BOSCH

BVMS

de Konfigurationshandbuch

Inhaltsverzeichnis

1	**Arbeiten mit der Hilfe**	**14**
1.1	Suchen nach Informationen	**14**
1.2	Drucken der Hilfe	**15**
2	**Einführung**	**16**
3	**Systemüberblick**	**18**
3.1	Hardware-Anforderungen	**19**
3.2	Software-Anforderungen	**19**
3.3	Lizenzanforderungen	**19**
4	**Konzepte**	**20**
4.1	BVMS Designkonzepte	**20**
4.1.1	System mit einem Management Server	**20**
4.1.2	Enterprise System	**21**
4.1.3	Server Lookup	**22**
4.1.4	Unmanaged Site	**23**
4.2	Aufzeichnung	**24**
4.2.1	Automated Network Replenishment (ANR)	**25**
4.2.2	Duale/Failover-Aufzeichnung	**26**
4.2.3	VRM-Aufzeichnungsmodi	**27**
4.2.4	Wiedergabe von VRM-Aufzeichnungsquellen	**30**
4.3	Alarmbearbeitung	**35**
4.4	ONVIF-Ereigniszuordnung	**37**
4.5	Abmeldung bei Inaktivität	**38**
4.6	Version unabhängiger Operator Client	**38**
4.6.1	Arbeiten im Kompatibilitätsmodus	**39**
4.7	Anzeigemodi einer Panoramakamera	**39**
4.7.1	360°-Panoramakamera – Boden- oder Deckenmontage	**40**
4.7.2	180°-Panoramakamera – Boden- oder Deckenmontage	**42**
4.7.3	360°-Panoramakamera – Wandmontage	**43**
4.7.4	180°-Panoramakamera – Wandmontage	**44**
4.7.5	Zugeschnittene Ansicht bei einer Panoramakamera	**45**
4.8	SSH-Tunneling	**46**
4.9	Multipathing	**46**
5	**Unterstützte Hardware**	**48**
5.1	Installieren von Hardware	**49**
5.2	Installation eines KBD Universal XF Keyboards	**49**
5.3	Verbinden eines Bosch IntuiKey Keyboards mit BVMS	**50**
5.3.1	Szenarios für Bosch IntuiKey Keyboard-Anschlüsse	**50**
5.3.2	Anschluss eines Bosch IntuiKey Keyboards an einen Decoder	**53**
5.3.3	Aktualisierung der Bosch IntuiKey Keyboard-Firmware	**53**
5.4	Verbinden einer Bosch Allegiant Kreuzschiene mit BVMS	**54**
5.4.1	Verbindung mit Bosch Allegiant Systemen – Überblick	**54**
5.4.2	Konfigurieren des Steuerungskanals	**56**
5.4.3	Bosch Allegiant Satellitensystem – Konzept	**58**
5.5	In BVMS unterstützte Allegiant CCL-Befehle	**59**
6	**Erste Schritte**	**61**
6.1	Installieren der Software-Module	**61**
6.2	Verwendung von Config Wizard	**61**
6.3	Starten des Configuration Client	**69**

6.4	Konfigurieren der Sprache des Configuration Client	**70**
6.5	Konfigurieren der Sprache des Operator Client	**70**
6.6	Nach Geräten suchen	**71**
6.7	Systemzugriff	**71**
6.8	Mittels Server Lookup	**71**
6.9	Konfiguration des Fernzugriffs	**72**
6.9.1	Fernzugriff	**72**
6.9.2	Ohne Enterprise System konfigurieren	**75**
6.9.3	Mit Enterprise System konfigurieren	**75**
6.10	Aktivieren der Softwarelizenzen	**75**
6.10.1	Herunterladen der Bundle-Informationsdatei	**76**
6.10.2	Abrufen der Computersignatur	**76**
6.10.3	Abrufen des Aktivierungsschlüssels	**77**
6.10.4	Aktivieren des Systems	**77**
6.11	Warten von BVMS	**77**
6.12	Austausch eines Geräts	**79**
6.12.1	Austausch eines MS/EMS	**79**
6.12.2	Austausch eines VRM	**80**
6.12.3	Austausch eines Encoders oder Decoders	**81**
6.12.4	Austausch eines Operator Client	**84**
6.12.5	Abschließende Tests	**84**
6.12.6	Wiederherstellen von Divar IP 3000/7000	**84**
6.13	Zeitsynchronisation konfigurieren	**84**
6.14	Speichermedien eines Encoders konfigurieren	**85**
7	**Erstellung eines Enterprise Systems**	**86**
7.1	Konfigurieren der Serverliste für Enterprise System	**86**
7.2	Erstellen einer Enterprise User Group	**87**
7.3	Erstellen eines Enterprise Accounts	**88**
8	**Konfigurieren von Kommandoskripten**	**90**
8.1	Verwalten von Kommandoskripten	**90**
8.2	Konfigurieren eines automatisch startenden Kommandoskripts	**91**
8.3	Importieren eines Kommandoskripts	**91**
8.4	Exportieren eines Kommandoskripts	**92**
8.5	Konfigurieren eines Start-Kommandoskripts (Seite „Einstellungen“)	**92**
9	**Verwalten von Konfigurationsdaten**	**93**
9.1	Aktivieren der letzten Konfiguration	**93**
9.2	Aktivieren einer Konfiguration	**94**
9.3	Exportieren von Konfigurationsdaten	**95**
9.4	Importieren von Konfigurationsdaten	**95**
9.5	Exportieren von Konfigurationsdaten auf OPC	**96**
9.6	Status des Encoders/Decoders überprüfen	**96**
9.7	SNMP-Überwachung konfigurieren	**96**
9.8	Erzeugen einer Auswertung	**97**
10	**Konfigurationsbeispiele**	**98**
10.1	Hinzufügen einer Bosch ATM/POS-Bridge	**98**
10.2	Hinzufügen eines Bosch Allegiant Kreuzschienen-Eingangsalarms	**99**
10.3	Hinzufügen und Konfigurieren von 2 Dinion IP Kameras mit VRM Aufzeichnung	**99**
11	**Allgemeine Fenster des Configuration Client**	**101**
11.1	Konfigurationsfenster	**101**

11.2	Menübefehle	**102**
11.3	Dialogfeld „Aktivierungs-Manager“ (Menü „System“)	**104**
11.4	Dialogfeld „Konfiguration aktivieren“ (Menü „System“)	**105**
11.5	Dialogfeld „Initialer Geräte-Scan“ (Menü „Hardware“)	**106**
11.6	Dialogfeld „Geräte mit globalem Standard-Passwort schützen“ (Menü „Hardware“)	**106**
11.7	Dialogfeld „Gerätepasswörter ändern“ (Menü „Hardware“)	**107**
11.8	Dialogfeld „Geräte-Firmware aktualisieren“ (Menü „Hardware“)	**108**
11.9	Dialogfeld „Geräte-IP und Netzwerkeinstellungen ändern“ (Menü „Hardware“)	**109**
11.10	Dialogfeld „Geräte-Monitor“ (Menü „Hardware“)	**111**
11.11	Dialogfeld „License Investigator“ (Menü „Werkzeuge“)	**111**
11.12	Dialogfeld „Lizenz-Manager“ (Menü „Werkzeuge“)	**111**
11.13	Dialogfelder „Auswertungen“ (Menü „Auswertungen“)	**112**
11.13.1	Dialogfeld „Aufzeichnungszeitpläne“	**112**
11.13.2	Dialogfeld „Geplante Aufzeichnungseinstellungen“	**112**
11.13.3	Dialogfeld „Aktionszeitpläne“	**112**
11.13.4	Dialogfeld „Kameras und Aufzeichnungsparameter”	**112**
11.13.5	Dialogfeld „Stream-Qualität"	**112**
11.13.6	Dialogfeld „Ereignis-Einstellungen”	**113**
11.13.7	Dialogfeld „Einstellungen für zusammengesetztes Ereignis”	**113**
11.13.8	Dialogfeld „Alarmeinstellungen“	**113**
11.13.9	Dialogfeld „Konfigurierte Benutzer”	**113**
11.13.10	Das Dialogfeld „Benutzergruppen und Konten”	**113**
11.13.11	Dialogfeld „Geräteberechtigungen“	**113**
11.13.12	Dialogfeld „Bedienberechtigungen“	**113**
11.13.13	Dialogfeld „Konfigurationsberechtigungen“	**114**
11.13.14	Dialogfeld „Berechtigungen für Benutzergruppen“	**114**
11.13.15	Dialogfeld „Sicherheitseinstellungen”	**114**
11.13.16	Dialogfeld „Umgangene Geräte“	**114**
11.14	Dialogfeld „Alarmeinstellungen“ (Menü „Einstellungen“)	**114**
11.15	Dialogfeld „SNMP-Einstellungen“ (Menü „Einstellungen“)	**114**
11.16	Dialogfeld „Optionen“ (Menü „Einstellungen“)	**115**
11.17	Dialogfeld „Fernzugriffseinstellungen“ (Menü „Einstellungen“)	**117**
11.17.1	Dialogfeld „Port Mapping-Tabelle“	**118**
12	**Seite Geräte**	**119**
12.1	Aktualisieren von Gerätestatus und -funktionen	**119**
12.2	Ändern des Passworts für IP-Geräte	**120**
12.3	Hinzufügen eines Geräts	**120**
12.4	Seite „Server-Liste/Adressbuch“	**123**
12.4.1	Dialogfeld „Server hinzufügen“	**124**
12.4.2	Konfigurieren von Server Lookup	**125**
12.4.3	Konfigurieren der Server-Liste	**125**
12.4.4	Export der Server-Liste	**125**
12.4.5	Import einer Server-Liste	**126**
12.5	Seite „NVRs“/„Failover-NVRs“/„Redundante NVRs“	**126**
12.6	Seite DiBos	**126**
12.6.1	Hinzufügen eines DiBos Systems per Suchvorgang	**126**
12.6.2	Seite Einstellungen	**127**
12.6.3	Seite Kameras	**127**
12.6.4	Seite Eingänge	**127**

12.6.5	Seite Relais	**128**
12.6.6	Konfigurieren der Integration eines DiBos Systems	**128**
12.7	Seite DVR (Digital-Videorekorder)	**128**
12.7.1	DVR-Geräte	**129**
12.7.2	Hinzufügen eines DVR-Geräts per Suchvorgang	**130**
12.7.3	Dialogfeld „Add DVR“ (DVR hinzufügen)	**130**
12.7.4	Registerkarte „Einstellungen“	**131**
12.7.5	Registerkarte „Kameras“	**131**
12.7.6	Registerkarte „Eingänge“	**131**
12.7.7	Registerkarte „Relais“	**131**
12.7.8	Konfigurieren der Integration eines DVR	**131**
12.8	Seite Kreuzschienen	**132**
12.8.1	Hinzufügen eines Bosch Allegiant Geräts	**132**
12.8.2	Konfigurieren eines Bosch Allegiant Geräts	**132**
12.8.3	Seite Ausgänge	**133**
12.8.4	Seite Eingänge	**134**
12.8.5	Seite Verbindung	**134**
12.8.6	Seite Kameras	**134**
12.9	Seite Arbeitsstation	**135**
12.9.1	Manuelles Hinzufügen einer Arbeitsstation	**135**
12.9.2	Konfigurieren eines Bosch IntuiKey Keyboards (Seite „Einstellungen“) (Arbeitsstation)	**136**
12.9.3	Aktivieren der Forensischen Suche auf einer Arbeitsstation (Seite „Einstellungen“)	**136**
12.9.4	Konfigurieren eines Start-Kommandoskripts (Seite „Einstellungen“)	**136**
12.9.5	Seite Einstellungen	**136**
12.9.6	Ändern der Netzwerkadresse einer Arbeitsstation	**138**
12.10	Seite "Decoder"	**138**
12.10.1	Manuelles Hinzufügen eines Encoders/Decoders	**139**
12.10.2	Dialogfeld „Encoder/Decoder bearbeiten“	**140**
12.10.3	Ändern des Passworts für einen Encoder/Decoder (Passwort ändern/Passwort eingeben)	**141**
12.10.4	Decoderprofil	**142**
12.10.5	Monitor-Anzeige	**143**
12.10.6	Konfigurieren eines Bosch IntuiKey Keyboards (Decoder)	**143**
12.10.7	Konfigurieren eines Decoders für den Einsatz mit einem Bosch IntuiKey Keyboard	**144**
12.10.8	Löschen des Decoder-Logos	**144**
12.11	Seite „Monitorgruppen“	**144**
12.11.1	Manuelles Hinzufügen einer Monitorgruppe	**145**
12.11.2	Konfigurieren einer Monitorgruppe	**145**
12.12	Seite „Monitorwand“	**146**
12.12.1	Manuelles Hinzufügen einer Monitorwand	**147**
12.13	Seite Kommunikationsgeräte	**148**
12.13.1	Hinzufügen eines E-Mail-/SMTP-Servers	**148**
12.13.2	Hinzufügen eines SMS-Geräts	**148**
12.13.3	Seite SMTP-Server	**149**
12.13.4	Konfigurieren eines Kommunikationsgeräts	**150**
12.13.5	Dialogfeld Test-E-Mail senden	**150**
12.13.6	GSM-Einstellungen / Seite SMSC-Einstellungen	**150**
12.14	Seite „ATM/POS“	**151**
12.14.1	Manuelles Hinzufügen einer Bosch ATM/POS-Bridge	**152**

12.14.2	Seite Bosch ATM/POS-Bridge	**152**
12.14.3	Konfigurieren eines Peripheriegeräts	**153**
12.14.4	Seite „DTP-Einstellungen“	**153**
12.14.5	Seite „ATM-Einstellungen“	**154**
12.14.6	Seite Eingänge	**154**
12.15	Foyer-Kartenleser	**154**
12.15.1	Dialogfeld „Foyer-Kartenleser hinzufügen“	**155**
12.15.2	Einstellungen für Foyer-Kartenleser-Seite	**155**
12.16	Seite Virtuelle Eingänge	**155**
12.16.1	Manuelles Hinzufügen virtueller Eingänge	**156**
12.17	Seite SNMP	**156**
12.17.1	Manuelles Hinzufügen eines SNMP	**157**
12.17.2	Konfigurieren eines SNMP Trap Receivers (Seite „SNMP Trap Receiver“)	**157**
12.17.3	Dialogfeld SNMP Trap Logger	**158**
12.18	Seite „Assign Keyboard“ (Tastatur zuweisen)	**158**
12.19	Seite Input / Output-Module	**160**
12.19.1	Manuelles Hinzufügen eines I/O-Moduls	**160**
12.19.2	Konfigurieren eines I/O-Moduls	**160**
12.19.3	Seite ADAM-Gerät	**161**
12.19.4	Seite Eingänge	**161**
12.19.5	Seite Relais	**161**
12.20	Seite "Allegiant CCL-Emulation"	**162**
12.20.1	Manuelles Hinzufügen einer Allegiant CCL-Emulation	**162**
12.20.2	Allegiant CCL-Befehle	**162**
12.20.3	Konfigurieren einer Allegiant CCL-Emulation	**163**
12.21	Seite „Mobile Video Service“	**163**
12.21.1	Mobiler Video-Service	**163**
12.21.2	Manuelles Hinzufügen eines Mobilen Video Services	**164**
12.22	Seite „Einbruchmeldezentralen”	**164**
12.22.1	Manuelles Hinzufügen einer Einbruchmeldezentrale	**165**
12.22.2	Seite "Einstellungen"	**165**
12.23	Seite „Zutrittskontrollsysteme“	**165**
12.23.1	Hinzufügen eines Zutrittskontrollsystems	**166**
12.23.2	Bearbeiten eines Zutrittskontrollsystems	**167**
12.23.3	Seite „Einstellungen“	**167**
12.24	Seite „Video Analytics“	**167**
12.24.1	Seite „Videoanalyse-Einstellungen“	**167**
12.24.2	Hinzufügen eines Videoanalysegeräts	**168**
12.24.3	Seite „Person Identification Device“	**168**
12.24.4	Hinzufügen eines Person Identification Device (PID)	**169**
12.24.5	Seite „PID“	**169**
12.24.6	Wiederherstellung des PID-Zugriffs nach Ausfall eines zentralen BVMS Servers	**170**
12.24.7	Hinzufügen von Kameras zu einem Person Identification Device (PID)	**171**
12.24.8	Konfigurieren von Kameraparametern für Person Identification-Alarme	**171**
12.24.9	Konfigurieren von Personengruppen	**172**
12.24.10	Hinzufügen eines LPR-Geräts	**172**
12.25	Seite VRM-Geräte	**173**
12.25.1	Hinzufügen eines VRM-Geräts per Suchvorgang	**174**
12.25.2	Manuelles Hinzufügen eines primären oder sekundären VRMs	**175**

12.25.3	Bearbeiten eines VRM-Geräts	**177**
12.25.4	Seite VRM-Einstellungen	**177**
12.25.5	Seite SNMP	**178**
12.25.6	Seite „Konten“	**178**
12.25.7	Seite Erweitert	**178**
12.25.8	Verschlüsseln der Aufzeichnung für VRM	**179**
12.25.9	Passwort für ein VRM-Gerät ändern	**180**
12.25.10	Hinzufügen eines VRM-Pools	**180**
12.25.11	Manuelles Hinzufügen eines Failover-VRM	**181**
12.25.12	Manuelles Hinzufügen eines gespiegelten VRM	**182**
12.25.13	Hinzufügen von Encodern per Suchvorgang	**183**
12.25.14	Hinzufügen von VSG-Geräten per Suchvorgang	**184**
12.25.15	Synchronisieren der BVMS Konfiguration	**184**
12.26	Seite „Pool“	**184**
12.26.1	Konfigurieren des automatischen Aufzeichnungsmodus auf einem Pool	**186**
12.26.2	Manuelles Hinzufügen eines Encoders/Decoders	**186**
12.26.3	Manuelles Hinzufügen eines iSCSI-Geräts	**187**
12.26.4	Manuelles Hinzufügen eines Video Streaming Gateway	**188**
12.26.5	Manuelles Hinzufügen eines iSCSI-Geräts der DSA E-Series	**189**
12.26.6	Hinzufügen von Encodern per Suchvorgang	**191**
12.26.7	Hinzufügen von VSG-Geräten per Suchvorgang	**192**
12.26.8	Duale Aufzeichnung im Gerätebaum konfigurieren	**193**
12.27	Bosch Encoder-/Decoder-Seite	**193**
12.28	Seite iSCSI-Gerät	**193**
12.28.1	iSCSI-Speicherpool	**194**
12.28.2	Manuelles Hinzufügen eines iSCSI-Geräts	**195**
12.28.3	Manuelles Hinzufügen eines iSCSI-Geräts der DSA E-Series	**195**
12.28.4	Konfigurieren eines iSCSI-Geräts	**197**
12.28.5	Seite „Basic Configuration“ (Grundkonfiguration)	**199**
12.28.6	Dialogfeld „Lastverteilung“	**200**
12.28.7	Verschieben eines iSCSI-Systems in einen anderen Pool (Pool ändern)	**201**
12.28.8	Seite LUNs	**201**
12.28.9	Hinzufügen einer LUN	**202**
12.28.10	Formatieren einer LUN	**203**
12.28.11	Dialogfeld iqn-Mapper	**203**
12.29	Seite „Video Streaming Gateway-Gerät“	**204**
12.29.1	Manuelles Hinzufügen eines Video Streaming Gateway	**205**
12.29.2	Bearbeiten eines Video Streaming Gateway	**206**
12.29.3	Hinzufügen einer Kamera zu einem VSG	**206**
12.29.4	Dialogfeld „Bosch Encoder hinzufügen“	**207**
12.29.5	Dialogfeld „ONVIF-Encoder hinzufügen“	**208**
12.29.6	Dialogfeld „JPEG-Kamera hinzufügen“	**210**
12.29.7	Dialogfeld „RTSP-Encoder hinzufügen“	**211**
12.29.8	Verschieben eines VSG in einen anderen Pool (Pool ändern)	**212**
12.29.9	Konfigurieren von Multicast (Registerkarte „Multicast“)	**212**
12.29.10	Konfigurieren der Protokollierung (Registerkarte „Erweitert“)	**213**
12.29.11	Starten des ONVIF Camera Event Driver Tool aus dem Configuration Client	**214**
12.30	Seite Nur Live	**214**
12.30.1	Hinzufügen von Nur-Live-Geräten per Suchvorgang	**214**

12.30.2	Manuelles Hinzufügen eines Encoders/Decoders	**215**
12.30.3	Angeben des Ziel-Passworts für einen Decoder (Authentifizieren ...)	**216**
12.31	Seite Lokale Archivierung	**217**
12.32	Seite „Unmanaged Site“	**218**
12.32.1	Manuelles Hinzufügen einer Unmanaged Site	**218**
12.32.2	Importieren von Unmanaged Sites	**218**
12.32.3	Seite „Unmanaged Site“	**219**
12.32.4	Hinzufügen eines Unmanaged Netzwerkgeräts	**219**
12.32.5	Konfiguration der Zeitzone	**220**
13	**Seite „Bosch Encoder/Decoder/Kamera“**	**221**
13.1	Hinzufügen eines Encoders zu einem VRM-Pool	**223**
13.2	Hinzufügen eines Nur-Live-Encoders	**223**
13.3	Hinzufügen eines Encoders mit lokaler Archivierung	**223**
13.4	Bearbeiten eines Encoders	**223**
13.4.1	Verschlüsseln von Live-Video (Encoder bearbeiten)	**223**
13.4.2	Aktualisieren der Gerätefunktionen (Encoder bearbeiten)	**224**
13.4.3	Dialogfeld „Encoder/Decoder bearbeiten“	**225**
13.5	Verwalten der Authentizitätsprüfung	**226**
13.5.1	Überprüfung der Authentizität	**227**
13.5.2	Konfigurieren der Authentifizierung	**228**
13.5.3	Hochladen eines Zertifikats	**228**
13.5.4	Download eines Zertifikats	**229**
13.5.5	Installierung eines Zertifikats auf einer Arbeitsstation	**229**
13.6	Angeben des Ziel-Passworts für einen Decoder (Authentifizieren ...)	**230**
13.7	Ändern des Passworts für einen Encoder/Decoder (Passwort ändern/Passwort eingeben)	**230**
13.8	Verschieben eines Encoders in einen anderen Pool (Pool ändern)	**231**
13.9	Wiederherstellung von Aufzeichnungen von einem ausgetauschten Encoder (Aufzeichnungen von Vorgänger zuweisen)	**232**
13.10	Konfigurieren von Encodern/Decodern	**233**
13.10.1	Speichermedien eines Encoders konfigurieren	**233**
13.10.2	Konfigurieren mehrerer Encoder/Decoder	**234**
13.10.3	Konfigurieren des Failover-Aufzeichnungsmodus auf einem Encoder	**235**
13.10.4	Seite „Recording Management“ (Aufzeichnungsverwaltung)	**236**
13.10.5	Seite „Aufzeichnungspräferenzen“	**236**
13.11	Konfigurieren von Multicast	**237**
14	**ONVIF Seite**	**239**
14.1	Hinzufügen eines Nur-Live-ONVIF-Geräts per Suchvorgang	**239**
14.2	Seite „ONVIF-Encoder"	**239**
14.3	Seite "ONVIF-Encoderereignis"	**240**
14.3.1	Hinzufügen und Entfernen eines ONVIF Profils	**242**
14.3.2	Exportieren einer ONVIF-Mapping-Tabelle	**243**
14.3.3	Importieren einer ONVIF Mapping-Tabelle	**243**
14.3.4	Konfigurieren einer ONVIF-Mapping-Tabelle	**244**
14.4	Seite „ONVIF Konfiguration“	**246**
14.4.1	Gerätezugriff	**247**
14.4.2	Datum/Zeit	**247**
14.4.3	Benutzerverwaltung	**248**
14.4.4	Seite „Videoencoderprofil”	**249**

14.4.5	Audioencoderprofil	**251**
14.4.6	Imaging allgemein	**252**
14.4.7	Gegenlichtkompensation	**253**
14.4.8	Belichtung	**253**
14.4.9	Fokus	**254**
14.4.10	Großer dynamischer Bereich	**255**
14.4.11	Weißabgleich	**256**
14.4.12	Netzwerkzugriff	**256**
14.4.13	Bereiche	**259**
14.4.14	Relais	**260**
14.5	Seite "ONVIF-Ereignisquelle"	**261**
14.6	ONVIF-Profile zuweisen	**262**
15	**Seite „Karten und Struktur“**	**263**
16	**Konfigurieren des logischen Baums**	**265**
16.1	Konfigurieren des Logischen Baums	**265**
16.2	Hinzufügen eines Geräts zum Logischen Baum	**265**
16.3	Entfernen eines Baumelements	**266**
16.4	Verwalten von Ressourcen-Dateien	**266**
16.4.1	Dialogfeld Ressourcen-Manager	**267**
16.4.2	Dialogfeld Ressource auswählen	**268**
16.5	Hinzufügen eines Dokuments	**268**
16.5.1	Dialogfeld URL hinzufügen	**269**
16.6	Dialogfeld „Link zu externer Anwendung“	**269**
16.7	Hinzufügen eines Kommandoskripts	**270**
16.8	Hinzufügen einer Kamerasequenz	**270**
16.8.1	Dialogfeld Kamerasequenzen	**271**
16.9	Verwalten von vorkonfigurierten Kamerasequenzen	**272**
16.9.1	Dialogfeld Kamerasequenz hinzufügen	**273**
16.9.2	Dialogfeld Sequenzschritt hinzufügen	**273**
16.10	Hinzufügen eines Ordners	**274**
16.11	Hinzufügen einer Karte	**274**
16.12	Hinzufügen eines Links zu einer anderen Karte	**274**
16.12.1	Dialogfeld Karte für Link auswählen	**275**
16.13	Zuordnen einer Karte zu einem Ordner	**275**
16.14	Verwalten von Geräten auf einer Karte	**275**
16.15	Ein Störungsrelais hinzufügen	**276**
16.15.1	Dialogfeld „Störungsrelais“	**277**
16.16	Konfigurieren der Geräteumgehung	**278**
17	**Seite Zeitpläne**	**279**
17.1	Seite Aufzeichnungszeitpläne	**279**
17.2	Seite Aktionszeitpläne	**280**
18	**Konfigurieren von Zeitplänen**	**282**
18.1	Konfigurieren eines Aufzeichnungszeitplans	**282**
18.2	Hinzufügen eines Aktionszeitplans	**283**
18.3	Konfigurieren eines Standard-Aktionszeitplans	**283**
18.4	Konfigurieren eines wiederkehrenden Aktionszeitplans	**284**
18.5	Entfernen eines Aktionszeitplans	**284**
18.6	Hinzufügen von Feiertagen und besonderen Tagen	**284**
18.7	Entfernen von Feiertagen und besonderen Tagen	**285**

18.8	Umbenennen eines Zeitplans	**286**
19	**Seite Kameras und Aufzeichnung**	**287**
19.1	Seite Kameras	**287**
19.2	Aufzeichnungseinstellungsseiten (nur NVR)	**291**
20	**Konfigurieren von Kameras und Aufzeichnungseinstellungen**	**292**
20.1	Kopieren und Einfügen in Tabellen	**292**
20.2	Kameratabelle exportieren	**293**
20.3	Konfigurieren von Stream-Qualitätseinstellungen	**294**
20.3.1	Dialogfeld Stream-Qualitätseinstellungen	**294**
20.4	Konfigurieren der Kameraeigenschaften	**297**
20.5	Konfigurieren von Aufzeichnungseinstellungen (nur VRM und Lokale Archivierung)	**297**
20.6	Konfigurieren von Aufzeichnungseinstellungen (nur NVR)	**298**
20.7	Dialogfeld Geplante Aufzeichnungseinstellungen (nur VRM und Lokale Archivierung)	**299**
20.8	Konfigurieren von PTZ Port-Einstellungen	**302**
20.9	Konfigurieren von voreingestellten Positionen und AUX-Kommandos	**302**
20.10	Dialogfeld „Voreingestellte Positionen und AUX-Kommandos“	**304**
20.11	ROI-Funktion konfigurieren	**304**
20.12	Kopieren der Aufzeichnungseinstellungen (nur NVR)	**305**
20.12.1	Dialogfeld Aufzeichnungseinstellungen kopieren (nur NVR)	**306**
20.13	ANR-Funktion konfigurieren	**306**
20.14	Duale Aufzeichnung in der Kameratabelle konfigurieren	**306**
20.15	Verwalten von Video-Streaming-Gateways	**307**
20.15.1	ONVIF-Profile zuweisen	**307**
21	**Seite Ereignisse**	**308**
21.1	Registerkarte „Entprelleinstellungen“	**309**
21.2	Registerkarte „Einstellungen” für die erweiterte Anzeige der Karte	**309**
21.3	Registerkarte „Einstellungen” für die Ereigniskonfiguration	**310**
21.4	Dialogfeld Kommandoskript-Editor	**311**
21.5	Zusammengesetztes Ereignis erzeugen / Dialogfeld Zusammengesetztes Ereignis bearbeiten	**311**
21.6	Dialogfeld Skriptsprache auswählen	**312**
21.7	Prioritäten des Dialogfelds „Ereignistyp“ bearbeiten	**312**
21.8	Dialogfeld Geräte auswählen	**312**
21.9	Dialogfeld „Textatenaufzeichnung“	**313**
22	**Seite Alarme**	**314**
22.1	Dialogfeld „Alarmeinstellungen“	**315**
22.2	Dialogfeld Bildfensterinhalt auswählen	**316**
22.3	Dialogfeld „Bildfensterinhalt auswählen“ (MG)	**317**
22.4	Dialogfeld Alarmoptionen	**317**
22.5	Dialogfeld Ressource auswählen	**321**
23	**Konfigurieren von Ereignissen und Alarmen**	**323**
23.1	Kopieren und Einfügen in Tabellen	**324**
23.2	Entfernen einer Tabellenzeile	**324**
23.3	Verwalten von Ressourcen-Dateien	**324**
23.4	Konfigurieren eines Ereignisses	**325**
23.5	Duplizieren eines Ereignisses	**325**
23.6	Protokollieren von Benutzerereignissen	**325**
23.7	Konfigurieren von Benutzerereignisschaltflächen	**326**
23.8	Erzeugen eines Zusammengesetzten Ereignisses	**327**

23.9	Bearbeiten eines Zusammengesetzten Ereignisses	**328**
23.10	Konfigurieren eines Alarms	**328**
23.11	Konfigurieren der Einstellungen aller Alarme	**329**
23.12	Vor- und Nachalarmdauer bei einem Alarm konfigurieren	**329**
23.13	Alarmaufzeichnung mit Textdaten auslösen	**330**
23.14	Textdaten einer Daueraufzeichnung hinzufügen	**331**
23.15	Alarmaufzeichnung schützen	**331**
23.16	Konfigurieren der blinkenden Hotspots	**331**
23.17	Ereignisse und Alarme für Zutrittskontrollsysteme	**332**
24	**Seite Benutzergruppen**	**334**
24.1	Seite Eigenschaften der Benutzergruppen	**336**
24.2	Seite Benutzereigenschaften	**337**
24.3	Seite Eigenschaften des Anmeldungspaares	**338**
24.4	Seite Kamerafreigaben	**339**
24.5	Seite „Prioritäten für Steuerungen“	**340**
24.6	Dialogfeld Freigaben für Benutzergruppen kopieren	**341**
24.7	Seite Decoder-Freigaben	**341**
24.8	Seite Ereignisse und Alarme	**342**
24.9	Dialogfeld LDAP Server-Einstellungen	**342**
24.10	Seite „Zugangsberechtigungen“	**344**
24.11	Seite Logischer Baum	**344**
24.12	Seite „Bedienerfunktionen“	**345**
24.13	Seite Prioritäten	**348**
24.14	Seite Benutzeroberfläche	**349**
24.15	Seite „Server-Zugriff“	**350**
24.16	Seite „Konfigurationsberechtigungen“	**351**
24.17	Seite „Berechtigungen für Benutzergruppen“	**352**
24.18	Seite „Kontorichtlinien“	**352**
24.18.1	Offline Operator Client	**354**
25	**Konfigurieren von Benutzern, Berechtigungen und Enterprise Access**	**358**
25.1	Erstellen einer Gruppe oder eines Kontos	**359**
25.1.1	Erstellen einer Standard-Benutzergruppe	**359**
25.1.2	Erstellen einer Enterprise User Group	**360**
25.1.3	Erstellen eines Enterprise Accounts	**360**
25.2	Erzeugen eines Benutzers	**361**
25.3	Erzeugen einer 4-Augen-Gruppe	**362**
25.4	Hinzufügen eines Anmeldungspaars zu einer 4-Augen-Gruppe	**363**
25.5	Konfigurieren der Admin-Gruppe	**363**
25.6	Konfigurieren von LDAP-Einstellungen	**364**
25.7	Zuordnen einer LDAP-Gruppe	**365**
25.8	Festlegen eines Freigabezeitplans für Benutzeranmeldungen	**366**
25.9	Konfigurieren von Bedienberechtigungen	**366**
25.10	Konfigurieren von Geräteberechtigungen	**367**
25.11	Konfigurieren verschiedener Prioritäten	**367**
25.12	Kopieren von Freigaben für Benutzergruppen	**368**
26	**Konfigurieren der videobasierten Brandmeldeanlage**	**369**
26.1	Konfigurieren einer Branderkennungskamera	**369**
26.2	Hinzufügen eines Encoders zu einem VRM-Pool	**370**
26.3	Hinzufügen von Encodern per Suchvorgang	**370**

26.4	Hinzufügen von Nur-Live-Geräten per Suchvorgang	**371**
26.5	Hinzufügen von Encodern mit lokaler Archivierung per Suchvorgang	**371**
26.6	Konfigurieren eines Brandereignisses	**372**
26.7	Konfigurieren eines Feueralarms	**372**
27	**Konfigurieren der MIC IP 7000, die mit einem VIDEOJET 7000 connect verbunden ist**	**373**
28	**Problembehandlung**	**374**
28.1	Konfigurieren der gewünschten Sprache in Windows	**376**
28.2	Wiederherstellen der Verbindung mit einem Bosch IntuiKey Keyboard	**377**
28.3	Reduzieren der Anzahl der Allegiant Kameras	**377**
28.4	Verwendete Ports	**377**
28.5	Ermöglicht die Protokollierung von ONVIF-Ereignissen	**383**
	Glossar	**385**
	Index	**395**

1 Arbeiten mit der Hilfe

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 20 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:

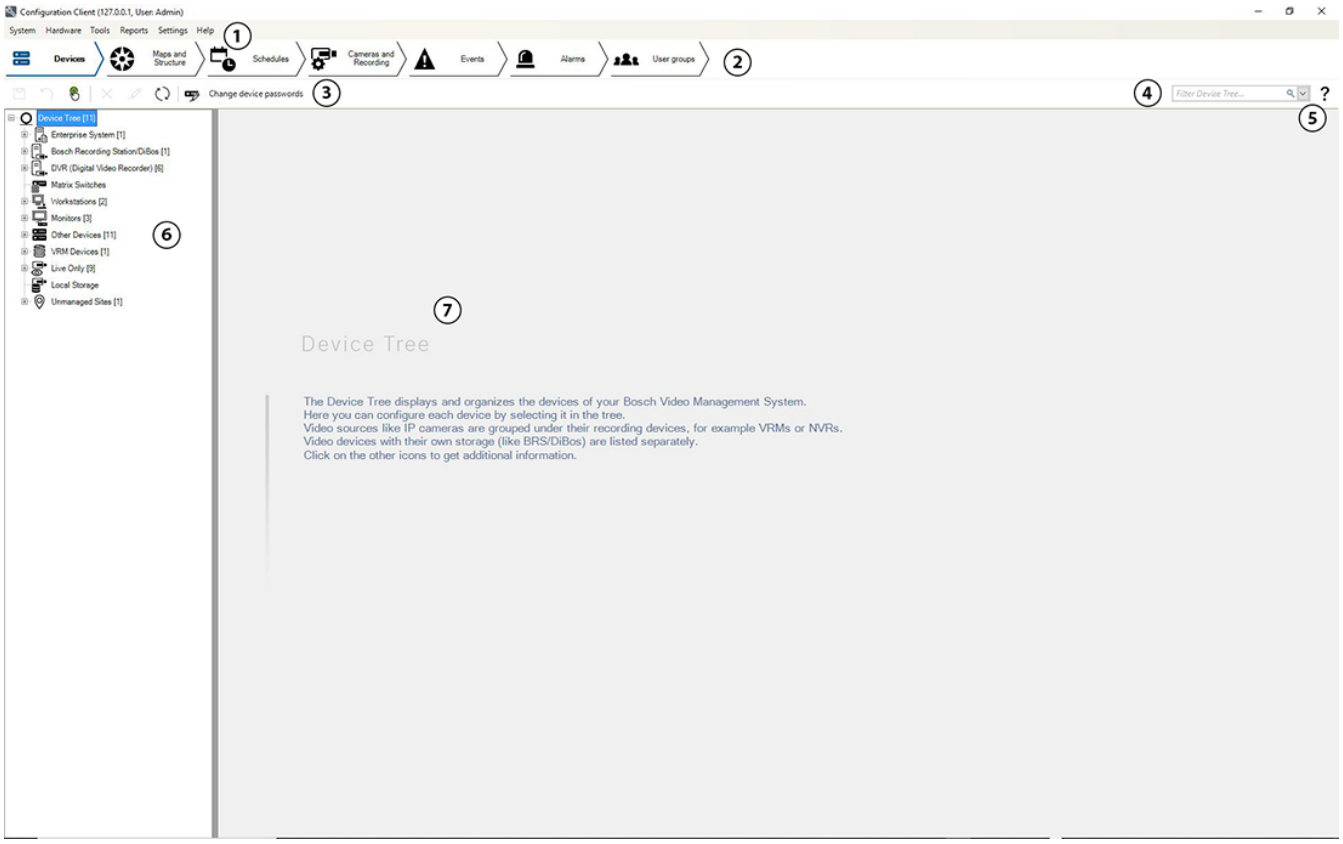
1. Klicken Sie mit der rechten Maustaste in das rechte Fenster, und wählen Sie **Drucken** aus.
   Das Dialogfeld **Drucken** wird geöffnet.
2. Klicken Sie auf **Drucken**.

✓ Das Thema wird auf dem angegebenen Drucker gedruckt.

2 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.



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 den BVMS Configuration Client an.
6	Auswahlfenster	Hierarchische Liste aller verfügbaren Geräte im System.
7	Konfigurationsfenster	Dient zum Konfigurieren des ausgewählten Geräts.

Dieses Handbuch führt Sie durch die Grundschritte für die Konfiguration und Bedienung von BVMS.
Ausführliche Informationen und schrittweise Anweisungen erhalten Sie im Konfigurationshandbuch und im Benutzerhandbuch sowie in der Online-Hilfe.

BVMS integriert digitale Video-, Audio- und weitere Dateien in jedem IP-Netzwerk.
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 Export Player zeigt exportierte Aufzeichnungen an.

Das Konzept des 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 den 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.

3 Systemüberblick

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.
Mobile Video Service (wählbar in Setup)	Bietet einen Transcoder-Dienst, der Live-Streams und aufgezeichnete Streams von einer in BVMS konfigurierten Kamera für die verfügbare Netzwerkbandbreite transcodiert. Dieser Dienst ermöglicht es Video Clients, beispielsweise einem iPhone oder Web Client, transcodierte Streams zu empfangen, z. B. bei unzuverlässigen Netzwerkverbindungen mit geringer Bandbreite.
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 und NVR-ähnliche Aufzeichnung, z. B. in Netzwerken mit geringer Bandbreite.

Komponente	Beschreibung
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.
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).

3.1 Hardware-Anforderungen

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

3.2 Software-Anforderungen

Siehe Datenblatt für BVMS.

3.3 Lizenzanforderungen

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

4 Konzepte

Dieses Kapitel enthält Hintergrundinformationen zu ausgewählten Themen.

4.1 BVMS Designkonzepte

System mit einem Management Server, Seite 20
Ein einzelnes BVMS Management Server-System ermöglicht die Verwaltung, Überwachung und Steuerung von bis zu 2000 Kameras bzw. Encodern.

Enterprise System, Seite 21
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 22
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 23
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.

4.1.1 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.

