS

Domain Name System. Ein DNS-Server konvertiert eine URL (z. B. www.myDevice.com) in eine IP-Adresse für Netzwerke, die das TCP/IP-Protokoll verwenden.

Dokument

BVMS unterstützt die folgenden Dokumenten-Dateiformate: HTM, URL, MHT, HTML und TXT.

DTP

Ein DTP-Gerät (Data Transform Processor) wandelt serielle Daten von ATM-Geräten in ein bestimmtes Datenformat um und sendet diese Daten über das Ethernet an BVMS. Sie müssen sicherstellen, dass ein Transformationsfilter im DTP-Gerät festgelegt ist. Diese Aufgabe wird durch eine separate Software vom Hersteller des DTP-Geräts ausgeführt.

Dual Streaming

Dual Streaming ermöglicht die gleichzeitige Codierung eines eingehenden Daten-Streams nach zwei verschiedenen, einzeln konfigurierten Einstellungen. Hierdurch werden zwei Daten-Streams erzeugt: einer zur Live- und Vorereignisaufzeichnung, ein zweiter zur kontinuierlichen, zur Bewegungs- und zur Alarmaufzeichnung.

Duplex

Begriff zur Definition der Richtung bei der Datenübertragung zwischen zwei Kommunikationspartnern. Halbduplex ermöglicht die Datenübertragung in beide Richtungen, jedoch nicht gleichzeitig. Vollduplex ermöglicht die gleichzeitige Datenübertragung in beide Richtungen.

DVR

Digital-Videorekorder

DWF

Design Web Format. Dient zur Anzeige technischer Zeichnungen auf einem PC-Monitor.

DynDNS

Dynamic Domain Name System. Ein DNS-Host-Dienst, der IP-Adressen in einer Datenbank bereithält. Dynamic DNS ermöglicht, mit dem Host-Namen des Geräts über das Internet eine Verbindung zum Gerät herzustellen. Siehe DNS.

Einbruchmeldezentrale

Generischer Name für das zentrale Gerät eines Einbruchsicherheitssystems von Bosch. Bedienteile, Module, Detektoren und weitere Geräte stellen eine Verbindung zur Systemsteuerung her.

Encoder

Wandelt einen analogen Stream in einen digitalen Stream um, beispielsweise zur Integration analoger Kameras in ein digitales System wie das Bosch Video Management System. Einige Encoder verfügen über lokale Archivierung (z. B. Flash-Karte oder USB-Festplatte) oder archivieren die Videodaten auf iSCSI-Geräten. IP-Kameras verfügen über einen integrierten Encoder.

Enterprise Access

Enterprise Access ist eine Funktion von BVMS, die aus einem oder mehreren Enterprise Accounts besteht. Jeder Enterprise Account enthält Gerätefreigaben für die Geräte eines bestimmten Management Servers.

Enterprise Account

Enterprise Account ist eine Autorisierung, mit der ein Enterprise Operator-Benutzer eine Verbindung mit den Geräten eines Management-Servers aufbaut, der Teil eines Enterprise Systems ist. In einem Enterprise Account werden alle Berechtigungen für die Geräte dieses Management-Servers konfiguriert. Operator Client kann gleichzeitig eine Verbindung mit allen Management-Server-Computern in einem Enterprise System herstellen. Dieser Zugriff wird entweder durch Mitgliedschaft in einer Enterprise User Group gesteuert oder durch die Gerätefreigaben, die im Enterprise Account für diesen Management-Server konfiguriert sind.

Enterprise Management Server

Enterprise Management Server ist ein BVMS Management Server, auf dem die Konfiguration von Enterprise User Groups gehostet wird. Sie benötigen mindestens eine Enterprise User Group, die sich auf mindestens einen Server-Computer bezieht. Die Rollen von Enterprise Management Server und Management Server können in einer Konfiguration kombiniert werden.

Enterprise System

Enterprise System ist eine Funktion des Bosch Video Management Systems, die es dem Benutzer des Operator Client ermöglicht, auf mehrere Management-Server-Computer gleichzeitig zuzugreifen.

Enterprise User Group

Enterprise User Group ist eine Benutzergruppe, die auf einem Enterprise Management Server konfiguriert ist. Enterprise User Group definiert die Benutzer, die Berechtigung zum gleichzeitigen Zugriff auf mehrere Management-Server Computer haben. Definiert die Bedienberechtigungen die für diese Benutzer verfügbar sind.

