

BVMS

Innehållsförteckning

1	Använda Hjälp	14
1.1	Hitta information	14
1.2	Skriva ut hjälpen	15
2	Inledning	16
2.1	BVMS-utgåvor	17
2.2	BVMS-licensaktiveringsöversikt	18
3	Systemöversikt	20
3.1	Maskinvarukrav	21
3.2	Programvarukrav	21
3.3	Licenskrav	21
4	Koncept	22
4.1	BVMS-designbegrepp	22
4.1.1	Ett enda Management Server-system	22
4.1.2	Enterprise System	23
4.1.3	Server Lookup	24
4.1.4	Unmanaged site	25
4.2	Inspelning	26
4.2.1	ANR (Automated Network Replenishment)	27
4.2.2	Dubbel strömning/reservinspelning	28
4.2.3	VRM-inspelningslägen	29
4.2.4	Uppspelning av VRM-inspelningskällor	32
4.2.5	Översikt över lagringsrelaterade händelser	37
4.3	Larmhantering	38
4.4	ONVIF-händelsemappning	39
4.5	Utloggning vid inaktivitet	40
4.6	Versionsoberoende Operator Client	41
4.6.1	Arbeta med kompatibilitetsläget	41
4.7	Visningslägen för en panoreringskamera	42
4.7.1	360° panoreringskamera – golv- eller takmonterad	42
4.7.2	180° panoreringskamera – golv- eller takmonterad	44
4.7.3	360° panoreringskamera – väggmonterad	45
4.7.4	180° panoreringskamera – väggmonterad	46
4.7.5	Beskuren vy på en panoreringskamera	47
4.8	SSH-tunnel	48
4.9	Flera sökvägar	48
5	Maskinvara som kan användas	49
5.1	Installation av maskinvara	49
5.2	Installera ett KBD Universal XF-tangentbord	50
5.3	Ansluta ett Bosch IntuiKey-tangentbord till BVMS	50
5.3.1	Scenarion för Bosch IntuiKey-tangentbordsanslutningar	50
5.3.2	Ansluta ett Bosch IntuiKey-tangentbord till en avkodare	52
5.3.3	Uppdatera Bosch IntuiKey-tangentbordets inbyggda programvara	53
5.4	Ansluta Bosch Allegiant-matrisen till BVMS	54
5.4.1	Översikt av Bosch Allegiant-anslutning	54
5.4.2	Konfigurera kontrollkanalen	56
5.4.3	Bosch Allegiant koncept för satellitsystem	58
5.5	Allegiant CCL-kommandon som stöds i BVMS	59
6	Komma igång	61

6.1	Installera programvarumodulerna	61
6.2	Använda konfigurationsguiden	61
6.3	Starta Configuration Client	68
6.4	Konfigurera språket för Configuration Client	69
6.5	Konfigurera språket för Operator Client	69
6.6	Söka efter enheter	70
6.7	Få åtkomst till systemet	70
6.8	Använda serversökning	70
6.9	Aktivera programvarulicenserna	71
6.9.1	Dialogrutan Licenshanterare (menyn Verktyg)	71
6.9.2	Dialogrutan Lägg till licens	72
6.9.3	Dialogrutan Licenshanterare (menyn Verktyg)	72
6.10	Underhålla BVMS	73
6.11	Byta en enhet	74
6.11.1	Byta en MS/EMS	74
6.11.2	Byta en VRM	75
6.11.3	Byta en kodare eller avkodare	76
6.11.4	Byta en operatörs klient	78
6.11.5	Sluttester	78
6.11.6	Återställa Divar IP 3000/7000	79
6.12	Konfigurera tidssynkronisering	79
6.13	Konfigurera lagringsmediet för en kodare	79
7	Skapa ett Enterprise System	81
7.1	Konfigurera serverlistan för Enterprise System	81
7.2	Skapa en Enterprise User Group	82
7.3	Skapa ett Enterprise Account	82
7.4	Tokenbaserad autentisering	83
8	Konfiguration av kommandoskript	85
8.1	Hantera kommandoskript	85
8.2	Konfigurera ett kommandoskript som startas automatiskt	86
8.3	Importera ett kommandoskript	86
8.4	Exportera ett kommandoskript	86
8.5	Konfigurera ett startkommandoskript (inställningssidan)	87
9	Hantera konfigurationsdata	88
9.1	Aktivera arbetskonfigurationen	88
9.2	Aktivera en konfiguration	89
9.3	Exportera konfigurationsdata	89
9.4	Importera konfigurationsdata	90
9.5	Exportera konfigurationsdata till OPC	91
9.6	Kontrollera status för kodare/avkodare	91
9.7	Konfigurera SNMP-övervakning	91
9.8	Skapa en rapport	91
10	Konfigurationsexempel	93
10.1	Lägga till en Bosch ATM/POS-brygga	93
10.2	Lägga till ett Bosch Allegiant-ingångslarm	94
10.3	Lägga till och konfigurera 2 Dinion IP-kameror med VRM-inspelning	94
11	Globala Configuration Client-fönster	96
11.1	Konfigurationsfönster	96
11.2	Menykommandon	97

11.3	Dialogrutan Aktiveringshanteraren (menyn System)	99
11.4	Aktivera dialogrutan Konfiguration (menyn System)	100
11.5	Dialogrutan Inledande enhetsskanning (menyn Maskinvara)	100
11.6	Skydda enheter med dialogrutan Globalt standardlösenord (menyn Maskinvara)	100
11.7	Skydda iSCSI-lagringar med dialogrutan för CHAP-lösenordet (maskinvarumenyn)	101
11.8	Dialogrutan Ändra enhetslösenord (menyn Maskinvara)	101
11.9	Dialogrutan Uppdatera enhetens fasta programvara (menyn Maskinvara)	102
11.10	Dialogrutan Ändra enhets-IP och nätverksinställningar (menyn Maskinvara)	103
11.11	Dialogrutan Enhetsövervakaren (menyn Maskinvara)	105
11.12	Dialogrutan Licenshanterare (menyn Verktyg)	105
11.13	Dialogrutan Licenshanterare (menyn Verktyg)	106
11.14	Dialogrutan Lägg till licens	107
11.15	Dialogrutor för rapporter (menyn Rapporter)	107
11.15.1	Dialogrutan Inspelningsscheman	107
11.15.2	Dialogrutan Schemalagda inspelningsinställningar	107
11.15.3	Dialogrutan Uppgiftsscheman	107
11.15.4	Dialogrutan Kameror och parametrar för inspelning	107
11.15.5	Dialogrutan Inställningar för inspelningskvalitet	107
11.15.6	Dialogrutan Händelseinställningar	107
11.15.7	Dialogrutan Inställningar för sammansatta händelser	107
11.15.8	Dialogrutan Larminställningar	108
11.15.9	Dialogrutan Konfigurerade användare	108
11.15.10	Dialogrutan Användargrupper och konton	108
11.15.11	Dialogrutan Enhetsbehörigheter	108
11.15.12	Dialogrutan Funktionsbehörigheter	108
11.15.13	Dialogrutan Konfigurationsbehörigheter	108
11.15.14	Dialogrutan Behörigheter för användargrupp	108
11.15.15	Dialogrutan Säkerhetsinställningar	108
11.15.16	Dialogrutan Enheter som har kringgåts	108
11.16	Dialogrutan Larminställningar (menyn Inställningar)	108
11.17	Dialogrutan SNMP-inställningar (menyn Inställningar)	109
11.18	Dialogrutan LDAP-inställningar (menyn Inställningar)	109
11.18.1	Associera en LDAP-grupp	111
11.19	Definiera LDAP-användargruppens ordning i dialogruta (menyn Inställningar)	111
11.20	Dialogrutan Inställningar för åtkomsttoken (menyn Inställningar)	112
11.21	Dialogrutan Inställningar för betrodda certifikat (menyn Inställningar)	113
11.22	Dialogrutan Alternativ (menyn Inställningar)	114
12	Sidan Enheter	117
12.1	Uppdatera tillstånd och funktioner för enheter	117
12.2	Ändra lösenordet för IP-enheter	118
12.3	Lägga till en enhet	118
12.4	Sidan Serverlista/adressbok	121
12.4.1	Dialogrutan Lägg till server	122
12.4.2	Konfigurera Server Lookup	122
12.4.3	Konfigurera serverlistan	122
12.4.4	Exportera serverlistan	122
12.4.5	Importera en serverlista	123
12.5	Sidan DVR (digital videospelare)	123
12.5.1	DVR-enheter	123