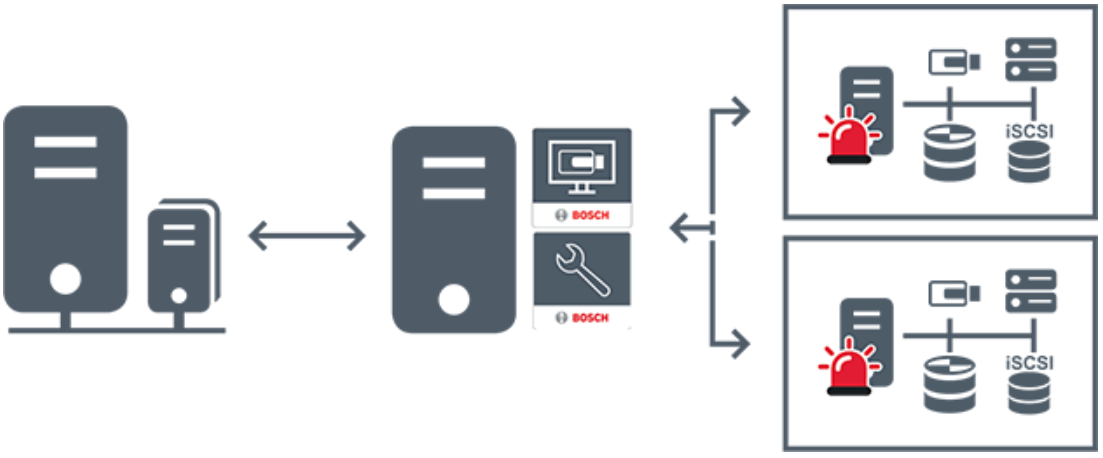
Zuständigkeiten:

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

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

4.1.2 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



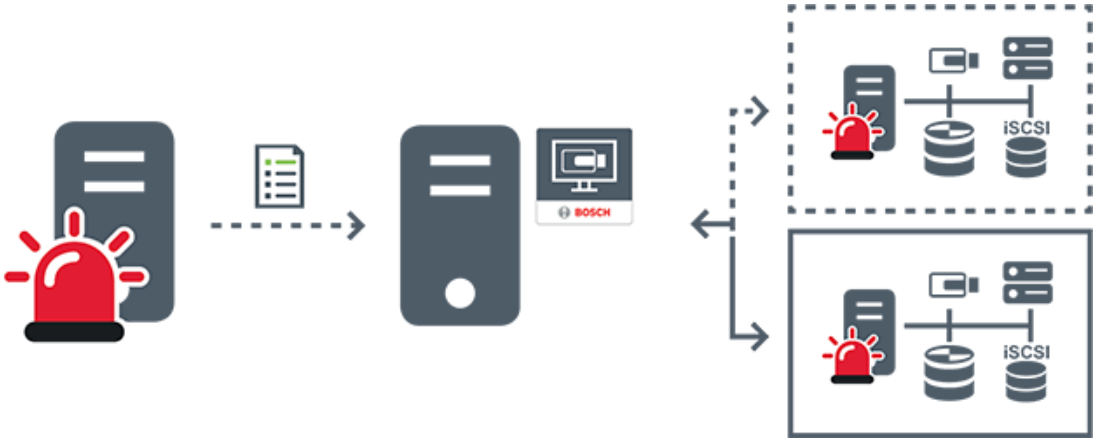
	Live, Wiedergabe, Ereignisse, Alarme
	BVMS Enterprise Management Server
	BVMS Operator Client / Configuration Client
	BVMS Subsystem

Siehe

- *Erstellung eines Enterprise Systems, Seite 86*
- *Konfigurieren der Serverliste für Enterprise System, Seite 86*
- *Konfigurieren von Benutzern, Berechtigungen und Enterprise Access, Seite 358*
- *Systemzugriff, Seite 71*

4.1.3 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 125*
- *Seite „Server-Liste/Adressbuch“, Seite 123*
- *Mittels Server Lookup, Seite 71*
- *Export der Server-Liste, Seite 125*
- *Import einer Server-Liste, Seite 126*

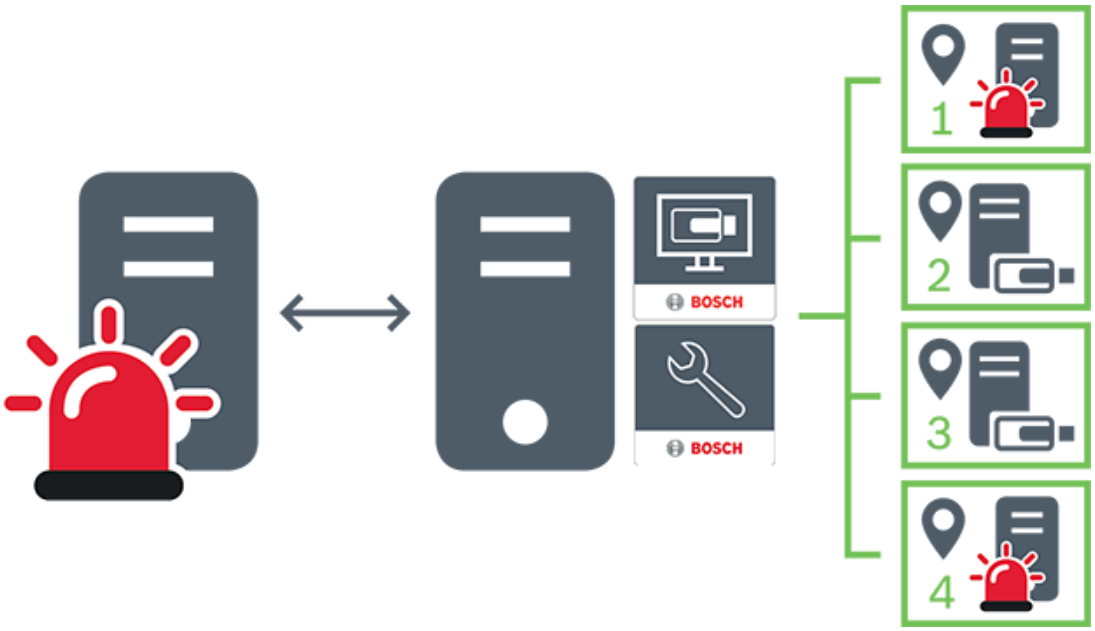
4.1.4 Unmanaged Site

- 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 eines sites 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 218*

4.2 Aufzeichnung

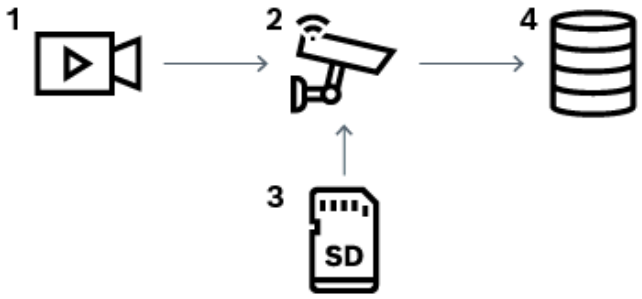
In diesem Kapitel werden die verschiedenen Aufzeichnungs- und Wiedergabefunktionen im System erläutert.

4.2.1 Automated Network Replenishment (ANR)

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.

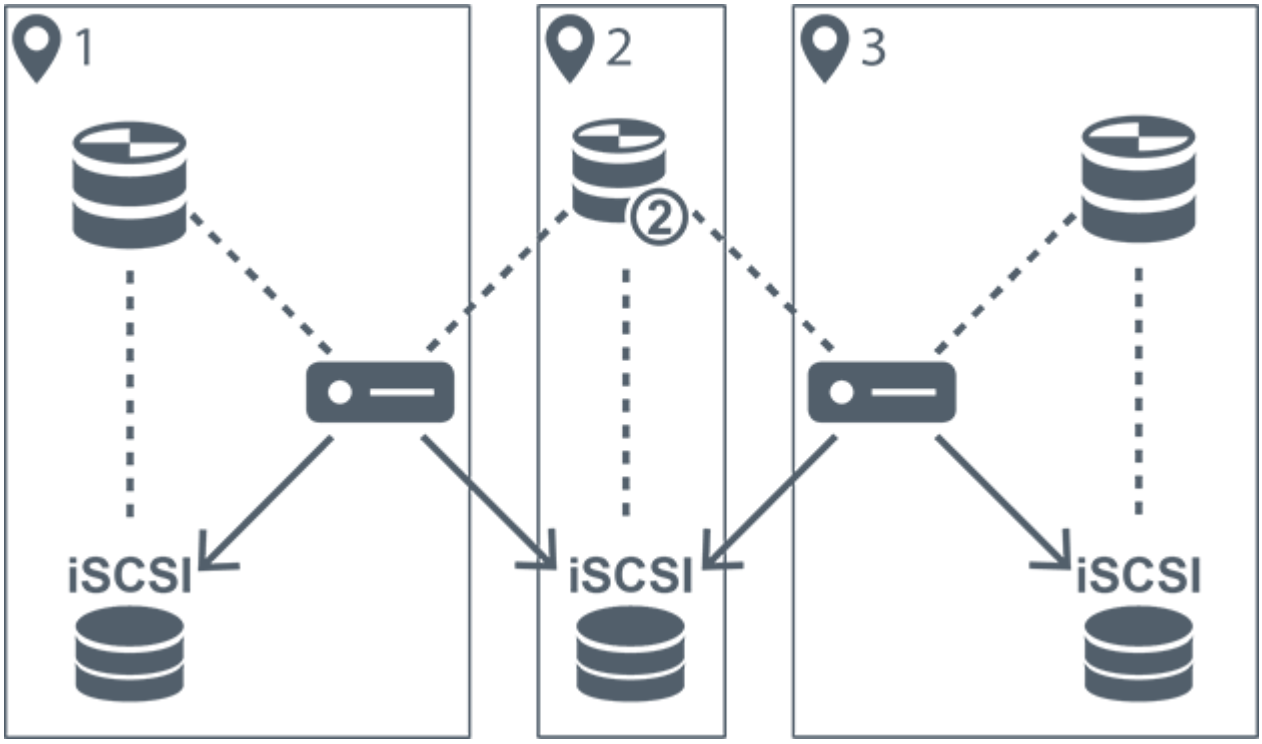
Siehe

- *Konfigurieren eines iSCSI-Geräts, Seite 197*
- *Speichermedien eines Encoders konfigurieren, Seite 85*
- *ANR-Funktion konfigurieren, Seite 306*

4.2.2 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 306*
- *Manuelles Hinzufügen eines gespiegelten VRM, Seite 182*
- *Manuelles Hinzufügen eines Failover-VRM, Seite 181*
- *Seite Kameras, Seite 287*

4.2.3 VRM-Aufzeichnungsmodi

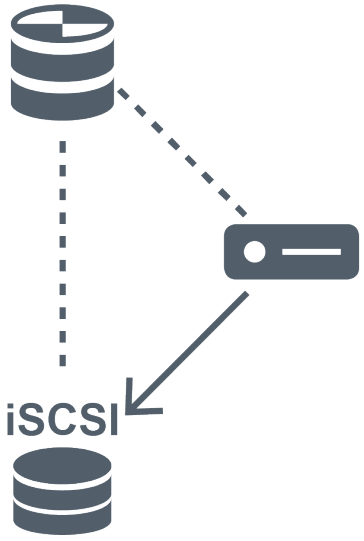
Dieses Kapitel enthält Grafiken, um mögliche VRM-Aufzeichnungsmodi zu veranschaulichen.
Liste möglicher VRM-Aufzeichnungsmodi:

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

– Failover-VRM-Aufzeichnung

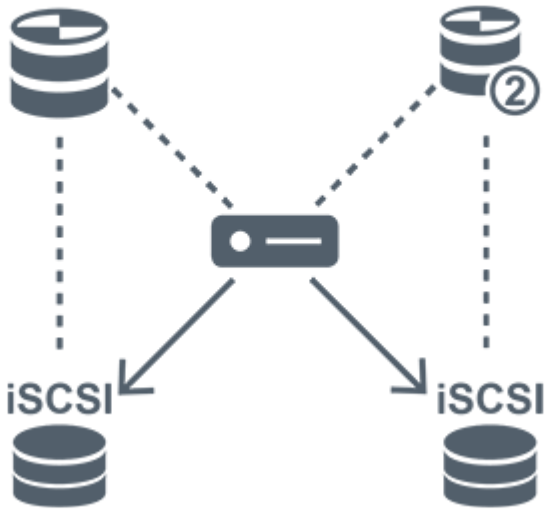
Für eine ANR-Aufzeichnung siehe Kapitel *Automated Network Replenishment (ANR), Seite 25*.

Primär-VRM-Aufzeichnung



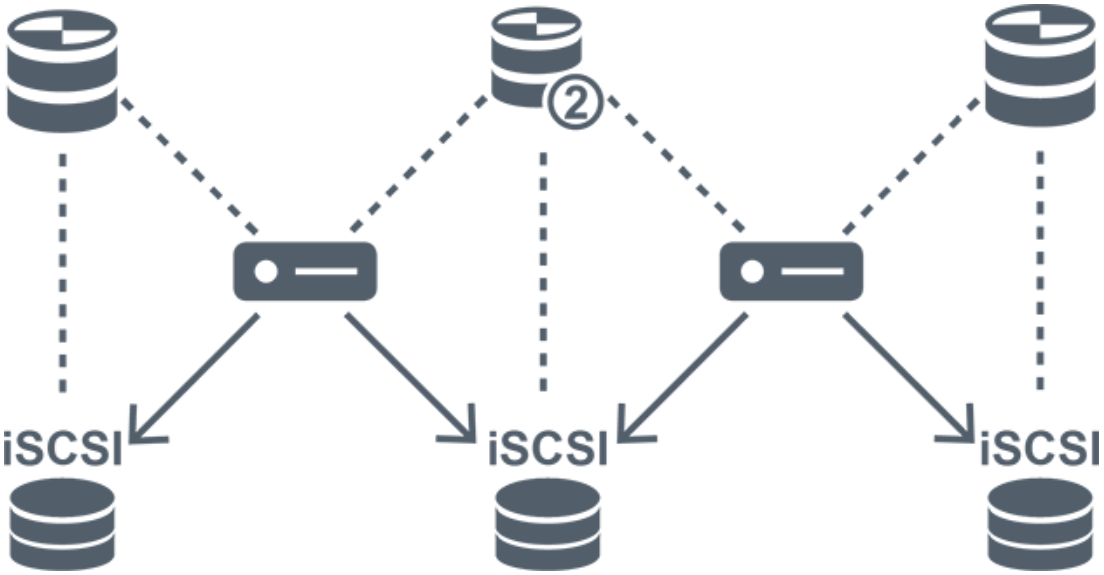
	Primärer VRM		Steuerungsverbindung
	iSCSI-Speichergerät	→	Video-Stream
	Encoder		

Gespiegelte VRM-Aufzeichnung



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

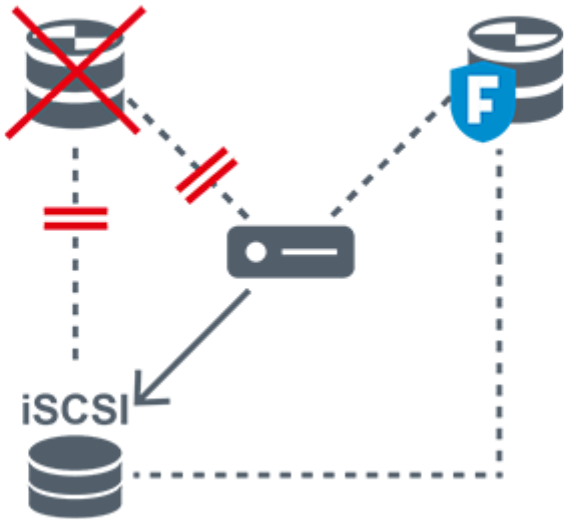
Sekundärer-VRM-Aufzeichnung



	Primärer VRM		Sekundärer VRM
	iSCSI-Speichergerät		Steuerungsverbindung

	Encoder	→	Video-Stream

Failover-VRM-Aufzeichnung



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

4.2.4 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 30*
- *Wiedergabe einer dualen VRM-Aufzeichnung, Seite 31*
- *Wiedergabe einer Primärer VRM-Aufzeichnung mit optionalem Failover-VRM, Seite 32*
- *Wiedergabe einer Sekundär-VRM-Aufzeichnung mit optionalem Failover-VRM, Seite 33*
- *Automatic Network Replenishment, Seite 34*

Wiedergabe einer einzelnen Aufzeichnung

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

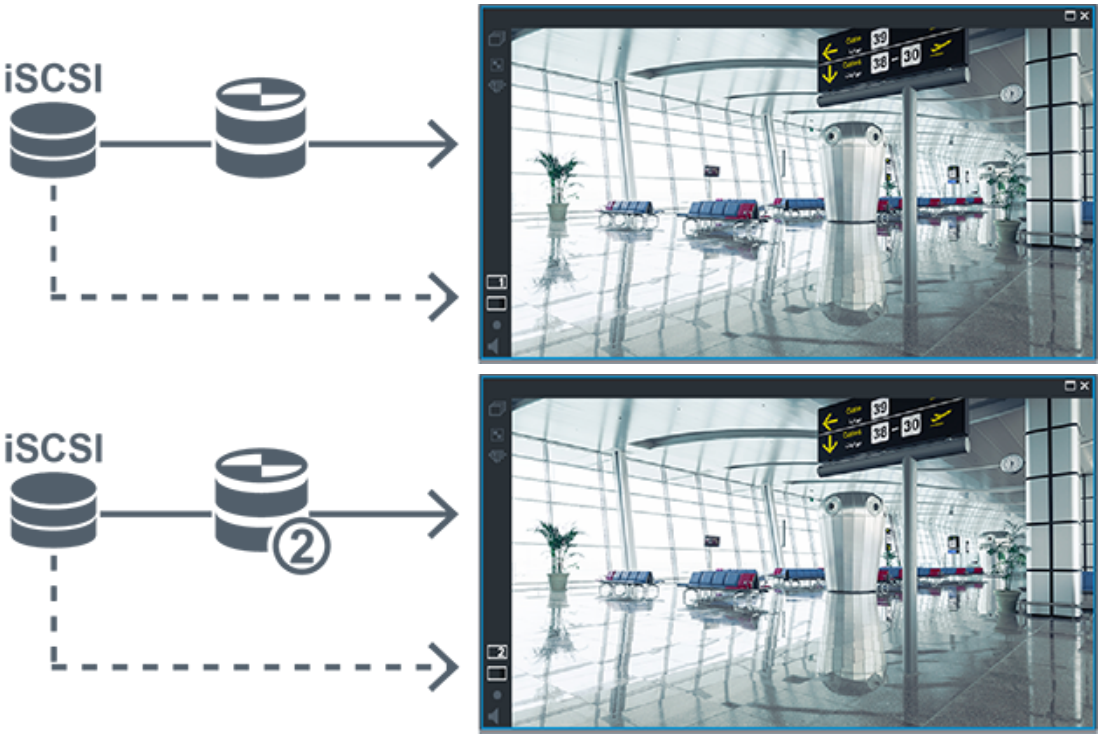
------>: Falls die Wiedergabe für diese Arbeitsstation konfiguriert ist, erfolgt sie direkt durch das iSCSI-Speichergerät.

iSCSI	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	iSCSI-Speichergerät
	Primärer VRM
2	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.

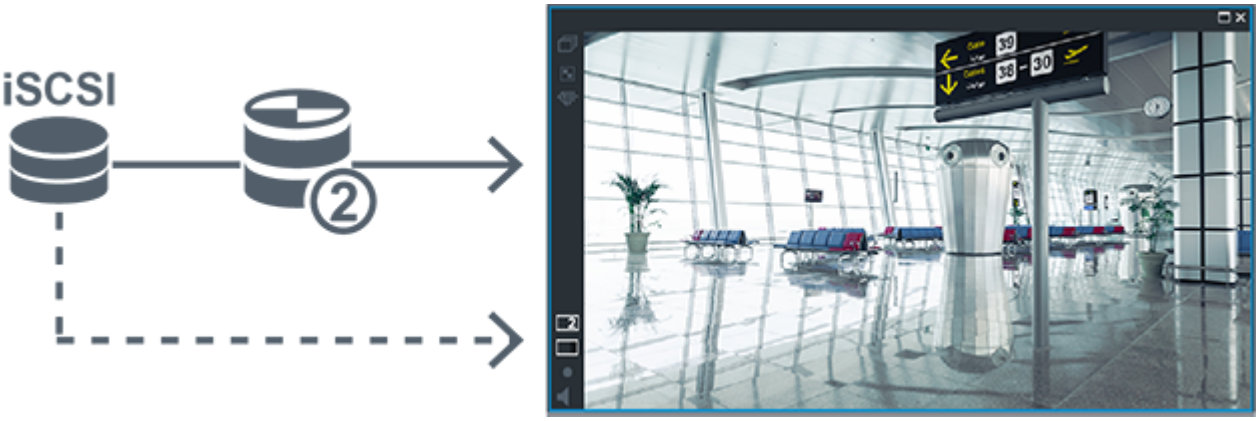
Ist der Primäre VRM nicht angeschlossen, ist eine Wiedergabe über den konfigurierten Failover-VRM möglich. Schließen Sie das Bildfenster und lassen Sie sich die Kamera erneut in einem Bildfenster anzeigen:

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:

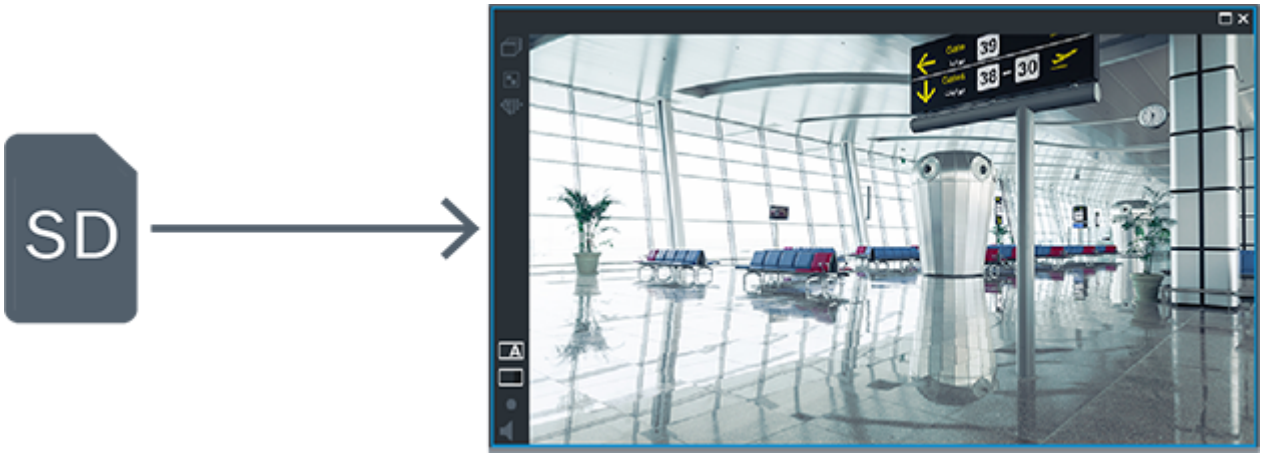
	iSCSI-Speichergerät
	Primärer VRM
	Sekundärer Failover-VRM
	Encoder

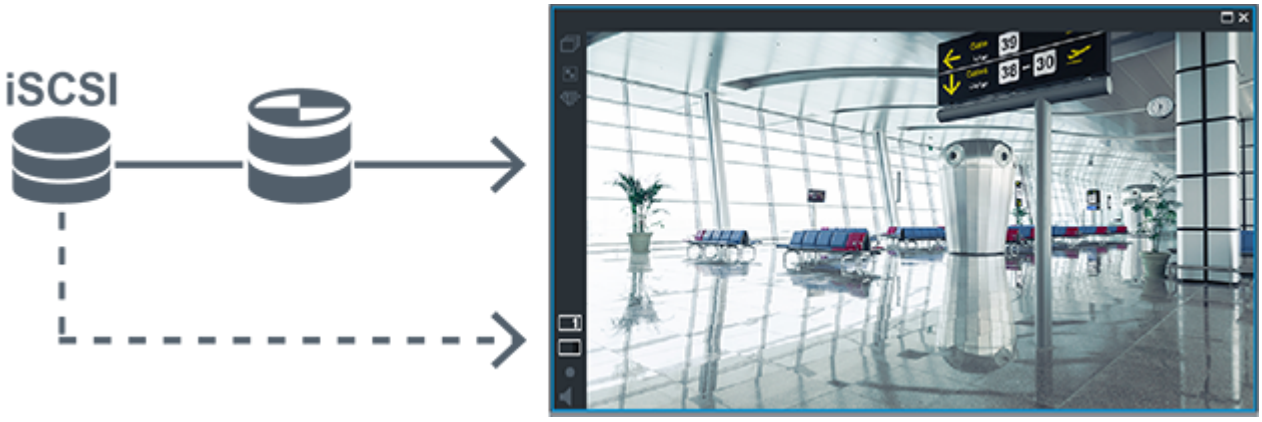
Die Encoder-Wiedergabe ist nur für einen begrenzten Aufzeichnungszeitraum möglich.

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	iSCSI-Speichergerät
	Primärer VRM
SD	SD-Karte

4.3 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. Bei jedem Alarm wird eine Reihe von Bildfenstern angelegt. Jedem Alarm können bis zu 5 Bildfenster zugeordnet werden. 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“. Mithilfe 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 329*

4.4 ONVIF-Ereigniszuordnung

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 244*
- *Ermöglicht die Protokollierung von ONVIF-Ereignissen, Seite 383*
- *Seite "ONVIF-Encoderereignis", Seite 240*

4.5 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 115*
- *Seite „Bedienerfunktionen“, Seite 345*

4.6 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

4.6.1 Arbeiten im Kompatibilitätsmodus

Diese Funktion ist in Version 5.5 und neuer verfügbar.
Ein BVMS Operator Client gibt Ihnen ein visuelles und textbasiertes Feedback über die Zustände.
Dabei sind folgende Operator Client-Zustände möglich:

-
  Der Operator Client ist mit dem Management Server verbunden.
-
  Der Operator Client ist nicht mit dem Management Server verbunden. Ein Grund ist möglicherweise die physische Trennung des Management Server vom Netzwerk.
-
  Dieser Status kann nur nach einer neu aufgebauten Verbindung mit dem Management Server angezeigt werden. Sämtliche betroffenen Funktionen arbeiten wieder, aber die Konfiguration des Operator Client ist aufgrund einer neueren auf dem System vorhandenen Konfiguration veraltet. Melden Sie sich erneut an, um die Konfiguration zu aktualisieren.
-
  Dieses Statussymbol wird angezeigt, wenn der Management Server über eine frühere BVMS Version als die Operator Client-Arbeitsstation verfügt.

4.7 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

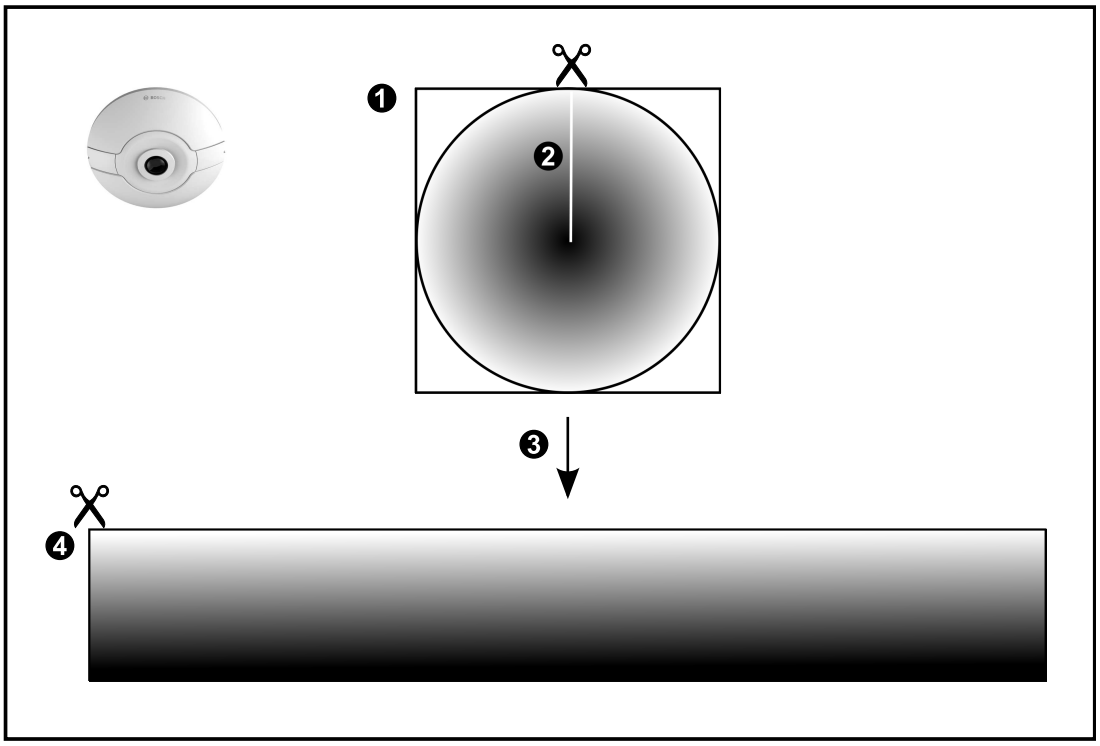
Panorama- und zugeschnittene Ansichtsmodi werden vom Entzerren-Prozess in BVMS erstellt. Entzerren in der Kamera wird nicht verwendet.
Der Administrator muss die Montageposition einer Panoramakamera im Configuration Client konfigurieren.
Sie können die Größe des Bildfensters einer Kamera bei Bedarf ändern.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

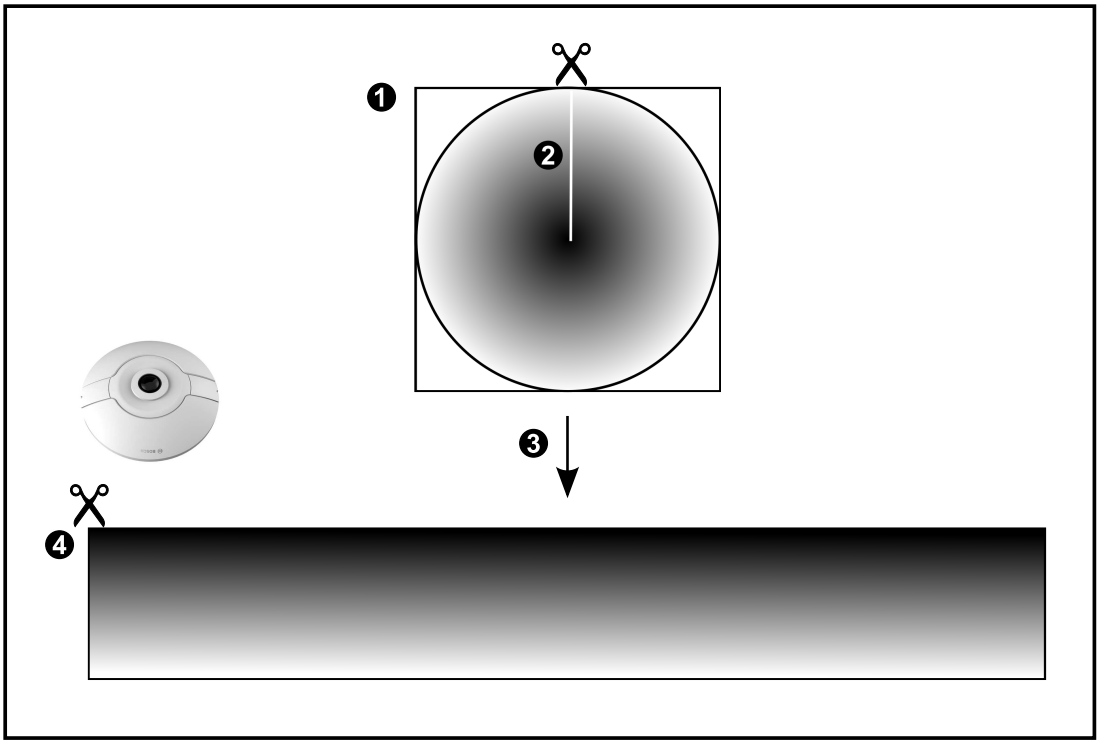
Siehe

– *Konfigurieren von voreingestellten Positionen und AUX-Kommandos, Seite 302*

4.7.1 360°-Panoramakamera – Boden- oder Deckenmontage

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



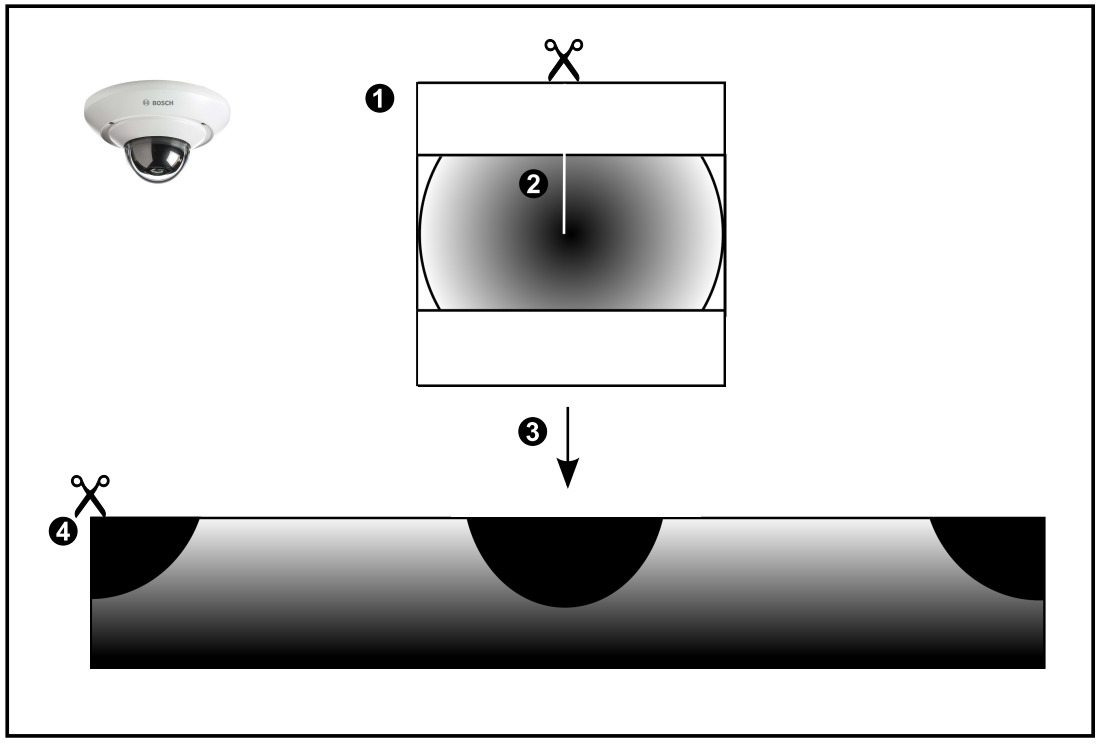


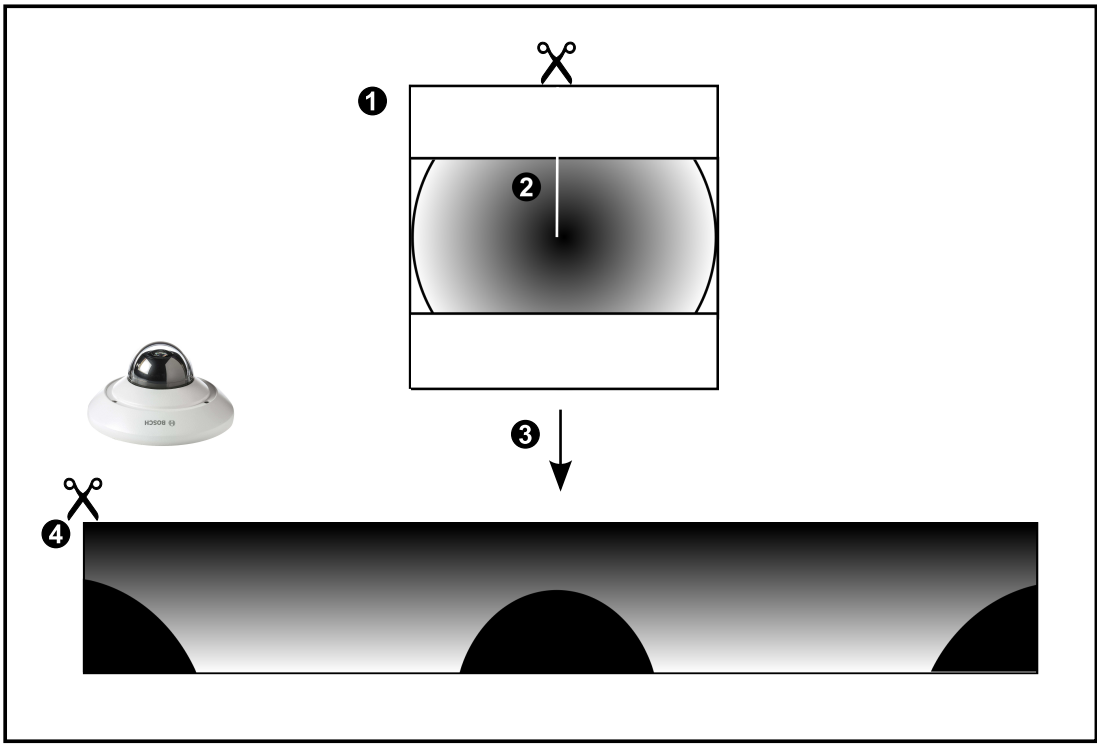
1	Ganzes Kreisbild	3	Entzerren

2	Schnittlinie (Position kann vom Bediener bei Ansicht ohne Zoom geändert werden)	4	Panorama-Ansicht

4.7.2 180°-Panoramakamera – Boden- oder Deckenmontage

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

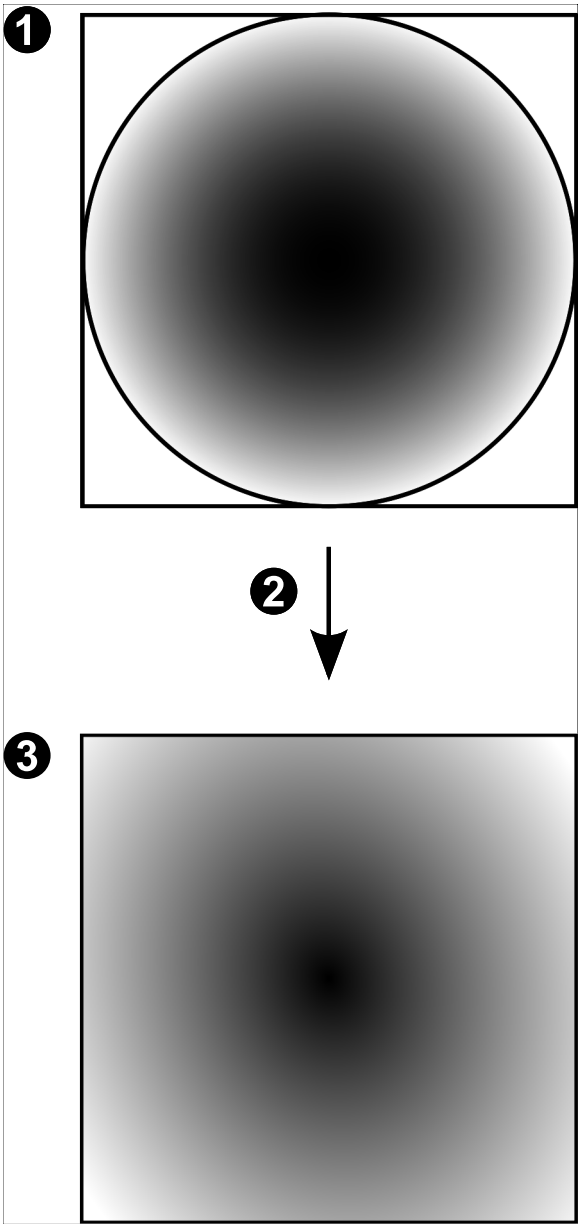




1	Ganzes Kreisbild	3	Entzerren
2	Schnittlinie (Position kann vom Bediener bei Ansicht ohne Zoom geändert werden)	4	Panorama-Ansicht

4.7.3 360°-Panoramakamera – Wandmontage

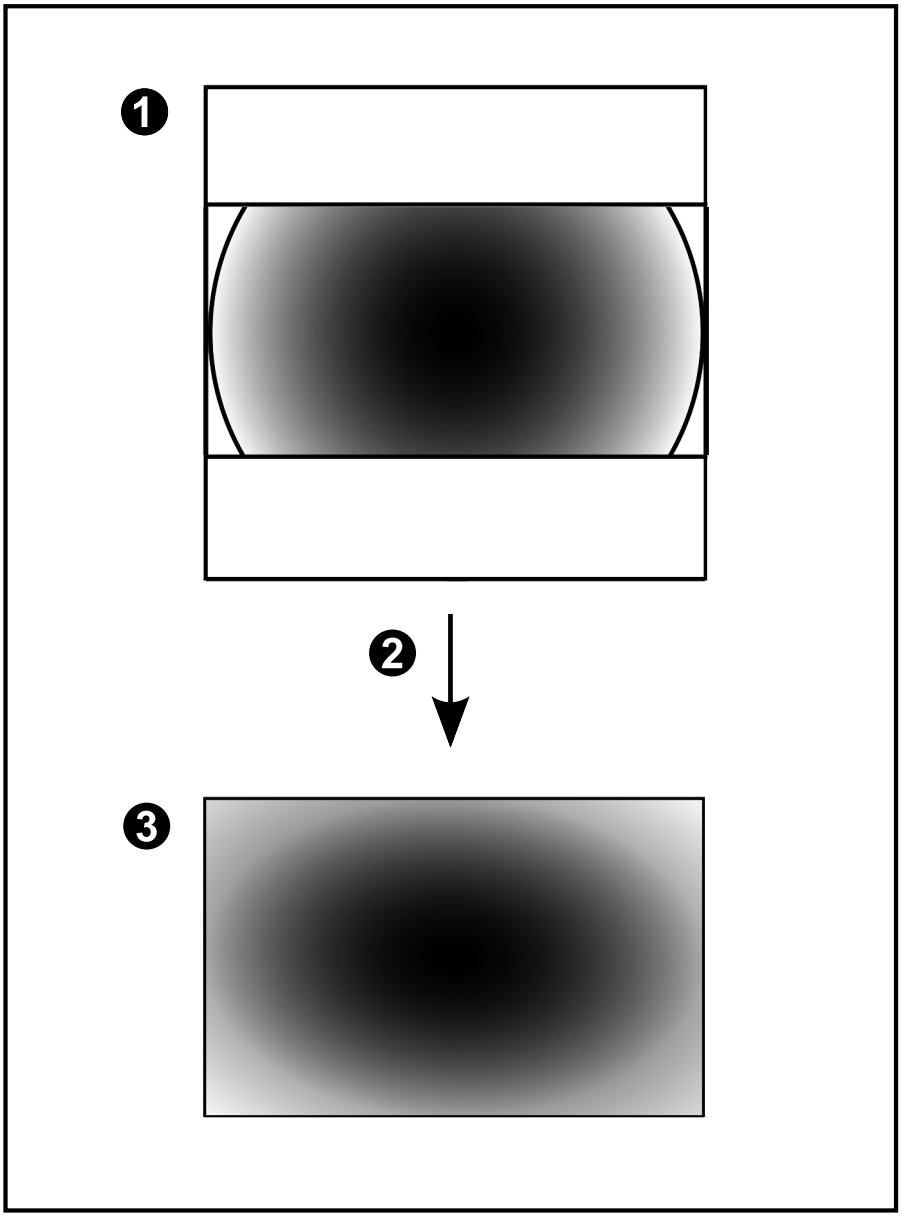
Die folgende Abbildung zeigt das Entzerren bei einer 360°-Kamera, die an einer Wand montiert ist.



1	Ganzes Kreisbild	3	Panorama-Ansicht
2	Entzerren		

4.7.4 180°-Panoramakamera – Wandmontage

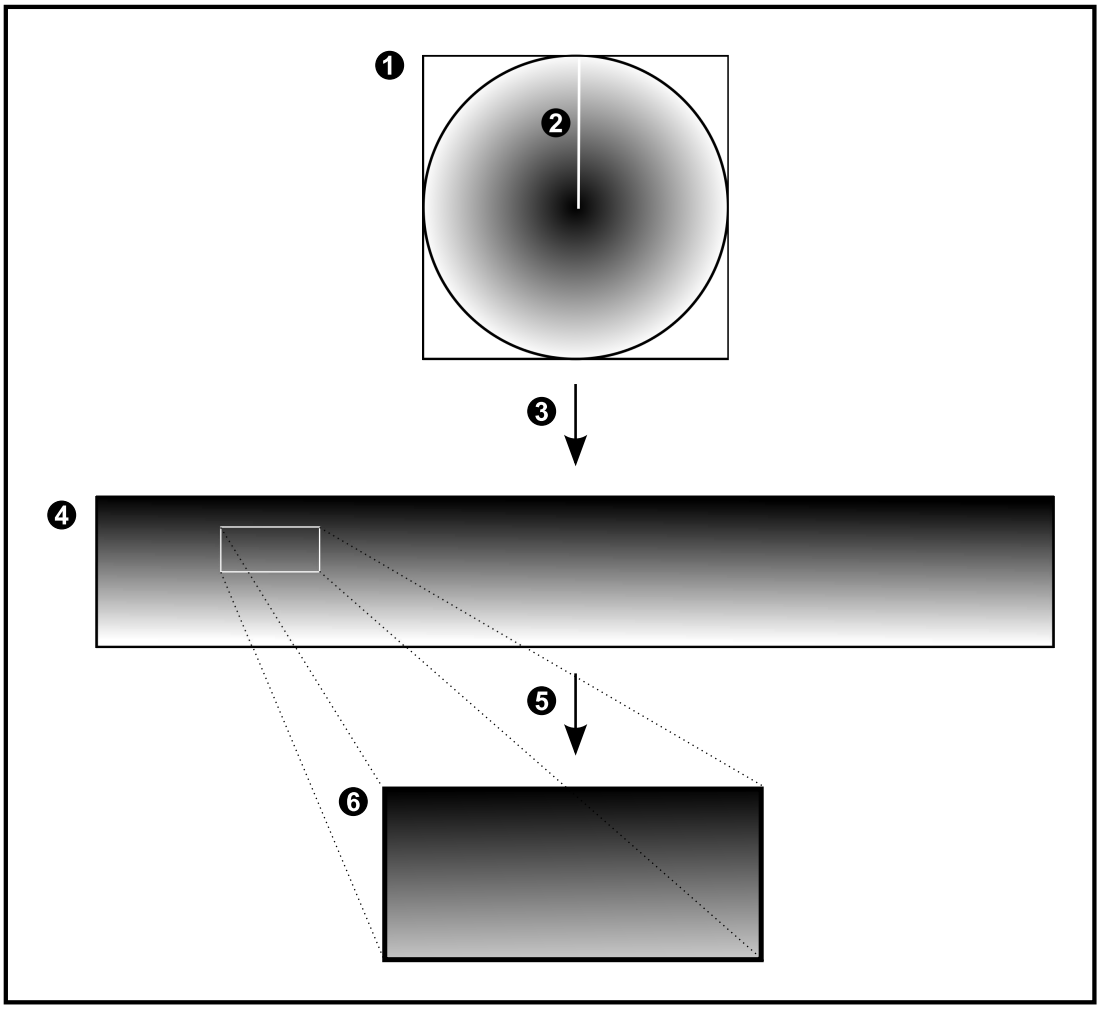
Die folgende Abbildung zeigt das Entzerren bei einer 180°-Kamera, die an einer Wand montiert ist.