Entprellzeit

Der Zeitbereich beginnt mit dem Auftreten eines Ereignisses. In diesem Zeitbereich werden normalerweise keine anderen Ereignisse desselben Typs angenommen. Dadurch wird verhindert, dass z. B. ein umschaltender Sensor eine große Anzahl an Ereignissen auslöst. Für Ereignisse mit unterschiedlichen Zuständen können Sie für jeden Zustand eine andere Prioritätseinstellung konfigurieren. Die folgenden Beispiele sollen Ihnen helfen, das Konzept der Entprellzeit besser zu verstehen. Beispiel 1 befasst sich mit Ereignissen desselben Zustands: Das Ereignis „Systeminfo“ tritt ein, und die konfigurierte Entprellzeit beginnt. Während dieser Zeit tritt ein weiteres Ereignis „Systeminfo“ ein. Dieses Ereignis „Systeminfo“ wird nicht als ein neues Ereignis angenommen. Beispiel 2 befasst sich mit Ereignissen mit unterschiedlichen Zuständen, aber gleicher Priorität: Ein Ereignis „Bewegung erkannt“ tritt ein, und die konfigurierte Entprellzeit beginnt. Während dieser Zeit tritt ein Ereignis „Bewegung beendet“ mit derselben Priorität ein. Das Ereignis „Bewegung beendet“ wird nicht als neues Ereignis angenommen. Beispiel 3 behandelt ebenfalls Ereignisse mit unterschiedlichen Zuständen, aber gleicher Priorität: Der virtuelle Eingang ist eingeschaltet. Die Prioritäten beider Zustandsänderungen sind identisch. Zu einem bestimmten Zeitpunkt wird der virtuelle Eingang ausgeschaltet, und die Entprellzeit beginnt. Während

dieser Entprellzeit wird der virtuelle Eingang eingeschaltet. Diese Zustandsänderung wird nicht als neues Ereignis angenommen, da sie dieselbe Priorität hat. Nach der Entprellzeit befindet sich der virtuelle Eingang in einem anderen Zustand. Das Einschalten erhält den Zeitstempel des Endes der Entprellzeit, und es beginnt keine neue Entprellzeit. Beispiel 4 befasst sich mit Ereignissen mit unterschiedlichen Zuständen und unterschiedlicher Priorität: Ein Ereignis „Bewegung erkannt“ tritt ein, und die konfigurierte Entprellzeit beginnt. Während dieser Zeit tritt das Ereignis „Bewegung beendet“ mit einer höheren Priorität ein. Das Ereignis „Bewegung beendet“ wird als neues Ereignis angenommen, die Entprellzeit beginnt jedoch nicht erneut. Beispiel 5 behandelt ebenfalls Ereignisse mit unterschiedlichen Prioritäten und Zuständen: Der virtuelle Eingang ist ausgeschaltet. Priorität für den Zustand eingeschaltet ist „5“, die Priorität für den Zustand ausgeschaltet ist „2“. Zu einem bestimmten Zeitpunkt wird der virtuelle Eingang eingeschaltet (Priorität „5“), und die Entprellzeit beginnt. Während dieser Entprellzeit wird der virtuelle Eingang ausgeschaltet (Priorität „2“). Diese Zustandsänderung wird als neues Ereignis angenommen, da sie eine höhere Priorität hat. Die Entprellzeit des ersten Einschaltens wird fortgesetzt. Weitere Zustandsänderungen werden während dieser Entprellzeit nicht angenommen.

Entzerren

Mit der Software wird das kreisförmige Bild eines Fischaugenobjektivs mit strahlenförmiger Verzerrung zu einem rechteckigen Bild für die normale Ansicht konvertiert (beim Entzerren wird ein verzerrtes Bild korrigiert).

Entzerren in der Kamera (Edge Dewarping)

Das in der Kamera vorgenommene Entzerren.

Ereignis

Zustand oder Status, der mit einem Alarm und/oder einer Aktion verknüpft ist. Ereignisse können durch zahlreiche Quellen entstehen, beispielsweise durch Kameras, Archivierungsgeräte, Verzeichnisse, digitale Eingänge usw. Zu Ereignissen zählen die Zustände „Aufzeichnungsstart“ und „Signalverlust“, die Meldung „Festplatte voll“, Benutzeranmeldungen, Auslöser für digitale Eingangssignale usw.