12.5.2	Lägga till en DVR-enhet genom avsökning	124
12.5.3	Dialogrutan Lagg till DVR	125
12.5.4	Fliken inställningar	125
12.5.5	Fliken Kameror	125
12.5.6	Fliken Ingångar	125
12.5.7	Fliken Reläer	126
12.5.8	Konfigurera integreringen för en DVR-enhet	126
12.6	Sidan Matrisväxlare	126
12.6.1	Lägga till en Bosch Allegiant-enhet	127
12.6.2	Konfigurera en Bosch Allegiant-enhet	127
12.6.3	Sidan Utgångar	127
12.6.4	Sidan Ingångar	128
12.6.5	Sidan Anslutning	128
12.6.6	Sidan Kameror	129
12.7	Sidan Arbetsstation	129
12.7.1	Lägga till en arbetsstation manuellt	129
12.7.2	Konfigurera ett Bosch IntuiKey-tangentbord (sidan Inställningar) (arbetsstation)	130
12.7.3	Aktivera brottsutredande sökningar på arbetsstationen (sidan Inställningar)	130
12.7.4	Konfigurera ett startkommandoskript (inställningssidan)	130
12.7.5	Sidan Inställningar	131
12.7.6	Ändra nätverksadressen för en arbetsstation	132
12.8	Sidan Avkodare	133
12.8.1	Lägga till en kodare/avkodare manuellt	133
12.8.2	Dialogruta för redigering av kodare/avkodare	134
12.8.3	Ändra lösenordet för en kodare/avkodare (Byt lösenord/Ange lösenord)	135
12.8.4	Avkodarprofil	136
12.8.5	Monitorvisning	137
12.8.6	Konfigurera ett Bosch IntuiKey-tangentbord (avkodare)	137
12.8.7	Konfigurera en avkodare för användning med ett Bosch IntuiKey-tangentbord	137
12.8.8	Ta bort avkodarlogo	138
12.9	Sidan Monitorgrupper	138
12.9.1	Lägga till en monitorgrupp manuellt	138
12.9.2	Konfigurera en monitorgrupp	139
12.10	Sidan Kommunikationsenheter	139
12.10.1	Lägga till en E-post-/SMTP-server	139
12.10.2	Sidan SMTP-server	140
12.10.3	Konfigurera en kommunikationsenhet	140
12.10.4	Skicka testmeddelande-dialogrutan	141
12.11	Bankomat/kassasida	141
12.11.1	Lägga till en Bosch ATM/POS-brygga manuellt	141
12.11.2	Sidan Bosch ATM/POS-brygga	142
12.11.3	Konfigurera kringutrustning	142
12.11.4	Sidan DTP-inställningar	143
12.11.5	Sidan ATM-inställningar	143
12.11.6	Sidan Ingångar	143
12.12	Nyckelkortsläsare	144
12.12.1	Dialogrutan Lagg till nyckelkortsläsare	144
12.12.2	Inställningar för sidan för nyckelkortsläsare	144
12.13	Sidan Virtuella ingångar	145

12.13.1	Lägga till virtuella ingångar manuellt	145
12.14	Sidan RMon och Snmp	145
12.14.1	Lägga till en SNMP manuellt	146
12.14.2	Konfigurera mottagare för SNMP-fälla (sidan Mottagare för SNMP-fälla)	146
12.14.3	Loggare av SNMP-fällor-dialogrutan	147
12.15	Sidan Tilldela tangentbord	147
12.16	Sidan I/O-moduler	149
12.16.1	Lägga till en I/O-modul manuellt	149
12.16.2	Konfigurera en I/O-modul	149
12.16.3	Sidan ADAM	150
12.16.4	Sidan Ingångar	150
12.16.5	Sidan Reläer	150
12.17	Sidan Allegiant-CCL-emulering	150
12.17.1	Lägga till en Allegiant-CCL-emulering manuellt	151
12.17.2	Allegiant CCL-kommandon	151
12.17.3	Konfigurera en Allegiant-CCL-emulering	151
12.18	Sidan Mobil videotjänst	152
12.18.1	Mobila videotjänster	152
12.18.2	Lägga till en Mobile Video Service (mobil videotjänst) manuellt	152
12.19	Sidan Inbrottspaneler	153
12.19.1	Lägga till en inbrottspanel manuellt	153
12.19.2	Sidan Inställningar	154
12.20	Sidan Passersystem	154
12.20.1	Lägga till ett passersystem	154
12.20.2	Redigera ett passersystem	155
12.20.3	Sidan Inställningar	155
12.21	Videoanalyssida	155
12.21.1	Inställningssida för Video Analytics	155
12.21.2	Lägga till en Video Analytics-enhet	155
12.21.3	Sidan Person Identification-enheter	156
12.21.4	Lägga till en Person Identification device (PID)	156
12.21.5	Sidan PID	157
12.21.6	Återställa åtkomst till ett PID efter ett BVMS-centralserveravbrott	157
12.21.7	Lägga till kameror i en Person Identification device (PID)	158
12.21.8	Konfigurera kameraparametrar för Person Identification-larm	158
12.21.9	Konfigurera persongrupper	159
12.21.10	Lägga till en LPR-enhet	160
12.22	Sidan VRM-enheter	161
12.22.1	Lägga till VRM-enheter genom avsökning	161
12.22.2	Lägga till en primär eller sekundär VRM manuellt	162
12.22.3	Redigera en VRM-enhet	164
12.22.4	Sidan VRM-inställningar	164
12.22.5	Sidan SNMP	164
12.22.6	Sidan Konton	164
12.22.7	Sidan Avancerad	165
12.22.8	Kryptera inspelning för VRM	165
12.22.9	Ändra lösenordet för en VRM-enhet	166
12.22.10	Lägga till en VRM-pool	167
12.22.11	Lägga till en reserv-VRM manuellt	167