1	Ganzes Kreisbild	3	Panorama-Ansicht
2	Entzerren		

4.7.5 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

4.8 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.

4.9 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 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
- VIDOS NVR-Computer
  Angeschlossen über das Netzwerk
- Analogkameras
  Angeschlossen an Encoder, BRS/DiBos Geräte
- Decoder
  Angeschlossen über das Netzwerk
- Monitore
  Angeschlossen an einen Decoder, eine Bosch Allegiant Kreuzschiene, eine BVMS Client-Arbeitsstation
- BRS/DiBos Geräte (unterstützte Software-Versionen finden Sie im BVMS Datenblatt)
  Angeschlossen über das Netzwerk
- 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.
- SMS-Gerät
  Angeschlossen an einen COM-Port des Management Server
- 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.

5.1 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)
- DiBos Systeme mit Kameras
- DVR-Systeme mit Kameras
- ATM/POS-Geräte
- I/O-Module
  Nur ADAM-Geräte werden unterstützt.

5.2 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
Weitere Informationen, Software und Dokumentation finden Sie unter www.boschsecurity.com auf der entsprechenden 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
- VIDOS NVR-Computer
  Angeschlossen über das Netzwerk
- Analogkameras
  Angeschlossen an Encoder, BRS/DiBos Geräte
- Decoder
  Angeschlossen über das Netzwerk
- Monitore
  Angeschlossen an einen Decoder, eine Bosch Allegiant Kreuzschiene, eine BVMS Client-Arbeitsstation
- BRS/DiBos Geräte (unterstützte Software-Versionen finden Sie im BVMS Datenblatt)

Angeschlossen über das Netzwerk

– 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

5.3 Verbinden eines Bosch IntuiKey Keyboards mit BVMS

Dieses Kapitel enthält Hintergrundinformationen zur Konfiguration eines Bosch IntuiKey-Keyboards

5.3.1 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

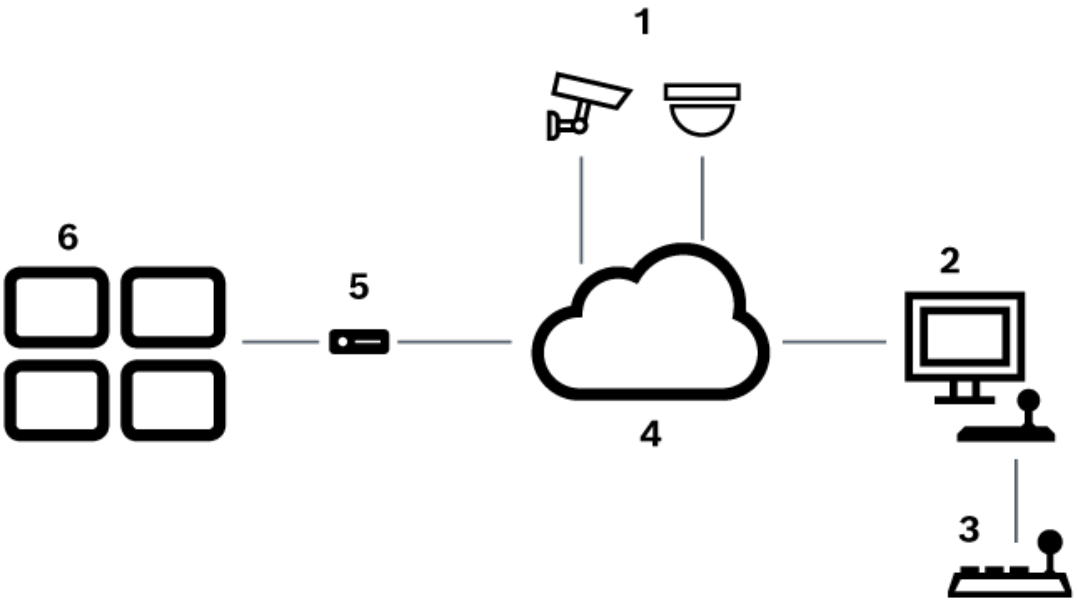


Abbildung 5.1: Szenario 1: An eine Bosch Video Management System Arbeitsstation angeschlossenes Bosch IntuiKey Keyboard

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

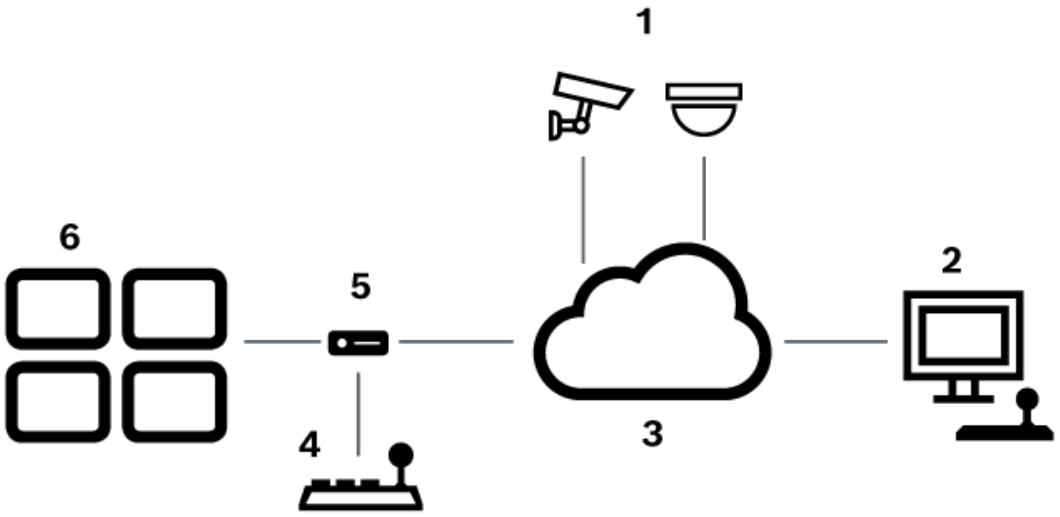


Abbildung 5.2: Szenario 2: An einen Decoder angeschlossenes Bosch IntuiKey Keyboard

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 158*

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

– *Konfigurieren eines Bosch IntuiKey Keyboards (Seite „Einstellungen“) (Arbeitsstation), Seite 136*
– *Konfigurieren eines Bosch IntuiKey Keyboards (Decoder), Seite 143*
– *Konfigurieren eines Decoders für den Einsatz mit einem Bosch IntuiKey Keyboard, Seite 144*

Siehe

– *Seite „Assign Keyboard“ (Tastatur zuweisen), Seite 158*

5.3.2 Anschluss eines Bosch IntuiKey Keyboards an einen Decoder

Konfigurieren des Decoders

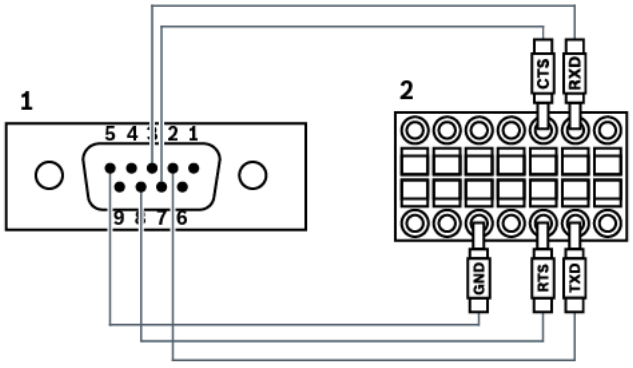
Siehe *Konfigurieren eines Decoders für den Einsatz mit einem Bosch IntuiKey Keyboard, Seite 144* .

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:



5.3.3 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.

5.4 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.

5.4.1 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.

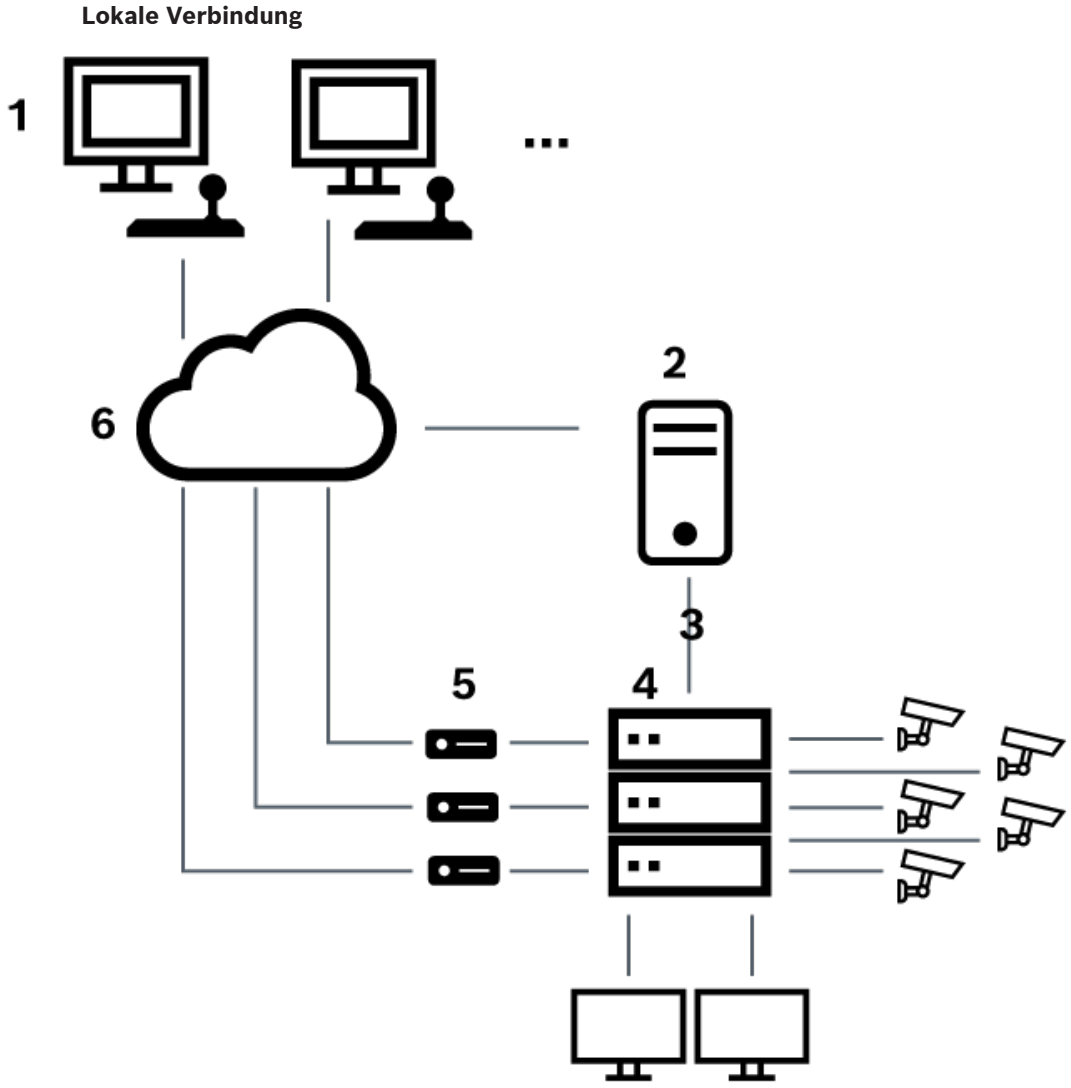


Abbildung 5.3: Lokale Verbindung des Bosch Video Management System mit einem Bosch Allegiant-Matrix-Switch

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

Entfernte Verbindung

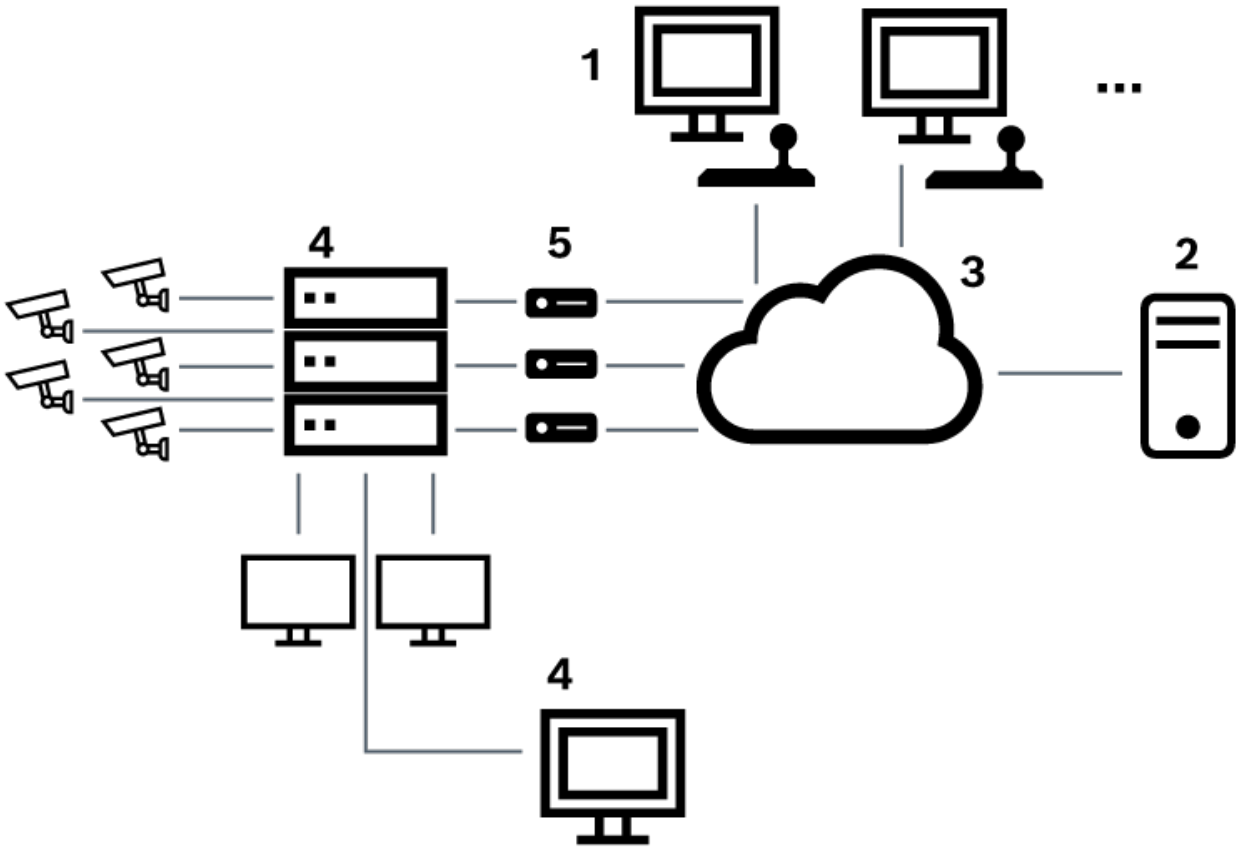


Abbildung 5.4: Entfernte Verbindung des Bosch Video Management System mit einem Bosch Allegiant-Matrix-Switch

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

5.4.2 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 132*

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

– *Konfigurieren eines Bosch Allegiant Geräts, Seite 132*

Siehe

– *Seite Kreuzschienen, Seite 132*

5.4.3 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.

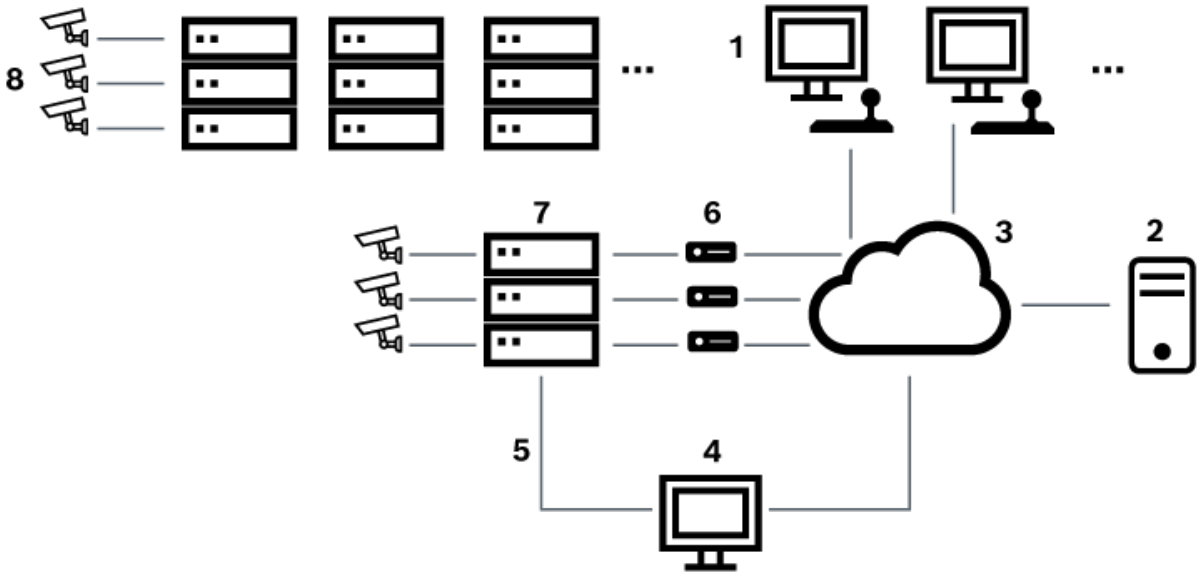


Abbildung 5.5: Mit Satellitenkreuzschienen erweitertes Bosch Allegiant System

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.

5.5 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	

Unterstützter Befehl	Beschreibung	Bemerkungen
Umschaltung/Sequenz		
REMOTE-TGL	Zwischen Schwenk/Neige/ Zoom-Steuerungsbefehlen wechseln	
PREPOS-SET	Vorposition einstellen	
PREPOS	Vorposition abrufen	
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	

6 Erste Schritte

Dieses Kapitel enthält Informationen zu den ersten Schritten mit BVMS.

6.1 Installieren der Software-Module

Hinweis!
DiBos Web Client darf nicht auf einem BVMS Computer installiert werden.
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.

6.2 Verwendung von Config Wizard

Der Config Wizard dient zur schnellen und einfachen Konfiguration kleinerer Systeme. Der Config Wizard verhilft Ihnen zu einem konfigurierten System einschließlich VRM, iSCSI-System, Mobile Video Service, Kameras, Aufzeichnungsprofilen 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.
Der Config Wizard fügt den lokalen VRM automatisch zu einer Standard-Software-Installation sowie zu DIVAR IP 3000 und DIVAR IP 7000 hinzu.
Bei einem DIVAR IP 3000 und einem DIVAR IP 7000 wird das lokale iSCSI-Gerät ebenfalls automatisch hinzugefügt, falls es nicht bereits verfügbar ist.
Bei einem DIVAR IP 3000 und einem DIVAR IP 7000 wird ein lokaler Mobile Video Service automatisch hinzugefügt, falls er 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**:**

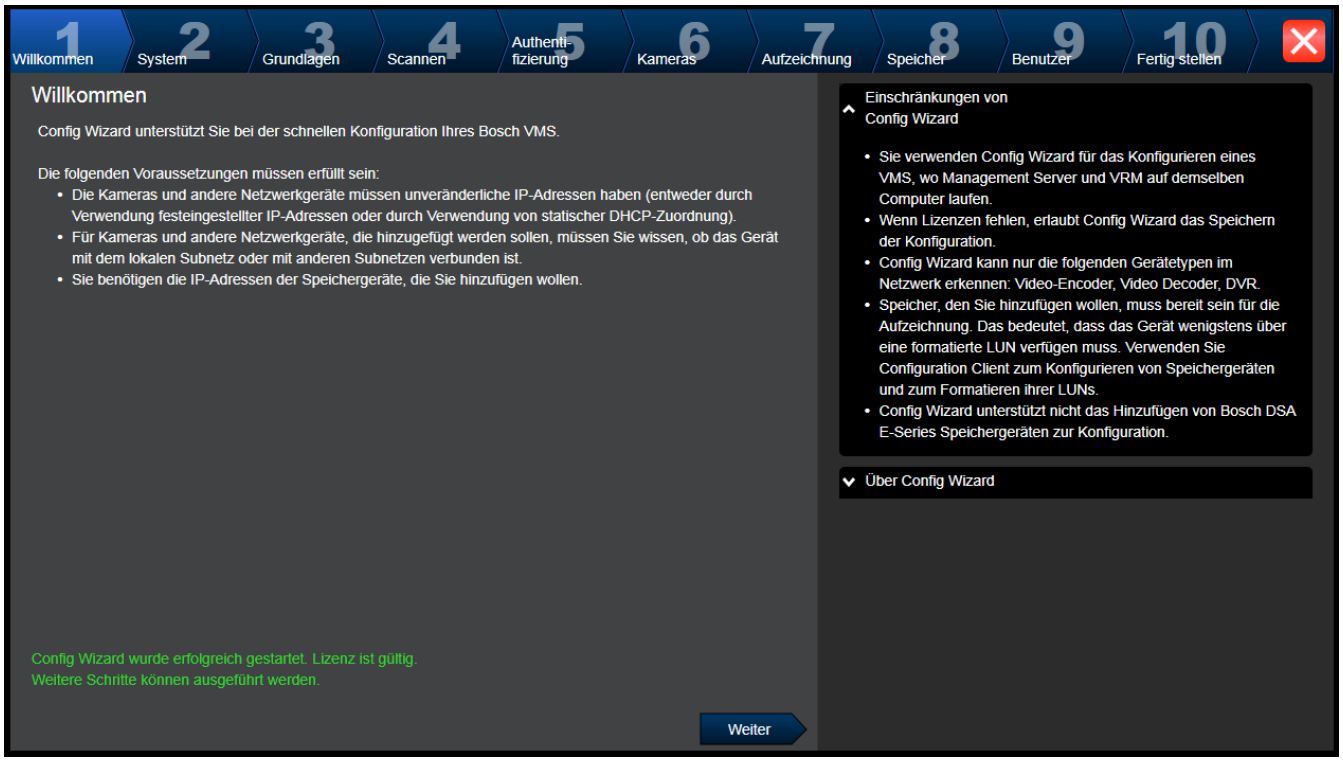
- Klicken Sie auf **Start** > **Alle Programme** > BVMS > Config Wizard.
  Die Seite Welcome wird angezeigt.

Verfügbare Seiten

- *Seite Welcome, Seite 62*
- *Seite System, Seite 62*
- *Seite Basic, Seite 63*
- *Seite Scan, Seite 64*
- *Seite Authentication, Seite 65*
- *Seite Cameras, Seite 66*

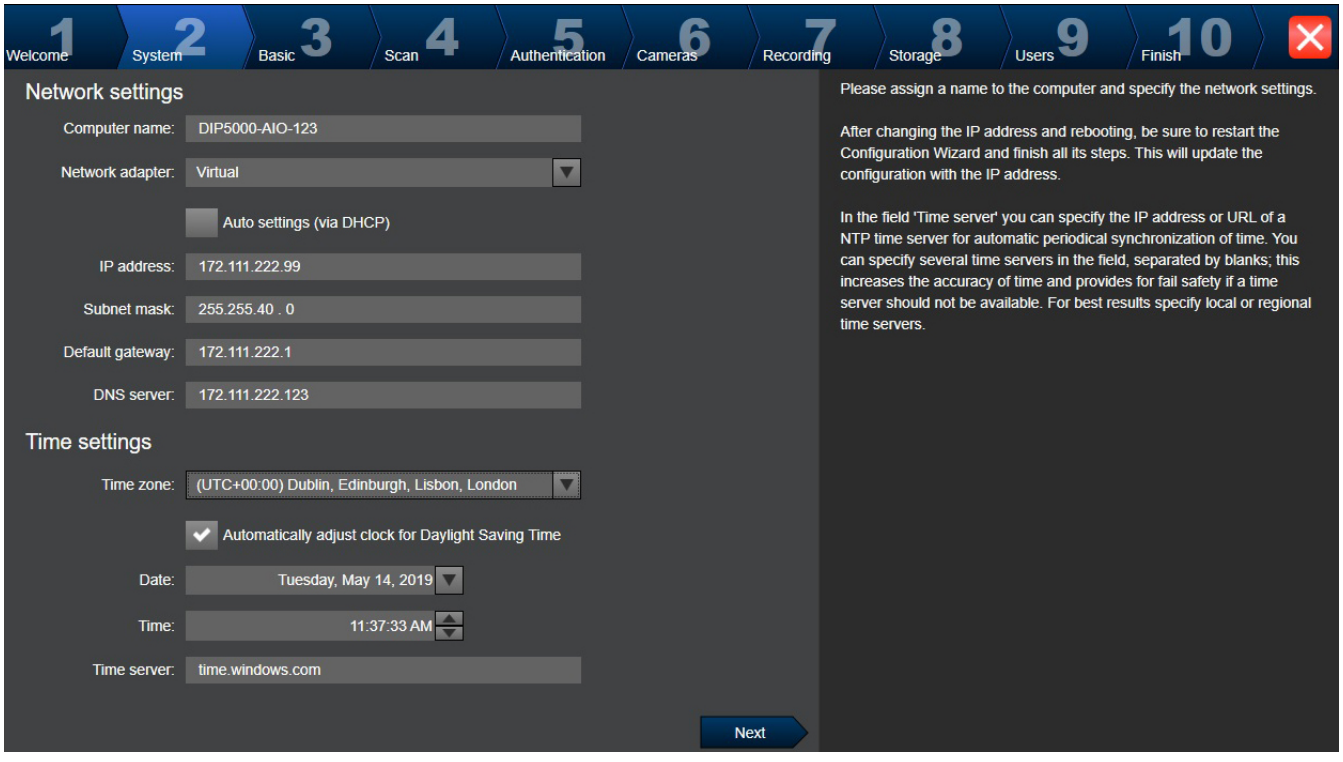
- *Seite Recording, Seite 66*
- *Seite Storage, Seite 67*
- *Seite Users, Seite 68*
- *Seite Finish, Seite 69*

Seite Welcome



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

Seite System

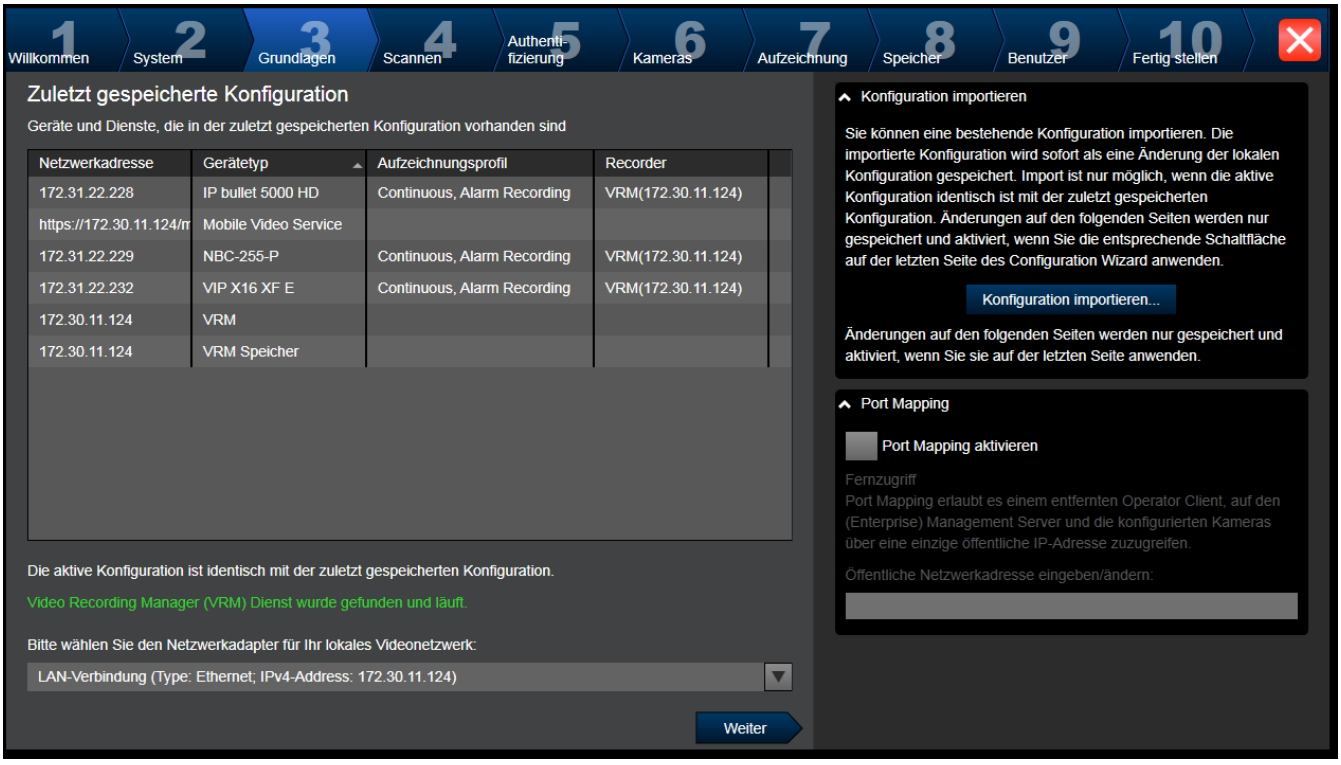


Hinweis!
Nur verfügbar für DIVAR IP 3000, DIVAR IP 7000, DIVAR IP all-in-one 5000, DIVAR IP all-in-one 6000 und DIVAR IP all-in-one 7000

Konfigurieren Sie die Netzwerkeinstellungen des Betriebssystems.
Konfigurieren Sie die Zeiteinstellungen des Betriebssystems.

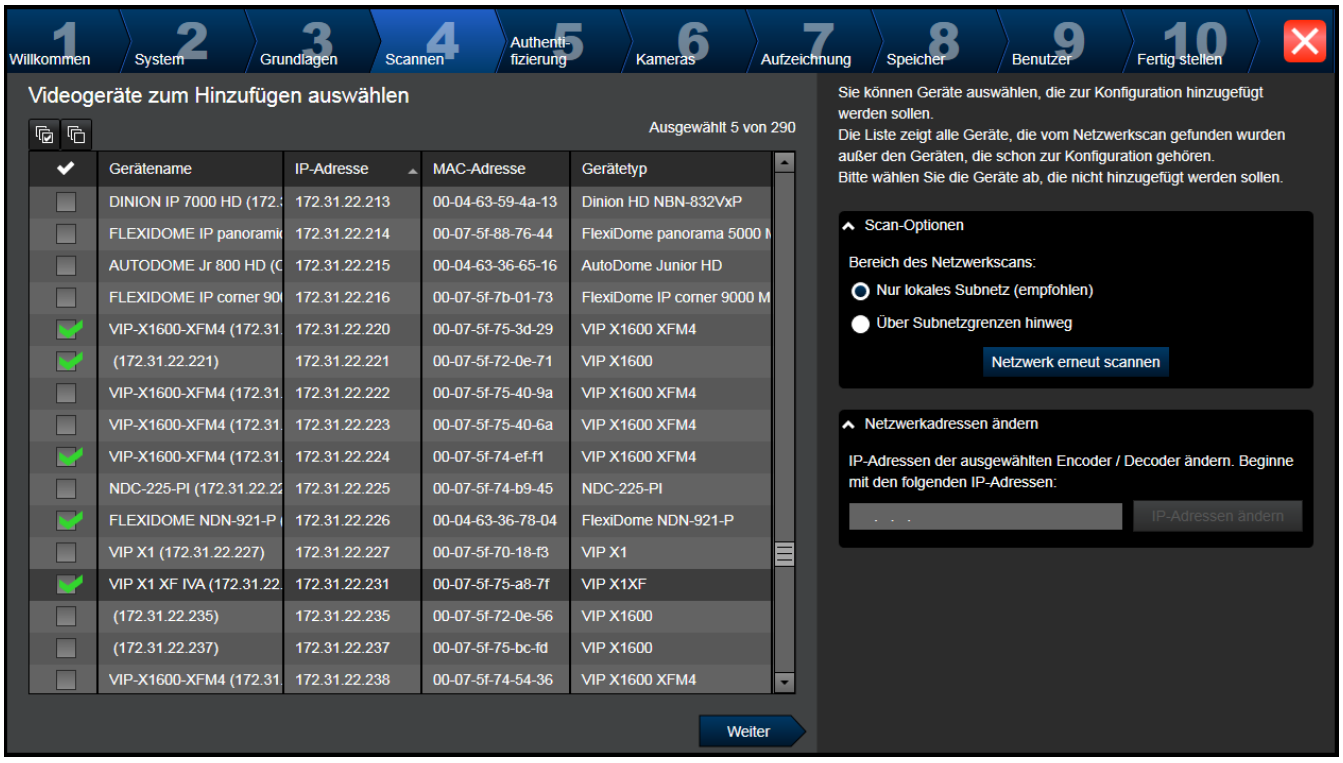
Hinweis:
Für eine Videoüberwachungsumgebung wird dringend empfohlen, einen Zeitserver festzulegen.
Sobald Sie auf **Next** klicken, werden die Einstellungen aktiviert.

Seite Basic



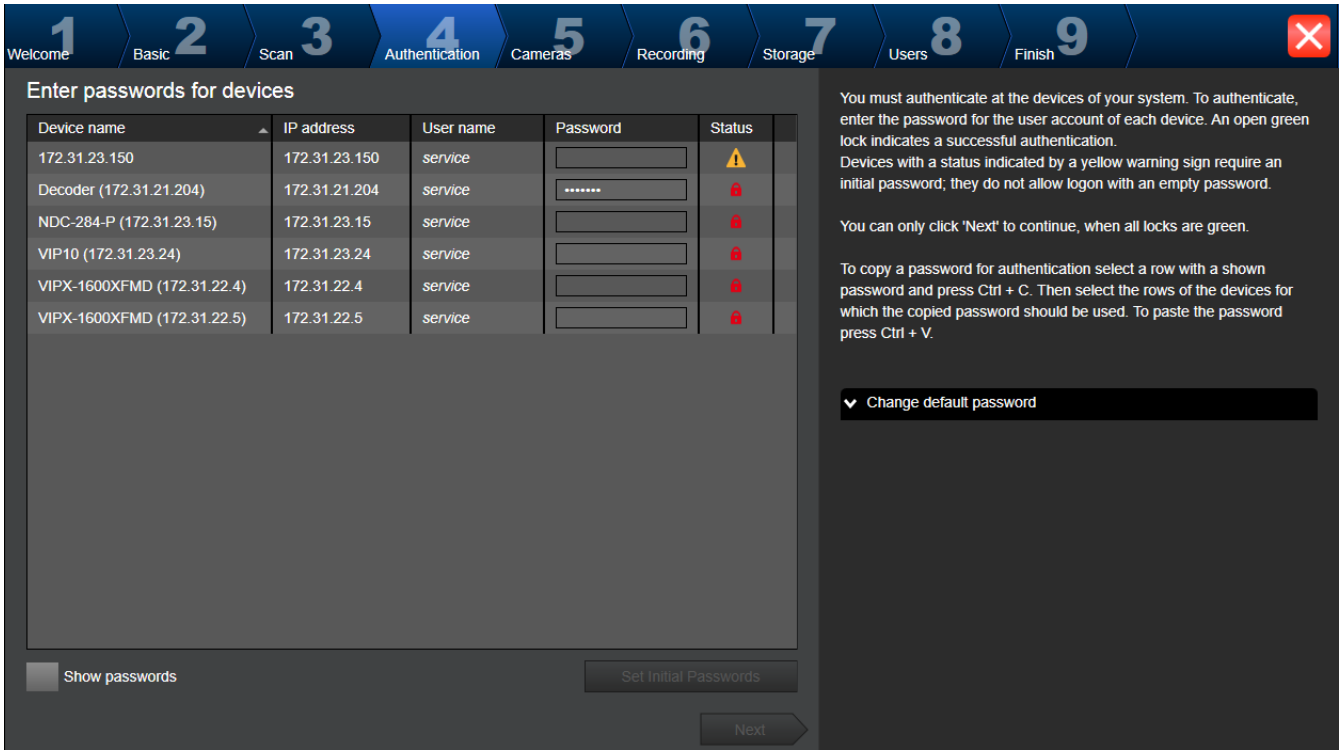
Diese Seite zeigt die zuletzt gespeicherte Konfiguration an. Sie können eine BVMS-Datei als eine Änderung der vorhandenen Konfiguration importieren. Wenn Sie auf **Next** klicken, wird diese Änderung gespeichert, aber nicht aktiviert.
Sie können den Netzwerkadapter Ihres Computers auswählen, der mit 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. Aktivieren Sie **Passwörter anzeigen** mit einem Klick.
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.

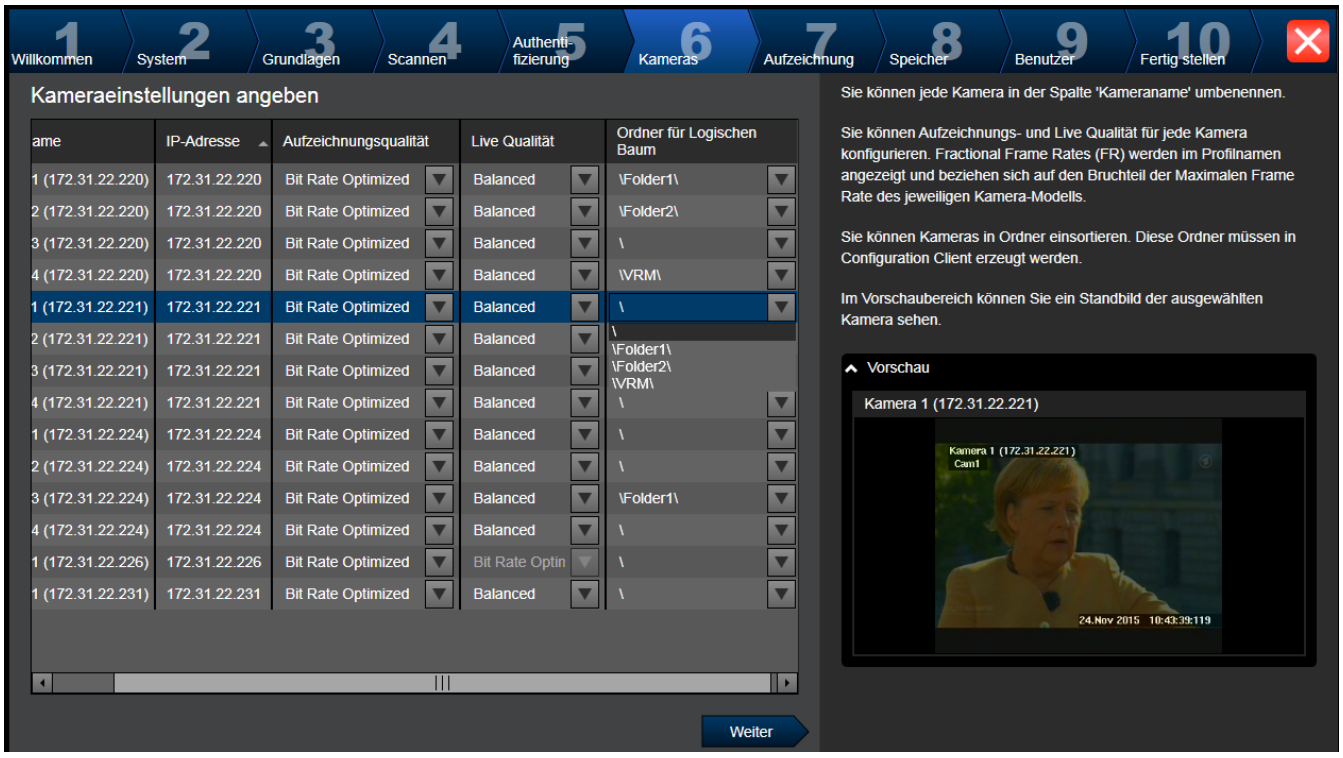
Die Passwortprüfung erfolgt automatisch, wenn Sie einige Sekunden lang kein weiteres Zeichen in dem Passwortfeld eingeben oder außerhalb des Passwortfelds klicken.
Sie können ein globales Standardpasswort für alle Geräte bereitstellen, die aktuell nicht durch ein Passwort geschützt werden.

Wenn ein Gerät ein erstes Passwort erfordert, wird ⚠ angezeigt.