Failover-VRM

Software in der BVMS Umgebung. Übernimmt bei Ausfall die Aufgaben des zugewiesenen Primären oder Sekundären VRM.

Gerätebaum

Hierarchische Liste aller verfügbaren Geräte im System.

Gerätefamilie

Bosch Encoder/IP-Kameras können zu einer der folgenden Gerätereihen gehören: Gerätefamilie 1, Gerätefamilie 2, Gerätefamilie 3. Geräte der Gerätefamilie 1 können nur Stream 1 aufzeichnen. Geräte der Gerätefamilie 2 können Stream 1 oder Stream 2 aufzeichnen. Geräte der Gerätefamilie 3 können Stream 1, Stream 2 oder nur I-Frames aufzeichnen.

Gespiegelte VRM

Software in der BVMS Umgebung. Sonderfall eines Sekundären VRM. Stellt sicher, dass die von einem oder mehreren Primären VRMs ausgeführte Aufzeichnung zusätzlich und gleichzeitig von einem anderen iSCSI-Ziel mit denselben Aufzeichnungseinstellungen ausgeführt wird.

GSM

Global System for Mobile Communication. Standard für digitale Mobiltelefone.

H.264

Standard zur Codierung (Komprimierung) digitaler Audio- und Videodaten für Multimedia-Anwendungen. Dieser Standard umfasst unterschiedliche Profile, die möglicherweise herstellerabhängig sind. Folgende Profile sind erhältlich: Baseline, Baseline+, Main Profile. Baseline (wird in Bosch Video Management System nicht verwendet) unterstützt 2 CIF. Baseline+ unterstützt 4 CIF und bietet eine bessere Bildqualität als Baseline. Main Profile unterstützt 4 CIF und bietet den überaus effizienten Komprimierungsalgorithmus CABAC (Context-Adaptive Binary Arithmetic Coding). Dieser ermöglicht eine hochwertige Codierung zur Archivierung.

H.265

H.265 ist ein Videokomprimierungsverfahren, das von ISO2 und ITU3 definiert und am 29. Oktober 2014 bestätigt wurde. Es ist ein Nachfolger von MPEG-4

AVC (Advanced Video Codec), auch H.264 genannt, und dient zur Komprimierung von Auflösungen von 4K und Ultra HD bis 36 Megapixel.

Hotspot

Maussensibles Symbol auf einer Karte. Hotspots werden im Configuration Client konfiguriert. Hotspots können z. B. Kameras, Relais oder Eingänge sein. Der Bediener kann mithilfe eines Hotspots ein Gerät in einem Gebäude suchen und wählen. Konfigurierte Hotspots können eine blinkende Hintergrundfarbe anzeigen, wenn ein bestimmtes Statusereignis oder ein Alarm eintritt.

I-Frame

Intra Frame. Teil eines Videokomprimierungsverfahrens. Enthält die Informationen eines vollständigen Bilds. Gegensatz: P- oder B-Frames, die Informationen über Änderungen gegenüber dem vorherigen oder nächsten Frame enthalten.

Intercom-Funktion

Dient zum Sprechen über die Lautsprecher eines Encoders. Dieser Encoder muss über einen Audioeingang und -ausgang verfügen. Die Intercom-Funktion kann pro Benutzergruppe freigegeben werden.

IPS

Images per Second (Bilder pro Sekunde). Anzahl der Videobilder, die pro Sekunde übertragen oder aufgezeichnet werden.

IQN

iSCSI Qualified Name. Der Initiatorname im IQN-Format dient zur Bereitstellung von Adressen für iSCSI-Initiatoren und -Ziele. Beim IQN-Mapping wird eine Initiatorgruppe erzeugt, die den Zugriff auf die LUNs eines iSCSI-Ziels steuert. Außerdem werden die Initiatornamen der einzelnen Encoder und des VRM in die Initiatorgruppe geschrieben. Nur die Geräte, deren Initiatorname in einer Initiatorgruppe enthalten ist, erhalten Zugriff auf eine LUN. Siehe LUN und iSCSI.

iSCSI

Internet Small Computer System Interface. Protokoll, das Speicher über ein TCP/IP-Netzwerk verwaltet. iSCSI ermöglicht den Zugriff auf gespeicherte Daten von jeder beliebigen Stelle im Netzwerk. Besonders seit der Einführung des Gigabit-Ethernet bietet es sich als kostengünstige Möglichkeit an, iSCSI-Speicher-Server einfach als entfernte Festplatten an ein Computer-Netzwerk anzuschließen. In der iSCSI-Terminologie wird der Server, der die Speicherressourcen bereitstellt, als iSCSI-Target (Ziel) und der Client, der die Verbindung zum Server herstellt und auf die Ressourcen des Servers zugreift, als iSCSI-Initiator bezeichnet.