12.22.12	Lägga till en speglad VRM manuellt	168
12.22.13	Lägga till kodare genom avsökning	169
12.22.14	Lägga till VSG-enheter genom avsökning	169
12.22.15	Synkronisera BVMS-konfigurationen	170
12.22.16	Importerar konfiguration från VRM	170
12.23	Poolsidan	170
12.23.1	Konfigurera automatiskt inspelningsläge för en pool	172
12.23.2	Lägga till en kodare/avkodare manuellt	172
12.23.3	Lägga till en iSCSI-enhet manuellt	173
12.23.4	Lägga till en Video Streaming Gateway manuellt	174
12.23.5	Lägga till en DSA E-Series iSCSI-enhet manuellt	175
12.23.6	Lägga till kodare genom avsökning	177
12.23.7	Lägga till VSG-enheter genom avsökning	178
12.23.8	Konfigurera dubbel strömning i enhetsträdet	178
12.24	Sidan Bosch-kodare/-avkodare	179
12.25	Sidan för iSCSI-enhet	179
12.25.1	iSCSI-lagringspool	179
12.25.2	Lägga till en iSCSI-enhet manuellt	180
12.25.3	Lägga till en DSA E-Series iSCSI-enhet manuellt	181
12.25.4	Konfigurera en iSCSI-enhet	183
12.25.5	Sidan Standardkonfiguration	184
12.25.6	Dialogrutan Belastningsutjämning	185
12.25.7	Flytta ett iSCSI-system till en annan pool (Ändra pool ...)	186
12.25.8	Sidan för LUN-enheter	186
12.25.9	Lägga till LUN	187
12.25.10	Formatera ett LUN	188
12.25.11	iqn-Mapper-dialogrutan	188
12.26	Sidan Video Streaming Gateway-enhet	189
12.26.1	Lägga till en Video Streaming Gateway manuellt	189
12.26.2	Redigera Video Streaming Gateway	191
12.26.3	Lägga till en kamera för en VSG-enhet	191
12.26.4	Dialogrutan Lägg till kodare från Bosch	192
12.26.5	Dialogrutan Lägg till ONVIF-kodare	193
12.26.6	Dialogrutan Lägg till JPEG-kameror	194
12.26.7	Dialogrutan Lägg till RTSP-kodare	195
12.26.8	Flytta en VSG till en annan pool (Ändra pool)	196
12.26.9	Konfigurera multicast (fliken Multicast)	196
12.26.10	Konfigurera loggning (fliken Avancerat)	197
12.26.11	Starta ONVIF Camera Event Driver Tool från Configuration Client	197
12.27	Sidan Endast live	198
12.27.1	Lägga till live-enheter från Bosch genom avsökning	198
12.27.2	Lägga till en kodare/avkodare manuellt	199
12.27.3	Ange mållösenord för en avkodare (Autentisera ...)	200
12.28	Sidan Lokal lagring	200
12.29	Sidan Unmanaged Site	201
12.29.1	Lägga till en unmanaged site manuellt	201
12.29.2	Importera ohanterade platser	201
12.29.3	Sidan Unmanaged Site	202
12.29.4	Lägga till en ohanterad nätverksenhet	202

12.29.5	Konfigurera tidszonen	203
13	Sidan Bosch-kodare/-avkodare/-kamera	204
13.1	Lägga till en kodare till en VRM-pool	205
13.2	Lägga till en kodare för endast live video	206
13.3	Lägga till en kodare för lokal lagring	206
13.4	Lägga till en kamera med en enda platshållare	206
13.5	Redigera en kodare	206
13.5.1	Kryptering av live-video (Redigera kodare)	206
13.5.2	Uppdatera enhetsfunktioner (Redigera kodare)	207
13.5.3	Dialogruta för redigering av kodare/avkodare	208
13.6	Hantera autentiseringskontroll	209
13.6.1	Kontroll av äkthet	209
13.6.2	Konfigurera autentisering	210
13.6.3	Ladda upp ett certifikat	211
13.6.4	Hämta ett certifikat	211
13.6.5	Installera ett certifikat på en arbetsstation	211
13.7	Ange mållösenord för en avkodare (Autentisera ...)	212
13.8	Ändra lösenordet för en kodare/avkodare (Byt lösenord/Ange lösenord)	212
13.9	Flytta en kodare till en annan pool (Ändra pool)	213
13.10	Återställa inspelningar från en utbytt kodare (Associera med inspelningar på tidigare enhet)	214
13.11	Konfigurera kodare/avkodare	214
13.11.1	Konfigurera lagringsmediet för en kodare	214
13.11.2	Konfigurera flera kodare / avkodare	215
13.11.3	Konfigurera reservinspelningsläge på en kodare	217
13.11.4	Sidan Inspelningshantering	217
13.11.5	Sidan Recording preferences	218
13.12	Konfigurera multicast	218
14	Sidan ONVIF	220
14.1	Lägga till en endast live-ONVIF-enhet genom avsökning	220
14.2	Sidan ONVIF-kodare	220
14.3	Sidan ONVIF-kodarhändelser	221
14.3.1	Lägga till och ta bort en ONVIF-profil	223
14.3.2	Exportera en tabell för mappning av ONVIF-fil	223
14.3.3	Importera en tabell för mappning av ONVIF-fil	224
14.3.4	Konfigurera en ONVIF-mappningstabell	225
14.4	Sidan ONVIF-konfiguration	226
14.4.1	Enhetsåtkomst	227
14.4.2	Datum/tid	227
14.4.3	Användarhantering	228
14.4.4	Sidan Videokodarprofil	229
14.4.5	Ljudkodarprofil	231
14.4.6	Bildvisning, allmänt	231
14.4.7	Motljuskompensation	232
14.4.8	Exponering	232
14.4.9	Fokus	233
14.4.10	Brett dynamiskt intervall	234
14.4.11	Vitbalans	234
14.4.12	Nätverksåtkomst	235
14.4.13	Områden	237

14.4.14	Reläer	238
14.5	Sidan ONVIF-händelsekälla	239
14.6	Tilldela en ONVIF-profil	239
15	Sidan Kartor och struktur	241
16	Konfigurera kartor och det logiska trädet	243
16.1	Konfigurera det logiska trädet	243
16.2	Lägga till en enhet till det logiska trädet	244
16.3	Ta bort ett trädobjekt	244
16.4	Hantera resursfiler	244
16.4.1	Resurshanteraren-dialogrutan	246
16.4.2	Välj resurs-dialogrutan	246
16.5	Lägga till ett dokument	247
16.5.1	Lägg till URL-dialogrutan	247
16.6	Dialogrutan Länk till extern applikation	248
16.7	Lägga till ett kommandoskript	248
16.8	Lägga till en kamerasekvens	248
16.8.1	Sekvensbyggare-dialogrutan	249
16.9	Hantera förkonfigurerade kamerasekvenser	249
16.9.1	Lägg till sekvens-dialogrutan	251
16.9.2	Lägg till sekvenssteg-dialogrutan	251
16.10	Lägga till en mapp	251
16.11	Lägga till en karta	251
16.12	Lägga till en länk till en annan karta	252
16.12.1	Välj karta för länk-dialogrutan	252
16.13	Tilldela en karta till en mapp	252
16.14	Hantera enheter på en anläggningskarta	253
16.15	Konfigurera globala kartor och kartvyportar	253
16.15.1	Konfigurera den globala kartan	254
16.15.2	Konfigurera kameror på den globala kartan	255
16.15.3	Lägga till kartor på den globala kartan	256
16.16	Lägga till en kartvyport	257
16.17	Aktivera Map-based tracking assistant för kartbaserad spårning	257
16.18	Lägga till ett felövervakningsrelä	258
16.18.1	Dialogrutan för felövervakningsrelä	258
16.19	Kringgå enheter	259
17	Sidan Scheman	260
17.1	Sidan Inspelningsscheman	260
17.2	Sidan Uppgiftsscheman	260
18	Konfigurera scheman	262
18.1	Konfigurera ett inspelningsschema	262
18.2	Lägga till ett uppgiftsschema	263
18.3	Konfigurera ett standarduppgiftsschema	263
18.4	Konfigurera ett återkommande uppgiftsschema	263
18.5	Ta bort ett uppgiftsschema	264
18.6	Lägga till helgdagar och undantagsdagar	264
18.7	Ta bort helgdagar och undantagsdagar	265
18.8	Ändra namn på ett schema	265
19	Sidan Kameror och inspelning	266
19.1	Sidan Kameror	266