So legen Sie ein erstes Passwort fest:

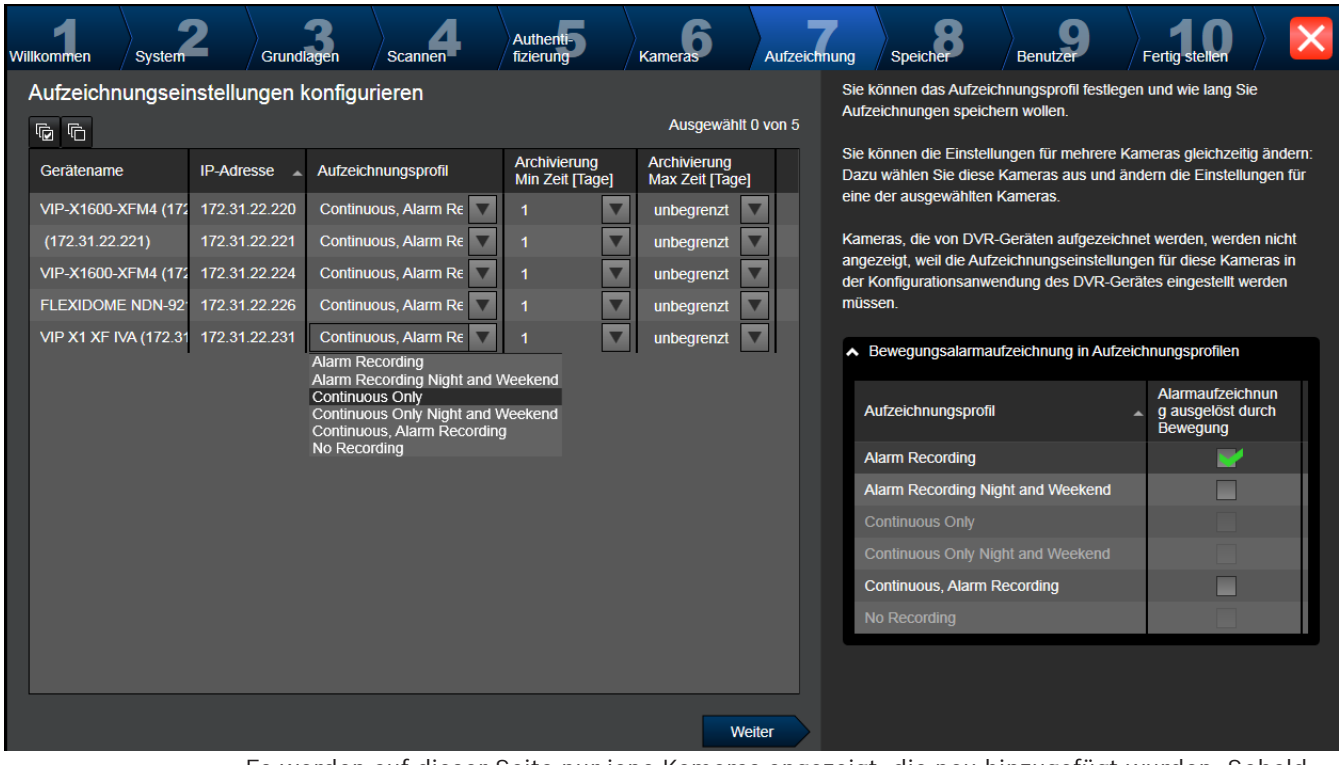
1. Geben Sie das Passwort im Feld **Passwort** ein.
2. Klicken Sie auf **Setzen Sie initiale Passwörter**.
   Das erste Passwort wird festgelegt.
   Hinweis: Solange Sie kein erstes Passwort für alle Geräte in der Liste festgelegt haben, die ein erstes Passwort benötigen, können Sie nicht fortfahren.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

Seite Cameras



Mithilfe dieser Seite können Sie die Kameras des Systems verwalten.

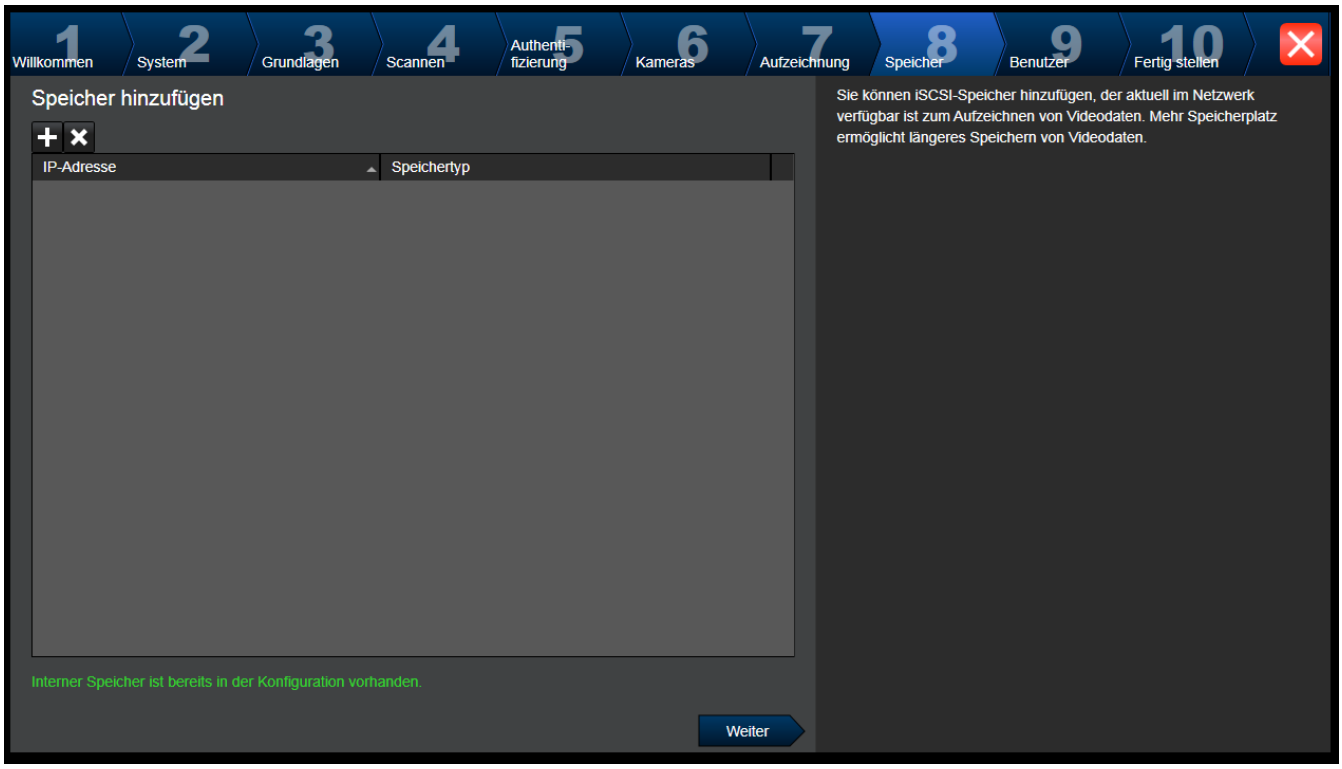
Seite Recording



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.

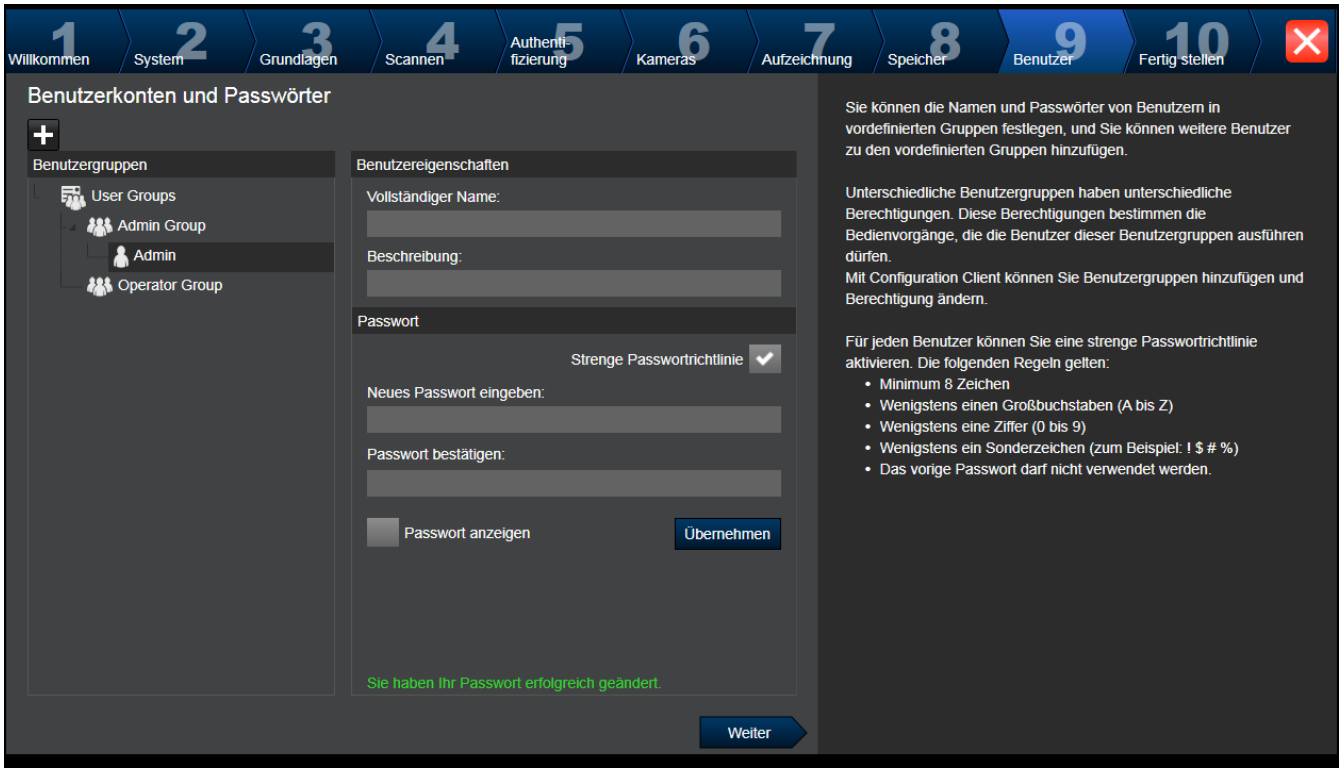
Sie können die Bewegungsaufzeichnung für die Aufzeichnung von Profilen mit aktivierter Aufzeichnung und Alarmaufzeichnung aktivieren. Konfigurieren Sie bei Bedarf die Aufzeichnung und Alarmaufzeichnung im Configuration Client (Dialogfeld **Geplante Aufzeichnungseinstellungen**).
VCA ist für jede neu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

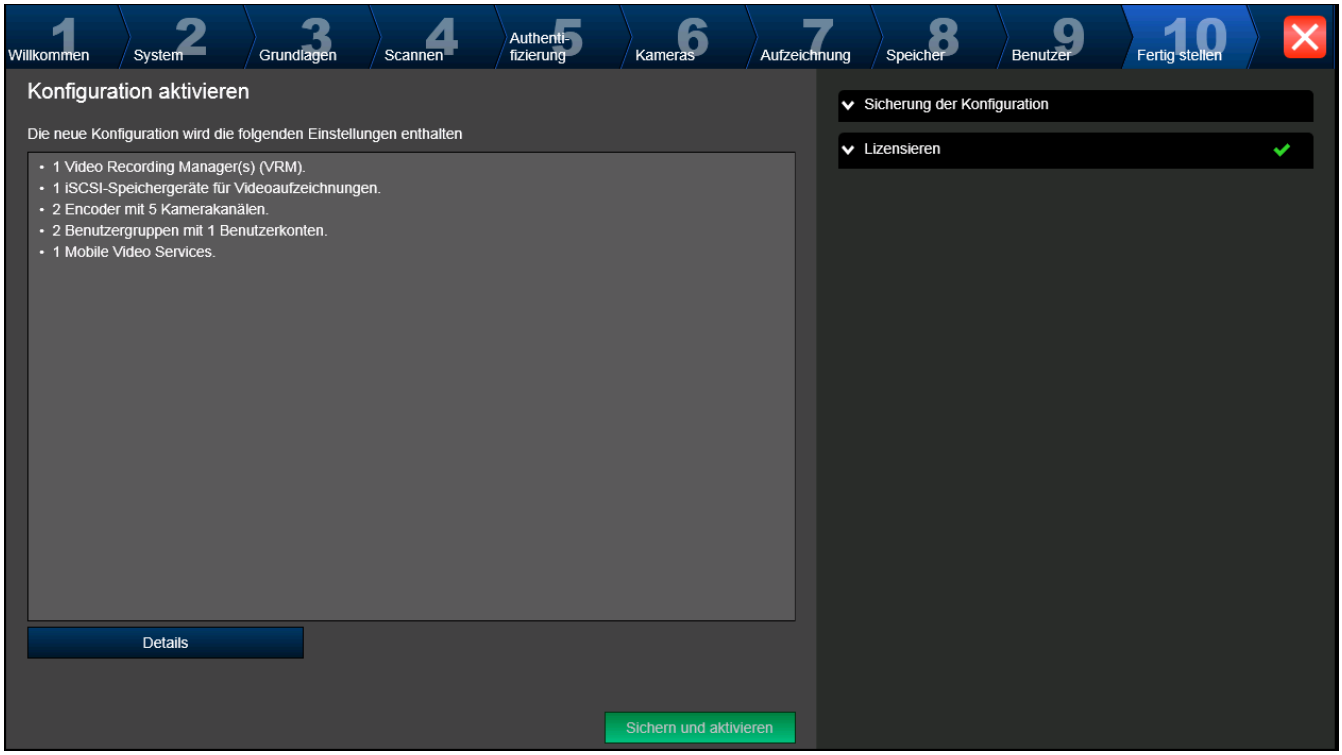
Es gelten die folgenden Regeln:

- – 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**.

6.3 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 **Die Passwortsrichtlinie wird missachtet** angezeigt und er wird dazu aufgefordert, 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 358*
- *Konfigurieren der Admin-Gruppe, Seite 363*

6.4 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.

6.5 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.

6.6 Nach Geräten suchen

Hauptfenster > **Geräte**

Sie können nach 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
- VIDOS-NVRs

Wenn Sie Geräte per Suchvorgang hinzufügen möchten, finden Sie im Kapitel *Seite Geräte, Seite 119* beim entsprechenden Gerätethema weiterführende Informationen.

Siehe

- *Hinzufügen eines VRM-Geräts per Suchvorgang, Seite 174*
- *Hinzufügen eines Nur-Live-ONVIF-Geräts per Suchvorgang, Seite 239*
- *Hinzufügen von Nur-Live-Geräten per Suchvorgang, Seite 214*
- *Hinzufügen eines Geräts, Seite 120*

6.7 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

6.8 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.

6.9 Konfiguration des Fernzugriffs

Sie können Fernzugriff entweder für ein einzelnes System ohne Enterprise System oder für ein Enterprise System konfigurieren.

6.9.1 Fernzugriff

Hinweis!
Um einen unbefugten Zugriff auf Videodaten über das Internet zu verhindern, empfehlen wir Ihnen ausdrücklich, alle Benutzer und Geräte in dem System mit einem geeigneten Passwort zu schützen.
Schützen Sie alle Bereiche der Kamera/des in Encoders (service/user/live) mit einem Passwort.

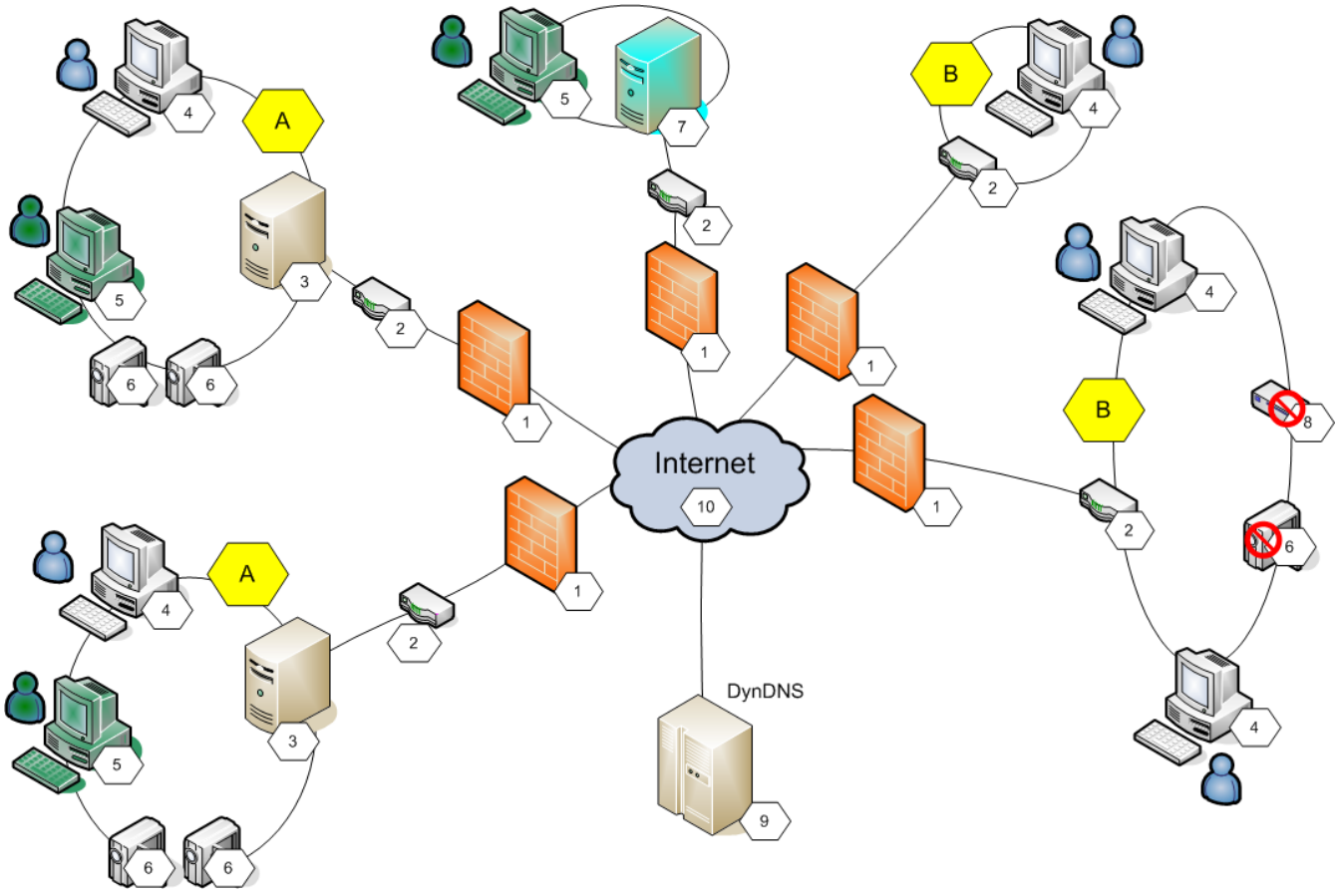
Verwandte Themen zur Änderung von Passwörtern

– *Seite Benutzereigenschaften, Seite 337*
– Passwort für einen Encoder/Decoder ändern
– *Passwort für ein VRM-Gerät ändern, Seite 180*

Ziel des Fernzugriffs bei BVMS ist die Verbindung verschiedener privater Netzwerke mit öffentlichen Netzwerken.
Es kann gleichzeitig oder nacheinander auf mehrere Netzwerke mit privaten (lokalen) Netzwerkadressen durch Operator Client-Computer über öffentliche Schnittstellen (Router) zugegriffen werden. Aufgabe des Routers ist die Übersetzung des eingehenden öffentlichen Netzwerkverkehrs in die entsprechende private Netzwerkadresse.
Die Benutzer von Operator Client können per Fernzugriff auf den Management Server oder Enterprise Management Server und ihre Geräte zugreifen.
Für folgende Geräte/Funktionen ist ein Fernzugriff nicht möglich:

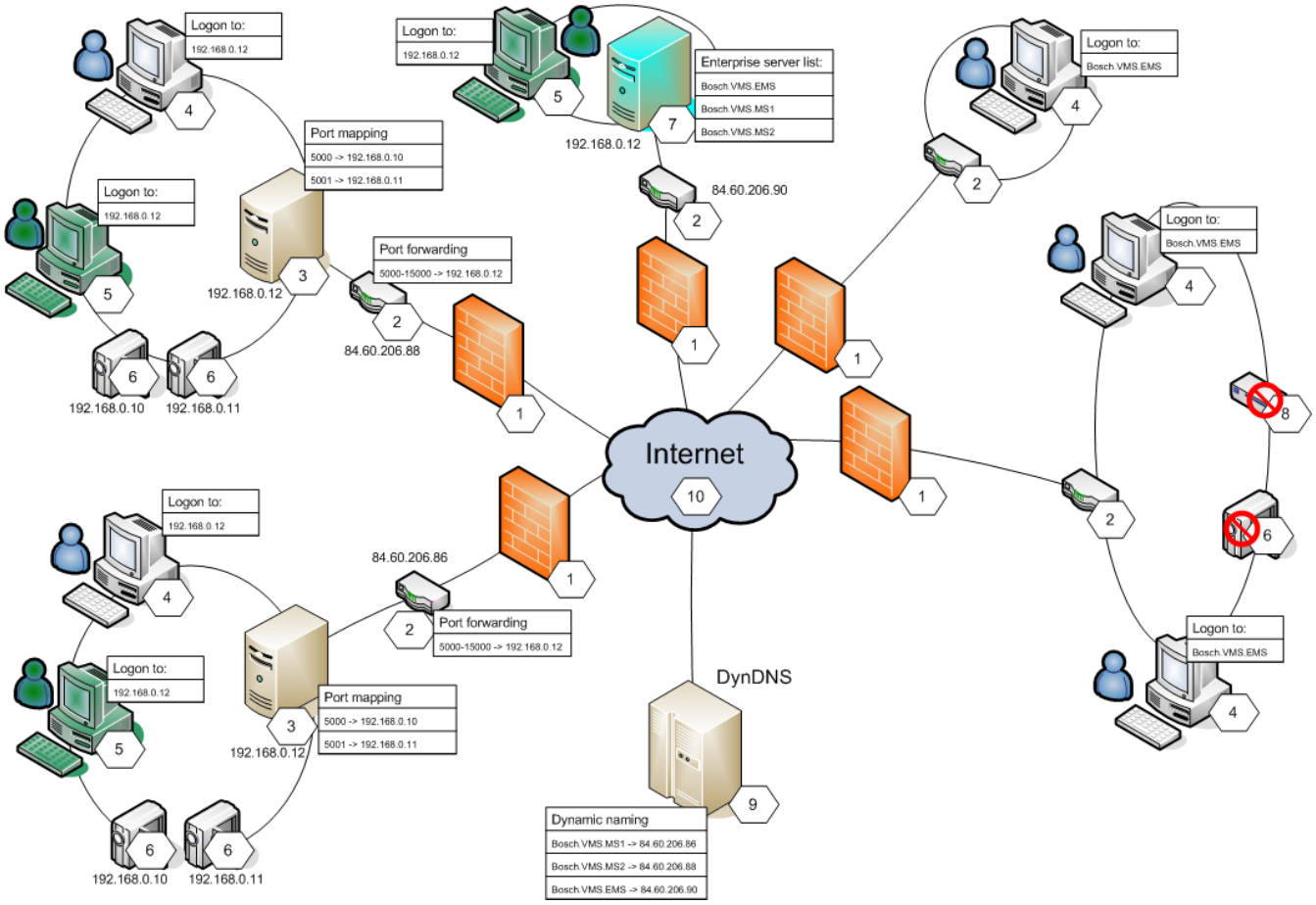
- Wiedergabe lokaler Speichermedien
- ONVIF
- DiBos
- Direkte iSCSI-Wiedergabe

Die folgende Abbildung zeigt ein Beispiel für Fernzugriff auf BVMS Geräte in einem einzigen System:



1	Firewall	**6**	IP-Kamera/Encoder
2	Router	**7**	Enterprise Management Server
3	Management Server	**8**	Decoder
4	Operator Client	**9**	DynDNS Server
5	Configuration Client	**10**	Internet
A	Remote-Netzwerk	**B**	Lokales Netzwerk

Die folgende Abbildung zeigt ein Beispiel für den Fernzugriff von einem privaten Netzwerk mit Enterprise System auf ortsferne BVMS Systeme:



1	Firewall	**6**	IP-Kamera/Encoder
2	Router Port-Weiterleitung	**7**	Enterprise Management Server Enterprise Server-Liste
3	Management Server Port Mapping	**8**	Decoder
4	Operator Client Anmelden bei	**9**	DynDNS Server Dynamische Benennung
5	Configuration Client Anmelden bei	**10**	Internet

Zum Aktivieren des Fernzugriffs eines Operator Client auf Geräte in einem Remote-Netzwerk, wird jedem Gerät neben der öffentlichen Netzwerkadresse des Routers eine öffentliche Port-Nummer zugeordnet. Für den Zugriff nutzt der Operator Client diese öffentliche Port-Nummer zusammen mit der öffentlichen Netzwerkadresse. Im privaten Netzwerk wird der eingehende Verkehr für die öffentliche Port-Nummer an die private Netzwerkadresse und Port-Nummer des entsprechenden Geräts weitergeleitet.
Sie können das Port Mapping im Configuration Client zur Verwendung durch den Operator Client konfigurieren.

Hinweis!
Darüber hinaus muss der Netzwerkadministrator die Port-Weiterleitung am Router des privaten Netzwerks konfigurieren. Der Netzwerkadministrator muss sicherstellen, dass der Fernzugriff über diese Schnittstellen außerhalb der BVMS Umgebung erfolgt.

Siehe
- *Dialogfeld „Fernzugriffseinstellungen“ (Menü „Einstellungen“), Seite 117*
- *Dialogfeld „Port Mapping-Tabelle“, Seite 118*

6.9.2 Ohne Enterprise System konfigurieren

So führen Sie die Konfiguration durch:
1. Konfigurieren Sie die Fernzugriffseinstellungen im Dialogfeld **Einstellungen für Fernzugriff**.
2. Konfigurieren des Routers

Verwandte Themen
- *Dialogfeld „Fernzugriffseinstellungen“ (Menü „Einstellungen“), Seite 117*

6.9.3 Mit Enterprise System konfigurieren

So führen Sie die Konfiguration durch:
1. Konfigurieren Sie die Serverliste.
2. Konfigurieren Sie Enterprise User Groups und Enterprise Accounts.
3. Konfigurieren Sie die Fernzugriffseinstellungen im Dialogfeld **Einstellungen für Fernzugriff**.
4. Konfigurieren des Routers

Verwandte Themen
- *Konfigurieren der Serverliste für Enterprise System, Seite 86*
- *Erstellen einer Gruppe oder eines Kontos, Seite 359*
- *Dialogfeld „Fernzugriffseinstellungen“ (Menü „Einstellungen“), Seite 117*

6.10 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.

Voraussetzungen
- die Berechtigungsnummer, die Sie von Bosch erhalten haben
- Computer mit Internetzugang
- Konto für den Bosch Security Systems Software License Manager

Vorgehensweise
Gehen Sie wie folgt vor, um die Softwarelizenzen zu aktivieren:
1. *Abrufen der Computersignatur, Seite 76*
2. *Abrufen des Aktivierungsschlüssels, Seite 77*
3. *Aktivieren des Systems, Seite 77*

Siehe
- *Dialogfeld „Lizenz-Manager“ (Menü „Werkzeuge“), Seite 111*

6.10.1 Herunterladen der Bundle-Informationsdatei

Wenn Sie BVMS Softwarepakete, Erweiterungen und optionale Funktionen bestellen, erhalten Sie von Bosch eine Berechtigungsnummer und in der Regel auch eine XML-Bundle-Datei, die alle Lizenzen für die Pakete, Erweiterungen und Optionen enthält, die sie bestellt haben.
Mit einer Bundle-Informationsdatei können Sie die Aktivierung der Softwarelizenzen vereinfachen.
Wenn Sie keine Bundle-Informationsdatei von Bosch erhalten haben, können Sie diese über den Bosch Security Systems Software License Manager herunterladen.

So laden Sie die Bundle-Informationsdatei herunter:

1. Geben Sie auf einem Computer mit Internetzugang folgende URL im Browser ein: https://activation.boschsecurity.com.
2. Melden Sie sich beim Bosch Security Systems Software License Manager an.
   Wenn Sie noch nicht über ein Konto verfügen, erstellen Sie ein neues Konto.
3. Klicken Sie auf Download Bundle File.
   Das Dialogfeld Download Original Bundle File wird angezeigt.
4. Geben Sie im Feld Authorization Number die Berechtigungsnummer ein, die Sie von Bosch erhalten haben, und klicken Sie auf Submit.
5. Speichern Sie die Bundle-Informationsdatei.

6.10.2 Abrufen der Computersignatur

So rufen Sie Ihre Computersignatur ab:

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 die Kontrollkästchen des Softwarepakets, der Funktionen und der Erweiterungen, die Sie aktivieren möchten. Geben Sie für die Erweiterungen die Anzahl der Lizenzen ein.
   oder
   Wenn Sie eine Bundle-Informationsdatei von Bosch erhalten haben, klicken Sie zum Importieren der Datei auf **Bundle Info importieren**.
   Wenn Sie keine Bundle-Informationsdatei erhalten haben, laden Sie diese über den Bosch Security Systems Software License Manager herunter (siehe *Herunterladen der Bundle-Informationsdatei, Seite 76*).
4. Klicken Sie auf **Aktivieren**.
   Das Dialogfeld **Lizenz Aktivierung** wird angezeigt.
5. Kopieren Sie die Computersignatur und fügen Sie sie in eine Textdatei ein.

Hinweis!
Die Computersignatur kann sich nach einem Austausch von Hardware-Komponenten auf dem Management Server-Computer ändern. Bei einer geänderten Computersignatur werden die Lizenzen des Basispakets ungültig.
Zur Vermeidung von Lizenzierungsproblemen schließen Sie zuerst die Hardware- und Software-Konfiguration ab, bevor Sie die Computersignatur generieren.
Folgende Hardware-Änderungen können die Basislizenz ungültig machen:
Austauschen der Netzwerkschnittstellenkarte
Hinzufügen einer virtuellen VMWare- oder VPN-Netzwerkschnittstelle
Hinzufügen oder Aktivieren einer WLAN-Netzwerkschnittstelle

6.10.3 Abrufen des Aktivierungsschlüssels

So rufen Sie einen Aktivierungsschlüssel **ab:**

1. Geben Sie auf einem Computer mit Internetzugang folgende URL im Browser ein: https://activation.boschsecurity.com.
2. Melden Sie sich beim Bosch Security Systems Software License Manager an. Wenn Sie noch nicht über ein Konto verfügen, erstellen Sie ein neues Konto.
3. Klicken Sie auf License Activation. Das Dialogfeld License Activation wird angezeigt.
4. Geben Sie im Feld Authorization Number die Berechtigungsnummer ein, die Sie von Bosch erhalten haben, und klicken Sie auf . Das Dialogfeld License Activation wird angezeigt.
5. Füllen Sie im Dialogfeld License Activation die folgenden Felder aus:
   - Computer Signature : Kopieren Sie die Computersignatur aus der Textdatei, in der Sie diese zuvor gespeichert haben, und fügen Sie sie hier ein.
   - Installation Site: Geben Sie hier die Informationen zum Installationsstandort an.
   - Comment: Geben Sie ggf. einen Kommentar ein (optional).
6. Klicken Sie auf Submit. Das Dialogfeld License Activation wird angezeigt. Es enthält eine Zusammenfassung Ihrer Lizenzaktivierung und den Lizenzaktivierungsschlüssel.
7. Kopieren Sie den Aktivierungsschlüssel und fügen Sie ihn in eine Textdatei ein oder schicken Sie ihn per E-Mail an die gewünschte E-Mail-Adresse.

6.10.4 Aktivieren des Systems

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 die Kontrollkästchen des Softwarepakets, der Funktionen und der Erweiterungen, die Sie aktivieren möchten. Geben Sie für die Erweiterungen die Anzahl der Lizenzen ein.
   oder
   Wenn Sie eine Bundle-Informationsdatei von Bosch erhalten haben, klicken Sie zum Importieren der Datei auf **Bundle Info importieren**.
   Wenn Sie keine Bundle-Informationsdatei erhalten haben, laden Sie diese über den Bosch Security Systems Software License Manager herunter (siehe *Herunterladen der Bundle-Informationsdatei, Seite 76*).
4. Klicken Sie auf **Aktivieren**. Das Dialogfeld **Lizenz Aktivierung** wird angezeigt.
5. Kopieren Sie den Lizenzaktivierungsschlüssel aus der Textdatei, in der Sie diesen zuvor gespeichert haben, und fügen Sie ihn im Feld **Lizenz-Aktivierungsschlüssel:** ein.
6. Klicken Sie auf **Aktivieren**. Die entsprechenden Softwarepakete werden aktiviert.
7. Klicken Sie auf **Schließen**, um das Dialogfeld **Lizenz-Manager** zu schließen.

6.11 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 78*.

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 78*.
– Speichern Sie die VRM-Konfigurationsdatei (config.xml).
  – Informationen zum Verfahren finden Sie unter *So speichern Sie die VRM-Konfiguration:, Seite 79*.

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:\Program Files (x86)\Bosch\Video Recording Manager\primary\VRM Server
  Bei einem Sekundären VRM finden Sie diese Datei in folgendem Verzeichnis:
  C:\Program Files (x86)\Bosch\Video Recording Manager\secondary\VRM Server

6.12 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 77*

6.12.1 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*.

6.12.2 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 > > > **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 und VRM zugewiesen wird.
Anderenfalls ist keine Authentifizierung beim iSCSI und keine direkte Wiedergabe vom iSCSI-Gerät möglich.

Verwandte Themen

– *Systemweites CHAP-Passwort , Seite 177*
– *Globales iSCSI-Verbindungs-Passwort (CHAP Passwort): , Seite 116*

6.12.3 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- oder NVR-Scan nicht, um nach Geräten mit Standardeinstellungen 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! Wenn Sie das Gerät von einem NVR löschen, gehen die Aufzeichnungen verloren.
– 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 > Rechtsklick auf > Klick auf **Decoder bearbeiten** > Dialogfeld **Decoder bearbeiten**

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.

6.12.4 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.

6.12.5 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.

6.12.6 Wiederherstellen von Divar IP 3000/7000

Weitere Informationen finden Sie in den Installationshandbüchern zum DIVAR IP 3000 bzw. DIVAR IP 7000. Im Kapitel zur Wiederherstellung des Geräts finden Sie entsprechende Informationen zur Vorgehensweise.

6.13 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.

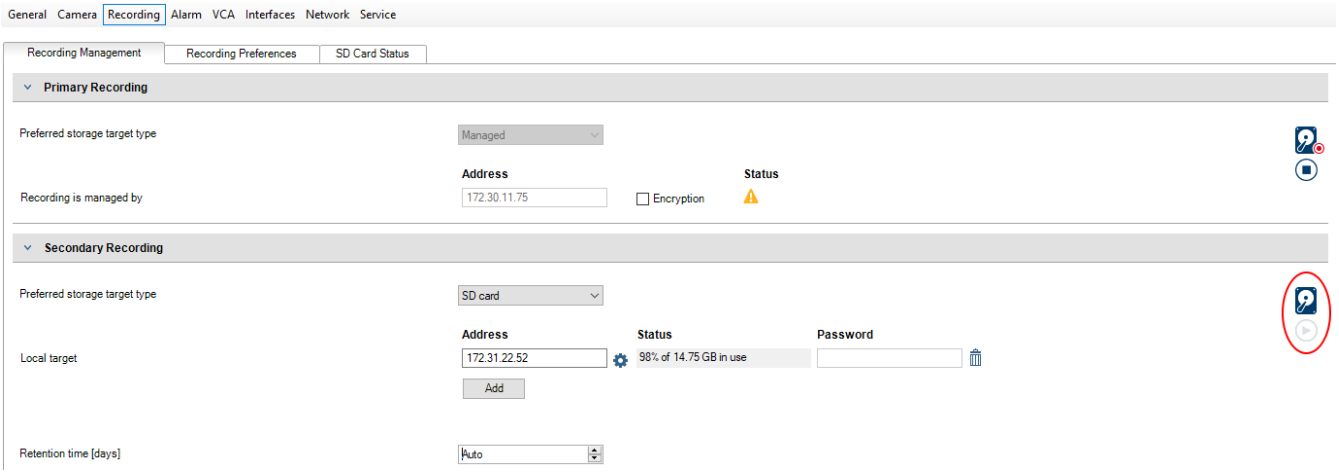
6.14 Speichermedien eines Encoders konfigurieren

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 236*
- *ANR-Funktion konfigurieren, Seite 306*

7 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 86*
2. *Erstellen einer Enterprise User Group, Seite 87*
3. *Erstellen eines Enterprise Accounts, Seite 88*

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

Siehe

– *Enterprise System, Seite 21*

7.1 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. Falls erforderlich, geben Sie eine öffentliche Netzwerkadresse (DNS-Name oder IP-Adresse) für den Fernzugriff ein.
4. Klicken Sie auf **OK**.

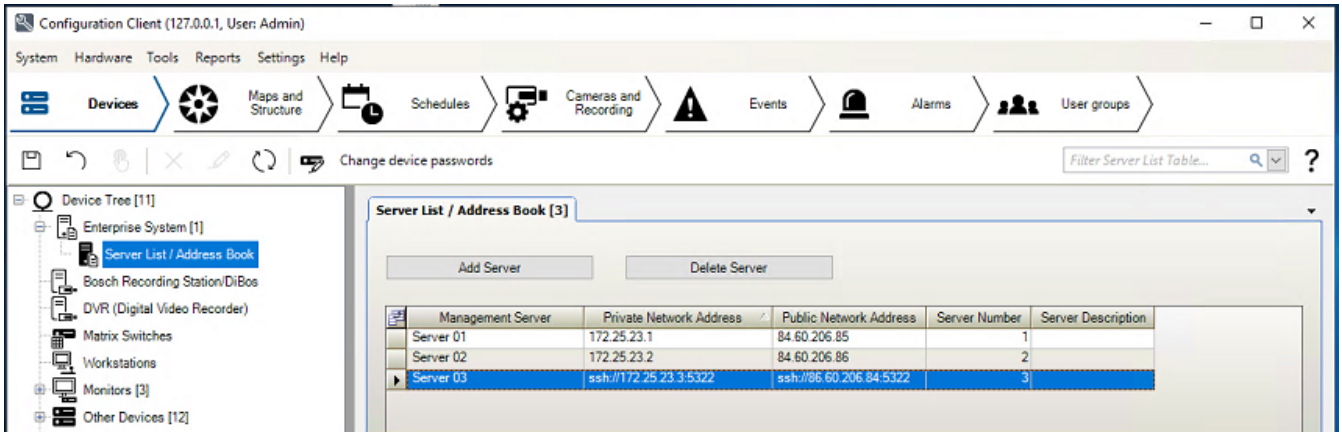
5. Wiederholen Sie diese Schritte, bis alle gewünschten Management Server-Computer hinzugefügt wurden.

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.
Der nachfolgende Screenshot zeigt ein Beispiel:



Siehe

- *Enterprise System, Seite 21*
- *Seite „Server-Liste/Adressbuch“, Seite 123*
- *Seite Benutzergruppen, Seite 334*
- *Mittels Server Lookup, Seite 71*

7.2 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 336*
- *Seite „Bedienerfunktionen“, Seite 345*
- *Seite Prioritäten, Seite 348*
- *Seite Benutzeroberfläche, Seite 349*
- *Seite „Server-Zugriff“, Seite 350*

7.3 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 das Passwort entsprechend der Passwortrichtlinie ein und bestätigen Sie es.
5. Klicken Sie auf **OK**.
   Ein neuer Enterprise Account wird dem 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 358*
- *Seite „Zugangsberechtigungen“, Seite 344*
- *Seite Logischer Baum, Seite 344*
- *Seite Ereignisse und Alarme, Seite 342*
- *Seite „Prioritäten für Steuerungen“, Seite 340*
- *Seite Kamerafreigaben, Seite 339*
- *Seite Decoder-Freigaben, Seite 341*

8 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.

8.1 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 311*

8.2 Konfigurieren eines automatisch startenden Kommandoskripts

Hauptfenster > **Alarme** > oder > Spalte **Alarmoptionen** > ...

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 317*
– *Konfigurieren eines Start-Kommandoskripts (Seite „Einstellungen“), Seite 92*

8.3 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 311*

8.4 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 311*

8.5 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 90*.

So konfigurieren Sie ein Start-Skript:

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

Siehe

– *Seite Arbeitsstation, Seite 135*

9 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.

9.1 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 106*
- *Dialogfeld „Konfiguration aktivieren“ (Menü „System“), Seite 105*

9.2 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 105*
- *Dialogfeld „Aktivierungs-Manager“ (Menü „System“), Seite 104*

9.3 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 95*

9.4 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 95*

9.5 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 OPC-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.

9.6 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 111*

9.7 SNMP-Überwachung konfigurieren

Hauptfenster

So führen Sie die Konfiguration durch:
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 114*

9.8 Erzeugen einer Auswertung

Hauptfenster

Sie können Auswertungen erzeugen, in denen Informationen zur aktuellen Konfiguration zusammengefasst werden.

So erzeugen Sie eine Auswertung:

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.

Siehe

- *Dialogfeld „Aufzeichnungszeitpläne“, Seite 112*
- *Dialogfeld „Aktionszeitpläne“, Seite 112*
- *Dialogfeld „Kameras und Aufzeichnungsparameter”, Seite 112*
- *Dialogfeld „Stream-Qualität", Seite 112*
- *Dialogfeld „Ereignis-Einstellungen”, Seite 113*
- *Dialogfeld „Einstellungen für zusammengesetztes Ereignis”, Seite 113*
- *Dialogfeld „Alarmeinstellungen“, Seite 113*
- *Dialogfeld „Konfigurierte Benutzer”, Seite 113*
- *Das Dialogfeld „Benutzergruppen und Konten”, Seite 113*
- *Dialogfeld „Bedienberechtigungen“, Seite 113*

10 Konfigurationsbeispiele

Dieses Kapitel enthält Beispiele zur Konfiguration ausgewählter Geräte im BVMS.

10.1 Hinzufügen einer Bosch ATM/POS-Bridge

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

Konfigurieren der 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 der 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 der ATM/POS-Bridge zum 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** wird angezeigt.
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.

10.2 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.

10.3 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 die Registerkarte für einen Zeitplan, beispielsweise .
2. Klicken Sie in der Spalte auf eine Zelle, und wählen Sie die Streamqualität aus.
3. Wählen Sie unter **Dauer- oder Voralarmaufzeichnung** in der Spalte **Auswählen** den gewünschten Aufzeichnungsmodus aus.
   Bei der Auswahl **Voralarm**: Klicken Sie in der Spalte **Dauer** auf eine Zelle, um die Dauer der Alarmaufzeichnung vor dem Alarm in Sekunden auszuwählen.
4. Klicken Sie unter **Alarmaufzeichnung** in der Spalte **Dauer** auf eine Zelle, und geben Sie die gewünschte Aufzeichnungszeit ein.
5. Wiederholen Sie diese Schritte, um die Aufzeichnungseinstellungen für die andere Kamera zu konfigurieren.

So aktivieren Sie die Forensische Suche auf einer Arbeitsstation:

Hauptfenster > **Geräte** > erweitern

1. Klicken Sie auf das Symbol Ihrer Arbeitsstation.
2. Klicken Sie auf die Registerkarte **Einstellungen**.
3. Aktivieren Sie das Kontrollkästchen **Forensic Search aktivieren**.

11 Allgemeine Fenster des Configuration Client

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

11.1 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.
	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.

11.2 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.

Befehle des Menüs Hardware

Initialer Geräte-Scan...	Zeigt das Dialogfeld **Initialer Geräte-Scan** an.
Geräte mit Standardpasswort schützen...	Zeigt das Dialogfeld **Geräte mit globalem Standardpasswort 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.