JPEG

Joint Photographic Expert Group. Codierung von Standbildern.

Karten-Anzeigebereich

Ein Karten-Anzeigebereich ist ein Bereich des Bildschirms, auf dem ein definierter Teil der globalen Geolocation-Karte angezeigt wird.

Karten-Dateien

BVMS unterstützt die folgenden Karten-Dateiformate: PNG und JPG.

Kommandoskript

Makro, das der Administrator zur Erzeugung einer automatischen Aktion, wie die Positionierung einer PTZ-Kamera oder Sendung von E-Mails, programmieren kann. Für diese Funktionalität bietet das Bosch Video Management System (VMS) einen spezifischen Befehlssatz. Die Kommandoskripte lassen sich in Client-Skripte und Server-Skripte unterteilen. Client-Skripte dienen zur Ausführung bestimmter Aktionen, die auf einer Client-Arbeitsstation ausgeführt werden können. Server-Skripte werden automatisch von einem im System ausgelösten Ereignis ausgeführt. Mögliche Argumente werden ihnen vom Ereignis übergeben, z. B. Datum und Uhrzeit. Ein Kommandoskript kann aus mehreren Scriptlets bestehen. Sie können ein Kommandoskript mit den folgenden Skriptsprachen erzeugen: C#, VB.Net. Die Ausführung von Kommandoskripten erfolgt als Reaktion auf Ereignisse oder Alarme, automatisch gemäß einem Zeitplan (nur Server-Skripte), manuell über den Logischen Baum oder manuell über Symbole oder Karten.

Lageplan-Dateien

BVMS unterstützt die folgenden Lageplan-Dateiformate: PNG, JPG, PDF und DWF.

LDAP

Lightweight Directory Access Protocol. Netzwerkprotokoll, das über TCP/IP ausgeführt wird und den Zugriff auf Verzeichnisse ermöglicht. Bei einem Verzeichnis kann es sich beispielsweise um eine Liste von Benutzergruppen und deren

Zugriffsrechten handeln. Das Bosch Video Management System verwendet es, um Zugriff auf dieselben Benutzergruppen zu erhalten wie MS Windows oder ein anderes Enterprise-Benutzerverwaltungssystem.

Lesezeichen

Wird für die Speicherung eines Zeitbereichs von Live- oder aufgezeichnetem Video verwendet. Dadurch wird das Kennzeichnen von bestimmten Szenen zur späteren Untersuchung ermöglicht. Darüber hinaus können Sie Ihre Untersuchungsergebnisse durch Exportieren eines Lesezeichens mit anderen Nutzern teilen.

Livemodus

Funktion des Operator Client. Dient zur Live-Ansicht von Videos.

Logbuch

Container zum Protokollieren aller Ereignisse im Bosch Video Management System.

Logische Nummer

Logische Nummern sind eindeutige IDs, die zur einfachen Referenzierung jedem Gerät im System zugeordnet werden. Logische Nummern sind nur innerhalb eines bestimmten Gerätetyps eindeutig. Ein typischer Einsatzbereich für logische Nummern sind Kommandoskripte.

Logischer Baum

Baum mit einer angepassten Struktur aller Geräte. Der Logische Baum dient im Operator Client zur Auswahl von Kameras und anderen Geräten. Im Configuration Client wird der „Vollständige Logische Baum“ konfiguriert (Seite „Karten und Struktur“) und auf die einzelnen Benutzergruppen zugeschnitten (Seite „Benutzergruppen“).

LUN

Logical Unit Number. Dient in der iSCSI-Umgebung zur Adressierung eines einzelnen Festplattenlaufwerks oder einer virtuellen Partition (Volume). Die Partition ist Teil eines RAID-Disk-Arrays (iSCSI-Target).