19.2	Sidor för inspelningsinställningar	270
20	Konfigurera kameror och inspelningsinställningar	271
20.1	Kopiera och klistra in i tabeller	271
20.2	Exportera kameratabellen	272
20.3	Konfigurera inställningarna för ström kvalitet	272
20.3.1	Kvalitetsinställningar för ström-dialogrutan	273
20.4	Konfigurera kameraegenskaper	275
20.5	Konfigurera inspelningsinställningar (endast VRMoch Lokal lagring)	275
20.6	Dialogrutan Schemalagda inspelningsinställningar (endast VRM och Lokal lagring)	276
20.7	Konfigurera PTZ-portinställningar	279
20.8	Konfigurera fördefinierade positioner och extra kommandon	279
20.9	Dialogrutan med fördefinierade positioner och extra kommandon	280
20.10	Konfigurera ROI-funktionen	281
20.11	Kopiera inspelningsinställningar	281
20.11.1	Dialogrutan Kopiera inspelningsinställningar	282
20.12	Konfigurera ANR-funktionen	282
20.13	Konfigurera dubbel strömning i kameratabellen	282
20.14	Hantera Video Streaming Gateway	283
20.14.1	Tilldela en ONVIF-profil	283
21	Sidan Händelser	284
21.1	Fliken Avstudsninginställningar	285
21.2	Fliken Inställningar för avancerad kartvisning	285
21.3	Fliken Inställningar för händelsekonfiguration	286
21.4	Redigerare för kommandoskript-dialogrutan	286
21.5	Skapa sammansatt händelse / dialogrutan Redigera sammansatt händelse	287
21.6	Välj skriptspråk-dialogrutan	287
21.7	Dialogrutan Redigera prioriteter för händelsetyp	288
21.8	Välj enheter-dialogrutan	288
21.9	Dialogrutan Inspelning av textdata	288
22	Sidan Larm	289
22.1	Dialogrutan Larminställningar	289
22.2	Välj bildruteinnehåll-dialogrutan	290
22.3	Dialogrutan Välj bildruteinnehåll (MG)	291
22.4	Larmalternativ-dialogrutan	292
22.5	Välj resurs-dialogrutan	295
23	Konfigurera händelser och larm	297
23.1	Kopiera och klistra in i tabeller	298
23.2	Ta bort en tabellrad	298
23.3	Hantera resursfiler	298
23.4	Konfigurera en händelse	298
23.5	Duplicera en händelse	298
23.6	Logga användarhändelse	299
23.7	Konfigurera knapp för användarhändelse	299
23.8	Skapa en sammansatt händelse	300
23.9	Redigera en sammansatt händelse	301
23.10	Konfigurera ett larm	301
23.11	Konfigurera inställningar för alla larm	301
23.12	Konfigurera längden på förlarm och efterlarm	302
23.13	Utlösa larminspelning med textdata	302

23.14	Lägga till textdata för kontinuerlig inspelning	303
23.15	Skydda larminspelning	303
23.16	Konfigurera blinkande aktiveringspunkter	303
23.17	Händelser och larm för passersystem	304
23.18	Händelser och larm för Person Identification	305
24	Sidan Användargrupper	306
24.1	Sidan Egenskaper för användargrupper	308
24.2	Sidan Användaregenskaper	308
24.3	Sidan Logga in paregenskaper	309
24.4	Sidan Kamerabehörigheter	310
24.5	Sidan Kontrollprioriteter	311
24.6	Kopiera behörigheter för användargrupp-dialogrutan	312
24.7	Sidan Avkodarbehörigheter	312
24.8	Sidan Händelser och larm	312
24.9	Sidan Inloggningsuppgifter	313
24.10	Sidan Logiskt träd	313
24.11	Sidan Användarfunktioner	314
24.12	Sidan Prioriteringar	317
24.13	Sidan Användargränssnitt	317
24.14	Sidan Serveråtkomst	319
24.15	Sidan Konfigurationsbehörigheter	319
24.16	Sidan Användargruppbehörigheter	321
24.17	Sidan Kontoprinciper	321
24.17.1	Operator Client offline	323
25	Konfigurerar användare, behörigheter och Enterprise Access	327
25.1	Skapa en grupp eller ett konto	328
25.1.1	Skapa en standardanvändargrupp	328
25.1.2	Skapa en Enterprise User Group	329
25.1.3	Skapa ett Enterprise Account	329
25.2	Skapa en användare	330
25.3	Skapa en grupp med dubbla behörigheter	331
25.4	Lägga till ett inloggningspar till en grupp med dubbel behörighet	331
25.5	Konfigurera den administrativa gruppen	332
25.6	Välja en associerad LDAP-grupp	333
25.7	Schemalägga en användares inloggningsbehörighet	333
25.8	Konfigurera funktionsbehörigheter	333
25.9	Konfigurera enhetsbehörigheter	334
25.10	Konfigurera flera prioriteringar	334
25.11	Kopiera behörigheter för användargrupper	335
26	Konfigurera videobaserat system för brandlarm	336
26.1	Konfigurera en branddetekteringskamera	336
26.2	Lägga till en kodare till en VRM-pool	337
26.3	Lägga till kodare genom avsökning	337
26.4	Lägga till live-enheter från Bosch genom avsökning	337
26.5	Lägga till kodare för lokal lagring genom avsökning	338
26.6	Konfigurera en brandhändelse	338
26.7	Konfigurera ett brandlarm	339
27	Konfigurera en MIC IP 7000 som är ansluten till en VIDEOJET 7000 connect	340
28	Felsökning	341

28.1	Konfigurera önskat språk i Windows	343
28.2	Återupprätta anslutningen till ett Bosch IntuiKey-tangentbord	343
28.3	Minska antalet Allegiant-kameror	343
28.4	Använda portar	343
28.5	Aktiveraloggning för ONVIF-händelser	349
	Ordlista	351
	Innehållsförteckning	360

1 Använda Hjälp



Obs!

Det här dokumentet beskriver vissa funktioner som inte är tillgängliga för BVMS Viewer. Detaljerad information om de olika BVMS utgåvorna finns i www.boschsecurity.com och BVMS snabbvalsguiden: [BVMS snabbvalsguide](#).

Du kan ta reda på hur du gör något i BVMS genom att använda onlinehjälp. Använd någon av följande metoder.

Använda Innehåll, Index eller Sök:

- ▶ På **Hjälp**-menyn klickar du på **Visa Hjälp**. Använd knappar och länkar för att navigera.

Så här får du hjälp med ett fönster eller en dialogruta:

- ▶ Klicka på  i verktygsfältet.

ELLER

- ▶ Tryck på F1 för att få hjälpinformation om ett programfönster eller en dialogruta.

1.1

Hitta information

Du kan hitta information i hjälpen på flera sätt.

Så här hittar du information i onlinehjälp:

1. På **Hjälp**-menyn klickar du på **Hjälp**.
2. Om rutan på vänster sida inte syns klickar du på knappen **Visa**.
3. Gör så här i hjälpfönstret:

Klicka på:	När du vill:
Innehåll	Visa innehållsförteckningen för Onlinehjälp. Klicka på varje bok för att visa sidor som är länkade till ämnen. Klicka på varje sida för att visa motsvarande ämne i rutan på höger sida.
Innehållsförteckning	Sök efter särskilda ord eller fraser, eller sök i en lista med indexnyckelord. Dubbelklicka på nyckelordet för att visa motsvarande ämne i rutan på höger sida.
Sök	Hitta ord och fraser i avsnittens innehåll. Skriv ordet eller frasen i textfältet, tryck på ENTER och välj ämnet som du vill se från listan med ämnen.