Befehle des Menüs Werkzeuge

Kommandoskript-Editor...	Zeigt das Dialogfeld **Kommandoskript-Editor** an.
Ressourcen-Manager...	Zeigt das Dialogfeld **Ressourcen-Manager** an.
Kamerasequenzen...	Zeigt das Dialogfeld **Kamerasequenzen** an.
Ressourcen-Konvertierer	Zeigt das Dialogfeld **Ressourcen-Konvertierer** an, wenn Kartenressourcen verfügbar sind.
RRAS-Konfiguration...	Zeigt das Dialogfeld **RRAS-Konfiguration** an.
Lizenz-Manager...	Zeigt das Dialogfeld **Lizenz-Manager** an.
Lizenz Inspektor...	Zeigt das Dialogfeld **Lizenz-Inspektor** an.

Befehle des Menüs Auswertungen

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.
Umgangene Geräte...	Zeigt das Auswertungs-Dialogfeld **Umgangene Geräte** an.

Befehle des Menüs Einstellungen

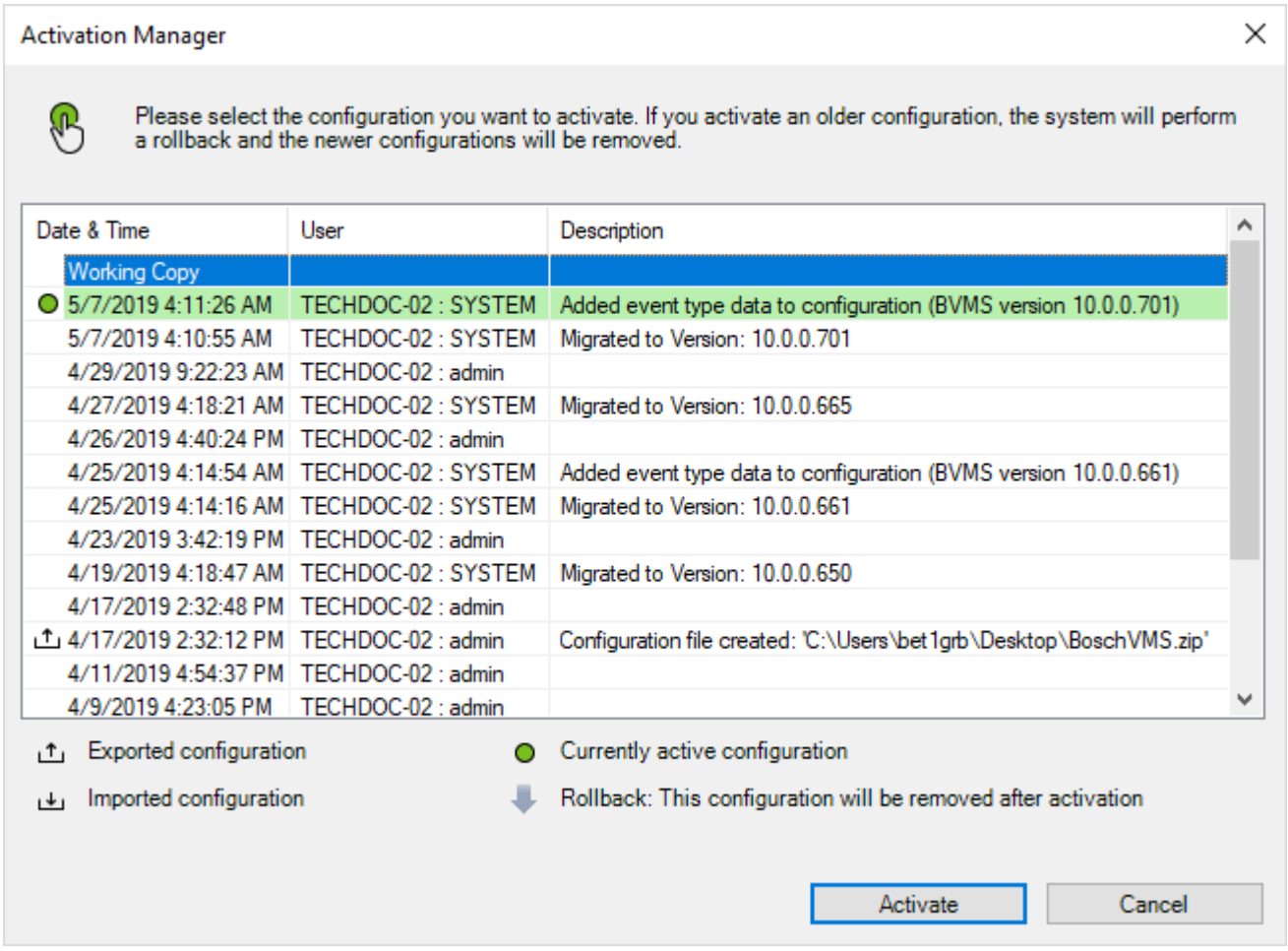
Alarmeinstellungen...	Zeigt das Dialogfeld **Alarmeinstellungen** an.
SNMP-Einstellungen...	Zeigt das Dialogfeld **SNMP-Einstellungen** an.
Aufzeichnungsqualitäten einstellen	Zeigt das Dialogfeld **Stream-Qualitätseinstellungen** an.
Optionen...	Zeigt das Dialogfeld **Optionen** an.
Einstellungen für Fernzugriff...	Zeigt das Dialogfeld **Einstellungen für Fernzugriff** an.

Befehle des Menüs Hilfe

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

11.3 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 93*
- *Aktivieren einer Konfiguration, Seite 94*

11.4 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.

Vor Aktivierung RRAS konfigurieren
Nur verfügbar, wenn Sie die Option **Port Mapping aktivieren** im Dialogfeld **Einstellungen für Fernzugriff** aktiviert haben.
Wenn dieses Kontrollkästchen aktiviert ist, wird das Dialogfeld **RRAS-Konfiguration** angezeigt, bevor die Aktivierung durchgeführt wird.

Siehe
– *Aktivieren der letzten Konfiguration, Seite 93*

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

Hauptfenster > Menü **Hardware** > Befehl **Initialer Geräte-Scan...**
Zeigt die Geräte mit gleichen IP-Adressen oder der Standard-IP-Adresse (192.168.0.1) an. Dient zum Ändern dieser IP-Adressen und Subnetzmasken.
Sie müssen zuerst die richtige Subnetzmaske angeben, bevor Sie eine IP-Adresse ändern.

11.6 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 Fähigkeiten 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 93*

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

Hauptfenster > **Geräte** > **Gerätepasswörter ändern** > Dialogfeld **Gerätepasswörter ändern**
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.

Geben Sie eine Zeichenfolge ein, und drücken Sie zum Filtern der angezeigten Element die Taste ENTER. 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. Ein aktiver Filter wird durch gekennzeichnet. 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.

Um die Filterung abzubrechen, klicken Sie auf .
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 234*.

11.8 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.

Geben Sie eine Zeichenfolge ein, und drücken Sie zum Filtern der angezeigten Element die Taste ENTER. 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. Ein aktiver Filter wird durch gekennzeichnet. 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.

Um die Filterung abzubrechen, klicken Sie auf .

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 234*.

11.9 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.

Geben Sie eine Zeichenfolge ein, und drücken Sie zum Filtern der angezeigten Element die Taste ENTER. 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. Ein aktiver Filter wird durch gekennzeichnet. 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.

Um die Filterung abzubrechen, klicken Sie auf .

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 234*.

11.10 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 96*

11.11 Dialogfeld „License Investigator“ (Menü „Werkzeuge“)

Hauptfenster > Menü **Werkzeuge** > Befehl **Lizenz Inspektor...** > Dialogfeld **Lizenz-Inspektor**
Sie können überprüfen, ob die Anzahl der installierten BVMS-Lizenzen die Anzahl der erworbenen Lizenzen übersteigt.

11.12 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.

Basispakete
Zeigt die verfügbaren Basispakete an.

Typnummer
Zeigt die Typennummer (CTN-Nummer) des ausgewählten Pakets bzw. der ausgewählten Funktion oder Erweiterung an.

Status
Zeigt den Lizenzstatus an, sofern zutreffend.

Optionale Features
Zeigt die verfügbaren Funktionen an.

Erweiterung
Zeigt die verfügbaren Erweiterungen und deren Anzahl an. Um die Anzahl zu ändern, zeigen Sie mit dem Mauszeiger rechts neben ein Kontrollkästchen, und klicken Sie auf den Aufwärts- oder Abwärtspfeil.

Aktivieren
Klicken Sie hier, um das Dialogfeld **Lizenz Aktivierung** anzuzeigen.

Bundle Info importieren
Klicken Sie hierauf, um eine XML-Datei zu importieren, die die von Bosch erhaltenen Bundle-Informationen enthält.

Neues Paket hinzufügen
Klicken Sie darauf, um ein Dialogfeld zum Auswählen einer neuen Lizenzdatei anzuzeigen.

Siehe
– *Aktivieren der Softwarelizenzen, Seite 75*

11.13 Dialogfelder „Auswertungen“ (Menü „Auswertungen“)

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

Siehe
– *Erzeugen einer Auswertung, Seite 97*

11.13.1 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.

11.13.2 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.

11.13.3 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.

11.13.4 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.

11.13.5 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.

11.13.6 Dialogfeld „Ereignis-Einstellungen”

Hauptfenster > Menü **Auswertungen** > Befehl **Ereigniseinstellungen...**

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.

11.13.7 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.

11.13.8 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.

11.13.9 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.

11.13.10 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.

11.13.11 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.

11.13.12 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.

11.13.13 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.

11.13.14 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.

11.13.15 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.

11.13.16 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.

11.14 Dialogfeld „Alarmeinstellungen“ (Menü „Einstellungen“)

Siehe *Dialogfeld „Alarmeinstellungen“, Seite 315* .

11.15 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*.

Systemkontact
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 96*

11.16 Dialogfeld „Optionen“ (Menü „Einstellungen“)

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

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.

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

Einstellungen für Monitorgruppen (MG)
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.
Diese Einstellung wird nach der Aktivierung der Konfiguration aktiviert.

Decoder benutzen einen beliebigen Stream, wenn sie sich mit der Kamera verbinden
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.

Logbuch-Konfiguration
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.

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.

Erweiterte Statusanzeige
Hotspot-Färbung in Karten deaktivieren
Dient zum Deaktivieren der blinkenden Hotspots in Karten.
Erweiterte Statusanzeige aktivieren (Hotspot auf Karten abhängig vom Status einfärben)
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 Alarm-Anzeige aktivieren (Hotspot-Färbung in Karten je nach 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.

Automatische Abmeldung

Automatische Abmeldung von Configuration Client nach dieser Zeit der Inaktivität erzwingen:
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.
Diese Einstellung wird nach der Aktivierung der Konfiguration aktiviert.

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.

Globales iSCSI-Verbindungs-Passwort (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.

Hinweis: Das iSCSI-CHAP-Passwort und das systemweite CHAP-Passwort müssen übereinstimmen.
Siehe *Systemweites CHAP-Passwort , Seite 177*

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

Siehe
– *Systemweites CHAP-Passwort , Seite 177*

11.17 Dialogfeld „Fernzugriffseinstellungen“ (Menü „Einstellungen“)

Hauptfenster > Menü **Einstellungen** > Befehl **Einstellungen für Fernzugriff...**
Dient zum Konfigurieren des Port Mapping für den Fernzugriff.
Fügen Sie einen oder mehrere Port-Bereiche hinzu. BVMS weist automatisch jeder privaten IP-Adresse eines konfigurierten Geräts eine andere öffentliche Port-Nummer aus diesem Bereich zu.
Für den Router, der das private Netzwerk mit dem öffentlichen Netzwerk verbindet, konfigurieren Sie dasselbe Port Mapping. Der Router leitet dann jedes Paket mit öffentlicher Port-Nummer aus dem öffentlichen Netz an die private IP-Adresse und Port-Nummer weiter. Private IP-Adresse und Port-Nummer wurden in der Port Mapping-Tabelle für diese öffentliche Port-Nummer konfiguriert.

Hinweis!
Zusätzlich müssen Sie im Router die Port-Weiterleitung entsprechend den Einstellungen in der Port Mapping-Tabelle manuell konfigurieren.

Port Mapping aktivieren
Klicken Sie hier, um Port Mapping zu aktivieren/deaktivieren.

Hinzufügen
Klicken Sie hier, um einen neuen Port-Bereich zur **Portbereiche**-Liste hinzuzufügen.

Bearbeiten
Klicken Sie hier, um einen ausgewählten Eintrag in der **Portbereiche**-Liste zu ändern.

Entfernen
Klicken Sie hier, um einen ausgewählten Eintrag in der **Portbereiche**-Liste zu löschen.

Private IP-Adresse (für Zugriff innerhalb eines LAN)
Wählen Sie die private IP-Adresse des lokalen Netzwerkadapters Ihres Management Server.

Öffentliche Netzwerkadresse (IP-Adresse oder DNS-Name, zum Zugriff von außerhalb, z.B. via Internet)
Geben Sie die öffentliche Netzwerkadresse dieses privaten Netzwerks an. Die Remote Operator Client meldet sich mit dieser öffentlichen Netzwerkadresse an, um Zugriff auf die Geräte dieses Management Server zu erlangen.

Port Mapping zeigen...
Klicken Sie hier, um das Dialogfeld **Port Mapping Tabelle** anzuzeigen.

Siehe
– *Fernzugriff, Seite 72*

11.17.1 Dialogfeld „Port Mapping-Tabelle“

Hauptfenster > Menü **Einstellungen** > Befehl **Einstellungen für Fernzugriff...** > Schaltfläche **Port Mapping zeigen...** > Dialogfeld **Port Mapping Tabelle**

Zeigt das Port Mapping für die IP-Adressen der konfigurierten Geräte in Ihrem BVMS an.
Sie können die Tabelle in die Zwischenablage kopieren und Einträge, die nicht durch das BVMS verwaltet werden, hinzufügen.

In die Zwischenablage kopieren

Klicken Sie hier, um die Port Mapping-Tabelle in die Zwischenablage zu kopieren. Dies hilft Ihnen bei der Erstellung eines Konfigurations-Skripts für das Port Mapping in einem Router (zum Beispiel einem RRAS-Service).

Protokoll

Zeigt das verwendete Netzwerkprotokoll für dieses Gerät an.
Sie können den Wert manuell ändern.

Privater Port

Zeigt die private Port-Nummer im privaten Netzwerk für dieses Gerät an.
Sie können den Wert manuell ändern.

Öffentlicher Port

Zeigt die öffentliche Port-Nummer an, mit der Operator Client aus öffentlichen Netzwerken auf das Gerät zugreift.
Sie können den Wert manuell ändern.

Fixiert

Klicken Sie hier, um die manuell zugewiesene Port-Nummer zu prüfen und zu ändern.
Klicken Sie hier, um die automatische Zuweisung einer Port-Nummer zu deaktivieren.

12 Seite Geräte

Hauptfenster > **Geräte**

Zeigt den Gerätebaum und die Konfigurationsseiten an.
Die Anzahl der einem Eintrag untergeordneten Elemente wird in eckigen Klammern angezeigt.
Dient zum Konfigurieren verfügbarer Geräte wie etwa Videodienste für Mobilgeräte, ONVIF-Encoder, Bosch Video Streaming Gateway-Geräte, Encoder, Decoder, VRMs, Encoder mit lokaler Archivierung, analoge Matrizen oder Peripheriegeräte wie ATM/POS-Brücken.

Hinweis:
Die Geräte werden in einem Baum dargestellt und nach physischer Netzwerkstruktur und Gerätekategorien gruppiert.
Videoquellen wie Encoder werden unter VRMs gruppiert. Digital-Videorekorder wie DiBos werden getrennt aufgeführt.

Geben Sie eine Zeichenfolge ein, und drücken Sie zum Filtern der angezeigten Element die Taste ENTER. 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. Ein aktiver Filter wird durch gekennzeichnet. 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.

Um die Filterung abzubrechen, klicken Sie auf .

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

12.1 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.

12.2 Ändern des Passworts für IP-Geräte

Hauptfenster > **Geräte** > **Gerätepasswörter ändern** > Dialogfeld **Gerätepasswörter ändern**
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 107*.

So ändern Sie die Einstellungen für mehrere Geräte:
Siehe *Konfigurieren mehrerer Encoder/Decoder, Seite 234*.

Siehe
– *Dialogfeld „Gerätepasswörter ändern“ (Menü „Hardware“), Seite 107*

12.3 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
- Bosch Recording Station/DiBos System
- 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 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
- VIDOS-NVRs

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 auf > Klick auf **Nach Encodern scannen** > Dialogfeld **BVMS Scan Wizard**

Hauptfenster > **Geräte** > erweitern > Rechtsklick auf > Klick auf **Nach Video Streaming Gateways scannen** > Dialogfeld **BVMS Scan Wizard**

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

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

Hauptfenster > **Geräte** > erweitern > erweitern > Rechtsklick auf > Klick auf **Nach Decodern scannen** > Dialogfeld **BVMS Scan Wizard**

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 auf > Klick auf **Nach VRM-Geräten scannen** > Dialogfeld BVMS Scan Wizard

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 174*
– *Hinzufügen eines Encoders zu einem VRM-Pool, Seite 223*
– *Hinzufügen eines Nur-Live-Encoders, Seite 223*
– *Hinzufügen eines Encoders mit lokaler Archivierung, Seite 223*
– *Nach Geräten suchen, Seite 71*

12.4 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.

Öffentliche Netzwerkadresse
Zeigt die öffentlichen Netzwerkadressen aller hinzugefügten Management Server-Computer an. Sie können jeden Eintrag ändern. Sie benötigen die öffentliche Netzwerkadresse für den Fernzugriff auf diesen Management Server-Computer.

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 86*
- *Konfigurieren von Server Lookup, Seite 125*
- *Export der Server-Liste, Seite 125*
- *Import einer Server-Liste, Seite 126*

Siehe
- *SSH-Tunneling, Seite 46*

12.4.1 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 öffentliche Netzwerkadresse oder den DNS-Namen für Routed Access ein.

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

12.4.2 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 22*
- *Seite „Server-Liste/Adressbuch“, Seite 123*
- *Mittels Server Lookup, Seite 71*

12.4.3 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. Falls erforderlich, geben Sie eine öffentliche Netzwerkadresse (DNS-Name oder IP-Adresse) für den Fernzugriff ein.
4. Klicken Sie auf **OK**.
5. 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 86*

12.4.4 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 22*
– Server-Liste
– *Seite „Server-Liste/Adressbuch“, Seite 123*

12.4.5 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 22*
– Server-Liste
– *Seite „Server-Liste/Adressbuch“, Seite 123*

12.5 Seite „NVRs“/„Failover-NVRs“/„Redundante NVRs“

Ab BVMS 5.0 werden NVRs, Failover-NVRs und redundante NVRs nicht mehr unterstützt.

12.6 Seite DiBos

Hauptfenster > **Geräte** > >

Zeigt die Eigenschaftsseiten eines ausgewählten DiBos Systems an.

Dient zum Integrieren eines DiBos Systems in das System.

Hinweis!

Das DiBos System selbst wird nicht konfiguriert. Es werden lediglich die Eigenschaften bezogen auf das BVMS festgelegt.

▸ Klicken Sie auf eine Registerkarte, um die entsprechende Eigenschaftsseite anzuzeigen.

Siehe

– *Konfigurieren der Integration eines DiBos Systems, Seite 128*

12.6.1 Hinzufügen eines DiBos Systems per Suchvorgang

Hauptfenster > **Geräte** > Rechtsklick auf > Befehl **BRS/DiBos System hinzufügen**

Dient zum Hinzufügen eines DiBos Systems zu Ihrem BVMS.

So fügen Sie ein DiBos System hinzu:

1. Klicken Sie mit der rechten Maustaste auf .
2. Klicken Sie auf **BRS/DiBos System hinzufügen**.
   Das Dialogfeld **BRS/DiBos System hinzufügen** wird angezeigt.
3. Geben Sie die erforderlichen Werte ein.
4. Klicken Sie auf **Scannen**.
   Das DiBos System wird dem System hinzugefügt.
5. Klicken Sie zur Bestätigung im angezeigten Meldungsfeld auf **OK**.

Dialogfeld „DiBos System hinzufügen“

Netzwerkadresse
Geben Sie den DNS-Namen oder die IP-Adresse des DiBos Systems ein.

Benutzername:
Geben Sie den Benutzernamen zum Anmelden beim DiBos System ein.

Passwort:
Geben Sie das Passwort zum Anmelden beim DiBos System ein.

12.6.2 Seite Einstellungen

Hauptfenster > **Geräte** > erweitern > > Registerkarte **Einstellungen**
Zeigt die Netzwerkeinstellungen des an Ihr System angeschlossenen DiBos Systems an. Dient zum Ändern der Einstellungen.

Siehe
– *Konfigurieren der Integration eines DiBos Systems, Seite 128*

12.6.3 Seite Kameras

Hauptfenster > **Geräte** > erweitern > > Registerkarte **Kameras**
Zeigt alle Kameras an, die im an Ihr System angeschlossenen DiBos System verfügbar sind. Dient zum Entfernen von Kameras.

Siehe
– *Konfigurieren der Integration eines DiBos Systems, Seite 128*

12.6.4 Seite Eingänge

Hauptfenster > **Geräte** > erweitern > > Registerkarte **Eingänge**
Zeigt alle Eingänge an, die im an Ihr System angeschlossenen DiBos System verfügbar sind. Dient zum Entfernen von Elementen.

Siehe
– *Konfigurieren der Integration eines DiBos Systems, Seite 128*

12.6.5 Seite Relais

Hauptfenster > **Geräte** > erweitern > > Registerkarte **Relais**

Zeigt alle Relais an, die im an Ihr System angeschlossenen DiBos System verfügbar sind.

Dient zum Entfernen von Elementen.

Siehe

– *Konfigurieren der Integration eines DiBos Systems, Seite 128*

12.6.6 Konfigurieren der Integration eines DiBos Systems

Hauptfenster > **Geräte** > erweitern >

Hinweis!

Das DiBos System selbst wird nicht konfiguriert, nur seine Integration in der BVMS.

So scannen Sie nach neuen DiBos-Geräten:

- Klicken Sie mit der rechten Maustaste auf , und klicken Sie dann auf **BRS/DiBos-System erneut scannen**.
  Das DiBos System wird nach neuen Geräten durchsucht, die daraufhin hinzugefügt werden.

So entfernen Sie ein Element:

1. Klicken Sie auf die Registerkarte **Kameras**, die Registerkarte **Relais** oder die Registerkarte **Eingänge**.
2. Klicken Sie mit der rechten Maustaste auf ein Element, und klicken Sie auf **Entfernen**.
   Das Element wird entfernt.

So benennen Sie ein DiBos-Gerät um:

1. Klicken Sie mit der rechten Maustaste auf ein DiBos Gerät, und klicken Sie auf **Umbenennen**.
2. Geben Sie einen neuen Namen für das Element ein.

12.7 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 129*
- *Konfigurieren der Integration eines DVR, Seite 131*

12.7.1 DVR-Geräte

Dieses Kapitel enthält Hintergrundinformationen über die DVR-Geräte, die in ein BVMS System integriert werden können.
Einige DVR-Modelle (z. B. DHR-700) 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 128*
- *Konfigurieren der Integration eines DVR, Seite 131*

12.7.2 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.

12.7.3 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 120*

12.7.4 Registerkarte „Einstellungen“

Hauptfenster > **Geräte** > > > Registerkarte **Einstellungen**
Zeigt die Netzwerkeinstellungen des an Ihr System angeschlossenen DVR an. Dient zum Ändern der Einstellungen.

12.7.5 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.

12.7.6 Registerkarte „Eingänge“

Hauptfenster > **Geräte** > > > Registerkarte **Eingänge**
Zeigt alle Eingänge des DVR an.
Dient zum Entfernen von Elementen.

12.7.7 Registerkarte „Relais“

Hauptfenster > **Geräte** > > > Registerkarte **Relais**
Zeigt alle Relais des DVR an. Dient zum Entfernen von Elementen.

12.7.8 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 120*
- *Seite DVR (Digital-Videorekorder), Seite 128*

12.8 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 132*
- *Verbinden einer Bosch Allegiant Kreuzschiene mit BVMS, Seite 54*

12.8.1 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.

12.8.2 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 50*
- *Seite Verbindung, Seite 134*
- *Seite Kameras, Seite 134*
- *Seite Ausgänge, Seite 133*
- *Seite Eingänge, Seite 134*

12.8.3 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 132*

12.8.4 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 132*

12.8.5 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 132*

12.8.6 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 132*

12.9 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
– Aktivieren der Forensischen Suche

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 135*
– *Konfigurieren eines Start-Kommandoskripts (Seite „Einstellungen“), Seite 136*

12.9.1 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.

12.9.2 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 135*

12.9.3 Aktivieren der Forensischen Suche auf einer Arbeitsstation (Seite „Einstellungen“)

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

Sie müssen die Forensic Search auf einer Arbeitsstation aktivieren.

Hinweis:

Aktivieren Sie auf jedem Encoder die Inhaltsanalyse. Verwenden Sie dazu im Gerätebaum die Seite VCA des jeweiligen Encoders.

So aktivieren Sie die Forensic Search:

- Aktivieren Sie das Kontrollkästchen **Forensic Search aktivieren**.

12.9.4 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 90*.

So konfigurieren Sie ein Start-Skript:

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

Siehe

– *Seite Arbeitsstation, Seite 135*

12.9.5 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.
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.

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.
Damit ein transcodierter Stream in BVMS verfügbar ist, muss entweder MVS installiert sein oder Ihr VRM-Computer einen integrierten Hardware-Transcoder besitzen.
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.

Forensic Search aktivieren
Klicken Sie darauf, um die Forensische Suche für diese Arbeitsstation zu aktivieren.

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.
Siehe *Globales iSCSI-Verbindungs-Passwort (CHAP Passwort): , Seite 116*

Live-Video von Video Streaming Gateway statt von der Kamera holen
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.

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 136*
- *Aktivieren der Forensischen Suche auf einer Arbeitsstation (Seite „Einstellungen“), Seite 136*
- *Globales iSCSI-Verbindungs-Passwort (CHAP Passwort): , Seite 116*

12.9.6 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.

12.10 Seite "Decoder"

Hauptfenster > **Geräte** > erweitern >

Dient zum Hinzufügen und Konfigurieren von Decodern.

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 71*
- *Seite „Bosch Encoder/Decoder/Kamera“, Seite 221*

12.10.1 Manuelles Hinzufügen eines Encoders/Decoders

Dient zum manuellen Hinzufügen eines Encoders oder Decoders. 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 oder -Decoder 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.
5. Klicken Sie auf **OK**.
   Das Gerät wird dem System hinzugefügt.
6. Wenn das Gerät ein erstes Passwort erfordert, wird angezeigt.
   Um ein erstes Passwort festzulegen, klicken Sie mit der rechten Maustaste auf das Gerätesymbol, und klicken Sie auf **Initialpasswort setzen...**.
   Das Dialogfeld **Passwort eingeben** wird angezeigt.
   Geben Sie ein Passwort für den service-Benutzer ein und klicken Sie auf **OK**.
   Das Symbol wird ausgeblendet und Sie können das Gerät verwenden.

Dialogfeld Encoder hinzufügen

Hauptfenster > **Geräte** > erweitern > erweitern > Rechtsklick auf > Klick auf **Encoder hinzufügen** > Dialogfeld **Encoder hinzufügen**
oder

Hauptfenster > **Geräte** > Rechtsklick auf > Klick auf **Encoder hinzufügen** > Dialogfeld **Encoder hinzufügen**
oder

Hauptfenster > **Geräte** > Rechtsklick auf > Klick auf **Encoder hinzufügen** > Dialogfeld **Encoder hinzufügen**
oder

Hauptfenster > **Geräte** > erweitern > Rechtsklick auf > Klick auf **Decoder hinzufügen** > Dialogfeld **Encoder hinzufügen**

IP-Adresse:
Geben Sie eine gültige IP-Adresse ein.

Encoder-Typ:/Decoder-Typ:
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.

12.10.2 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 > Rechtsklick auf > Klick auf **Decoder bearbeiten** > Dialogfeld **Decoder bearbeiten**
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:
- VID 7000
- VID 8000
- VIP XD HD

Hinweis!
Die Verbindung zwischen einem Decoder und einem Encoder ist nur sicher, wenn beide mit einer sicheren Verbindung konfiguriert werden.

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*

12.10.3 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 216*

12.10.4 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.

12.10.5 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.

12.10.6 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 158*
- *Szenarios für Bosch IntuiKey Keyboard-Anschlüsse, Seite 50*
- *Anschluss eines Bosch IntuiKey Keyboards an einen Decoder, Seite 53*

12.10.7 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 50*
- *Anschluss eines Bosch IntuiKey Keyboards an einen Decoder, Seite 53*
- *Aktualisierung der Bosch IntuiKey Keyboard-Firmware, Seite 53*

12.10.8 Löschen des Decoder-Logos

Klicken Sie hier, um das Logo zu löschen, das auf der Webseite des Decoders konfiguriert wurde.

12.11 Seite „Monitorgruppen“

Hauptfenster > **Geräte** > erweitern >

Ermöglicht Ihnen, Monitorgruppen hinzuzufügen und zu konfigurieren. Sie weisen einer BVMS Arbeitsstation in eine Monitorgruppe zu.

Hinweis!
Es ist nicht möglich, eine Monitorgruppe von Operator Client aus zu steuern, wenn die Verbindung zum Management Server unterbrochen ist.

Siehe
- *Manuelles Hinzufügen einer Monitorgruppe, Seite 145*
- *Konfigurieren einer Monitorgruppe, Seite 145*
- *Konfigurieren von voreingestellten Positionen und AUX-Kommandos, Seite 302*
- *Konfigurieren eines Alarms, Seite 328*
- *Dialogfeld Alarmoptionen, Seite 317*
- *Dialogfeld „Bildfensterinhalt auswählen“ (MG), Seite 317*

12.11.1 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.

12.11.2 Konfigurieren einer Monitorgruppe

Hauptfenster > **Geräte** > erweitern > >

Hinweis!
Es ist nicht möglich, eine Monitorgruppe von Operator Client aus zu steuern, wenn die Verbindung zum Management Server unterbrochen ist.

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.

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 145*

12.12 Seite „Monitorwand“

Hauptfenster > **Geräte** >
Ermöglicht das Hinzufügen einer Monitorwand-Anwendung. Diese Anwendung ermöglicht die Steuerung der Monitorwand-Hardware vom Operator Client aus. Kein Server ist an der Steuerung der Monitorwand beteiligt. Dadurch wird sichergestellt, dass der Benutzer vom Operator Client immer in der Lage ist, die Monitorwand zu steuern, auch wenn der Management Server offline ist.

Name
Geben Sie einen Anzeigenamen für Ihre Monitorwand ein.

Monitor
Wählen Sie einen Monitor aus, der mit einem Decoder verbunden ist.
Wenn Sie einen Decoder hinzufügen, mit dem 2 Monitore verbunden sind, müssen Sie das Dialogfeld **Decoder bearbeiten** des Decoders anzeigen und die Gerätefunktionen dieses Decoders aktualisieren. Fügen Sie für jeden Monitor eine weitere Monitorwand hinzu.

Maximale Anzahl von Kameras zum Verbinden:
Geben Sie die maximale Anzahl an Kameras ein, die in der Monitorwand angezeigt werden dürfen. Wenn Sie das Feld leer lassen, kann der Betreiber so viele Kameras anzeigen wie Bildfenster auf dem Monitorwand-Layout verfügbar sind.

Standbilder aktivieren
Klicken Sie darauf, wenn Sie einen Snapshot für jeden Monitor im Operator Client anzeigen möchten. Dieser Snapshot wird regelmäßig aktualisiert.

Startsequenz
Wählen Sie eine Kamerasequenz für die erste Anzeige auf der Monitorwand aus, wenn der Bediener diese Monitorwand startet.

Hinweis!
Beim Löschen einer Sequenz im Dialogfeld **Kamerasequenzen** wird diese Sequenz automatisch aus der Liste **Initialsequenz** einer Monitorwand entfernt, wenn sie dort konfiguriert wurde.

Siehe
– *Dialogfeld Kamerasequenzen, Seite 271*

12.12.1 Manuelles Hinzufügen einer Monitorwand

Hauptfenster > **Geräte** > erweitern > Rechtsklick auf > Klick auf **Monitorwand hinzufügen**

Fügen Sie den erforderlichen Decoder zum BVMS hinzu, bevor Sie die Monitorwand hinzufügen.
Nachdem Sie die Monitorwand hinzugefügt haben, kann der Operator Client-Benutzer diese Monitorwand steuern. Der Benutzer kann die Monitoranordnung ändern und den Monitoren Encoder zuweisen.

Hinzufügen:

1. Wählen Sie den gewünschten Decoder aus.
2. Geben Sie ggf. die maximale Anzahl von Kameras ein und konfigurieren Sie Miniaturansichten.
3. Klicken Sie auf **OK**.
4. Klicken Sie auf .
5. Klicken Sie auf **Karten und Struktur**.
6. Klicken Sie auf **Struktur**.
7. Ziehen Sie die Monitorwand zum Logischen Baum.
8. Konfigurieren Sie ggf. den Zugriff auf die Monitorwand mit entsprechenden Berechtigungen für Benutzergruppen.

Dialogfeld Monitorwand hinzufügen

Name
Geben Sie einen Anzeigenamen für Ihre Monitorwand ein.

Monitor
Wählen Sie einen Monitor aus, der mit einem Decoder verbunden ist.
Wenn Sie einen Decoder hinzufügen, mit dem 2 Monitore verbunden sind, müssen Sie das Dialogfeld **Decoder bearbeiten** des Decoders anzeigen und die Gerätefunktionen dieses Decoders aktualisieren. Fügen Sie für jeden Monitor eine weitere Monitorwand hinzu.

Maximale Anzahl von Kameras zum Verbinden:
Geben Sie die maximale Anzahl an Kameras ein, die in der Monitorwand angezeigt werden dürfen. Wenn Sie das Feld leer lassen, kann der Betreiber so viele Kameras anzeigen wie Bildfenster auf dem Monitorwand-Layout verfügbar sind.

Standbilder aktivieren
Klicken Sie darauf, wenn Sie einen Snapshot für jeden Monitor im Operator Client anzeigen möchten. Dieser Snapshot wird regelmäßig aktualisiert.

Startsequenz
Wählen Sie eine Kamerasequenz für die erste Anzeige auf der Monitorwand aus, wenn der Bediener diese Monitorwand startet.

12.13 Seite Kommunikationsgeräte

Hauptfenster > **Geräte** > erweitern >
Dient zum Hinzufügen oder Konfigurieren eines Kommunikationsgeräts.
Sie können folgende Kommunikationsgeräte konfigurieren:
– E-Mail
– SMS (GSM- oder SMSC-Service Provider)

Siehe
– *Konfigurieren eines Kommunikationsgeräts, Seite 150*

12.13.1 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.

12.13.2 Hinzufügen eines SMS-Geräts

So fügen Sie ein Kommunikationsgerät hinzu:

1. Erweitern Sie , klicken Sie mit der rechten Maustaste auf und klicken Sie auf **SMS-Gerät hinzufügen**.
   Das Dialogfeld **SMS-Gerät hinzufügen** wird angezeigt.
2. Geben Sie die erforderlichen Einstellungen ein.
3. Klicken Sie auf **OK**.
   Das Kommunikationsgerät wird dem System hinzugefügt.

Dialogfeld SMS-Gerät hinzufügen

Name:
Geben Sie den Namen des SMS-Servers ein, der angezeigt werden soll.

GSM-Modem
Klicken Sie darauf, um ein GSM-Modem hinzuzufügen.

SMSC Dial-Up
Klicken Sie darauf, um ein Hayes-kompatibles Modem hinzuzufügen, das eine Verbindung zu einem SMSC-Service Provider herstellen kann.

12.13.3 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*

12.13.4 Konfigurieren eines Kommunikationsgeräts

Hauptfenster > **Geräte** > erweitern > erweitern

So konfigurieren Sie ein Kommunikationsgerät:

1. Klicken Sie auf das erforderliche Gerät: oder .
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 148*
- *Hinzufügen eines SMS-Geräts, Seite 148*
- *Seite SMTP-Server, Seite 149*
- *GSM-Einstellungen / Seite SMSC-Einstellungen, Seite 150*

12.13.5 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*

12.13.6 GSM-Einstellungen / Seite SMSC-Einstellungen

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

Dient zum Konfigurieren der SMS-Einstellungen Ihres BVMS. Auf der Seite **Ereignisse** können Sie einer SMS-Nachricht ein Ereignis zuordnen. Wenn dieses Ereignis eintritt, sendet das System eine SMS. Überschreitet die Anzahl der eingegebenen Zeichen die maximal zulässige Anzahl (in der Regel 160), wird eine SMS in mehrere Teile unterteilt.

Gerät:

Wählen Sie den erforderlichen COM-Port aus, an den das externe Modem angeschlossen ist. Verfügt Ihr Computer über ein internes Modem, wählen Sie den entsprechenden Eintrag aus.

Geschwindigkeit
Wählen Sie die erforderliche Übertragungsrate aus.

PIN (nur bei GSM-Gerät)
Geben Sie die PIN für die Berechtigungsprüfung auf dem Gerät ein.

Datenformat (nur bei SMSC-Gerät)
Wählen Sie das erforderliche Datenformat aus. Sie erhalten die erforderlichen Informationen hierzu von Ihrem Service Provider.

Unicode (nur bei GSM-Gerät)
Aktivieren Sie das Kontrollkästchen, um Unicode-Zeichen zu ermöglichen. Die maximale Anzahl zulässiger Zeichen wird dadurch auf 80 reduziert.

Wählfolge (nur bei SMSC-Gerät)
Geben Sie die Nummer für die Verbindung zum SMSC-Service Provider ein. Sie erhalten diese Nummer von Ihrem Service Provider.

Passwort: (nur bei SMSC-Gerät)
Geben Sie bei Bedarf das Passwort ein, das das Gerät für die Verbindung zum SMSC-Service Provider benötigt. Sie erhalten die erforderlichen Informationen hierzu von Ihrem Service Provider.

Protokoll (nur bei SMSC-Gerät)
Wählen Sie das erforderliche Protokoll aus, das das Gerät für die Verbindung zum SMSC-Service Provider verwendet. Sie erhalten die erforderlichen Informationen hierzu von Ihrem Service Provider.

Empfänger
Geben Sie die Mobiltelefonnummer des Empfängers der SMS-Nachrichten ein. Beziehen Sie dabei auch die internationale Vorwahl (ohne Pluszeichen (+)) mit ein (z. B. +49170123456).

Nachricht (max. 160 Zeichen)
Geben Sie den Text der SMS ein.

SMS Testnachricht
Klicken Sie darauf, um eine SMS-Testnachricht zu senden.

Siehe
- *Konfigurieren eines Kommunikationsgeräts, Seite 150*

12.14 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 98*
- *Konfigurieren eines Peripheriegeräts, Seite 153*

12.14.1 Manuelles Hinzufügen einer Bosch ATM/POS-Bridge

Hauptfenster > **Geräte** > erweitern > Rechtsklick auf > **Bosch ATM/POS-Bridge hinzufügen**

Dient zum Hinzufügen einer Bosch ATM/POS-Bridge.

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 an, die als Überwachungsport der 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 98*

12.14.2 Seite Bosch ATM/POS-Bridge

Hauptfenster > **Geräte** > erweitern > erweitern > > Registerkarte **Bosch ATM/POS-Bridge**

Dient zum Konfigurieren einer Bosch ATM/POS-Bridge.

IP-Adresse:
Geben Sie die IP-Adresse des Geräts ein.

Port 1:
Geben Sie die entsprechende Port-Nummer an, die als Überwachungsport der 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 153*
- *Hinzufügen einer Bosch ATM/POS-Bridge, Seite 98*

12.14.3 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 154*
- *Seite Bosch ATM/POS-Bridge, Seite 152*
- *Seite „DTP-Einstellungen“, Seite 153*

12.14.4 Seite „DTP-Einstellungen“

Hauptfenster > **Geräte** > erweitern > erweitern >
Dies ermöglicht Ihnen die Konfiguration eines DTP-Geräts mit maximal 4 ATM-Geräten, die mit diesem DTP-Gerät verbunden sind.

Serieller Port
Wählen Sie den entsprechenden Port in der Liste aus.

Siehe
- *Seite „ATM-Einstellungen“, Seite 154*
- *Konfigurieren eines Peripheriegeräts, Seite 153*

12.14.5 Seite „ATM-Einstellungen“

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

Dies ermöglicht Ihnen die Konfiguration eines ATM-Geräts, das mit einem DTP 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 Ereignis **Nicht authentifiziert** ist für ein ATM-Gerät zwar verfügbar, jedoch 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 153*

12.14.6 Seite Eingänge

Hauptfenster > **Geräte** > erweitern > erweitern > > Registerkarte **Eingänge**

Dient zum Konfigurieren von Eingängen einer Bosch ATM/POS-Bridge.

Siehe

– *Konfigurieren eines Peripheriegeräts, Seite 153*
– *Hinzufügen einer Bosch ATM/POS-Bridge, Seite 98*

12.15 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.

12.15.1 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.

12.15.2 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**

12.16 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.

12.16.1 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.

12.17 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 157*

12.17.1 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 157*

12.17.2 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.

12.17.3 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 157*

12.18 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 144*
- *Konfigurieren eines Bosch IntuiKey Keyboards (Seite „Einstellungen“) (Arbeitsstation), Seite 136*
- *Konfigurieren eines Bosch IntuiKey Keyboards (Decoder), Seite 143*

12.19 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 160*

12.19.1 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.

12.19.2 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 160*

12.19.3 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.

12.19.4 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.

12.19.5 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.

12.20 Seite "Allegiant CCL-Emulation"

Hauptfenster > **Geräte** > erweitern >

Dient zum Aktivieren der Allegiant CCL-Emulation.

In BVMS unterstützte Allegiant CCL-Befehle, Seite 59 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 163*

12.20.1 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.

12.20.2 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.

12.20.3 Konfigurieren einer Allegiant CCL-Emulation

Hauptfenster > **Geräte**> erweitern >

Um die CCL-Befehle zu verwenden, benötigen Sie das CCL-Benutzerhandbuch. Dieses Handbuch ist im Online-Produktkatalog im Dokumentenbereich jeder LTC-Allegiant Kreuzschiene verfügbar.
Im Abschnitt *In BVMS unterstützte Allegiant CCL-Befehle, Seite 59* sind die CCL-Befehle aufgeführt, die im 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 162*

12.21 Seite „Mobile Video Service“

Hauptfenster > **Geräte** >

Dient zum Hinzufügen eines oder mehrerer Transcodier-Dienst-Einträge zum BVMS. Dieser Transcoder-Dienst passt den Video-Stream von einer in BVMS konfigurierten Kamera an die verfügbare Netzwerkbandbreite an. Dies ermöglicht es mobilen Video-Clients wie einem iPhone, iPad oder Web Client, Videodaten im Live Modus oder Playback Modus über unzuverlässige Netzwerkverbindungen mit beschränkter Bandbreite zu empfangen.

Siehe

– *Manuelles Hinzufügen eines Mobilen Video Services, Seite 164*

12.21.1 Mobiler Video-Service

Mobile Video Service transcodiert Video-Streams von der Quelle für die verfügbare Bandbreite der angeschlossenen Clients. Die Schnittstellen des Mobile Video Service sind ausgelegt für Clients auf mehreren Plattformen, z. B. mobile Geräte (iOS, iPad, iPhone) und Windows Internet Explorer HTML Client.
Mobile Video Service basiert auf Microsoft Internet Information Service.
Ein mobiler Service kann mehrere Clients gleichzeitig bedienen.
Für Grenzwerte siehe Datenblatt und die technischen Hinweise zu Mobile Video Service verfügbar im Online-Produktkatalog für BVMS.