Management-Server

BVMS Server, der Geräte verwaltet.

Master Control Software

Software, die als Schnittstelle zwischen dem Bosch Video Management System und einem Allegiant Gerät dient. Zum Einsatz kommt die Version 2.8 oder höher.

MHT

Auch als „Web-Archiv“ bezeichnet. Dateiformat, das sämtliche HTML- und Bilddateien einer Internet-Site in einer Datei speichern kann. Zur Vermeidung von Problemen wird empfohlen, MHT-Dateien nur mit Internet Explorer 7.0 oder höher zu erzeugen.

Monitorgruppe

Gruppe von Monitoren, die an Decoder angeschlossen sind. Die Monitorgruppe kann zur Alarmverarbeitung in einem bestimmten physischen Bereich verwendet werden. Eine Installation mit drei physisch getrennten Kontrollräumen könnte beispielsweise über drei Monitorgruppen verfügen. Die Monitore einer Monitorgruppe sind logisch in Reihen und Spalten konfiguriert und können in verschiedenen Anordnungen angezeigt werden, z. B. Vollbildansicht oder Vierfachteilung.

Multipath

Technologie im Computerspeicher für mehrere physische definierte Pfade, die den Datenserver mit einem Speicherziel (mithilfe verschiedener Controller, Busse, Switches etc.) als Failover- oder Lastverteilungslösung (Redundanz, Effizienz) verbindet.

Multipathing

Verwenden der Multipathing-Technologie für Computerspeicher.

Netzwerküberwachung

Messung netzwerkbezogener Werte und Auswertung dieser Werte anhand konfigurierbarer Grenzwerte.

NVR

Bosch Network Video Recorder (Netzwerk-Videorecorder); Computer im Bosch Video Management System, auf dem Audio- und Videodaten gespeichert werden und der als Failover-NVR oder als Redundanter NVR fungiert. Dieser NVR unterscheidet sich vom VIDOS NVR, der in das Bosch Video Management System integriert werden kann.

OID

Object Identifier. Begriff in der SNMP-Umgebung. Bestimmt eine MIB-Variable.

ONVIF

Open Network Video Interface Forum Globaler Standard für Netzwerkvideoprodukte. ONVIF-konforme Geräte sind in der Lage, Livevideo, Audio, Metadaten und Steuerdaten auszutauschen sowie

sicherzustellen, dass sie automatisch erkannt und mit Netzwerkanwendungen verbunden werden, wie z. B. mit Videomanagementsystemen.

Operator Client

Bestandteil des Bosch Video Management Systems, das die Benutzeroberfläche für Systemüberwachung und -betrieb bereitstellt.

Operator Client-Workstation

Computer in der Bosch Video Management System-Umgebung zur Videoanzeige im Live- und Wiedergabemodus sowie für verschiedene Konfigurationsaufgaben. Operator Client ist auf diesem Computer installiert.

P-frame

Predicted Frame. Teil eines Videokomprimierungsverfahrens.

PID

Person Identification Device. Es extrahiert Merkmale einer Person aus einem Bild, z. B. das Gesicht. Er führt spezielle Algorithmen aus, die eine Person innerhalb eines Videostreams identifizieren können.

Port

1) Bei Computern und Telekommunikationsgeräten ist ein Port (Substantiv) im Allgemeinen ein bestimmter Bereich, der für den physischen Anschluss an ein anderes Gerät dient. Dies geschieht in der Regel über eine Buchse und einen Stecker. Ein PC ist gewöhnlich mit einem oder mehreren seriellen Ports sowie mit einem parallelen Port ausgestattet. 2) In der Programmierung ist ein Port (Substantiv) ein „logischer Verbindungsbereich“ im weiteren Sinn. Im engeren Sinn wird in Netzwerken, die das Internet-Protokoll TCP/IP verwenden, mit „Port“ die Art und Weise bezeichnet, in der ein Client-Programm ein bestimmtes Server-Programm angibt, das sich auf einem Computer in einem Netzwerk befindet. Komplexere Anwendungen, die TCP/IP verwenden, wie das Web-Protokoll „Hypertext Transfer Protocol“, verfügen über Ports mit fest zugeordneten Nummern. Diese werden als „Well-known Ports“ bezeichnet, die von der Internet Assigned Numbers Authority (IANA) zugeordnet wurden. Andere Anwendungsprozesse erhalten die Port-Nummern für jede Verbindung dynamisch. Wenn ein Service (Server-Programm) gestartet wird, „bindet“ er sich an seine designierte Port-Nummer. Will ein Client-Programm diesen Server verwenden, muss es ebenfalls eine Bindung an die designierte Port-Nummer anfordern. Die Port-Nummern liegen zwischen 0 und 65535. Die Ports 1 bis 1023 sind für bestimmte privilegierte Services reserviert. Port 80 ist standardmäßig für den HTTP-Service definiert und muss daher nicht in der URL (Uniform Resource Locator) angegeben werden.