Texter från användargränssnittet är markerade med **fet stil**.

- ▶ Pilen uppmanar dig att klicka på den understruken texten eller på ett föremål i programmet.

Närliggande ämnen

- ▶ Klicka för att visa ett avsnitt med information för det programfönster du för tillfället använder. Detta avsnitt tillhandahåller information om programmets fönsterreglage.

Koncept, sidan 22 ger bakgrundsinformation om valda frågor.



Obs!

Den här symbolen anger en potentiell risk för skador på egendom eller förlust av data.

1.2 Skriva ut hjälpen

Du kan skriva ut avsnitt och information direkt från webbläsarens fönster medan du använder onlinehjälp.

Skriva ut ett hjälpaavsnitt:

1. Högerklicka in den högra rutan och välj **Skriv ut**.
Dialogrutan **Skriv ut** öppnas.
 2. Klicka på **Skriv ut**.
- ✓ Avsnittet skrivs ut till angiven skrivare.

2 Inledning

Klicka på länken så kommer du åt licenserna för den öppna källkod som används av BVMS och mobilappen:

<http://www.boschsecurity.com/oss/>



Omfattas av ett eller flera krav som anges i patentlist.hevcadvance.com.

Den här handboken beskriver de grundläggande stegen i konfigurationen med BVMS. Detaljerad hjälp och stegvisa instruktioner finns i konfigurationshandboken eller använd onlinehjälp.

BVMS

BVMS integrerar digital video, ljud och data i alla typer av IP-nätverk.

Systemet består av följande programvarumoduler:

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

Vill du ha ett system i drift så ska du utföra följande uppgifter:

- Installera tjänster (Management Server och VRM)
- Installera Operator Client och Configuration Client
- Ansluta till nätverk
- Ansluta enheter till nätverk
- Grundkonfiguration:
 - Lägg till enheter (t.ex. genom enhetssökning)
 - Bygg logisk struktur
 - Konfigurera scheman, kameror, händelser och larm
 - Konfigurera användargrupper

BVMS Export Player

BVMS Export Player visar exporterade inspelningar.

BVMS Viewer

BVMS Viewer är en IP-videosäkerhetsapplikation för livevisning och uppspelning av bilder från kameror och inspelningsanordningar som är anslutna till ett Bosch-nätverk.

Programvarupaketet består av en Operator Client för livevisning och uppspelning av bilder och en Configuration Client. BVMS Viewer har funktioner för den senaste IP-videoproduktportföljen från Bosch såväl som äldre videoenheter från Bosch.

Klicka på länken om du vill öppna licenserna för den öppna källkod som används av BVMS Viewer:

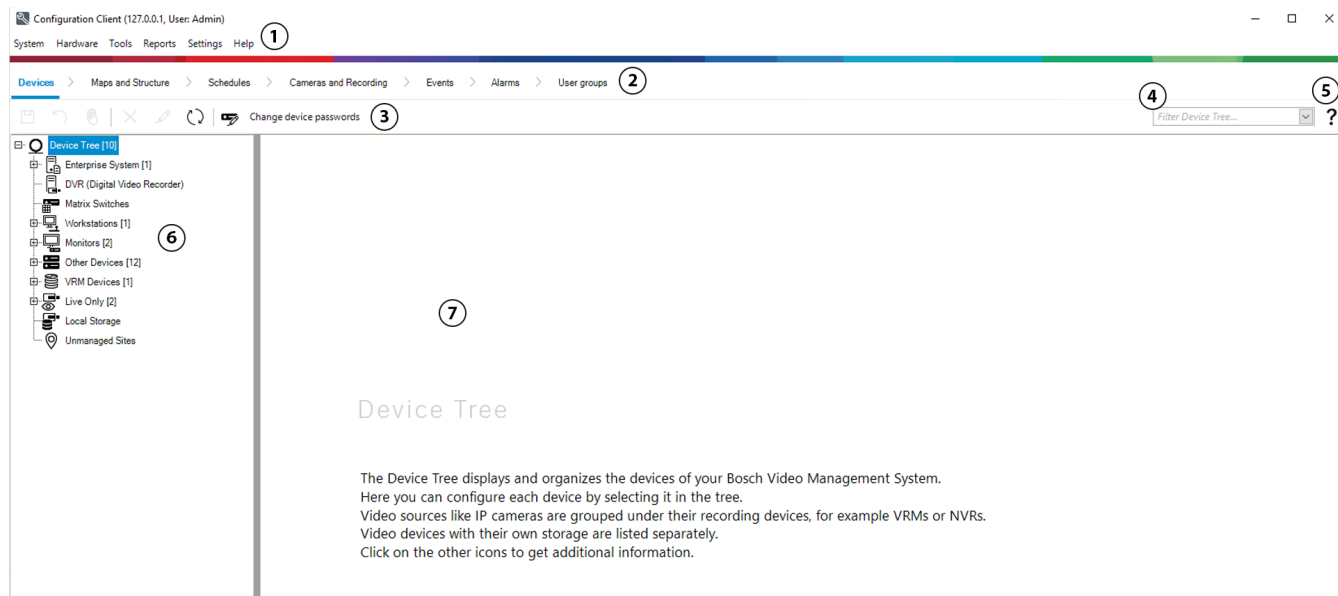
<http://www.boschsecurity.com/oss>.

BVMS Configuration Client

Tanken med BVMS Configuration Client är att börja med att konfigurera enheterna och sedan konfigurera det logiska trädet. Efter dessa två steg kan scheman, inspelningar, händelser och larm för enheterna konfigureras på deras respektive sidor. Det sista steget är att konfigurera användargrupperna på användargruppsidan. När du har konfigurerat alla sidor från vänster till höger är allt konfigurerat och operatören kan börja använda Operator Client.

När du har konfigurerat varje sida sparar du konfigurationen genom att klicka på  i menyn Verktyg.

Om du vill göra ändringarna synliga i BVMS Operator Client klickar du på



1	Menyrad	Välj ett menykommando.
2	Sidrad	Låter dig konfigurera alla steg som krävs från vänster till höger.
3	Verkttygsfält	Visar tillgängliga knappar utifrån den aktiva fliken. Visa verktygstips genom att hålla pekaren över en ikon.
4	Sökindikator	Låter dig söka efter en specifik enhet och deras motsvarande överordnade i enhetsträdet.
5	Hjälpikon	Visar onlinehjälp för BVMS Configuration Client.
6	Urvalsfönster	Hierarkisk lista över alla tillgängliga enheter i systemet.
7	Konfigurationsfönster	Låter dig konfigurera den valda enheten.

BVMS Operator Client

2.1

BVMS-utgåvor

De olika BVMS utgåvorna erbjuder dig full skalbarhet, så att du kan utöka ditt videoövervakningssystem enligt dina behov.

Följande utgåvor av BVMS är tillgängliga:

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

BVMS Viewer och BVMS Professional är endast programvaruprodukter. Du kan inte använda dem på Bosch DIVAR IP enheter.

Du kan använda BVMS Lite och BVMS Plus på Bosch DIVAR IP enheter eller som programvaruprodukter på någon annan maskinvara.
 Detaljerad information om de olika BVMS utgåvorna finns i www.boschsecurity.com och BVMS snabbvalsguiden:
[BVMS Snabbvalshandbok](#).

2.2 BVMS-licensaktiveringsöversikt

Det här kapitlet innehåller en översikt över licensaktiveringen av BVMS.