Internet Information Service

Konfigurieren Sie die Einstellungen für den Internet Information Service auf dem Computer, auf dem Sie MVS für BVMS installieren möchten.

Installationshinweise

Sie können keinen Mobile Video Service (MVS) im Configuration Client hinzufügen, wenn die Zeit des Configuration Client-Computers und Mobile Video Service-Computers nicht synchronisiert ist. Stellen Sie sicher, dass die Zeit auf allen betroffenen Computern synchronisiert ist.

Installieren und konfigurieren Sie den Internet Information Service (IIS) vor der Installation des Mobile Video Service. Wenn IIS nicht installiert ist, wird das BVMS Setup zur Installation des Mobile Video Service abgebrochen.

Wählen Sie die Komponente des Mobile Video Service für die Installation beim BVMS Setup. Sie können VRM und Mobile Video Service nicht auf demselben Computer installieren.

Wir empfehlen außerdem, Mobile Video Service nicht auf einem Computer zu installieren, auf dem der Management Server installiert ist.

Mit der Mobile App können Sie die folgenden Aufgaben ausführen:

- Videos wiedergeben
  - Live
  - Wiedergabe
- Netzwerk und Server überwachen

Siehe

- *Manuelles Hinzufügen eines Mobilen Video Services, Seite 164*

12.21.2 Manuelles Hinzufügen eines Mobilen Video Services

Hauptfenster > **Geräte** > Rechtsklick auf > Klick auf **Mobilen Video Service hinzufügen**

Sie können einen oder mehrere Mobile Video Service-Einträge zu Ihrem BVMS hinzufügen.

Zum Hinzufügen:

1. Geben Sie den URI des Mobile Video Service ein.
2. Klicken Sie auf **OK**.

✓ Mobile Video Service und Management Server erkennen sich jetzt, und der Mobile Video Service kann die Konfigurationsdaten vom Management Server empfangen.

Dialogfeld Mobilen Video Service hinzufügen

URI

Geben Sie die URL des Mobile Video Service ein. Befolgen Sie die Syntaxregeln des Beispiels:

https://www.MyDomain.org/mvs

Der Eintrag muss immer mit https:// beginnen, auch wenn Sie keinen verschlüsselten Zugriff auf dem Webserver konfiguriert haben.

12.22 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.

12.22.1 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.

12.22.2 Seite "Einstellungen"

Hauptfenster > **Geräte** > erweitern > erweitern > > Registerkarte **Einstellungen**
Dient zum Ändern der Verbindungseinstellungen der Einbruchmeldezentrale.

12.23 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.

12.23.1 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

Netzwerkadresse / HTTPS 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.

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.

12.23.2 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.

12.23.3 Seite „Einstellungen“

Hauptfenster > **Geräte** > erweitern > > > Registerkarte **Einstellungen**

Dient zum Ändern der Verbindungseinstellungen des Zutrittskontrollsystems.

12.24 Seite „Video Analytics“

Hauptfenster > > **Geräte** > erweitern >

Dient zum Hinzufügen von Video Analytics, Person Identification Devices (PID) und LPR-Geräten.

12.24.1 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

12.24.2 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.

12.24.3 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.

12.24.4 Hinzufügen eines Person Identification Device (PID)

Hinweis!
Bei einem Ausfall des zentralen Servers 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. Das Symbol im Gerätebaum enthält einen roten Punkt. 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 zentralen BVMS Servers, Seite 170*
- *So exportieren Sie Konfigurationsdaten:, Seite 95*

12.24.5 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.

12.24.6 Wiederherstellung des PID-Zugriffs nach Ausfall eines zentralen BVMS Servers

Hinweis!

Bei einem Ausfall des zentralen Servers 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 78*. 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 zentralen BVMS 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 zentralen Servers. Schließen Sie alle erweiterten Eigenschaften ein.
3. Importieren Sie die BVMS Konfigurationssicherung.

Siehe

– *Exportieren von Konfigurationsdaten, Seite 95*

12.24.7 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.

12.24.8 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.

12.24.9 Konfigurieren von Personengruppen

Hauptfenster > > **Geräte** > erweitern >

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 314*

12.24.10 Hinzufügen eines LPR-Geräts

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

LPR-Geräte identifizieren und erfassen Fahrzeugkennzeichen. Sie können LPR-Ereignisse und -Alarme entsprechend konfigurieren.
Wenn das LPR-Gerät bestimmte Kennzeichen erkennen soll, müssen Sie zunächst eine Liste der relevanten Kennzeichen direkt im LPR-Gerät konfigurieren. Detaillierte Informationen finden Sie in der Benutzerdokumentation des Geräts.

Hinweis!
Das Gerät muss verbunden und verfügbar sein.
BVMS stellt nur eine Verbindung her, wenn auf dem LPR-Gerät die Authentifizierung aktiviert ist und Benutzername und Passwort angegeben sind. Benutzername und Passwort dürfen nicht leer sein.

So fügen Sie ein LPR-Gerät hinzu:

1. Klicken Sie mit der rechten Maustaste auf .
2. Klicken Sie auf **LPR-Gerät hinzufügen**.
   Das Dialogfeld **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 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.

12.25 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 197*.

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 237*
- *Synchronisieren der BVMS Konfiguration, Seite 184*
- *Seite VRM-Einstellungen, Seite 177*
- *Seite „Pool“, Seite 184*
- *Seite iSCSI-Gerät, Seite 193*
- *Passwort für ein VRM-Gerät ändern, Seite 180*

12.25.1 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 197*.

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 120*
- *Seite VRM-Geräte, Seite 173*
- *Konfigurieren eines iSCSI-Geräts, Seite 197*
- *Duale/Failover-Aufzeichnung, Seite 26*

12.25.2 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 177*
- *Manuelles Hinzufügen eines gespiegelten VRM, Seite 182*
- *Manuelles Hinzufügen eines Failover-VRM, Seite 181*

12.25.3 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 175*

12.25.4 Seite VRM-Einstellungen

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

Server-Initiatorname
Zeigt den iSCSI-Initiatornamen des VRM Server an.

Systemweites CHAP-Passwort
Geben Sie das Passwort ein, das Sie im iSCSI-Speichergerät konfiguriert haben. Das CHAP-Passwort ist für den VRM gültig und wird automatisch an alle Geräte gesendet. Für Wiedergabe-Clients ist keine zusätzliche Konfiguration notwendig. Sie müssen die iSCSI-

Systeme manuell mit dem CHAP-Passwort konfigurieren. Wenn Sie ein CHAP-Passwort verwenden, müssen alle Speichersysteme so konfiguriert sein, dass sie das CHAP-Passwort verwenden. Nur ein systemweites CHAP-Passwort wird vom VRM-System unterstützt.
Siehe *Globales iSCSI-Verbindungs-Passwort (CHAP Passwort): , Seite 116*

12.25.5 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.

12.25.6 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.

12.25.7 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 diese Option nur bei Bedarf, beispielsweise wenn der technische Kundendienst eine vollständige Hauptspeicherübersicht anfordert.

Telnet-Unterstützung
Aktivieren Sie diese Option, wenn Zugriffe über das Telnet-Protokoll unterstützt werden sollen. Aktivieren Sie diese Option nur bei Bedarf.

Hinweis!
Die umfassende Protokollierung benötigt erhebliche Prozessorleistung und Festplattenkapazität.
Verwenden Sie die umfassende Protokollierung nicht im Dauerbetrieb.

12.25.8 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 **Aufzeichnungsverschlüsselung**.
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 **Erzeugen**.
   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 **Aufzeichnungsverschlüsselung**.
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 **Aufzeichnungsverschlüsselung**.

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 .

12.25.9 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.

12.25.10 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 194*

12.25.11 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 26*

12.25.12 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 175*
- *Duale/Failover-Aufzeichnung, Seite 26*

12.25.13 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. Klicken Sie mit der rechten Maustaste auf das Feld und klicken Sie anschließend auf **Zellinhalt in Spalte kopieren**.

   In der Spalte **Status** wird die erfolgreiche Anmeldung mit angezeigt.

   Fehlgeschlagene Anmeldungen werden mithilfe von angezeigt.
   zeigt an, dass das Gerät ein erstes Passwort erfordert.
   Um das erste Passwort festzulegen, geben Sie es im Feld **Passwort** ein.

   Der Status ändert sich zu .
   Wiederholen Sie diesen Schritt für alle Geräte, die ein erstes Passwort benötigen.
   Hinweis: Solange Sie kein erstes Passwort für alle Geräte in der Liste festgelegt haben, die ein erstes Passwort benötigen, können Sie nicht fortfahren.
5. Klicken Sie auf **Fertig stellen**.
   Das Gerät wird zum Gerätebaum hinzugefügt.

12.25.14 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.

12.25.15 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.

12.26 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 aus irgendeinem Grund keine Speicherblöcke mehr zur Verfügung stellt: Systemausfall, Netzwerkfehler, keine freie Kapazität.
Sie können die zweite Liste leer lassen. In diesem Fall ist kein Failover möglich, aber die Anzahl der erforderlichen iSCSI-Sitzungen verringert sich und kein Speicherplatz auf dem Sekundärziel ist zugeordnet. Dadurch verringert sich der System-Overhead, und die Systemspeicherzeit wird verlängert.

– **Automatisch**
Die Lastverteilung wird automatisch konfiguriert. Jedem Encoder werden automatisch 2 iSCSI-Ziele zugewiesen, und dem Encoder werden Blöcke auf diesen beiden iSCSI-Zielen zugeordnet.

Plausibilitätsprüfungsperiode (Tage)
Verschieben Sie den Schieberegler, um den gewünschten Zeitraum zu konfigurieren. Nach diesem Zeitraum wird das iSCSI-Ziel stündlich überprüft und Blöcke werden neu zugeordnet, falls notwendig.

Nutzung Zweit-Target
Aktivieren oder deaktivieren Sie die Verwendung eines Sekundärziels.

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 202*
– *Hinzufügen eines VRM-Pools, Seite 180*

12.26.1 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 235*

12.26.2 Manuelles Hinzufügen eines Encoders/Decoders

Dient zum manuellen Hinzufügen eines Encoders oder Decoders. 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 oder -Decoder 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.
5. Klicken Sie auf **OK**.
   Das Gerät wird dem System hinzugefügt.
6. Wenn das Gerät ein erstes Passwort erfordert, wird angezeigt.
   Um ein erstes Passwort festzulegen, klicken Sie mit der rechten Maustaste auf das Gerätesymbol, und klicken Sie auf **Initialpasswort setzen...**.
   Das Dialogfeld **Passwort eingeben** wird angezeigt.
   Geben Sie ein Passwort für den service-Benutzer ein und klicken Sie auf **OK**.
   Das Symbol wird ausgeblendet und Sie können das Gerät verwenden.

Dialogfeld Encoder hinzufügen

Hauptfenster > **Geräte** > erweitern > erweitern > Rechtsklick auf > Klick auf **Encoder hinzufügen** > Dialogfeld **Encoder hinzufügen**
oder

Hauptfenster > **Geräte** > Rechtsklick auf > Klick auf **Encoder hinzufügen** > Dialogfeld **Encoder hinzufügen**
oder

Hauptfenster > **Geräte** > Rechtsklick auf > Klick auf **Encoder hinzufügen** > Dialogfeld **Encoder hinzufügen**
oder

Hauptfenster > **Geräte** > erweitern > Rechtsklick auf > Klick auf **Decoder hinzufügen** > Dialogfeld **Encoder hinzufügen**

IP-Adresse:
Geben Sie eine gültige IP-Adresse ein.

Encoder-Typ:/Decoder-Typ:
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.

12.26.3 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.

Passwort
Geben Sie das Passwort zur Authentifizierung auf dem Gerät ein.

Verwandte Themen
– *Hinzufügen eines VRM-Geräts per Suchvorgang, Seite 174*

12.26.4 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

Name
Geben Sie den gewünschten Anzeigenamen für das Gerät 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

VSG-Instanz	rcpp-Port	HTTPS-Port
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**.

Test
Klicken Sie hier, um sich mit den oben eingegebenen Anmeldeinformationen auf dem Gerät zu authentifizieren.

Siehe
– *Bearbeiten eines Video Streaming Gateway, Seite 206*

12.26.5 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 199*
- *Formatieren einer LUN, Seite 203*

12.26.6 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. Klicken Sie mit der rechten Maustaste auf das Feld und klicken Sie anschließend auf **Zellinhalt in Spalte kopieren**.

   In der Spalte **Status** wird die erfolgreiche Anmeldung mit angezeigt.

   Fehlgeschlagene Anmeldungen werden mithilfe von angezeigt.

   zeigt an, dass das Gerät ein erstes Passwort erfordert.
   Um das erste Passwort festzulegen, geben Sie es im Feld **Passwort** ein.

   Der Status ändert sich zu .
   Wiederholen Sie diesen Schritt für alle Geräte, die ein erstes Passwort benötigen.
   Hinweis: Solange Sie kein erstes Passwort für alle Geräte in der Liste festgelegt haben, die ein erstes Passwort benötigen, können Sie nicht fortfahren.
5. Klicken Sie auf **Fertig stellen**.
   Das Gerät wird zum Gerätebaum hinzugefügt.

12.26.7 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.

12.26.8 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 306*
- *ANR-Funktion konfigurieren, Seite 306*
- *Duale/Failover-Aufzeichnung, Seite 26*

12.27 Bosch Encoder-/Decoder-Seite

Informationen zur Konfiguration eines Bosch Encoders/Decoders finden Sie unter *Seite „Bosch Encoder/Decoder/Kamera“, Seite 221*.

12.28 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 195*
- *Manuelles Hinzufügen eines iSCSI-Geräts der DSA E-Series, Seite 195*
- *Konfigurieren eines iSCSI-Geräts, Seite 197*
- *Hinzufügen einer LUN, Seite 202*

– *Formatieren einer LUN, Seite 203*

12.28.1 iSCSI-Speicherpool

Ein Speicherpool ist ein Container für ein oder mehrere iSCSI-Speichersysteme, die dieselben Lastverteilungseigenschaften haben. Die Encoder/IP-Kameras, die einem Speicherpool zugeordnet sind, werden mit diesen gemeinsamen Lastverteilungseinstellungen aufgezeichnet. Ein Speicherpool kann verwendet werden, um eine logische Abbildung der Netzwerktopologie zum VRM 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 **automatischen** Modus: 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 184*

12.28.2 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.

Passwort
Geben Sie das Passwort zur Authentifizierung auf dem Gerät ein.

Verwandte Themen
– *Hinzufügen eines VRM-Geräts per Suchvorgang, Seite 174*

12.28.3 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 199*
- *Formatieren einer LUN, Seite 203*

12.28.4 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 199*
- *Dialogfeld „Lastverteilung“, Seite 200*
- *Dialogfeld iqn-Mapper, Seite 203*
- *Formatieren einer LUN, Seite 203*

12.28.5 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]
Diese Option wird nur für die E-Serie angezeigt.
Da 256 die maximale Anzahl der LUNs eines Speicherarrays ist, darf die Größe der LUNs nicht zu klein gewählt werden (da andernfalls in der Zukunft keine weiteren LUNs erstellt werden können, wenn ein zusätzliches Rack 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.
Hinweis: Bei FAS-Archivierungssystemen kann es mehrere Stunden dauern, bis LUNs vollständig gelöscht sind. Während dieser Zeit kann die Gesamtkapazität der neu erstellten LUNs verringert werden. Sie können neue LUNs mit voller Kapazität erst dann erstellen, nachdem die alten LUNs vollständig gelöscht wurden.

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)
Aktivieren Sie diese Option, wenn Sie statt des angegebenen RAID-Typs RAID-5 lieber den zuverlässigeren RAID-Typ RAID 6 verwenden möchten.

Zusatzinformationen
Weitere Informationen werden hier angezeigt, 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 195*

12.28.6 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.

12.28.7 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.

12.28.8 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 184*
- *Hinzufügen einer LUN, Seite 202*
- *Hinzufügen eines VRM-Geräts per Suchvorgang, Seite 174*

12.28.9 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 > erweitern > > Klick auf **Hinzufügen**

Dient zum Hinzufügen einer LUN.

Id

Geben Sie die ID der LUN ein.

Siehe

– *Seite „Pool“, Seite 184*
– *Seite LUNs, Seite 201*

12.28.10 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.

Konfiguration:

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 201*

12.28.11 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 174*
- *Konfigurieren eines iSCSI-Geräts, Seite 197*

12.29 Seite „Video Streaming Gateway-Gerät“

Hauptfenster > **Geräte** > erweitern > 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 206*
- *ONVIF Seite, Seite 239*

12.29.1 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

Name
Geben Sie den gewünschten Anzeigenamen für das Gerät 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**.

Test
Klicken Sie hier, um sich mit den oben eingegebenen Anmeldeinformationen auf dem Gerät zu authentifizieren.

Siehe
– *Bearbeiten eines Video Streaming Gateway, Seite 206*

12.29.2 Bearbeiten eines Video Streaming Gateway

Hauptfenster > **Geräte** > erweitern > 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 205*

12.29.3 Hinzufügen einer Kamera zu einem VSG

Hauptfenster > **Geräte** > erweitern > 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“, Seite 207*
– *Dialogfeld „ONVIF-Encoder hinzufügen“, Seite 208*
– *Dialogfeld „JPEG-Kamera hinzufügen“, Seite 210*
– *Dialogfeld „RTSP-Encoder hinzufügen“, Seite 211*

12.29.4 Dialogfeld „Bosch Encoder hinzufügen“

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

Rechtsklick auf > **Encoder/Kamera hinzufügen** > Schaltfläche **Bosch Encoder**

Sie können Ihrem VSG-Gerät einen Encoder von Bosch hinzufügen.

Name

Geben Sie den gewünschten Anzeigenamen für das Gerät ein.

Netzwerkadresse

Geben Sie die Netzwerkadresse des Geräts ein.

Typ

Zeigt den erkannten Gerätetyp an, sofern unterstützt.

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.

Test

Klicken Sie hier, um sich mit den oben eingegebenen Anmeldeinformationen auf dem Gerät zu authentifizieren.

Eigenschaften

Klicken Sie, um die für dieses Gerät verfügbaren und gewünschten Funktionen zu aktivieren.

Audio	Klicken Sie, um Audio zu aktivieren, wenn für dieses Gerät verfügbar.
PTZ	Klicken Sie, um PTZ zu aktivieren, wenn für dieses Gerät verfügbar.
Kameraprotokoll	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.
Videoeingang 1 verwenden - **Videoeingang 4 verwenden**	Klicken Sie, um die Videoeingänge auszuwählen, wenn Sie ein Mehrkanal-Gerät konfigurieren.

Siehe

– *Hinzufügen einer Kamera zu einem VSG, Seite 206*

12.29.5 Dialogfeld „ONVIF-Encoder hinzufügen“

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

Rechtsklick auf > **Encoder/Kamera hinzufügen** > Schaltfläche **ONVIF-Encoder hinzufügen**

oder

Hauptfenster > **Geräte** > Kontextmenü von > Befehl **ONVIF-Encoder hinzufügen**

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 den gewünschten Anzeigenamen für das Gerät ein.

Netzwerkadresse / Port
Geben Sie die Netzwerkadresse des Geräts ein. Ändern Sie bei Bedarf die Port-Nummer.

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.

Test
Klicken Sie hier, um sich mit den oben eingegebenen Anmeldeinformationen auf dem Gerät zu authentifizieren.

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.

Eigenschaften

Gerätetyp	Zeigt den abgerufenen Gerätetyp an.
Hersteller	Zeigt den abgerufenen Herstellernamen an.
Modell	Zeigt den abgerufenen Modellnamen an.
Firmware-Version	Zeigt die abgerufene Firmware-Version an.

Aux-Befehl	Wenn das Kontrollkästchen aktiviert ist, werden AUX-Kommandos unterstützt.
Anzahl der Videoeingangskanäle	Geben Sie die gewünschte Anzahl von Videoeingängen ein.
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.
Zugeordnete Gateway-Kanäle	Geben Sie die gewünschte Anzahl von Gateway-Kanälen ein.
Kameraprotokoll	Wählen Sie das gewünschte Kameraprotokoll aus.
Videoeingang {0} verwenden	Aktivieren Sie das Kontrollkästchen, um den entsprechenden Videoeingang zu verwenden.
ONVIF Profil	Wenn diese Option unterstützt wird, wählen Sie das Profil aus, das Sie konfigurieren möchten.

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 206*

12.29.6 Dialogfeld „JPEG-Kamera hinzufügen“

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

Rechtsklick auf > **Encoder/Kamera hinzufügen** > Schaltfläche **JPEG-Kamera**
Sie können eine JPEG Kamera Ihrem VSG Gerät hinzufügen.

Name
Geben Sie den gewünschten 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.

Test
Klicken Sie hier, um sich mit den oben eingegebenen Anmeldeinformationen auf dem Gerät zu authentifizieren.

Eigenschaften

Anzahl der Videoeingangskanäle	Geben Sie die Anzahl der verfügbaren Videoeingänge ein, sofern verfügbar.
Bildrate [ips]	Geben Sie die gewünschte Bildfrequenzrate ein.

Siehe
– *Hinzufügen einer Kamera zu einem VSG, Seite 206*

12.29.7 Dialogfeld „RTSP-Encoder hinzufügen“

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

Rechtsklick auf > **Encoder/Kamera hinzufügen** > Schaltfläche **RTSP-Kamera**
Sie können einen RTSP-Encoder Ihrem VSG Gerät hinzufügen.

Name
Geben Sie den gewünschten 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.

Test
Klicken Sie hier, um sich mit den oben eingegebenen Anmeldeinformationen auf dem Gerät zu authentifizieren.

Eigenschaften

Anzahl der Videoeingangskanäle	Geben Sie die Anzahl der verfügbaren Videoeingänge ein, sofern verfügbar.

Siehe

– *Hinzufügen einer Kamera zu einem VSG, Seite 206*

12.29.8 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.

12.29.9 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 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** > 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.

12.29.10 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 diese Option nur bei Bedarf, beispielsweise wenn der technische Kundendienst eine vollständige Hauptspeicherübersicht anfordert.

Telnet-Unterstützung
Aktivieren Sie diese Option, wenn Zugriffe über das Telnet-Protokoll unterstützt werden sollen. Aktivieren Sie diese Option nur bei Bedarf.

Hinweis!
Die umfassende Protokollierung benötigt erhebliche Prozessorleistung und Festplattenkapazität.
Verwenden Sie die umfassende Protokollierung nicht im Dauerbetrieb.

12.29.11 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.

12.30 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 239*.

Siehe

- *Hinzufügen eines Nur-Live-Encoders, Seite 223*
- *Nach Geräten suchen, Seite 71*
- *Seite „Bosch Encoder/Decoder/Kamera“, Seite 221*
- *ONVIF Seite, Seite 239*
- *Konfigurieren von Multicast, Seite 237*

12.30.1 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. Klicken Sie mit der rechten Maustaste auf das Feld und klicken Sie anschließend auf **Zellinhalt in Spalte kopieren**.
   In der Spalte **Status** wird die erfolgreiche Anmeldung mit angezeigt.
   Fehlgeschlagene Anmeldungen werden mithilfe von angezeigt.
   zeigt an, dass das Gerät ein erstes Passwort erfordert.
   Um das erste Passwort festzulegen, geben Sie es im Feld **Passwort** ein.
   Der Status ändert sich zu .
   Wiederholen Sie diesen Schritt für alle Geräte, die ein erstes Passwort benötigen.
   Hinweis: Solange Sie kein erstes Passwort für alle Geräte in der Liste festgelegt haben, die ein erstes Passwort benötigen, können Sie nicht fortfahren.
5. Klicken Sie auf **Fertig stellen**.
   Das Gerät wird zum Gerätebaum hinzugefügt.

12.30.2 Manuelles Hinzufügen eines Encoders/Decoders

Dient zum manuellen Hinzufügen eines Encoders oder Decoders. 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 oder -Decoder 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.
5. Klicken Sie auf **OK**.
   Das Gerät wird dem System hinzugefügt.

6. Wenn das Gerät ein erstes Passwort erfordert, wird angezeigt.
   Um ein erstes Passwort festzulegen, klicken Sie mit der rechten Maustaste auf das Gerätesymbol, und klicken Sie auf **Initialpasswort setzen...**.
   Das Dialogfeld **Passwort eingeben** wird angezeigt.
   Geben Sie ein Passwort für den service-Benutzer ein und klicken Sie auf **OK**.
   Das Symbol wird ausgeblendet und Sie können das Gerät verwenden.

Dialogfeld Encoder hinzufügen

Hauptfenster > **Geräte** > erweitern > erweitern > Rechtsklick auf > Klick auf **Encoder hinzufügen** > Dialogfeld **Encoder hinzufügen**
oder

Hauptfenster > **Geräte** > Rechtsklick auf > Klick auf **Encoder hinzufügen** > Dialogfeld **Encoder hinzufügen**
oder

Hauptfenster > **Geräte** > Rechtsklick auf > Klick auf **Encoder hinzufügen** > Dialogfeld **Encoder hinzufügen**
oder

Hauptfenster > **Geräte** > erweitern > Rechtsklick auf > Klick auf **Decoder hinzufügen** > Dialogfeld **Encoder hinzufügen**

IP-Adresse:
Geben Sie eine gültige IP-Adresse ein.

Encoder-Typ:/Decoder-Typ:
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.

12.30.3 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 141*

12.31 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. Klicken Sie mit der rechten Maustaste auf das Feld und klicken Sie anschließend auf **Zellinhalt in Spalte kopieren**.
   In der Spalte **Status** wird die erfolgreiche Anmeldung mit angezeigt.
   Fehlgeschlagene Anmeldungen werden mithilfe von angezeigt.
   zeigt an, dass das Gerät ein erstes Passwort erfordert.
   Um das erste Passwort festzulegen, geben Sie es im Feld **Passwort** ein.
   Der Status ändert sich zu .
   Wiederholen Sie diesen Schritt für alle Geräte, die ein erstes Passwort benötigen.
   Hinweis: Solange Sie kein erstes Passwort für alle Geräte in der Liste festgelegt haben, die ein erstes Passwort benötigen, können Sie nicht fortfahren.
5. Klicken Sie auf **Fertig stellen**.
   Das Gerät wird zum Gerätebaum hinzugefügt.

Siehe
– *Konfigurieren von Multicast, Seite 237*
– *Hinzufügen eines Encoders mit lokaler Archivierung, Seite 223*
– *Seite „Bosch Encoder/Decoder/Kamera“, Seite 221*
– *Nach Geräten suchen, Seite 71*

12.32 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 23*
- *Manuelles Hinzufügen einer Unmanaged Site, Seite 218*
- *Importieren von Unmanaged Sites, Seite 218*
- *Konfiguration der Zeitzone, Seite 220*

12.32.1 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 23*
- *Seite „Unmanaged Site“, Seite 218*

12.32.2 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 dem Logischen Baum jetzt die Unmanaged Sites hinzufügen.
   Hinweis: Wenn ein Fehler auftritt und die Datei nicht importiert werden kann, wird eine entsprechende Fehlermeldung angezeigt.

12.32.3 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.

12.32.4 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 23*.

Passwort:
Geben Sie das gültige Passwort ein, sofern verfügbar. Weitere Informationen zu Zugangsdaten finden Sie unter *Unmanaged Site, Seite 23*.

Siehe
– *Unmanaged Site, Seite 23*

12.32.5 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 218*

13 Seite „Bosch Encoder/Decoder/Kamera“

Dieses Kapitel enthält Informationen zur Konfiguration von Encodern und Decodern in Ihrem System.
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. Klicken Sie mit der rechten Maustaste auf das Feld und klicken Sie anschließend auf **Zellinhalt in Spalte kopieren**.

In der Spalte **Status** wird die erfolgreiche Anmeldung mit angezeigt.

Fehlgeschlagene Anmeldungen werden mithilfe von angezeigt.

zeigt an, dass das Gerät ein erstes Passwort erfordert.
Um das erste Passwort festzulegen, geben Sie es im Feld **Passwort** ein.

Der Status ändert sich zu .
Wiederholen Sie diesen Schritt für alle Geräte, die ein erstes Passwort benötigen.
Hinweis: Solange Sie kein erstes Passwort für alle Geräte in der Liste festgelegt haben, die ein erstes Passwort benötigen, können Sie nicht fortfahren.

5. Klicken Sie auf **Fertig stellen**.
   Das Gerät wird zum Gerätebaum hinzugefügt.

Siehe
- *Nach Geräten suchen, Seite 71*

13.1 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 183*.

Siehe
- *Hinzufügen eines Geräts, Seite 120*

13.2 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 214*.

Siehe
- *Hinzufügen eines Geräts, Seite 120*
- *Seite Nur Live, Seite 214*

13.3 Hinzufügen eines Encoders mit lokaler Archivierung

Informationen zum Hinzufügen eines Encoders mit lokaler Archivierung per Suchvorgang finden Sie unter *Seite Lokale Archivierung, Seite 217*.

Siehe
- *Hinzufügen eines Geräts, Seite 120*
- *Seite Lokale Archivierung, Seite 217*

13.4 Bearbeiten eines Encoders

13.4.1 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 237*
- *Dialogfeld „Encoder/Decoder bearbeiten“, Seite 225*

13.4.2 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 > Rechtsklick auf > Klick auf **Decoder bearbeiten** > Dialogfeld **Decoder bearbeiten**

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 225*

13.4.3 Dialogfeld „Encoder/Decoder bearbeiten“

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

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:
- VID 7000
- VID 8000
- VIP XD HD

Hinweis!
Die Verbindung zwischen einem Decoder und einem Encoder ist nur sicher, wenn beide mit einer sicheren Verbindung konfiguriert werden.

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*

13.5 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 227*

13.5.1 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 228*
- *Hochladen eines Zertifikats, Seite 228*
- *Download eines Zertifikats, Seite 229*
- *Installierung eines Zertifikats auf einer Arbeitsstation, Seite 229*

13.5.2 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 .

13.5.3 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 .

13.5.4 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.

13.5.5 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*.

13.6 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 230*

13.7 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 230*

13.8 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.

13.9 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.

13.10 Konfigurieren von Encodern/Decodern

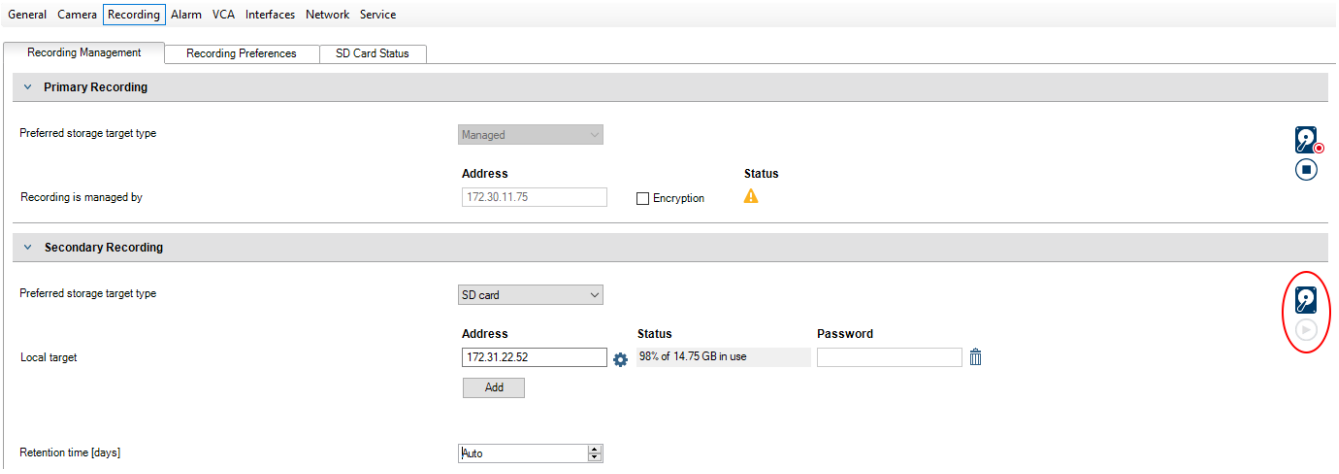
13.10.1 Speichermedien eines Encoders konfigurieren

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 236*
- *ANR-Funktion konfigurieren, Seite 306*

13.10.2 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 **Zellinhalt kopieren 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.

13.10.3 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 186*

13.10.4 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 233*

13.10.5 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 184*

13.11 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*

14 ONVIF Seite

Hauptfenster > **Geräte** > erweitern >
oder
Hauptfenster > **Geräte** > erweitern > erweitern > erweitern > > erweitern

Siehe
- *Seite „Video Streaming Gateway-Gerät“, Seite 204*
- *Seite Nur Live, Seite 214*

14.1 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.

14.2 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.

Videoeingänge

Geben Sie die Anzahl der Kameras ein, die mit diesem Encoder verbunden sind.

Audioeingänge

Geben Sie die Anzahl der Audioeingänge ein, die mit diesem Encoder verbunden sind.

Alarmeingänge

Geben Sie die Anzahl der Alarmeingänge ein, die mit diesem Encoder verbunden sind.

Relais

Geben Sie die Anzahl der Relais ein, die mit diesem Encoder verbunden sind.

Siehe

- *Seite "ONVIF-Encoderereignis", Seite 240*
- *Hinzufügen eines Nur-Live-Encoders, Seite 223*
- *Konfigurieren einer ONVIF-Mapping-Tabelle, Seite 244*

14.3 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

- *ONVIF-Ereigniszuordnung, Seite 37*
- *Konfigurieren einer ONVIF-Mapping-Tabelle, Seite 244*

14.3.1 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.

14.3.2 Exportieren einer ONVIF-Mapping-Tabelle

Hauptfenster > **Geräte** > erweitern > 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 240*

14.3.3 Importieren einer ONVIF Mapping-Tabelle

Hauptfenster > **Geräte** > erweitern > 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.

14.3.4 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 > 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 383*
- *ONVIF-Ereigniszuordnung, Seite 37*
- *Seite "ONVIF-Encoderereignis", Seite 240*
- *Seite "ONVIF-Ereignisquelle", Seite 261*

14.4 Seite „ONVIF Konfiguration“

Hauptfenster > **Geräte** > erweitern erweitern > 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.

14.4.1 Gerätezugriff

Hauptfenster > **Geräte** > erweitern > 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.

14.4.2 Datum/Zeit

Hauptfenster > **Geräte** > erweitern > 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
Wählen 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.

14.4.3 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.

14.4.4 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.

14.4.5 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.

14.4.6 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.

14.4.7 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.

14.4.8 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.

14.4.9 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].

14.4.10 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.

14.4.11 Weißabgleich

Hauptfenster > **Geräte** > erweitern > 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).

14.4.12 Netzwerkzugriff

Hauptfenster > **Geräte** > erweitern > 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.

14.4.13 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.
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.

Kategorie	Definierte Werte	Beschreibung
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.

14.4.14 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.

14.5 Seite "ONVIF-Ereignisquelle"

Hauptfenster > **Geräte** > Erweitern > Erweitern > Erweitern > Erweitern > Erweitern > Erweitern > Registerkarte **ONVIF Ereignisquelle**
oder
Hauptfenster > **Geräte** > Erweitern > Erweitern > > Registerkarte **ONVIF Ereignisquelle**
oder
Hauptfenster > **Geräte** > Erweitern > Erweitern > Erweitern > Erweitern > Erweitern > Erweitern > Registerkarte **ONVIF Ereignisquelle**
oder
Hauptfenster > **Geräte** > Erweitern > Erweitern > > Registerkarte **ONVIF Ereignisquelle**
oder
Hauptfenster > **Geräte** > Erweitern > Erweitern > Erweitern > Erweitern > Erweitern > Erweitern > Registerkarte **ONVIF Ereignisquelle**
oder
Hauptfenster > **Geräte** > Erweitern > Erweitern > Erweitern > > Registerkarte **ONVIF 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 37*
– *Konfigurieren einer ONVIF-Mapping-Tabelle, Seite 244*

14.6 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 287*

15 Seite „Karten und Struktur“

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 festlegen.

Zeigt den Gerätebaum, den Logischen Baum und das Fenster „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-Dateien, Zuweisen der Dateien zu Knoten
- Erzeugen von Hotspots auf einer Karte
- Erstellen eines Störungsrelais

Beispiele für Ressourcen-Dateien:

- Lageplan-Dateien
- Dokument-Dateien
- Web-Dateien
- Audio-Dateien
- Kommandoskripte
- Kamerasequenz-Dateien

Beispiele für Hotspots:

- Kameras
- Eingänge
- Relais
- Kommandoskripte
- Sequenzen
- Links zu anderen Karten
- Leser eines Zutrittskontrollsystems

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.
	Erzeugt einen Ordner im Logischen Baum.
	Zeigt ein Dialogfeld zum Hinzufügen von Kartenressourcen-Dateien an.
	Zeigt ein Dialogfeld zum Hinzufügen einer Dokumentdatei an (HTML, HTM, TXT, URL, MHT).

	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.

Geben Sie eine Zeichenfolge ein, und drücken Sie zum Filtern der angezeigten Element die Taste ENTER. 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. Ein aktiver Filter wird durch gekennzeichnet. 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.

Um die Filterung abzubrechen, klicken Sie auf .

16 Konfigurieren des logischen Baums

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 267*
- *Dialogfeld Ressource auswählen, Seite 268*
- *Dialogfeld Kamerasequenzen, Seite 271*
- *Dialogfeld Kamerasequenz hinzufügen, Seite 273*
- *Dialogfeld Sequenzschritt hinzufügen, Seite 273*
- *Dialogfeld URL hinzufügen, Seite 269*
- *Dialogfeld Karte für Link auswählen, Seite 275*
- *Dialogfeld „Störungsrelais“, Seite 277*
- *Dialogfeld „Link zu externer Anwendung“, Seite 269*

16.1 Konfigurieren des Logischen Baums

Siehe
- *Seite „Karten und Struktur“, Seite 263*

16.2 Hinzufügen eines Geräts zum Logischen Baum

Hauptfenster > **Karten und Struktur**

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 gedrückt halten.

Siehe
- *Seite „Karten und Struktur“, Seite 263*

16.3 Entfernen eines Baumelements

Hauptfenster > **Karten und Struktur**

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 263*

16.4 Verwalten von Ressourcen-Dateien

Hauptfenster > **Karten und Struktur** >
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 268*

16.4.1 Dialogfeld Ressourcen-Manager

Hauptfenster > **Karten und Struktur** > > **Ressourcen-Manager** Dialogfeld

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.

16.4.2 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 274*
- *Zuordnen einer Karte zu einem Ordner, Seite 275*
- *Hinzufügen eines Dokuments, Seite 268*

16.5 Hinzufügen eines Dokuments

Hauptfenster > **Karten und Struktur**

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 266*.

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 268*
- *Verwalten von Ressourcen-Dateien, Seite 266*

16.5.1 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 268*

16.6 Dialogfeld „Link zu externer Anwendung“

Hauptfenster > **Karten und Struktur** > > **Ressourcen-Manager** Dialogfeld > > **Link zu einer externen Anwendung** Dialogfeld

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.

16.7 Hinzufügen eines Kommandoskripts

Hauptfenster > **Karten und Struktur**

Bevor Sie ein Kommandoskript hinzufügen können, müssen Sie zunächst Kommandoskript-Dateien importieren oder erzeugen.
Weitere Informationen finden Sie unter *Konfigurieren von Kommandoskripten, Seite 90*.

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 268*

16.8 Hinzufügen einer Kamerasequenz

Hauptfenster > **Karten und Struktur**

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 271*

16.8.1 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.

Hinweis!
Beim Löschen einer Sequenz im Dialogfeld **Kamerasequenzen** wird diese Sequenz automatisch aus der Liste **Initialsequenz** einer Monitorwand entfernt, wenn sie dort konfiguriert wurde.

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
- *Seite „Monitorwand“, Seite 146*
- *Verwalten von vorkonfigurierten Kamerasequenzen, Seite 272*

16.9 Verwalten von vorkonfigurierten Kamerasequenzen

Hauptfenster > **Karten und Struktur**

Sie können folgende Aufgaben zum Verwalten von Kamerasequenzen durchführen:
- Erzeugen 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 271*

16.9.1 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.

16.9.2 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.

16.10 Hinzufügen eines Ordners

Hauptfenster > **Karten und Struktur**

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 263*

16.11 Hinzufügen einer Karte

Hauptfenster > **Karten und Struktur**

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 266*.

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 268*

16.12 Hinzufügen eines Links zu einer anderen Karte

Hauptfenster > **Karten und Struktur**

Wenn mindestens zwei Karten vorhanden sind, können Sie einer Karte einen Link hinzufügen, der auf die andere Karte verweist, so dass 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 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.

16.12.1 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.

16.13 Zuordnen einer Karte zu einem Ordner

Hauptfenster > **Karten und Struktur**

Bevor Sie Karten zuweisen können, müssen Sie zunächst Kartenressourcen-Dateien importieren.

Weitere Informationen finden Sie unter *Verwalten von Ressourcen-Dateien, Seite 266*.

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 263*
- *Dialogfeld Ressource auswählen, Seite 268*

16.14 Verwalten von Geräten auf einer Karte

Hauptfenster > **Karten und Struktur**

Bevor Sie Geräte auf einer Karte 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 ordnen Sie Elemente auf einer Karte an:

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 der Karte.
3. Ziehen Sie die Elemente an die gewünschten Stellen auf der Karte.

So entfernen Sie ein Element des Logischen Baums nur von der Karte:

1. Klicken Sie mit der rechten Maustaste auf die Karte, und klicken Sie auf **Unsichtbar**.
   Das Element wird aus der Karte 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 auf **Sichtbar auf einer Karte**.

So entfernen Sie ein Element von der Karte und aus dem Vollständigen Logischen Baum:

- Klicken Sie mit der rechten Maustaste auf das Element im Logischen Baum, und klicken Sie auf **Entfernen**.
  Das Element wird von der Karte 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 einer Karte bzw. heben die Umgehung auf:

1. Klicken Sie mit der rechten Maustaste auf das bestimmte Gerät auf der Karte.
2. Klicken Sie auf **Umgehen**/**Umgehung aufheben**.

Hinweis!
Es ist möglich, umgangene Geräte über das Suchfeld zu filtern.

Siehe

- *Konfigurieren der Geräteumgehung, Seite 278*
- *Seite „Karten und Struktur“, Seite 263*

16.15 Ein Störungsrelais hinzufügen

Hauptfenster > **Karten und Struktur** > > 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.

16.15.1 Dialogfeld „Störungsrelais“

Hauptfenster > **Karten und Struktur** > > 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.

16.16 Konfigurieren der Geräteumgehung

Hauptfenster > **Karten und Struktur**

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 einer Karte, Seite 275*

Hinweis!
Es ist möglich, umgangene Geräte über das Suchfeld zu filtern.