POS

Akronym für Point of Sale (Kassensystem).

Primärer VRM

Synonym für VRM.

PTZ-Kamera

Kamera mit Schwenk-, Neige- und Zoom-Funktion.

Punkt

Ein mit dem Sicherheitssystem verbundenes Erkennungsgerät. Individuelle Melder auf dem Bedienteil und mit benutzerdefiniertem Text. Der Text kann eine einzelne Tür, einen Bewegungssensor, einen Rauchmelder oder einen geschützten Bereich wie OBEN oder GARAGE beschreiben.

RAID

Redundant Array of Independent Disks (Redundante Anordnung unabhängiger Festplatten). Dient zur Organisation zweier oder mehrerer Festplatten, als wären sie ein Laufwerk. Daten werden auf diesem Laufwerk gemeinsam genutzt oder repliziert. Auf diese Weise werden größere Speicherkapazität, höhere Zuverlässigkeit sowie höhere Geschwindigkeit erzielt.

RCP

Remote Control Protocol

Referenzbild

Ein Referenzbild wird kontinuierlich mit dem aktuellen Videobild verglichen. Wenn das aktuelle Videobild in den markierten Bereichen vom Referenzbild abweicht, wird ein Alarm ausgelöst. Auf diese Weise können Sie Manipulationen erkennen, die anderenfalls unerkannt blieben, wie z. B. das Drehen der Kamera.

ROI

Region of Interest, Zielbereich. Die ROI-Funktion dient zum Einsparen von Bandbreite beim Zoomen in einen Ausschnitt des Kamerabildes bei einer feststehenden HD-Kamera. Dieser Ausschnitt verhält sich wie bei einer PTZ-Kamera.

RTP

Realtime Transport Protocol: Transportprotokoll für Video und Audio in Echtzeit

RTSP

Real Time Streaming Protocol. Netzwerkprotokoll zur Steuerung der kontinuierlichen Übertragung von audiovisuellen Daten oder Software über IP-basierte Netzwerke.

Rückspulzeit

Anzahl der Sekunden für die Umschaltung eines Bildfensters in die zeitversetzte Wiedergabe.

Sekundärer VRM

Software in der BVMS Umgebung. Stellt sicher, dass die von einem oder mehreren primären VRMs ausgeführte Aufzeichnung zusätzlich und gleichzeitig von einem anderen iSCSI-Ziel ausgeführt wird. Die Aufzeichnungseinstellungen können sich von den Einstellungen des Primären VRM unterscheiden.

Server Lookup

Zugriffsmethode für den Benutzer eines Configuration Client oder Operator Client zur sequenziellen Verbindung mit verschiedenen System-Access Points. Bei einem System-Access Point kann es sich um einen Management-Server oder einen Enterprise Management Server handeln.

Skimming

Sabotage eines Foyer-Kartenlesers. Ein Skimming-Gerät liest die Kartendaten des Magnetstreifens, ohne dass der Karteninhaber dies merkt.

SNMP

Simple Network Management Protocol. IP-basiertes Protokoll, mit dessen Hilfe Informationen von Netzwerkgeräten abgerufen (GET), Parameter für Netzwerkgeräte gesetzt (SET) und Benachrichtigungen über bestimmte Ereignisse empfangen (EVENT) werden können.

TCP

Transmission Control Protocol

TCP/IP

Transmission Control Protocol/Internet Protocol. Auch bekannt als Internetprotokoll-Suite. Kommunikationsprotokolle für die Datenübertragung über ein IP-Netzwerk.