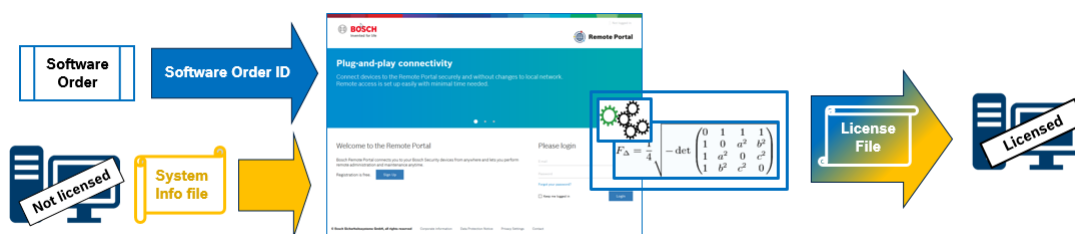
Licensbeställning

- Beställ med hjälp av Bosch orderdisken.
- Orderbekräftelsen innehåller det nya programorder-ID som krävs för den senare programaktiveringsprocessen.
- Från och med BVMS 11.0 är baspaketet och utbyggnadslicensen för BVMS inte längre beroende av programversionen.

Licensaktivering

- Bosch Remote Portal (<https://www.remote.boschsecurity.com>) ersätter Bosch **Licenshanterare**.
- En ny användarregistrering krävs i Bosch Remote Portal.
- Systeminformationsfilen och programvarans order-ID är obligatoriska indata för licensaktiveringen.
- Remote Portal genererar licensfilen och innehåller all aktiveringsinformation. Lägg till den här filen i det installerade BVMS-systemet.
- Aktiveringsprocessen definierar startdatumet för programvarans försäkringsperiod. Slutdatumet visas på **Licenshanterare** av BVMS Configuration Client.

Aktiveringsprocess för programvarulicens



Så här aktiverar du programvarulicenserna:

1. Beställ programvaruprodukter
 - Beställ dina programvaruprodukter genom att följa Bosch standardbeställningsprocessen.
 - Programvarubeställningar kan bestå av en eller flera produkter i en eller flera produktutgåvor.
2. Ta emot beställnings-ID för programvara
 - Resultatet av beställningen är en bekräftelse på programvaruorder som innehåller programvarans order-ID.
 - Programvarans order-ID gör det möjligt att ansluta den installerade programvaran (på operativsystem och hårdvara) till de beställda programvaruprodukterna.
3. Aktivera licensen
 - Obligatorisk indata för licensaktivering är systeminformationsfilen som representerar det unika operativsystemet och maskinvaran där programvaran är installerad.

- Aktiveringen ansluter programvarans order-ID till den installerade programvaran och skapar licensfilen som utdata.
- Aktiveringen definierar attribut för systemet, till exempel start- och slutdatum för programvarusäkring.
- 4. Aktivera programvaran
- För att aktivera programvaran lägger du till licensfilen i den installerade programvaran.
- Licensfilerna aktiverar BVMS funktionerna enligt de aktiverade objekten.

**Obs!****Licensfilen innehåller följande aktiveringsinformation:**

- BVMS-produktutgåva
- BVMS-version som tillåts
- Utgångsdatum på programvaruförsäkring
- Antal utbyggnads-/funktionslicenser

Se

- *Aktivera programvarulicenserna, sidan 71*

3 Systemöversikt



Obs!

Det här dokumentet beskriver vissa funktioner som inte är tillgängliga för BVMS Viewer. Detaljerad information om de olika BVMS utgåvorna finns i www.boschsecurity.com och BVMS snabbvalsguiden: [BVMS snabbvalsguide](#).

Om du planerar att installera och konfigurera BVMS bör du gå en systemutbildning om BVMS. I versionskommentarerna om den aktuella versionen av BVMS finns information om vilka versioner av den fasta programvaran och maskinvaran som stöds och andra viktiga uppgifter. Datablad om Bosch arbetsstationer och servrar innehåller information om på vilka datorer BVMS kan installeras.

Programvarumodulerna BVMS kan även installeras på en dator.

Viktiga komponenter

Komponent	Beskrivning
Management Server (kan anges i Inställningar)	Hantering av videoströmmar, larmhantering, prioritetshantering, hanterings loggbok, användarhantering, hantering av enhetsstatus. Ytterligare Enterprise System-licens: Hantera Enterprise User Group-grupper och Enterprise Account-konton.
Config Wizard	Enkel och snabb installation av ett inspelningssystem.
Configuration Client (kan anges i Inställningar)	Systemkonfiguration och administration för Operator Client.
Operator Client (kan anges i Inställningar)	Liveövervakning, lagringshämtning och uppspelning, larm och åtkomst till flera Management Server-datorer samtidigt.
Video Recording Manager (kan anges i Inställningar)	Distribuerar lagringskapacitet på iSCSI-enheter till kodarna och hanterar belastningsutjämnningen mellan flera iSCSI-enheter. Strömmar ljud- och videouppspelningsdata från iSCSI till Operator Client.
Mobile Video Service (kan anges i Inställningar)	Har en kodkonverteringstjänst som konverterar den direktsända och inspelade videoströmmen från en kamera som konfigurerats i BVMS till den tillgängliga nätverksbandbredden. Den här tjänsten aktiverar videoklienter som iPhone eller webbklienter för att ta emot konverterade strömmar, t.ex. för opålitliga nätverksanslutningar med begränsad bandbredd.
Webbklient	Du kan visa livevideo och inspelad video via webbläsaren.
Mobilapp	Du kan använda mobilappen på iPhone eller iPad för att visa livevideo och inspelad video.
Bosch Video Streaming Gateway (kan anges i Inställningar)	Gör det möjligt att integrera tredjepartskameror, t.ex. i nätverk med låg bandbredd.

Komponent	Beskrivning
Cameo SDK (kan anges i Inställningar)	Cameo SDK används för att bädda in direktsända och inspelade BVMS bildrutor i en extern tredjepartstillämpning. Bildrutorna följer de BVMS-baserade användarbehörigheterna. De Cameo SDK innehåller vissa av de BVMS Operator Client funktioner som gör att du kan skapa tillämpningar som liknar Operator Client.
Client Enterprise SDK	Client Enterprise SDK används för att kontrollera och övervaka Operator Client i ett Enterprise System med hjälp av externa tillämpningar. Med SDK kan du bläddra på enheter som kan nås via den aktiva anslutna Operator Client-klienten samt styra vissa användargränssnittsfunktioner.
Client SDK / Server SDK	Server SDK används för att kontrollera och övervaka Management Server med hjälp av skript och externa tillämpningar. Du kan använda gränssnitten om du har ett giltigt administratörskonto. De Client SDK används för att styra och övervaka Operator Client med hjälp av externa tillämpningar och skript (som ingår i den tillhörande serverkonfigurationen).

3.1 Maskinvarukrav

Se databladet för BVMS. Det finns också datablad för datorplattformar.

3.2 Programvarukrav

Viewer kan inte installerad där någon annan BVMS-komponent är installerad.

Se databladet för BVMS.

3.3 Licenskrav

Se databladet för BVMS tillgängliga licenser.

4 Koncept



Obs!

BVMS Viewer har bara grundläggande funktioner. Avancerade funktioner ingår i BVMS Professional. Detaljerad information om de olika BVMS utgåvorna finns på www.boschsecurity.com och BVMS Snabbvalsguiden: [BVMS snabbvalsguide](#).

Detta kapitel tillhandahåller bakgrundsinformation om valda frågor.