Siehe

– *Verwalten von Geräten auf einer Karte, Seite 275*

17 Seite Zeitpläne

Hauptfenster >

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 282*

17.1 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 282*

- *Hinzufügen von Feiertagen und besonderen Tagen, Seite 284*
- *Entfernen von Feiertagen und besonderen Tagen, Seite 285*
- *Umbenennen eines Zeitplans, Seite 286*

17.2 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 283*
- *Konfigurieren eines Standard-Aktionszeitplans, Seite 283*
- *Konfigurieren eines wiederkehrenden Aktionszeitplans, Seite 284*
- *Entfernen eines Aktionszeitplans, Seite 284*
- *Hinzufügen von Feiertagen und besonderen Tagen, Seite 284*
- *Entfernen von Feiertagen und besonderen Tagen, Seite 285*
- *Umbenennen eines Zeitplans, Seite 286*

18 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 279*
- *Seite Aktionszeitpläne, Seite 280*

18.1 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 279*

18.2 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 280*

18.3 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 280*

18.4 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 280*

18.5 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 280*

18.6 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 279*
– *Seite Aktionszeitpläne, Seite 280*

18.7 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 279*
- *Seite Aktionszeitpläne, Seite 280*

18.8 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 279*
- *Seite Aktionszeitpläne, Seite 280*

19 Seite Kameras und Aufzeichnung

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.

Geben Sie eine Zeichenfolge ein, und drücken Sie zum Filtern der angezeigten Element die Taste ENTER. 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. Ein aktiver Filter wird durch gekennzeichnet. 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.

Um die Filterung abzubrechen, klicken Sie auf .

19.1 Seite Kameras

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.
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

▸ 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.

Stream 1 - Codec / Stream 2 - Codec (nur VRM und lokaler Speicher)
Klicken Sie auf eine Zelle, um den gewünschten Codec zum Codieren des Streams auszuwählen.

Stream 1 - Qualität / Stream 2 - Qualität
Wählen Sie die gewünschte Streamqualität für die Live-Anzeige oder Aufzeichnung aus. Sie konfigurieren die Qualitätseinstellungen im Dialogfeld **Stream-Qualitätseinstellungen**.

Stream 1 - Aktive Plattform / Stream 2 - Aktive Plattform
Zeigt den Namen der Plattformeinstellungen im Dialogfeld **Stream-Qualitätseinstellungen** an. Diese Spalte ist schreibgeschützt und zeigt an, welche Profileinstellungen auf den Encoder geschrieben werden.

Hinweis!
Nur anwendbar, wenn die Streamqualitätsprofile „quiet“, „standard“ oder „busy“ ausgewählt sind:
Der Wert **Aktive Plattform** ändert sich, wenn Sie den Codec der ausgewählten Kamera ändern. Die Zielbitrate wird automatisch angepasst und der Name der Plattformeinstellungen wird angezeigt.

Live Video - Stream (nur VRM sowie Nur Live und lokaler Speicher)
Klicken Sie auf eine Zelle, um den Stream für einen VRM oder einen Encoder mit lokaler Archivierung / Nur-Live--Encoder auszuwählen.

Live Video - Profil (nur für ONVIF-Kameras verfügbar)
Klicken Sie auf eine Zelle, um nach verfügbaren Tokens für Live-Profile dieser ONVIF-Kamera zu suchen.
Wenn Sie den Eintrag **<Automatisch>** auswählen, wird automatisch der Stream mit der höchsten Qualität verwendet.

Live Video - ROI
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 zugewiesen 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.

Aufzeichnung - Einstellung
Klicken Sie auf eine Zelle, um die erforderliche Aufzeichnungseinstellung auszuwählen. Sie konfigurieren die verfügbaren Aufzeichnungseinstellungen im Dialogfeld **Geplante Aufzeichnungseinstellungen**.

Aufzeichnung - Profil (nur für ONVIF-Kameras verfügbar)
Klicken Sie auf eine Zelle, um nach verfügbaren Tokens für Aufzeichnungsprofile dieser ONVIF-Kamera zu suchen. Wählen Sie den gewünschten Eintrag aus.

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.

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 306*
- *Konfigurieren von voreingestellten Positionen und AUX-Kommandos, Seite 302*
- *Konfigurieren von PTZ Port-Einstellungen, Seite 302*
- *Konfigurieren von Stream-Qualitätseinstellungen, Seite 294*
- *Kopieren und Einfügen in Tabellen, Seite 292*
- *ANR-Funktion konfigurieren, Seite 306*
- *Kameratabelle exportieren, Seite 293*
- *ONVIF-Profile zuweisen, Seite 307*
- *ROI-Funktion konfigurieren, Seite 304*

19.2 Aufzeichnungseinstellungsseiten (nur NVR)

Hauptfenster > **Kameras und Aufzeichnung** > > auf eine Registerkarte für einen Aufzeichnungszeitplan klicken (z. B.)

Dient zum Konfigurieren der Aufzeichnungseinstellungen für alle dem NVR Ihres Systems zugeordneten Encoder.

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.

Wählen Sie in der Spalte ein Kontrollkästchen aus, um Audio zu aktivieren.

Live-/Vorereignisaufzeichnung

Klicken Sie in der Spalte **Qualität** auf eine Zelle, um die Streamqualität des Liveanzeigemodus (erforderlich bei zeitversetzter Wiedergabe) und des Vorereignis-Aufzeichnungsmodus (erforderlich bei Bewegungs- und Alarmaufzeichnung) von Stream 2 auszuwählen. Sofern duales Streaming bei diesem Encoder aktiviert ist, können Sie Stream 1 zur Live- oder Vorereignisaufzeichnung auswählen.

Wählen Sie in der Spalte ein Kontrollkästchen aus, 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.

Wählen Sie in der Spalte ein Kontrollkästchen aus, 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 292*
- *Konfigurieren von Aufzeichnungseinstellungen (nur NVR), Seite 298*
- *Kopieren der Aufzeichnungseinstellungen (nur NVR), Seite 305*

20 Konfigurieren von Kameras und Aufzeichnungseinstellungen

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 287*
- *Dialogfeld Geplante Aufzeichnungseinstellungen (nur VRM und Lokale Archivierung), Seite 299*
- *Dialogfeld Stream-Qualitätseinstellungen, Seite 294*
- *Dialogfeld „Voreingestellte Positionen und AUX-Kommandos“, Seite 304*
- *Dialogfeld Aufzeichnungseinstellungen kopieren (nur NVR), Seite 306*

20.1 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 in**, 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 **Zellinhalt kopieren 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 **Zellinhalt kopieren 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 287*
- *Dialogfeld Geplante Aufzeichnungseinstellungen (nur VRM und Lokale Archivierung), Seite 299*
- *Seite Ereignisse, Seite 308*
- *Seite Alarme, Seite 314*

20.2 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.

20.3 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.

20.3.1 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, Bildrate, 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
Wählen Sie die gewünschte Videoauflösung aus. Für HD-Qualität konfigurieren Sie die SD-Qualität für Stream 2.

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.

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 mit einer Auflösung von bis zu 1080p und ab Firmware 6.40 unterstützt.

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. Klicken Sie auf **Automatisch**, um I-Frames nach Bedarf einzufügen. Der Eintrag 1 bedeutet, dass I-Frames kontinuierlich generiert werden. Der Eintrag 2 gibt an, dass nur jedes zweite Bild ein I-Frame ist, und 3 gibt an, dass nur jedes dritte Bild ein I-Frame ist, usw. Die dazwischenliegenden Frames werden als P-Frames codiert.

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:
Die Einstellung der Videoqualität erfolgt in Abhängigkeit von der Bewegung und Detailgenauigkeit im Video. Wenn Sie die Kontrollkästchen **Automatisch** aktivieren, wird automatisch das optimale Verhältnis zwischen Bewegungs- und Bilddefinition eingestellt.

VIP X1600 XFM4-Einstellungen
Ermöglicht es Ihnen, die folgenden H.264-Einstellungen für das Encoder-Modul VIP X 1600 XFM4 zu konfigurieren.
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 294*

20.4 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 287*

20.5 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 299*

20.6 Konfigurieren von Aufzeichnungseinstellungen (nur NVR)

Hauptfenster > **Kameras und Aufzeichnung** > Klick auf > Klick auf eine Registerkarte für einen Aufzeichnungszeitplan (z. B.)

Konfigurieren Sie zunächst die Qualitätsstufen des Streams, bevor Sie die Aufzeichnungseinstellungen konfigurieren.

Hinweis: Zur Aufzeichnung muss der entsprechende NVR ordnungsgemäß konfiguriert sein (**Geräte** > erweitern > > Registerkarte **Festplattenarchivierung**).

Hinweis!

Bei allen Encodern werden die Live-Anzeigeeinstellungen auch für die Vorereignisaufzeichnung verwendet.

Bei Encodern, die Dual Streaming unterstützen, werden die Einstellungen für Live-/Vorereignisaufzeichnung, Bewegungsaufzeichnung und Alarmaufzeichnung unabhängig voneinander konfiguriert.

Bei Encodern, die nur einen Stream unterstützen (z. B. der VideoJet 8004), nutzen Live-Anzeige und Aufzeichnung denselben Stream. In diesem Fall haben die Aufzeichnungseinstellungen Priorität, sodass die Live-Anzeige die Einstellungen der Stream-Qualität für Dauer-, Bewegungs- und Alarmaufzeichnung verwendet. Eine Einstellung für Live-/Vorereignisaufzeichnung kann nur eingegeben werden, wenn die Daueraufzeichnung deaktiviert ist.

Sie können den Live-Stream für eine Arbeitsstation oder für einen Encoder von Stream 2 (Standardeinstellung) auf Stream 1 umschalten (**Geräte** > erweitern > > Registerkarte **Einstellungen** > **Einstellungen aus der Tabelle "Kameras und Aufzeichnung" überschreiben**). Diese Einstellung hat keine Auswirkung auf die Vorereignisaufzeichnung.

So konfigurieren Sie Aufzeichnungseinstellungen:

1. Wählen Sie in der Spalte von **Daueraufzeichnung** die gewünschte Stream-Qualität aus oder deaktivieren Sie die Daueraufzeichnung.
2. Aktivieren Sie in der Spalte ein Kontrollkästchen, um Audio zu aktivieren.

3. Wählen Sie in der Spalte von **Live-/Vorereignisaufzeichnung** die gewünschte Stream-Qualität aus oder wählen Sie Stream 1 aus.
4. Aktivieren Sie in der Spalte ein Kontrollkästchen, um Audio zu aktivieren.
5. Wählen Sie in der Spalte von **Bewegungsaufzeichnung** die gewünschte Stream-Qualität aus oder deaktivieren Sie die Bewegungsaufzeichnung.
6. Aktivieren Sie in der Spalte ein Kontrollkästchen, um Audio zu aktivieren.
7. Klicken Sie in der Spalte **Vorereignis [s]** auf eine Zelle und geben Sie die gewünschte Zeit ein.
8. Klicken Sie in der Spalte **Nachereignis [s]** auf eine Zelle und geben Sie die gewünschte Zeit ein.
9. Wählen Sie in der Spalte von **Alarmaufzeichnung** die gewünschte Stream-Qualität aus oder deaktivieren Sie die Alarmaufzeichnung.
10. Aktivieren Sie in der Spalte ein Kontrollkästchen, um Audio zu aktivieren.
11. Klicken Sie in der Spalte **Vorereignis [s]** auf eine Zelle und geben Sie die gewünschte Zeit ein.
12. Klicken Sie in der Spalte **Nachereignis [s]** auf eine Zelle und geben Sie die gewünschte Zeit ein.

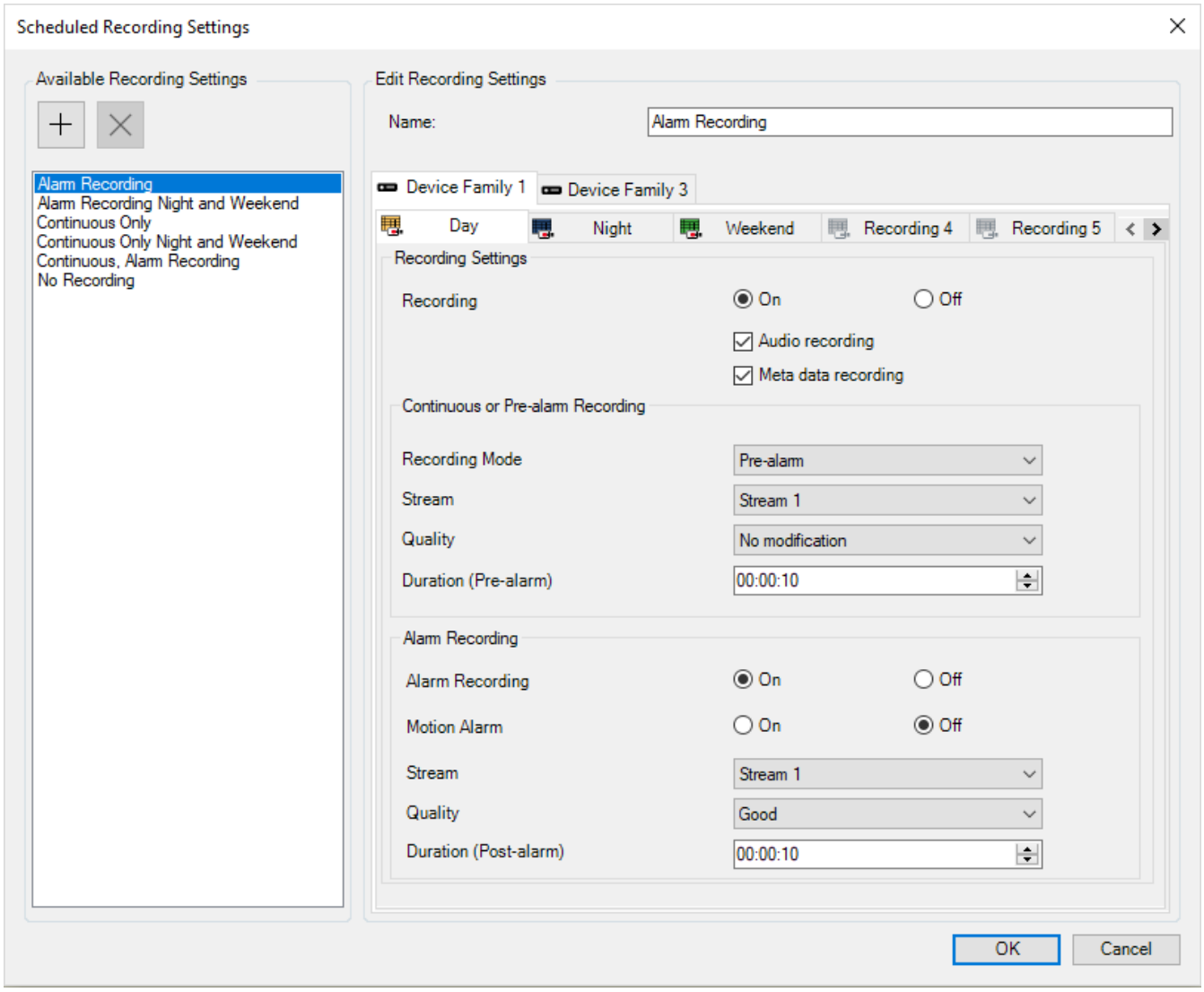
Hinweis!
Wenn die Vorereigniszeit für Bewegungsaufzeichnung und für Alarmaufzeichnung nicht identisch ist, wird der höhere Wert für beide Aufzeichnungsarten verwendet.
Wenn sich die konfigurierte Vorereigniszeit und ein vorangehender Alarm oder eine Bewegungsaufzeichnung überschneiden, startet die Vorereignisaufzeichnung nach Abschluss der vorangehenden Aufzeichnung.

Detaillierte Informationen zu den verschiedenen Feldern finden Sie in der Online-Hilfe unter dem entsprechenden Anwendungsfenster.

Siehe
– *Seite Kameras, Seite 287*

20.7 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.

Wählen Sie die gewünschte Gerätefamilie aus, um die für diese Gerätefamilie gültigen Aufzeichnungseinstellungen zu konfigurieren.

Wählen Sie für die ausgewählte Gerätefamilie einen Aufzeichnungsplan aus, 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.

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 292*
- *Konfigurieren von Aufzeichnungseinstellungen (nur VRM und Lokale Archivierung), Seite 297*

20.8 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.

20.9 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 304*
- *Konfigurieren von PTZ Port-Einstellungen, Seite 302*
- *Konfigurieren eines Alarms, Seite 328*
- *Dialogfeld Bildfensterinhalt auswählen, Seite 316*
- *Dialogfeld Alarmoptionen, Seite 317*
- *Dialogfeld „Bildfensterinhalt auswählen“ (MG), Seite 317*

20.10 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 302*
- *Konfigurieren von voreingestellten Positionen und AUX-Kommandos, Seite 302*

20.11 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 287*

20.12 Kopieren der Aufzeichnungseinstellungen (nur NVR)

Hauptfenster > **Kameras und Aufzeichnung** > auf ein Symbol für ein Aufzeichnungsgerät klicken (z. B.) > auf eine Registerkarte für einen Aufzeichnungszeitplan klicken (z. B.)

Sie können Aufzeichnungseinstellungen von einem Aufzeichnungszeitplan in einen anderen kopieren.

So kopieren Sie die Aufzeichnungseinstellungen einer ausgewählten Tabellenzeile:

1. Wählen Sie eine Tabellenzeile mit den gewünschten Aufzeichnungseinstellungen aus.
2. Klicken Sie auf . Das Dialogfeld **Aufzeichnungseinstellungen kopieren** wird angezeigt.
3. Wählen Sie in der Liste einen Aufzeichnungszeitplan aus, in den Sie die Einstellungen kopieren möchten.
4. Klicken Sie auf **Aktuelle Auswahl kopieren**.
5. Klicken Sie auf **OK**. Die Aufzeichnungseinstellungen der ausgewählten Tabellenzeile werden kopiert.

So kopieren Sie alle Aufzeichnungseinstellungen eines Aufzeichnungszeitplans:

1. Klicken Sie auf . Das Dialogfeld **Aufzeichnungseinstellungen kopieren** wird angezeigt.
2. Wählen Sie in der Liste einen Aufzeichnungszeitplan aus, in den Sie die Einstellungen kopieren möchten.
3. Klicken Sie auf **Alle kopieren**.
4. Klicken Sie auf **OK**. Die Aufzeichnungseinstellungen aller Tabellenzeilen werden kopiert.

20.12.1 Dialogfeld Aufzeichnungseinstellungen kopieren (nur NVR)

Hauptfenster > **Kameras und Aufzeichnung** > auf ein Symbol für ein Aufzeichnungsgerät klicken, beispielsweise > auf eine Registerkarte "Aufzeichnungsplan" klicken (beispielsweise) >

Dient zum Kopieren von Aufzeichnungseinstellungen von einem Aufzeichnungszeitplan in einen anderen.

Alle kopieren

Klicken Sie darauf, um alle Aufzeichnungseinstellungen des ausgewählten Zeitplans in einen anderen Zeitplan zu kopieren.

Aktuelle Auswahl kopieren

Klicken Sie darauf, um nur die Aufzeichnungseinstellungen der ausgewählten Tabellenzeilen in einen anderen Zeitplan zu kopieren.

20.13 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 306*
- *Seite Kameras, Seite 287*
- *Speichermedien eines Encoders konfigurieren, Seite 233*

20.14 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 193*
- *ANR-Funktion konfigurieren, Seite 306*
- *Duale/Failover-Aufzeichnung, Seite 26*
- *Seite Kameras, Seite 287*

20.15 Verwalten von Video-Streaming-Gateways

Siehe

- *Seite „Video Streaming Gateway-Gerät“, Seite 204*
- *Dialogfeld „Bosch Encoder hinzufügen“, Seite 207*
- *Dialogfeld „ONVIF-Encoder hinzufügen“, Seite 208*
- *Dialogfeld „JPEG-Kamera hinzufügen“, Seite 210*
- *Dialogfeld „RTSP-Encoder hinzufügen“, Seite 211*

20.15.1 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 287*

21 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.

Geben Sie eine Zeichenfolge ein, und drücken Sie zum Filtern der angezeigten Element die Taste ENTER. 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. Ein aktiver Filter wird durch

gekennzeichnet. 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.

Um die Filterung abzubrechen, klicken Sie auf .

Siehe

- *Konfigurieren von Ereignissen und Alarmen, Seite 323*
- *Konfigurieren von Kommandoskripten, Seite 90*
- *Dialogfeld „Optionen“ (Menü „Einstellungen“), Seite 115*
- *Konfigurieren der blinkenden Hotspots, Seite 331*

21.1 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.

21.2 Registerkarte „Einstellungen” für die erweiterte Anzeige der Karte

Die Konfiguration der Farbstatus auf Karten ist nur möglich, wenn Sie die Option **Erweiterte Statusanzeige aktivieren (Hotspot auf Karten abhängig vom Status einfärben)** oder **Erweiterte Alarm-Anzeige aktivieren (Hotspot-Färbung in Karten je nach Alarm)** im Dialogfeld **Optionen** aktivieren.

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.

21.3 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**

21.4 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 90*

21.5 Zusammengesetztes Ereignis erzeugen / Dialogfeld Zusammengesetztes Ereignis bearbeiten

Hauptfenster > **Ereignisse** >
Dient zum Erzeugen bzw. Ändern eines Zusammengesetzten Ereignisses.

Geben Sie eine Zeichenfolge ein, und drücken Sie zum Filtern der angezeigten Element die Taste ENTER. 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. Ein aktiver Filter wird durch gekennzeichnet. 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.

Um die Filterung abzubrechen, klicken Sie auf .

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 327*
- *Bearbeiten eines Zusammengesetzten Ereignisses, Seite 328*

21.6 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 90*

21.7 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.

21.8 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.

21.9 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 330*

22 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.

Geben Sie eine Zeichenfolge ein, und drücken Sie zum Filtern der angezeigten Element die Taste ENTER. 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. Ein aktiver Filter wird durch gekennzeichnet. 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.

Um die Filterung abzubrechen, klicken Sie auf .

- 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.

Gerät

Klicken Sie in der Spalte **Priorität** auf eine Zelle, um die Alarmpriorität für den ausgewählten Alarm einzugeben (**100** bedeutet geringe Priorität, **1** hohe Priorität). Klicken Sie in der Spalte **Titel** auf eine Zelle, um den Alarmtitel einzugeben, der im BVMS angezeigt werden soll, beispielsweise in der Alarmliste. Klicken Sie in der Spalte **Farbe** auf eine Zelle, um ein Dialogfeld zum Auswählen einer Farbe für den Alarm anzuzeigen, die im Operator Client angezeigt werden soll, beispielsweise in der Alarmliste.

Alarmidentität

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 Audio-Datei anzuzeigen, die bei Alarm wiedergegeben werden soll.

Alarmoptionen
Klicken Sie in einer Zelle auf ..., um das Dialogfeld **Alarmoptionen** anzuzeigen.

Siehe
– *Alarmbearbeitung, Seite 35*

22.1 Dialogfeld „Alarmeinstellungen“

Hauptfenster > **Alarme** >

Registerkarte Alarmeinstellungen

Max. Bildfenster pro Alarm:
Geben Sie die maximale Anzahl der bei Alarm anzuzeigenden Alarmfenster ein.

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 den mehrzeiligen Alarmmodus des Alarmfensterbereichs zu aktivieren.

Hinweis!
Für bestehende Alarmkonfigurationen ist der mehrzeilige Alarmmodus aktiviert, für neue Alarmkonfigurationen ist er deaktiviert und der Einfachanzeige-Modus 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 329*

22.2 Dialogfeld Bildfensterinhalt auswählen

Hauptfenster > **Alarme** > oder > Spalte **Alarmfenster** > in einer der Spalten **1-5** auf ... klicken
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!
Eine im Alarmfenster angezeigte Karte wird zur Anzeige optimiert und enthält nur die Ausgangsansicht der originalen Kartendatei.

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 **Operator Client Funktionen** konfiguriert (siehe *Seite „Bedienerfunktionen“, Seite 345*).

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 „Bedienerfunktionen“, Seite 345*
- *Konfigurieren eines Alarms, Seite 328*

22.3 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.

22.4 Dialogfeld Alarmoptionen

Hauptfenster > **Alarme** > oder > Spalte **Alarmoptionen** > ...

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.
Abweichende Alarmdauer-Einstellungen	Das Kontrollkästchen wird automatisch aktiviert, wenn Sie das Kontrollkästchen **Aufzeichnen** aktivieren und die Kamera ANR unterstützt.
Aux-Kommando	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.

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 Leerzeichen getrennt – ein (Beispiel: name@provider.com).
SMS	Aktivieren Sie das Kontrollkästchen, um bei Alarm eine SMS zu senden.
Gerät:	Wählen Sie ein SMS-Gerät aus.
Empfänger:	Geben Sie die Mobiltelefonnummer der Empfänger ein.
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, aber nicht 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. Senden einer SMS, 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.
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.

Siehe
- *Dialogfeld „Bildfensterinhalt auswählen“ (MG), Seite 317*
- *Alarmaufzeichnung mit Textdaten auslösen, Seite 330*
- *Konfigurieren eines Alarms, Seite 328*
- *Vor- und Nachalarmdauer bei einem Alarm konfigurieren, Seite 329*

22.5 Dialogfeld Ressource auswählen

Hauptfenster > **Alarme** > oder > Spalte **Alarmidentität** > Spalte **Audiodatei** > auf ... 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.

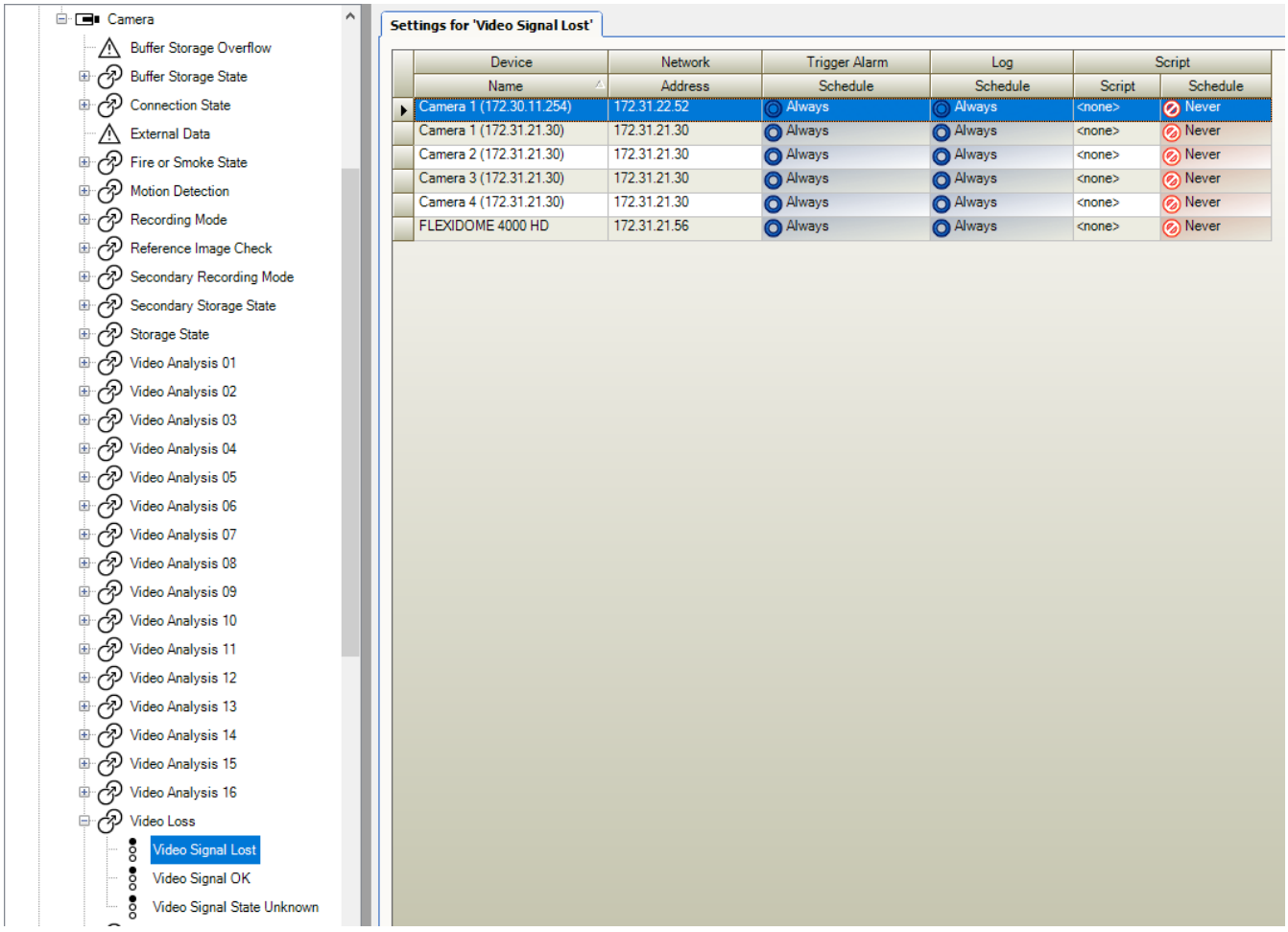
Siehe
- *Konfigurieren eines Alarms, Seite 328*
- *Verwalten von Ressourcen-Dateien, Seite 324*

23 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 309*
- *Registerkarte „Einstellungen” für die erweiterte Anzeige der Karte, Seite 309*
- *Registerkarte „Einstellungen” für die Ereigniskonfiguration, Seite 310*
- *Dialogfeld Kommandoskript-Editor, Seite 311*
- *Zusammengesetztes Ereignis erzeugen / Dialogfeld Zusammengesetztes Ereignis bearbeiten, Seite 311*
- *Dialogfeld Skriptsprache auswählen, Seite 312*
- *Prioritäten des Dialogfelds „Ereignistyp“ bearbeiten, Seite 312*
- *Dialogfeld Geräte auswählen, Seite 312*
- *Dialogfeld „Textatenaufzeichnung“, Seite 313*
- *Dialogfeld „Alarmeinstellungen“, Seite 315*
- *Dialogfeld Bildfensterinhalt auswählen, Seite 316*
- *Dialogfeld Alarmoptionen, Seite 317*

23.1 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 292*.

23.2 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 308*

23.3 Verwalten von Ressourcen-Dateien

Ausführliche Informationen finden Sie im:
- *Verwalten von Ressourcen-Dateien, Seite 266*.

23.4 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 308*

23.5 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 308*

23.6 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 308*

23.7 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.

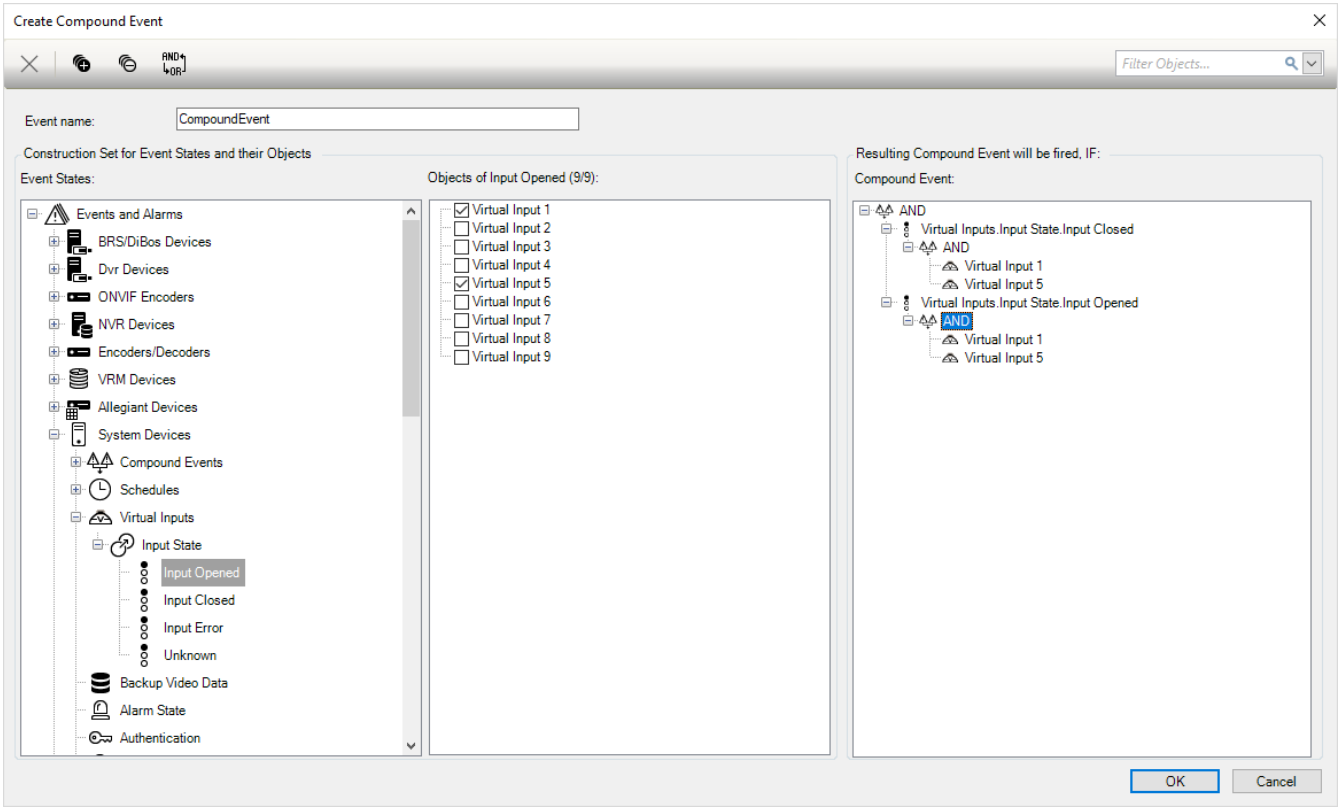
6. Klicken Sie in der Spalte **Skript** - **Zeitplan** auf eine Zelle und wählen Sie einen Zeitplan aus.
   Der Zeitplan bestimmt, wann das Kommandoskript ausgeführt wird.

Siehe
– *Seite Ereignisse, Seite 308*

23.8 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 308*

23.9 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 308*

23.10 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 325*
- *Seite Alarme, Seite 314*
- *Dialogfeld Bildfensterinhalt auswählen, Seite 316*
- *Dialogfeld Alarmoptionen, Seite 317*

23.11 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 315*

23.12 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 317*

23.13 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 317*
- *Dialogfeld „Textatenaufzeichnung“, Seite 313*

23.14 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.

23.15 Alarmaufzeichnung schützen

Hauptfenster > **Alarme**
Bevor Sie einen Alarm konfigurieren können, müssen Sie unter **Ereignisse** ein Ereignis konfigurieren.

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 317*

23.16 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 Farbstatus auf Karten ist nur möglich, wenn Sie die Option **Erweiterte Statusanzeige aktivieren (Hotspot auf Karten abhängig vom Status einfärben)** oder **Erweiterte Alarm-Anzeige aktivieren (Hotspot-Färbung in Karten je nach Alarm)** im Dialogfeld **Optionen** aktivieren.

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 *Gerät , Seite 314* auf der *Seite Alarme, Seite 314*.

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 308*
- *Dialogfeld „Optionen“ (Menü „Einstellungen“), Seite 115*

23.17 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.

24 Seite Benutzergruppen

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).

Registerkarte Benutzergruppen

Klicken Sie darauf, um die Seiten für die Konfiguration der Rechte der Standardbenutzergruppe anzuzeigen.

Registerkarte Enterprise User Groups (nur verfügbar mit gültiger Lizenz für Enterprise)

Klicken Sie hier, um die Seiten für die Konfiguration der Berechtigungen einer Enterprise User Group anzuzeigen.

Registerkarte Enterprise Access (nur verfügbar mit gültiger Lizenz für Enterprise)

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.
	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, in dem Sie Berechtigungen von einer gewählten Benutzergruppe in eine andere Benutzergruppe kopieren können.
	Klicken Sie darauf, um die Seiten für die Konfiguration der Berechtigungen dieser Gruppe anzuzeigen.
	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 – Passwort	– 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

Geben Sie eine Zeichenfolge ein, und drücken Sie zum Filtern der angezeigten Element die Taste ENTER. 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. Ein aktiver Filter wird durch gekennzeichnet. 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.

Um die Filterung abzubrechen, klicken Sie auf .

24.1 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
- Zuordnung einer 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

Zugeordnete LDAP-Gruppe
Geben Sie den Namen der LDAP-Benutzergruppe ein, die Sie für das System verwenden möchten.
Sie können auch auf ein Element in der Liste **LDAP Gruppen** doppelklicken.

LDAP Gruppen
Zeigt die verfügbaren LDAP-Benutzergruppen an. LDAP-Gruppen werden im Dialogfeld **LDAP Server-Einstellungen** konfiguriert.

Suche nach Gruppen
Klicken Sie hier, um die verfügbaren LDAP-Benutzergruppen in der Liste **LDAP Gruppen** anzuzeigen. Um eine Suche nach Benutzergruppen durchführen zu können, müssen Sie im Dialogfeld **LDAP Server-Einstellungen** die entsprechenden Einstellungen vornehmen.

Einstellungen
Klicken Sie hier, um das Dialogfeld **LDAP Server-Einstellungen** anzuzeigen.

Gruppe zuordnen
Klicken Sie darauf, um die ausgewählte LDAP-Gruppe dieser Benutzergruppe zuzuordnen.

Gruppe entfernen
Klicken Sie hier, um die Gruppe aus dem Feld **Zugeordnete LDAP-Gruppe** zu entfernen. Die Zuordnung der LDAP-Gruppe zur BVMS Benutzergruppe wird entfernt.

Reihenfolge ändern...
Klicken Sie hier, um die Liste **LDAP Nutzergruppenreihenfolge ändern** anzuzeigen. 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.

Siehe
- *Konfigurieren von LDAP-Einstellungen, Seite 364*
- *Zuordnen einer LDAP-Gruppe, Seite 365*
- *Festlegen eines Freigabezeitplans für Benutzeranmeldungen, Seite 366*

24.2 Seite Benutzereigenschaften

Hauptfenster > **Benutzergruppen** > Registerkarte **Benutzergruppen** > > 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.

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!
Es wird dringend empfohlen, ein bestimmtes Passwort für alle neuen Benutzer zuzuweisen und diese bei der Anmeldung zum Ändern ihres Passworts anzuhalten.

Hinweis!
Clients des Mobile Video Service, Web Client, der Bosch iOS-App und SDK-Clients können 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.

24.3 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.

Siehe

– *Hinzufügen eines Anmeldungspaars zu einer 4-Augen-Gruppe, Seite 363*

24.4 Seite Kamerafreigaben

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 **Operator Client 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 **Operator Client 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 **Operator Client 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 **Operator Client 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 **Operator Client Funktionen** freigegeben ist.

PTZ/ROI
Aktivieren Sie ein Kontrollkästchen, um die Verwendung der PTZ-Steuerung oder der ROI-Funktion dieser Kamera zu ermöglichen.
Sie können dieses Kontrollkästchen nur aktivieren oder deaktivieren, wenn die PTZ-Steuerung oder die ROI-Funktion einer Kamera auf der Seite **Operator Client 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 **Operator Client 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 **Operator Client Funktionen** freigegeben ist.

Referenzbild
Aktivieren Sie das Kontrollkästchen, um die Aktualisierung des Referenzbilds dieser Kamera zu ermöglichen.

24.5 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 367*

24.6 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*

24.7 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.

24.8 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.

24.9 Dialogfeld LDAP Server-Einstellungen

Hauptfenster > **Benutzergruppen** > Registerkarte **Benutzergruppen** > > Registerkarte **Bedienberechtigungen** > Registerkarte **Eigenschaften der Benutzergruppen** > Schaltfläche **Einstellungen**
oder

Hauptfenster > **Benutzergruppen** > Registerkarte **Enterprise User Groups** > > Registerkarte **Bedienberechtigungen** > Registerkarte **Eigenschaften der Benutzergruppen** > Schaltfläche **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 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.

Anonym
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.

Benutze die folgenden Zugangsdaten

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
– *Konfigurieren von LDAP-Einstellungen, Seite 364*

24.10 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.

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.: ! $ # %).

Neues Passwort eingeben: / Passwort bestätigen
Geben Sie das Passwort für diesen Management Server ein, und bestätigen Sie es.

Siehe
– *Richtlinie für sichere Passwörter , Seite 358*
– *Erstellen eines Enterprise Accounts, Seite 360*

24.11 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 367*

24.12 Seite „Bedienerfunktionen“

Hauptfenster> **Benutzergruppen** > Registerkarte **Benutzergruppen** > > Registerkarte **Bedienberechtigungen** > Registerkarte **Operator Client Funktionen**
oder

Hauptfenster > **Benutzergruppen** > Registerkarte **Enterprise User Groups** > > Registerkarte **Bedienberechtigungen** > Registerkarte **Operator Client 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.

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.

Alarmanzeige
Aktivieren Sie das Kontrollkästchen, um die Alarmanzeige freizugeben. Wenn Sie diese Option aktivieren, wird gleichzeitig die Option **Alarmverarbeitung** deaktiviert.

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.

Hinweis!
Konfigurieren Sie die Berechtigungen zur Einschränkung und Freigabe eines Benutzerkontos auf Ihrem DIVAR AN-Gerät je nach Bedarf. Erstellen Sie einen Benutzer in BVMS mit denselben Anmeldeinformationen und konfigurieren Sie die Berechtigungen für die Einschränkungen und Freigaben entsprechend.
Die Anzeige von beschränkten Videos wird dabei nicht beeinflusst und muss separat konfiguriert werden.

Video sperren
Aktivieren Sie das Kontrollkästchen, um die Beschränkung von Videodaten zuzulassen.

Videosperrung aufheben
Wählen Sie das Kontrollkästchen aus, um eine Beschränkung und eine Freigabe der Videodaten zu ermöglichen.

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.

Zugriff auf VRM-Monitor
Aktivieren Sie das Kontrollkästchen, um den Zugriff auf die VRM Monitor Software 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).

Personenverwaltung
Aktivieren Sie das Kontrollkästchen, um dem Benutzer von Operator Client zu ermöglichen, Personen für Person Identification-Alarme zu verwalten.

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 38*

24.13 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 367*

24.14 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 Alarmmodus oder nur den Alarmmodus 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.

Einstellungen beim Herunterfahren sichern

Aktivieren Sie das Kontrollkästchen, damit sich das System den letzten Zustand der Benutzeroberfläche merkt, wenn sich der Benutzer vom Operator Client abmeldet. Wenn das Kontrollkästchen deaktiviert ist, startet der Operator Client immer mit der konfigurierten Benutzeroberfläche.

Standardwert wiederherstellen

Klicken Sie darauf, um die Standardeinstellungen dieser Seite wiederherzustellen. Alle Listeneinträge werden auf ihre Standardeinstellungen zurückgesetzt.

24.15 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 Servers.

Server-Nummer

Anzeige der Nummer des Management Servers. Diese Nummer wird von einem Bosch IntuiKey Keyboard zur Auswahl des gewünschten Management Servers verwendet.

Zugriff

Klicken Sie auf die Kontrollkästchen, wenn Sie Zugriff auf den Management Server gewähren möchten. Dieser Management Server ist nun ein Enterprise Management Server.

Zugriff

Geben Sie den Namen des Enterprise Accounts ein, der auf dem Management Server konfiguriert wurde.