Textdaten

Daten eines POS oder ATM wie Datum und Uhrzeit oder Kontonummer, die zusammen mit den Videodaten gespeichert werden, um zusätzliche Informationen für eine Auswertung zu liefern.

Trap

Begriff in der SNMP-Umgebung für eine unaufgeforderte Meldung von einem überwachten Gerät (Agent) an das Netzwerküberwachungssystem (Manager) zu einem Ereignis in diesem Gerät.

Trunkline

Analoge Ausgänge einer analogen Matrix, die mit einem Encoder verbunden sind. Daher können Matrizen als Videoquellen im Bosch Video Management System eingesetzt werden.

UDP

User Datagram Protocol. Verbindungsloses Protokoll für den Datenaustausch über ein IP-Netzwerk. Für die Videoübertragung ist UDP aufgrund seines geringeren Overheads effizienter als TCP.

Umgehen/Umgehung aufheben

Das Umgehen eines Geräts bedeutet, dass vom Gerät ausgelöste Alarme ignoriert werden, in der Regel für die Dauer mildernder Umständen wie z. B. Wartungsarbeiten. Das Aufheben der Umgehung bedeutet, dass die Alarme nicht mehr ignoriert werden.

Unmanaged Site

Element des Gerätebaums in BVMS, das Videonetzwerkgeräte wie digitale Videorekorder enthalten kann. Diese Geräte werden nicht vom Management Server Ihres Systems verwaltet. Der Benutzer des Operator Client kann bei Bedarf eine Verbindung zu den Geräten einer Unmanaged Site herstellen.

URL

Uniform Resource Locator

VCA

Video-Content-Analyse: Computeranalyse von Videostreams bestimmen, was in der überwachten Szene geschieht. Siehe auch: IVA (Intelligent Video Analytics)

Verweilzeit

Voreingestellte Zeitdauer, für die eine Kamera während einer Kamerasequenz bis zur Anzeige der nächsten Kamera in einem Bildfensterbereich angezeigt wird.

Video Analytics

Die Videoanalyse ist ein Softwareprozess, bei dem ein Kamerabild mit den gespeicherten Bildern bestimmter Personen oder Objekte verglichen werden. Bei einer Übereinstimmung löst die Software einen Alarm aus.

Video Streaming Gateway (VSG)

Virtuelles Gerät, mit dem die Integration von Bosch Kameras, ONVIF-Kameras, JPEG-Kameras und RTSP-Encodern ermöglicht wird.

Videoauflösung

Gibt die mit den Videosignalen übertragenen horizontalen und vertikalen Pixel an. 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 = verschlüsselt 1280 x 720 1080p = verschlüsselt 1920 x 1080

Virtueller Eingang

Wird zur Weiterleitung von Ereignissen aus Fremdsystemen an das Bosch Video Management System verwendet.

VRM

Video Recording Manager. Software-Paket im Bosch Video Management System, das das Archivieren von Videodaten (MPEG-4 SH++, H.264 und H.265) mit Audio- und Metadaten auf iSCSI-Geräten im Netzwerk verwaltet. VRM verwaltet eine Datenbank, die Informationen zur Aufzeichnungsquelle und eine Liste mit den zugehörigen iSCSI-Laufwerken enthält. VRM wird als Dienst auf einem Computer des Bosch Video Management System Netzwerks ausgeführt. VRM speichert Videodaten nicht selbst, sondern weist den Encodern Speicherkapazitäten auf iSCSI-Geräten zu und regelt die Lastverteilung auf mehrere iSCSI-Geräte. VRM streamt die Wiedergabe von iSCSI zu Operator Clients.

Zeitversetzte Wiedergabe

Gibt das aufgezeichnete Bild der ausgewählten Kamera in einem Bildfenster am Live-Bildschirm wieder. Die Startzeit (Anzahl der Sekunden in der Vergangenheit oder Rückspulzeit) kann konfiguriert werden.

Zusammengesetztes Ereignis

Kombination verschiedener Ereignisse. Die Kombination verwendet boolesche Ausdrücke, d. h. UND und ODER. Sie können nur Statusänderungen kombinieren, beispielsweise die Änderung eines Verbindungsstatus von „verbunden“ in „unterbrochen“ oder die Aktivierung eines Zeitplans.

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Niederlande
www.boschsecurity.com
© Bosch Security Systems B.V., 2025

Gebäudelösungen für ein besseres Leben

202506201238