4.1 BVMS-designbegrepp

Ett enda Management Server-system, sidan 22

Med ett enda BVMS Management Server-system kan du hantera, övervaka och styra upp till 2 000 kameror/kodare.

Enterprise System, sidan 23

En Enterprise Management Server ger samtidig åtkomst till flera Management Servers. Enterprise System ger fullständig åtkomst till händelser och larm från flera delsystem.

Server Lookup, sidan 24

Funktionen Server Lookup visar en lista över tillgängliga BVMS Management Servers för BVMS Operator Client. Operatören kan välja en server i listan med tillgängliga servrar. När klienten har anslutits till Management Server har den fullständig åtkomst till Management Server.

Unmanaged site, sidan 25

Enheter kan grupperas i unmanaged sites. Enheter under unmanaged sites övervakas inte av Management Server. Management Server visar en lista med unmanaged sites för Operator Client. Operatören kan ansluta till platsen på begäran och komma åt direktsända och inspelade videodata. Händelse- och larmhantering är inte tillgängligt med en unmanaged site.

4.1.1 Ett enda Management Server-system

- En enda BVMS Management Server kan hantera upp till 2 000 kanaler.
- Med ett BVMS Management Server kan du hantera, övervaka och styra hela systemet.
- BVMS Operator Client ansluter till Management Server och tar emot händelser och larm från BVMS Management Server och visar direktsänd och inspelad video.
- I de flesta fall finns alla enheter i ett lokalt nätverk med hög bandbredd och låg latens.

Uppgifter:

- Konfiguration av data
- Händelselogg (loggbok)
- Användarprofiler
- Användarprioriteringar
- Licensiering
- Händelse- och larmhantering

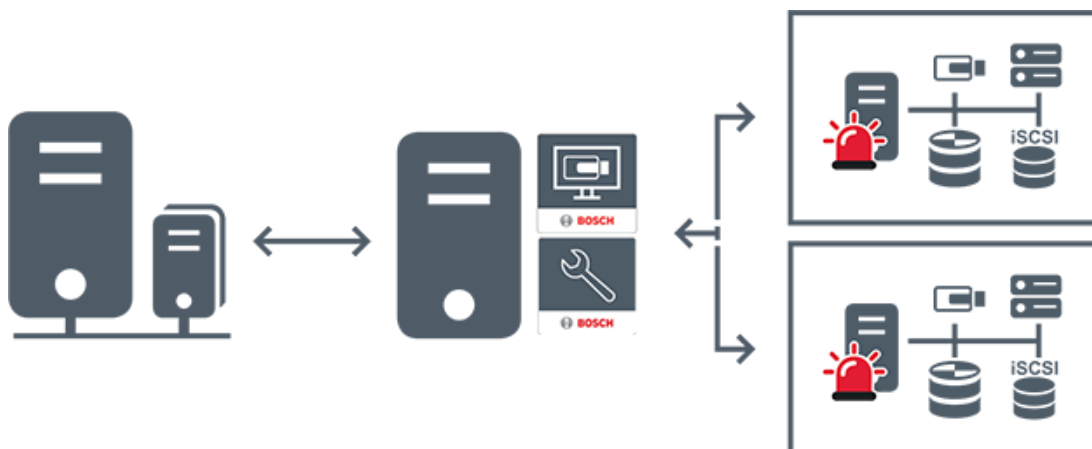


	Live, uppspelning, händelser, larm
	Management Server
	Operator Client / Configuration Client
	Kameror
	VRM
	iSCSI
	Andra enheter

4.1.2

Enterprise System

- Med BVMS Enterprise System kan Operator Client-användare komma åt flera Management Servers (delsystem) samtidigt.
- Klienter som är anslutna till en Enterprise-server har fullständig åtkomst till alla kameror och inspelningar från delsystemen.
- Klienter som är anslutna till en Enterprise-server har fullständig överblick i realtid över händelser och larm i alla delsystem.
- Typiska tillämpningsområden:
 - Tunnelbanesystem
 - Flygplatser



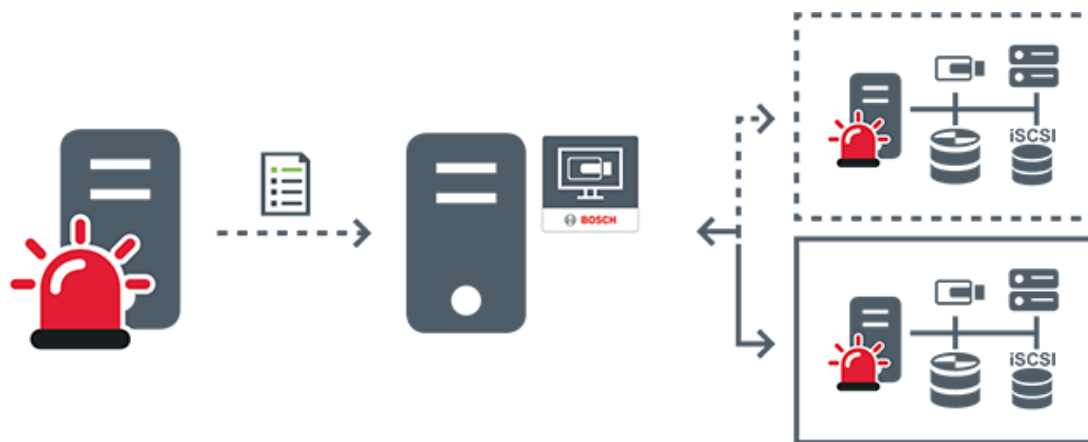
	Live, uppspelning, händelser, larm
	BVMS Enterprise Management Server
	BVMS Operator Client / Configuration Client
	BVMS-delsystem

Se

- Skapa ett Enterprise System, sidan 81
- Konfigurera serverlistan för Enterprise System, sidan 81
- Konfigurerar användare, behörigheter och Enterprise Access, sidan 327
- Få åtkomst till systemet, sidan 70

4.1.3**Server Lookup**

- Med funktionen BVMS Server Lookup kan operatörer ansluta till en BVMS Management Server från en angiven lista med servrar.
- En enskild Configuration Client- eller Operator Client-användare kan ansluta till flera av systemets accesspunkter i följd.
- Systemets accesspunkter kan vara Management Server eller Enterprise Management Server.
- Server Lookup använder en dedikerad Management Server som värd för serverlistan.
- Funktionellt sett kan Server Lookup och Management Server eller Enterprise Management Server köras på en enda dator.
- Server Lookup hjälper dig att hitta systemets accesspunkter med hjälp av deras namn eller beskrivningar.
- När den har anslutits till Management Server tar Operator Client emot händelser och larm från BVMS Management Server och visar direktsänd och inspelad video.