Enterprise Account Passwort

Klicken Sie darauf, um ein Dialogfeld zur Eingabe des Passworts des Enterprise Accounts zu öffnen, der auf dem Management Server konfiguriert wurde.

Enterprise Account Passwort
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 359*
- *Erstellung eines Enterprise Systems, Seite 86*
- *Konfigurieren der Serverliste für Enterprise System, Seite 86*

24.16 Seite „Konfigurationsberechtigungen“

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. Die Berechtigung zum Starten des Configuration Client beinhaltet Schreibschutz.

Anmelde-Berechtigungen
Aktivieren Sie das Kontrollkästchen, um eine Anmeldung beim Configuration Client zuzulassen.

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 der Kontrollkästchen **Benutzergruppen konfigurieren** und **Benutzer konfigurieren** ist aus Sicherheitsgründen ausgeschlossen.

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.

24.17 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 351*

24.18 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 358*

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**

24.18.1 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.

24.18.1.1 Im Offline-Modus arbeiten

Wenn Operator Client von einem Management Server getrennt wird, wird ein entsprechendes Symbol im Logischen Baum auf den 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.

Statusanzeige von Operator Client

Ein BVMS Operator Client gibt Ihnen ein visuelles und textbasiertes Feedback über die Zustände.

Dabei sind folgende Operator Client-Zustände möglich:

-

  Der Operator Client ist mit dem Management Server verbunden.

–

Der Operator Client ist nicht mit dem Management Server verbunden. Ein Grund ist möglicherweise die physische Trennung des Management Server vom Netzwerk.

–

Dieser Status kann nur nach einer neu aufgebauten Verbindung mit dem Management Server angezeigt werden. Sämtliche betroffenen Funktionen arbeiten wieder, aber die Konfiguration des Operator Client ist aufgrund einer neueren auf dem System vorhandenen Konfiguration veraltet. Melden Sie sich erneut an, um die Konfiguration zu aktualisieren.

–

Dieses Statussymbol wird angezeigt, wenn der Management Server über eine frühere BVMS Version als die Operator Client-Arbeitsstation verfügt.

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).

25 Konfigurieren von Benutzern, Berechtigungen und Enterprise Access

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 **Die Passwortsrichtlinie wird missachtet** angezeigt und er wird dazu aufgefordert, 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 **Die Passwortsrichtlinie wird missachtet** wird angezeigt und zeigt eine Liste mit allen Benutzern, für die kein Passwort festgelegt wurde.

Um die Konfiguration zu aktivieren, legen Sie die fehlenden Passwörter fest.

Siehe
- *Seite „Kontorichtlinien“, Seite 352*
- *Seite Eigenschaften der Benutzergruppen, Seite 336*
- *Seite Benutzereigenschaften, Seite 337*
- *Seite Eigenschaften des Anmeldungspaares, Seite 338*
- *Seite Kamerafreigaben, Seite 339*
- *Seite „Prioritäten für Steuerungen“, Seite 340*
- *Dialogfeld Freigaben für Benutzergruppen kopieren, Seite 341*
- *Seite Decoder-Freigaben, Seite 341*
- *Seite Ereignisse und Alarme, Seite 342*
- *Dialogfeld LDAP Server-Einstellungen, Seite 342*
- *Seite „Zugangsberechtigungen“, Seite 344*
- *Seite Logischer Baum, Seite 344*
- *Seite „Bedienerfunktionen“, Seite 345*
- *Seite Prioritäten, Seite 348*
- *Seite Benutzeroberfläche, Seite 349*
- *Seite „Server-Zugriff“, Seite 350*

25.1 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.

25.1.1 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 336*
- *Seite „Bedienerfunktionen“, Seite 345*
- *Seite Prioritäten, Seite 348*
- *Seite Benutzeroberfläche, Seite 349*

25.1.2 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 336*
- *Seite „Bedienerfunktionen“, Seite 345*
- *Seite Prioritäten, Seite 348*
- *Seite Benutzeroberfläche, Seite 349*
- *Seite „Server-Zugriff“, Seite 350*

25.1.3 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 das Passwort entsprechend der Passwortrichtlinie ein und bestätigen Sie es.
5. Klicken Sie auf **OK**.
   Ein neuer Enterprise Account wird dem 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 358*
- *Seite „Zugangsberechtigungen“, Seite 344*
- *Seite Logischer Baum, Seite 344*
- *Seite Ereignisse und Alarme, Seite 342*
- *Seite „Prioritäten für Steuerungen“, Seite 340*
- *Seite Kamerafreigaben, Seite 339*
- *Seite Decoder-Freigaben, Seite 341*

25.2 Erzeugen eines Benutzers

Hauptfenster > **Benutzergruppen** > Registerkarte **Benutzergruppen**
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. Klicken Sie auf , um das Passwort zu aktivieren.

Siehe
- *Seite Benutzereigenschaften, Seite 337*
- *Richtlinie für sichere Passwörter , Seite 358*
- *Seite Benutzergruppen, Seite 334*

25.3 Erzeugen einer 4-Augen-Gruppe

Hauptfenster > **Benutzergruppen** > Registerkarte **Benutzergruppen**
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.

Siehe
- *Hinzufügen eines Anmeldungspaars zu einer 4-Augen-Gruppe, Seite 363*
- *Seite Eigenschaften der Benutzergruppen, Seite 336*
- *Seite „Bedienerfunktionen“, Seite 345*
- *Seite Prioritäten, Seite 348*
- *Seite Benutzeroberfläche, Seite 349*

25.4 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.

Siehe

- *Erzeugen einer 4-Augen-Gruppe, Seite 362*
- *Seite Eigenschaften des Anmeldungspaares, Seite 338*

25.5 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 334*
- *Seite Benutzereigenschaften, Seite 337*
- *Richtlinie für sichere Passwörter , Seite 358*

25.6 Konfigurieren von LDAP-Einstellungen

Hauptfenster > **Benutzergruppen** > Registerkarte **Benutzergruppen** > > Registerkarte **Bedienberechtigungen**
oder

Hauptfenster > **Benutzergruppen** > Registerkarte **Enterprise User Groups** > > Registerkarte **Bedienberechtigungen**

Hinweis!
Geben Sie die Suchpfade korrekt ein. Falsche Pfade können die Suche auf einem LDAP-Server deutlich verlangsamen.

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.

Sie können LDAP-Gruppen in Standardbenutzergruppen oder in Enterprise User Groups konfigurieren.

So konfigurieren Sie LDAP-Einstellungen:
1. Klicken Sie auf die Registerkarte **Eigenschaften der Benutzergruppen**.
2. Nehmen Sie im Feld **LDAP-Eigenschaften** die erforderlichen Einstellungen vor.

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

Siehe
- *Dialogfeld LDAP Server-Einstellungen, Seite 342*
- *Seite Eigenschaften der Benutzergruppen, Seite 336*

25.7 Zuordnen einer LDAP-Gruppe

Hauptfenster > **Benutzergruppen** > Registerkarte **Benutzergruppen** > > Registerkarte **Bedienberechtigungen**
oder

Hauptfenster > **Benutzergruppen** > Registerkarte **Enterprise User Groups** > > Registerkarte **Bedienberechtigungen**

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.

So ordnen Sie eine LDAP-Gruppe zu:
1. Klicken Sie auf die Registerkarte **Eigenschaften der Benutzergruppen**.
2. Klicken Sie im Feld **LDAP-Eigenschaften** auf **Einstellungen**.
   Das Dialogfeld **LDAP Server-Einstellungen** wird angezeigt.
3. Geben Sie die Einstellungen des LDAP-Servers ein, und klicken Sie auf **OK**.

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.

- Doppelklicken Sie in der Liste **LDAP Gruppen** auf eine LDAP-Gruppe.
  Diese LDAP-Gruppe wird in das Feld **Zugeordnete LDAP-Gruppe** eingetragen.

Siehe
- *Dialogfeld LDAP Server-Einstellungen, Seite 342*
- *Seite Eigenschaften der Benutzergruppen, Seite 336*

25.8 Festlegen eines Freigabezeitplans für Benutzeranmeldungen

Hauptfenster > **Benutzergruppen** > Registerkarte **Benutzergruppen** > > Registerkarte **Bedienberechtigungen**
oder

Hauptfenster > **Benutzergruppen** > Registerkarte **Enterprise User Groups** > > Registerkarte **Bedienberechtigungen**
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.

25.9 Konfigurieren von Bedienberechtigungen

Hauptfenster > **Benutzergruppen** > Registerkarte **Benutzergruppen** > > Registerkarte **Bedienberechtigungen**
oder

Hauptfenster > **Benutzergruppen** > Registerkarte **Enterprise User Groups** > > Registerkarte **Bedienberechtigungen**
- 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 336*
- *Seite „Bedienerfunktionen“, Seite 345*
- *Seite Prioritäten, Seite 348*
- *Seite Benutzeroberfläche, Seite 349*

– *Seite „Server-Zugriff“, Seite 350*

25.10 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 344*
– *Seite Ereignisse und Alarme, Seite 342*
– *Seite „Prioritäten für Steuerungen“, Seite 340*
– *Seite Kamerafreigaben, Seite 339*
– *Seite Decoder-Freigaben, Seite 341*

25.11 Konfigurieren verschiedener Prioritäten

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 340*
– *Seite Prioritäten, Seite 348*

25.12 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.

26 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 369*
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 223*
   – *Hinzufügen eines Nur-Live-Encoders, Seite 223*
   – *Hinzufügen eines Encoders mit lokaler Archivierung, Seite 223*
3. Konfigurieren Sie ein Brandereignis für diese Kamera.
   – *Konfigurieren eines Brandereignisses, Seite 372*
4. Konfigurieren Sie den Alarm für das Brandereignis.
   – *Konfigurieren eines Feueralarms, Seite 372*

Siehe

- *Hinzufügen eines Encoders zu einem VRM-Pool, Seite 370*
- *Hinzufügen eines Nur-Live-Encoders, Seite 223*
- *Hinzufügen eines Encoders mit lokaler Archivierung, Seite 223*
- *Konfigurieren eines Brandereignisses, Seite 372*
- *Konfigurieren eines Feueralarms, Seite 372*

26.1 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.

26.2 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 183*.

Siehe

– *Hinzufügen eines Geräts, Seite 120*

26.3 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. Klicken Sie mit der rechten Maustaste auf das Feld und klicken Sie anschließend auf **Zellinhalt in Spalte kopieren**.
   In der Spalte **Status** wird die erfolgreiche Anmeldung mit angezeigt.
   Fehlgeschlagene Anmeldungen werden mithilfe von angezeigt.
   zeigt an, dass das Gerät ein erstes Passwort erfordert.
   Um das erste Passwort festzulegen, geben Sie es im Feld **Passwort** ein.
   Der Status ändert sich zu .
   Wiederholen Sie diesen Schritt für alle Geräte, die ein erstes Passwort benötigen.
   Hinweis: Solange Sie kein erstes Passwort für alle Geräte in der Liste festgelegt haben, die ein erstes Passwort benötigen, können Sie nicht fortfahren.
5. Klicken Sie auf **Fertig stellen**.
   Das Gerät wird zum Gerätebaum hinzugefügt.

26.4 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. Klicken Sie mit der rechten Maustaste auf das Feld und klicken Sie anschließend auf **Zellinhalt in Spalte kopieren**.
   In der Spalte **Status** wird die erfolgreiche Anmeldung mit angezeigt.
   Fehlgeschlagene Anmeldungen werden mithilfe von angezeigt.
   zeigt an, dass das Gerät ein erstes Passwort erfordert.
   Um das erste Passwort festzulegen, geben Sie es im Feld **Passwort** ein.
   Der Status ändert sich zu .
   Wiederholen Sie diesen Schritt für alle Geräte, die ein erstes Passwort benötigen.
   Hinweis: Solange Sie kein erstes Passwort für alle Geräte in der Liste festgelegt haben, die ein erstes Passwort benötigen, können Sie nicht fortfahren.
5. Klicken Sie auf **Fertig stellen**.
   Das Gerät wird zum Gerätebaum hinzugefügt.

26.5 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. Klicken Sie mit der rechten Maustaste auf das Feld und klicken Sie anschließend auf **Zellinhalt in Spalte kopieren**.
   In der Spalte **Status** wird die erfolgreiche Anmeldung mit angezeigt.
   Fehlgeschlagene Anmeldungen werden mithilfe von angezeigt.
   zeigt an, dass das Gerät ein erstes Passwort erfordert.
   Um das erste Passwort festzulegen, geben Sie es im Feld **Passwort** ein.
   Der Status ändert sich zu .
   Wiederholen Sie diesen Schritt für alle Geräte, die ein erstes Passwort benötigen.
   Hinweis: Solange Sie kein erstes Passwort für alle Geräte in der Liste festgelegt haben, die ein erstes Passwort benötigen, können Sie nicht fortfahren.
5. Klicken Sie auf **Fertig stellen**.
   Das Gerät wird zum Gerätebaum hinzugefügt.

26.6 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.

26.7 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.

27 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**.

28 Problembehandlung

Dieses Kapitel enthält Informationen zur Behebung bekannter Probleme im BVMS Configuration Client.

Probleme nach der Aktualisierung des Bosch Video Management System

Problem	Ursache	Lösung
Der NVR führt nach der Aktualisierung des Bosch Video Management System keine Aufzeichnungen mehr durch.	Die Verbindung zwischen dem NVR und Management Server war nach der Aktualisierung getrennt. Möglicherweise wurde durch die Aktualisierung die BVMS Datenbank auf dem Management Server geändert. Der NVR muss diese Änderungen „kennen“.	Stellen Sie die Verbindung zwischen dem NVR und Management Server wieder her.

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 376*
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 70* oder *Konfigurieren der Sprache des Operator Client, Seite 70*
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 376*

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 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.	Nehmen Sie keine Änderung vor.

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 377*

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	Ändern Sie die Einstellung in der Konfigurationsdatei des Operator Client in Mikrofon.

Problem	Ursache	Lösung
	einen Standardeintrag, der möglicherweise nicht mit Ihrer Systemkonfiguration übereinstimmt. Diese Einstellung wird bei jedem Start des Operator Client wiederhergestellt.	

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 Management System verbunden sind, können Sie die Anzahl reduzieren. Dadurch werden unnötige Systemlasten vermieden.	Siehe *Reduzieren der Anzahl der Allegiant Kameras, Seite 377*.

Support

Supportdienstleistungen erhalten Sie unter https://www.boschsecurity.com/xc/en/support/.

Bosch Security and Safety Systems bietet Support in diesen Bereichen:
- Apps und Tools
- Building Information Modeling
- Inbetriebnahme
- 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**: https://www.boschsecurity.com/xc/en/support/training/

28.1 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.

28.2 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.

28.3 Reduzieren der Anzahl der Allegiant Kameras

Zur Bearbeitung der Allegiant Datei benötigen Sie die Allegiant Master Control Software.

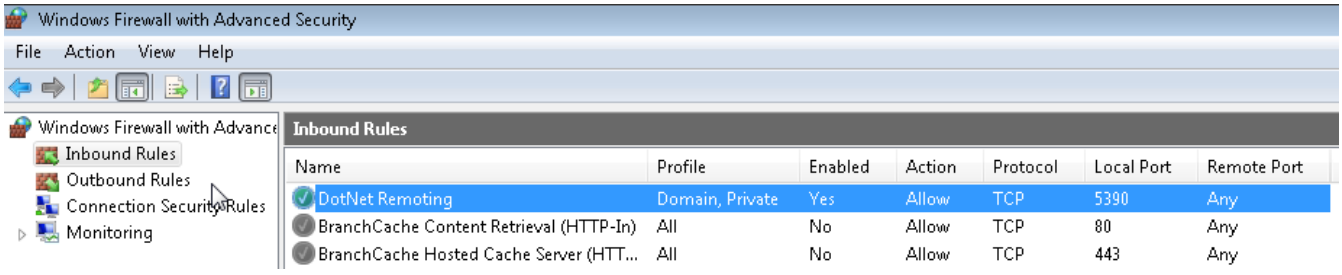
So reduzieren Sie die Anzahl der Allegiant Kameras:

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 120*).

28.4 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! Nutzen Sie für den Betrieb über das Internet sichere Verbindungen wie VPN oder Fernzugriff.
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.

Beispiel für eine einfache Eingehend-Regel in der Windows 7-Firewall.



Management Server-/Enterprise Management Server-Ports

Server (Listener)	Protokoll	Eingehende Ports	Client (Requester)	Bemerkung
Management Server	UDP	123	Encoder	TimeServer NTP

Server (Listener)	Protokoll	Eingehende Ports	Client (Requester)	Bemerkung
Management Server	TCP	5322	Operator Client,	SSH-Verbindung
Management Server	TCP	5389	ONVIF-Gerät	ONVIF-Proxy, Ereignisbenachrichtigung
Management Server	TCP	5390	Operator Client, Configuration Client,	.NET Remoting
Management Server	TCP	5392	Operator Client, Configuration Client, Mobile Video Service, BVMS SDK-Anwendung	WCF, gateway.push.apple.com
Management Server	TCP	5393	Operator Client, VRM, MVS	Data-Access-Service
Management Server	TCP	5395	Configuration Client, Operator Client	Benutzereinstellungen, Datenübertragung
Management Server	UDP	12544	SNMP-Client	BVMS SNMP-Port für GET-Abfragen

Video Recording Manager-Ports

Server (Listener)	Protokoll	Eingehende Ports	Client (Requester)	Bemerkung
VRM	TCP	554	RTSP-Client	RTSP-Stream abrufen
VRM	TCP	1756	Management Server, Configuration Client	über RCP+
VRM	UDP	1757	Management Server, Operator Client	Scan-Zielübermittlung
VRM	UDP	1758	Management Server, Configuration Client	Scan-Reaktion
VRM	UDP	1800	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

Mobile Video Service-Ports

Server (Listener)	Protokoll	Eingehende Ports	Client (Requester)	Bemerkung
Mobile Video Service	TCP	80	Management Server, Operator Client, Configuration Client, HTML-Client, mobile Apps	Zugriff über http
Mobile Video Service	TCP	443	Management Server, Operator Client, Configuration Client, HTML-Client, mobile Apps	Zugriff über https
Mobile Video Service	TCP	2195	Apple Push-Benachrichtigung	Mac iOS
Mobile Video Service	UDP	1064-65535	Encoder, VRM	
Mobile Video Service-Transcoder	TCP	5382	Mobile Video Service-Mobilfunkanbieter	Medienstream
Mobile Video Service-Transcoder	TCP	5385	Mobile Video Service-Mobilfunkanbieter	Medienstream
Mobile Video Service BVMS Anbieter	TCP	5383	Operator Client	Medienstream
Mobile Video Service-Mobilfunkanbieter	TCP	5384	HTML-Client, mobile Apps	Medienstream
Mobile Video Service-Transcoder	TCP	5385	Mobile Video Service-Mobilfunkanbieter	Medienstream

iSCSI-Speichersystemports

Konfigurieren Sie die Portweiterleitung am angeschlossenen Router für dieses Gerät.

Server (Listener)	Protokoll	Eingehend-Ports	Client (Requester)	Hinweis
iSCSI-Speichersystem	TCP	3260	Encoder, VRM, Configuration Client	

Bosch Video Streaming Gateway-Ports

Server (Listener)	Protokoll	Eingehende Ports	Client (Requester)	Bemerkung
Bosch Video Streaming Gateway	TCP	8756-8762	VRM, Management Server, Configuration Client	RCP+

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	1757	VRM Configuration Client	Scan-Zielübermittlung
Bosch Video Streaming Gateway	TCP	1758	VRM Configuration Client	Scan-Reaktion
Bosch Video Streaming Gateway	TCP	1800	VRM Configuration Client	Scan-Ziel für Multicast
Bosch Video Streaming Gateway	UDP	1064-65535	Encoder, VRM	

ONVIF-Kameraports

Konfigurieren Sie die Portweiterleitung am angeschlossenen Router für dieses Gerät.

Server (Listener)	Protokoll	Eingehende Ports	Client (Requester)	Bemerkung
ONVIF-Kamera	TCP	80	Management Server, VSG, Configuration Client, Operator Client	Zugriff über http
ONVIF-Kamera	TCP	443	Management Server, VSG, Configuration Client, Operator Client	Zugriff über https
ONVIF-Kamera	RTSP	554	Management Server, VSG, Configuration Client, Operator Client	

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	Live-Streaming
Operator Client	TCP	443	Encoder	Fernzugriff, verschlüsselte Live-Ansicht

Encoder-Ports

Konfigurieren Sie die Portweiterleitung am angeschlossenen Router für dieses Gerät.

Server (Listener)	Protokoll	Eingehende Ports	Client (Requester)	Bemerkung
Encoder	TCP	1756	Decoder, Management Server, VRM, Operator Client, Configuration Client, BVMS SDK Anwendung	über RCP+
Encoder	UDP	1757	Decoder, Management Server, Operator Client	Scan-Ziel
Encoder	UDP	1758	Decoder, Management Server, Operator Client	Scan-Reaktion
Encoder	UDP	1800	Decoder, Management Server, Operator Client	Scan-Ziel für Multicast
Encoder	TCP	80	Operator Client, BVMS SDK-Anwendung, VSG	Zugriff über http
Encoder	TCP	443	Operator Client, BVMS SDK-Anwendung, VSG	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

Optionale Encoder-Ports

Server (Listener)	Protokoll	Eingehende Ports	Client (Requester)	Bemerkung
FTP	TCP	21		
SSDP	UDP	1900		
UPnP	UDP	3702		
SRTSP	UDP	9554		
RTSP-Senden	UDP	15344, 15345		

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	über RCP+
Decoder	UDP	1757	Management Server, Operator Client	Scan-Ziel
Decoder	UDP	1758	Management Server, Operator Client	Scan-Reaktion

Server (Listener)	Protokoll	Eingehende Ports	Client (Requester)	Bemerkung
Decoder	UDP	1800	Management Server, Operator Client	Scan-Ziel für Multicast-Netzwerk
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

BRS/DiBos-Ports

Server (Listener)	Protokoll	Eingehende Ports	Client (Requester)	Hinweis
DiBos 8.7/ BRS 8.10	TCP	808	Management Server, Configuration Client	Webservice Für DiBos Version 8.7 wird ein Patch benötigt.
Wahlweise:				
BRS/DiBos	TCP	135	Operator Client, Management Server, Configuration Client	DCOM, wird verwendet, wenn der Webservice nicht funktioniert oder die verwendete DiBos-Version keinen Webservice unterstützt. Firewall muss deaktiviert sein.
BRS/DiBos	UDP	135	Operator Client, Management Server, Configuration Client	DCOM, wird verwendet, wenn der Webservice nicht funktioniert oder die verwendete DiBos-Version keinen Webservice unterstützt. Firewall muss deaktiviert sein.

DVR-Ports

Konfigurieren Sie die Portweiterleitung am angeschlossenen Router für dieses Gerät.

Server (Listener)	Protokoll	Eingehend-Ports	Client (Requester)	Hinweis
DVR	TCP	80	Management Server, Configuration Client, Operator Client	Zugriff über http

Barco Monitorwand

Server (Listener)	Protokoll	Eingehend-Ports	Client (Requester)	Hinweis
Barco Monitorwand	TCP	1756	Management Server, Operator Client, Configuration Client, BVMS SDK-Anwendung	über RCP+
Barco Monitorwand	UDP	1757	Management Server, Operator Client	Scan-Ziel
Barco Monitorwand	UDP	1758	Management Server, Operator Client	Scan-Reaktion
Barco Monitorwand	UDP	1800	Management Server, Operator Client	Scan-Ziel für Multicast-Netzwerk

PID, Person Identification-Ports

Server (Listener)	Protokoll	Eingehende Ports	Client (Requester)	Bemerkung
PID	TCP	8443	Management Server	Zugriff über https

LPR, BVMS Geräteadapter-Ports

Server (Listener)	Protokoll	Eingehende Ports	Client (Requester)	Bemerkung
BVMS Geräteadapter	TCP	32000	Tattile Kamera	VRC

AMS, Access Management System-Ports

Server (Listener)	Protokoll	Eingehende Ports	Client (Requester)	Bemerkung
AMS	TCP	62904	Management Server	Zugriff über https

28.5 Ermöglicht die Protokollierung von ONVIF-Ereignissen

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.

Zum Aktiveren der Protokollierung:

1. Öffnen Sie die Datei *%programfiles(x86)%\Bosch\VMS\AppData\Server \CentralServer\BVMSLogCfg.xml* in einen entsprechenden Editor, zum Beispiel Notepad. Starten Sie die Anwendung Notepad als Administrator.
2. Navigieren Sie zur Zeile, die nachfolgenden String enthält:
   Add logging for onvif events of a device by network address
   Die kommentierte Zeile enthält eine kurze Erklärung.
3. Als Protokollnamen geben Sie *OnvifEvents.<Networkaddress>* ein.
   Geben Sie nur *OnvifEvents* ein, um das Ereignis für alle ONVIF-Geräte zu protokollieren.
4. Geben Sie als Pegelwert *DEBUG* für alle eingehenden und abgehenden Ereignisse ein.
   Geben Sie *INFO* für alle abgehenden Ereignisse ein.
   Geben Sie *WARN* oder *ERROR* zum Deaktivieren ein.

Die folgenden Zeilen zeigen ein Beispiel für die Protokollierung der Ereignisse von Gerät 172.11.122.22 mit allen abgehenden und eingehenden Ereignissen:

```
<logger name="OnvifEvents.172.11.122.22" additivity="false">
<level value = "DEBUGGEN"/>
<appender-ref ref="OnvifRollingFileAppender"/>
</logger>
```

Siehe

- *Konfigurieren einer ONVIF-Mapping-Tabelle, Seite 244*
- *ONVIF-Ereigniszuordnung, Seite 37*

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.

Aktivierungsschlüssel

Nummer, die der Benutzer zur Aktivierung der erworbenen Lizenzen eingeben muss. Sie erhalten den Aktivierungsschlüssel, nachdem Sie die Berechtigungsnummer im Software License Manager des Bosch Security System eingegeben haben.

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.

Berechtigungsnummer

Nummer, die Sie von Bosch für die bestellten Softwarelizenzen erhalten. Sie müssen die Berechtigungsnummer im Software License Manager des Bosch Security System eingeben, um den Aktivierungsschlüssel zu erhalten. Darüber hinaus benötigen Sie die Computersignatur, um die erworbenen Lizenzen zu aktivieren.

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- und aufgezeichneten Videobildern einer einzelnen Kamera, Karte oder HTML-Datei verwendet.

Bildfensterbereich

Container für Bildfenster, strukturiert durch eine Bildfensteranordnung.

Bildfensterleiste

Symbolleiste eines Bildfensters.

BIS

Building Integration System

Bosch ATM/POS-Bridge

Empfängt Zeichenfolgen über ein serielles Kabel/ eine COM-Schnittstelle und leitet diese Zeichenfolgen über ein Ethernet-Kabel (TCP/IP) weiter. Bei den Zeichenfolgen handelt es sich gewöhnlich um POS-Daten oder ATM-Transaktionen.

BRS

Bosch Recording Station. Software für Video-Aufzeichnung und Video-Verwaltung

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.

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.

Fernzugriff

Der Fernzugriff macht die Verbindung verschiedener privater Netzwerke mit öffentlichen Netzwerken möglich. Es kann gleichzeitig oder nacheinander auf mehrere Netzwerke mit privaten (lokalen) Netzwerkadressen durch Operator Client-Computer über öffentliche Schnittstellen (Router) zugegriffen werden. Aufgabe des Routers ist die Übersetzung des eingehenden öffentlichen Netzwerkverkehrs in die entsprechende private Netzwerkadresse. Der Benutzer des Operator

Client können auf den Management Server oder Enterprise Management Server und ihre Geräte per Fernzugriff zugreifen.

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

JPEG

Joint Photographic Expert Group. Codierung von Standbildern.

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.

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.

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.

NoTouchDeployment

Methode für das automatische Herunterladen, Installieren und Ausführen von .NET-Anwendungen ohne Änderung der Registrierung oder gemeinsamer Systemkomponenten. Im Bosch Video Management System wird No-Touch Deployment zur Aktualisierung der Operator-Clients vom Management-Server eingesetzt. Die Aktualisierung erfolgt, wenn eine neue Version auf dem Management-Server abgelegt wird und jeder Benutzer sich beim Operator Client anmeldet. Wenn Sie mit einem Operator Client gegen mehrere Management-Server-Computer arbeiten, verwendet das No-Touch Deployment nur die Software-Version, die auf dem Management-Server gespeichert ist, an dem der Operator Client sich zuletzt erfolgreich angemeldet hatte. Sobald Sie versuchen, sich bei einem anderen Management-Server mit einer anderen Anwendungsversion anzumelden, zeigt diese den Management-Server als nicht online an, da die Software-Versionen nicht übereinstimmen.

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.

Port Mapping

Über Port Mapping können Remote-Computer eine Verbindung zu einem bestimmten Computer oder Dienst innerhalb eines privaten LAN (Local Area Network) herstellen.

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.

URI

Uniform Resource Identifier. String für die Identifikation einer Netzwerk-Ressource. Jede URI besteht aus Schema, Autorisierung, Pfad, Abfrage, Fragment. Nur Schema und Fragment sind obligatorisch für Mobile Video Service. Beispiel: http:<scheme>//example.com<authority>/over/therepath>?name=ferret<query>#nose<fragment>

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

VIDOS NVR

VIDOS Network Video Recorder. Software, die Audio- und Videodaten von IP-Encodern auf einem RAID 5-Disk-Array oder einem anderen Datenträger speichert. VIDOS NVR enthält Funktionen zum Wiedergeben und Abrufen aufgezeichneter Videodaten. Sie können Kameras in das Bosch Video Management System integrieren, die mit einem VIDOS NVR-Computer verbunden sind.

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.

Index

Ziffern

4-Augen-Prinzip 338

A

Absturz
Configuration Client 376
aktivieren 93
Bosch Video Management System 75
Frühere Konfiguration 94
Aktivierung 96
Konfiguration 93
verzögert 93, 105
Aktualisieren 374
Gerätefunktionen 83, 225
Alarmaufzeichnung 315, 330, 331
Alarmaufzeichnung schützen 330, 331
Alarmaufzeichnungsmodus 297, 299
Alarme
Sortierreihenfolge 315
Alarmkarte 316
Alarmpriorität 367
Alarmsequenz 315, 330
Alarmsirenen ausschalten 347
Allegiant
CCL-Emulation 121, 163
Firmware-Version 48, 50
Netzwerk-Host-Programm 57
PTZ-Kamera 290
Satellitensystem 58
Steuerungskanal 57, 58
zu viele Kameras 377
Allegiant CCL-Befehle 59
Allegiant CCL-Emulation 162
Zugriff verweigert 162
Allegiant Datei 377
Allegiant Kreuzschiene 120, 132
Allgemeine Alarmeinstellungen 329
Analoge Matrix 132
analoge Monitorgruppe 115, 121
ANR 85, 233, 289
Anzeigemodi einer Panoramakamera 39
Arbeitsstation 115
ASF 346
ATM POS-Gerät 120
Audio-Intercom-Funktion 347
auf Hilfe zugreifen 14
Aufzeichnungsmodus
automatisch 185
Failover 184
Aufzeichnungspräferenzen 236
Aufzeichnungsqualität 294
Aufzeichnungstabelle 287
Authentizität prüfen 228
automatische Abmeldung 116
Automatische Alarmanzeige 36
automatische Neuanmeldung 93
Automatischer Aufzeichnungsmodus 185
automatischer Neustart 93
Automatisches Popup-Verhalten bei Alarm 36

B

Befehlsscript
Bosch Script API Hilfe 90
Beispiele 98
Bosch ATM/POS-Bridge hinzufügen 98
Hinzufügen, Bosch Allegiant Eingangsalarm 99
VRM Aufzeichnung konfigurieren 99
Benutzer
Entfernen 337
Löschen 337
Benutzer entfernen 337
Benutzer löschen 337
Benutzerereignisschaltfläche 325, 326
Benutzergruppen 334, 336
Benutzeroberflächeneinstellungen
VIP XD 144
Benutzerspezifische Ereignisse 308, 327
Berechtigungen 263, 265
Besondere Tage 284
Bildformat 16:9 349
blinkende Gerätesymbole 309, 332
Bosch ATM/POS-Bridge hinzufügen 98
Bosch IntuiKey Keyboard 48, 49, 50, 53, 121, 135, 144, 158
Bosch Script API Hilfe 90
Bosch Video Management System 17
aktivieren 75
aktualisieren 374
GUI-Sprache 375
Lizenzierung 75
Online-Hilfe 14
Übersicht 17
BVIP-Decoder 83, 225
hinzufügen 139, 186, 215
BVIP-Decoder hinzufügen 139, 186, 215
BVIP-Encoder 83, 225
hinzufügen 139, 186, 215
BVIP-Encoder hinzufügen 139, 140, 186, 215, 225

BVIP-Encoder:Hinzufügen 140, 225
BVIP-Gerät
Passwort 142, 222, 230
Webseite 222

C

CABAC 296
CCL-Emulation 163
CCTV-Keyboard 158
Verbindungsverlust 375
CHAP-Passwort 177
Client-Kommandoskript
Alarm angenommen 320
Beim Starten ausgeführt 91, 92, 136
CLL-Befehle 162
codecs 297
Codieren auf NVRs 119, 177
Connection String 116

D

Datenblatt 18
DCZ-Keyboard 158
Decoder
Bosch IntuiKey Keyboard 144
Decoder:Ziel-Passwort 216, 230
DiBos
Version 48, 50
DiBos-Gerät 120
Digitaler Videorekorder 120
digitales Keyboard 158
Dome-Kamera 302, 304
Doppelte IP-Adressen 106
Drucken der Hilfe 15
DSA E-Series 190, 191, 196, 197
DTP3N 153
Dual Streaming 137
Duale Aufzeichnung 26, 193, 306
Duplizieren eines Ereignisses 325
DVR-Gerät 129
DynDNS 73

E

Einbruchmeldezentrale 164, 165
E-Mail-Gerät 120
Encoder
hinzufügen 183, 191, 222, 370
Webseite 222
Encoder hinzufügen 183, 191, 222, 370
Encoder: Failover-Aufzeichnungsmodus 235
Enterprise Management Server 350
Enterprise System 21, 86
Enterprise User Groups 334
Erstellen
Befehlsscript 90
Erstkamera 146
Erzwungenen Passwortschutz deaktivieren 106
Erzwungener Passwortschutz 106
exportieren
ASF 346
Kameratabelle 293
Kommandoskript 92
Konfigurationsdaten 95
Konfigurationsdaten an OPC 96

F

Failover VRM 26
Failover-Aufzeichnungsmodus 184
Encoder 235
Failover-VRM 123, 181
Feiertage 284
Fernzugriff 73, 86, 117, 125
Feuererkennungskamera 369
Filtern 107, 108, 109, 119, 264, 287, 308, 311, 314, 336
Firewall 208
Firmware-Upgrade
Bosch IntuiKey Keyboard 53
Forensic Search 136
Forensische Suche 100, 135, 137
Frühere Konfiguration 94

G

Gerät verschieben 201, 212, 231
Geräte ohne Passwortschutz 93
Geräteaustausch 77, 79
Gerätebaum 119, 177, 263
Gerätebereich 263
Gerätefunktionen
Aktualisieren 83, 225
Geräte-Monitor 96
getrennt 355
Globales Standardpasswort 69, 93, 106
große LUN 185, 189, 195, 201, 202
große LUNs 185
Grundkonfiguration 198
GUI-Sprache 375

H

H.264 296
H.264-Anti-Blocking-Filter 296
HD-Kameras 349
Hilfe 14, 15
Hinzufügen, Bosch Allegiant Eingangsalarm 99

Hotspots 263
HTML-Dateien 263

I

I/O-Module 121
importieren
Kommandoskript 91
Ressourcen-Dateien 266
Inaktivität 116
Inhalt ersetzen 266
Intercom-Funktion 347
iPad 163, 164
IP-Adresse
ändern 107, 120, 138, 234
Duplikate 106
IP-Adresse ändern 107, 120, 138, 234
iPhone 163, 164
IQN-Mapping 198
iSCSI-Gerät 198
iSCSI-Passwort 177
iSCSI-Speicherpool 173, 194
iSCSI-Speichersystem 194

K

Kamerarundgang 263, 272, 273
Kamerasequenz 263, 272, 273
Karte
blinkende Hotspots 309, 332
Karten 263
Karten-Link 274
KBD Universal XF Keyboard 48, 49, 121, 135
kein Passwort 93
Klingeln deaktivieren 347
Kommandoscript
Exportieren 92
Importieren 91
Kommandoskript 263, 270
Kompatibilitätsmodus 38
Komplettsystem 61
Konfigurationsassistent
Mobile Video Service 61
Konfigurationsdaten
Exportieren 95
Konfigurationsdaten an OPC
exportieren 96
Kontaktklappern 328
Kopieren und einfügen 292

L

LDAP-Benutzer 336
LDAP-Benutzergruppen 336, 365
LDAP-Gruppe 365
leeres Passwort 93
Link zu Karte 274
Lizenzierung
Bosch Video Management System 75
Konfigurationsassistent 69
Stratus-Server 75
Logbuchdatenbank 116
Connection String 116
Logischer Baum 265, 320
LUNS
größer als 2 TB 185

M

Management Server 18, 21, 355
Manuelle Aufzeichnung 39, 315, 330
Mehrfachauswahl 265, 266
Melder
Umgehen, 347, 348
Menübefehle 102
MIC IP 7000 373
Mobile Video Service 61
Mobiler Video-Service 163
Monitorgruppe 145, 315, 320
Einfachanzeige 145
Erstkamera 145
hinzufügen 145
OSD 145
Startkamera 145
Vierfachteilung 145
Multicast 208
Multimonitorbetrieb 349

N

Nachalarmdauer 299
Nachereignisdauer 299
Nachereigniszeit 297
Nachereigniszeit 291
Netzwerkadresse
Ändern 138, 234
Netzwerkadresse ändern 138, 234
Netzwerküberwachungsgerät 120
Neue DiBos Geräte 130, 131
neue DiBos-Geräte 128
nicht verbunden 355
NVR 18

O

Offline 337, 355
Offline-Modus 354
Online-Anwendungshilfe 14
ONVIF Media profile 289
ONVIF Protokollierung 383

ONVIF-Ereignisse protokollieren 383
OPC-Server 374
Operator Client 17, 265

P

Panoramakamera
Anzeigemodi 39
Passwort 142, 222, 230
Passwort ändern 142, 180, 222, 230, 337
Passwort fehlt 93
Passwortänderung 142, 180, 222, 230, 337
Peripheriegerät 120
Person Identification
Hinzufügen eines Person Identification Device 169
Hinzufügen von Kameras zu Person Identification Device 171
Person Identification Device 168
Pool
ändern 231
Gerät verschieben 201, 212, 231
VRM 180, 231
Pool ändern 231
Pool hinzufügen
VRM 180
Pooling 173, 194
Port Mapping 73, 117
Portweiterleitung 73
Primärer Failover-VRM 181
Primärer VRM 26, 123, 175
Profil 294
Protokollierung 178, 325, 328
PTZ-Bedienfeld
Sperren 340
PTZ-Kamera 302, 304
Allegiant 290
PTZ-Sperre 340, 348, 367
PTZ-Steuerung
Sperren 348

R

RAM-Aufzeichnung 299
Redundante Aufzeichnung 26
Redundanter VRM 26, 123, 182
Region of Interest 289, 340
Relais
Störung 277
Remote-Export 39
Ressourcen-Dateien 266
importieren 266
ROI 304, 340
ROI-Funktion 289
Routed Access 124

S

Scan
Encoder 122
Encoder mit lokaler Archivierung 122
Nur-Live-Encoder 122
VRM 123
scannen
in Subnetzen 115
über Subnetze 115
Scannen nach IP-Adresskonflikten 106
Seite "Allegiant CCL-Emulation" 162
Sekundäre Aufzeichnung 193, 306
Sekundärer Failover-VRM 181
Sekundärer VRM 26, 123, 176
Sequenz 273
Server ID 79
Server Lookup 125
Server-Initiatorname 177
Server-Liste
Spalten hinzufügen 87, 125
Spalten löschen 87, 125
Server-Netzwerk 218, 219, 220
SMS-Gerät 120
SNMP-Einstellungen 114
SNMP-Traps
Abrufen 114
Senden 114
Softwareaktualisierung 374
Sortierreihenfolge
Alarme 315
Sperren 367
Sprache 375
Configuration Client 115
Operator Client 336
Sprechtaste 347
Standard-IP-Adresse 106
Standardkonfiguration 198
Standardpasswort 93, 106
Standard-Stream 135, 289
Status 96, 102, 107, 108, 109
Status aktualisieren 102, 107, 108, 109
Steuern einer Kamera 297
Steuerung einer Kamera 100
Störungsrelais 277
Stratus-Server
Lizenzierung 75

Stream 289, 301
Suchen
Geräte 107, 108, 109, 119, 264, 287, 308, 311, 314, 336
Information in der Hilfe 14
Synchronisieren
VRM-Konfiguration 184
Synchronisierung 84
Systemanforderungen 18

T

Textdaten einer Daueraufzeichnung hinzufügen 313
Textdatenaufzeichnung auslösen 330, 331
Transcoder-Dienst 163, 164
Typennummer 111

U

Übernehmen, PTZ-Steuerung 367
UHD-Kameras 137
Umgehen
Melder 347, 348
Unabhängiger Operator Client 354
Unmanaged Site hinzufügen 218, 220
Unzuverlässiges Netzwerk 163

V

verbinden
Allegiant Kreuzschiene und BVMS 54
Bosch IntuiKey Keyboards und BVMS 50
Versionshinweise 18
verzögerte Aktivierung 93, 105
Video Analytics 167
Video Streaming Gateway 120
Videoanalysegerät hinzufügen 168
VIDEOJET 7000 connect 373
Vierfachteilung 145
VIP X1600 XFM4 296
VIP XD 48
Vierfachteilung 145
VIP XD
Benutzeroberflächeneinstellungen 144
Halbduplex-Modus 144
virtueller Eingang 120
Voralarmaufzeichnung 299
Voreingestellte Positionen entfernen 302
Vorereignisdauer 299
Vorereigniszeit 297
Vorereigniszeit 291
VPN 73
VRM
Failover 26, 123, 181
hinzufügen 174
pool 180, 231
Pool hinzufügen 180
Primär 26, 175
Primärer Failover 181
Primärspannung 123
Redundant 26, 123, 182
Sekundär 26, 176
Sekundärer 123
Sekundärer Failover 181
VRM 3.50 184
VRM hinzufügen 174
VRM Aufzeichnung konfigurieren 99
VRM-Speicherpool 173, 194

W

WAN 73, 117
Webclient 164
WLAN 163, 164

Z

Zeitserver 84
Zeitsynchronisation 84
Zeitzone 218, 219
Zielbereich 304
Ziel-Datenrate 296
Ziel-Passwort 216, 230
zu viele Allegiant Kameras 377
Zugriff verweigert
Allegiant CCL-Emulation 162
Zusammengesetzte Ereignisse 308, 327
Zutrittskontrollsysteme 166

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Netherlands
www.boschsecurity.com
© Bosch Security Systems B.V., 2020