	Direktsända och inspelade händelser och larm på begäran – anslutet system
---	---

	Direktsända och inspelade händelser och larm på begäran – ej anslutet system
	Management Server
	Serverlista
	Operator Client
	BVMS är anslutet via serverlistan
	BVMS är inte anslutet via serverlistan

Se

- *Konfigurera Server Lookup, sidan 122*
- *Sidan Serverlista/adressbok, sidan 121*
- *Använda serversökning, sidan 70*
- *Exportera serverlistan, sidan 122*
- *Importera en serverlista, sidan 123*

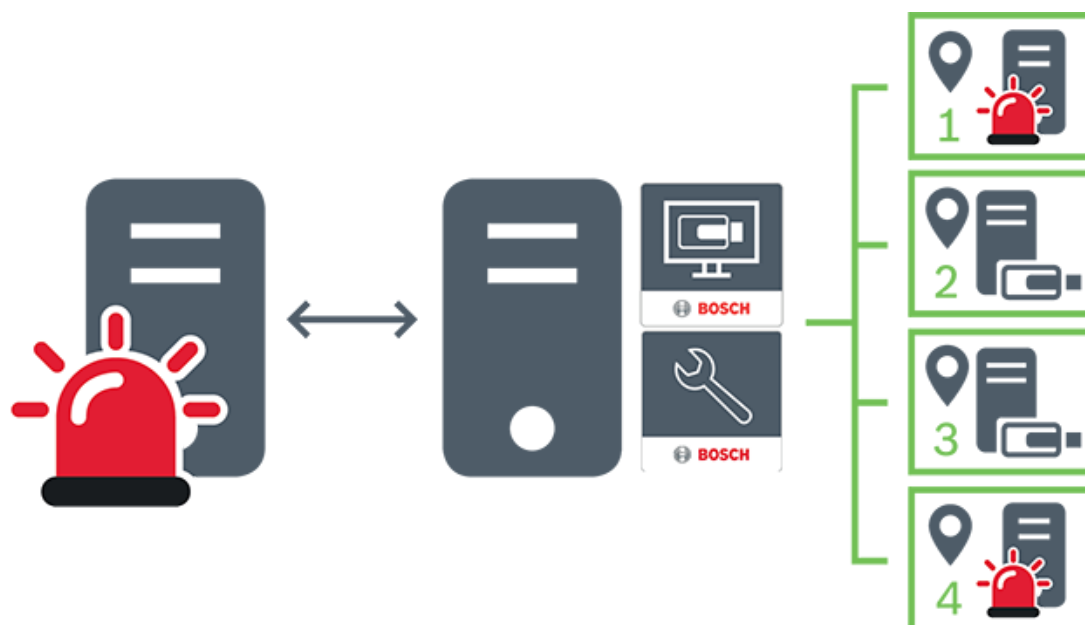
4.1.4**Unmanaged site**

- Ett designalternativ för BVMS-system med många mindre delsystem.
- Med det här alternativet kan du konfigurera upp till 9 999 platser på en enda BVMS Management Server
- Operatörer kan komma åt direktsända och inspelade videodata från upp till 20 sites samtidigt.
- sites kan grupperas i mappar eller placeras på kartor för enklare navigering. Med fördefinierade användarnamn och lösenord kan operatörer snabbt ansluta till en site.

En unmanaged site-systemdesign stöder både IP-baserade BVMS-system och analoga DVR-lösningar:

- Bosch DIVAR AN 3000/5000 analoga inspelare
- DIVAR hybrid-inspelare
- DIVAR network-inspelare
- IP-baserad inspelning på DIP 3000/7000-enheter
- Ett enda BVMS Management Server-system

Att lägga till en site för central övervakning kräver endast en licens per site och är oberoende av antalet kanaler på denna site.



	Live, uppspelning, händelser, larm
	Direktsänd och inspelad videotrafik på begäran
	Management Server
	Operator Client / Configuration Client
	site
	DVR

Se

- *Lägga till en unmanaged site manuellt, sidan 201*

4.2

Inspelning

I det här kapitlet beskrivs de olika inspelnings- och uppspelningsfunktionerna i systemet.

4.2.1 ANR (Automated Network Replenishment)



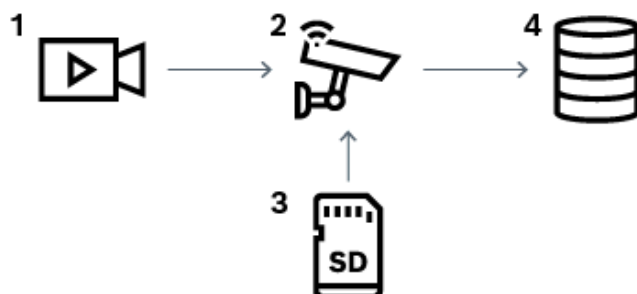
Obs!

BVMS Viewer har bara grundläggande funktioner. Avancerade funktioner ingår i BVMS Professional. Detaljerad information om de olika BVMS utgåvorna finns på www.boschsecurity.com och BVMS Snabbvalsguiden: [BVMS snabbvalsguide](#).

Avsedd användning

Om ett fel uppstår i nätverket eller på den centrala lagringsplatsen ser ANR-funktionen till att kodaren överför den lokalt buffrade inspelningen av den saknade tidsperioden till den centrala lagringsplatsen när felet har åtgärdats.

I följande diagram visas hur videodata överförs efter ett åtgärdat fel i nätverket eller på lagringsplatsen.



1	Video
2	Kodare, IP-nätverk
3	SD-kort (slingbuffert)
4	iSCSI-mål (central lagringsplats)

Exempel: Lösning vid nätverksfel

Vid ett oväntat nätverksfel används ANR-funktionen för att överföra den lokalt buffrade inspelningen till den centrala lagringsplatsen när nätverket är tillgängligt igen.

Exempel: Lagring av videodata när nätverket inte är tillgängligt

En tunnelbana har ingen nätverksanslutning till den centrala lagringsplatsen mellan stationerna. Det är bara vid hållplatserna som den buffrade inspelningen kan överföras till den centrala lagringsplatsen.

Se till att tidsperioden som krävs för att överföra den buffrade inspelningen inte överskrider tidsperioden för ett stopp.

Exempel: ANR för larminspelning

Förlarmsinspelning lagras lokalt. Förlarmsinspelningen överförs endast till den centrala lagringsplatsen vid ett larm. Om inget larm har gått överförs inte den gamla förlarmsinspelningen till den centrala lagringsplatsen och belastar därmed inte nätverket.

Begränsningar



Obs!

Du kan inte använda uppspelning från det lokala lagringsmediet när lösenorden för "användare" och "live" har angetts på kodaren. Ta bort lösenorden vid behov.

ANR-funktionen fungerar bara med VRM-inspelning.

ANR-funktionen fungerar inte med en kodare där en säker anslutning för livevisning har konfigurerats.

Du måste ha konfigurerat lagringsmediet för en kodare för att kunna använda ANR-funktionen.

Kodaren som du konfigurerar ANR-funktionen för måste ha fast programvara av version 5.90 eller senare. Alla kodartyper stöder inte ANR-funktionen.

Du kan inte använda ANR-funktionen med dubbel strömning.

iSCSI-lagringssystemet måste vara rätt konfigurerat.

Följande lista innehåller möjliga orsaker om du inte kan konfigurera ANR-funktionen:

- Kodaren är inte åtkomlig (fel IP-adress, nätverksfel osv.).
- Lagringsmediet för kodaren är inte åtkomligt eller är skrivskyddat.
- Den fasta programvaran är av fel version.
- Kodartypen stöder inte ANR-funktionen.
- Dubbel strömning är aktiv.

Se

- *Konfigurera en iSCSI-enhet, sidan 183*
- *Konfigurera lagringsmediet för en kodare, sidan 79*
- *Konfigurera ANR-funktionen, sidan 282*

4.2.2

Dubbel strömning/reservinspelning

Avsedd användning

En primär VRM hanterar normala inspelningar av kamerorna i systemet. Du använder en sekundär VRM-enhet för att få dubbel strömning av kamerorna.

Med dubbel strömning kan du spela in videodata från samma kamera till olika platser.

Dubbel strömning utförs normalt med andra ströminställningar och inspelningslägen. Ett specialfall av dubbla inspelningar är att du kan konfigurera speglade inspelningar: samma videosignal spelas in två gånger på olika platser.

Dubbel inspelning sker genom att 2 VRM-servrar används för att hantera flera iSCSI-enheter som kan placeras på olika platser.

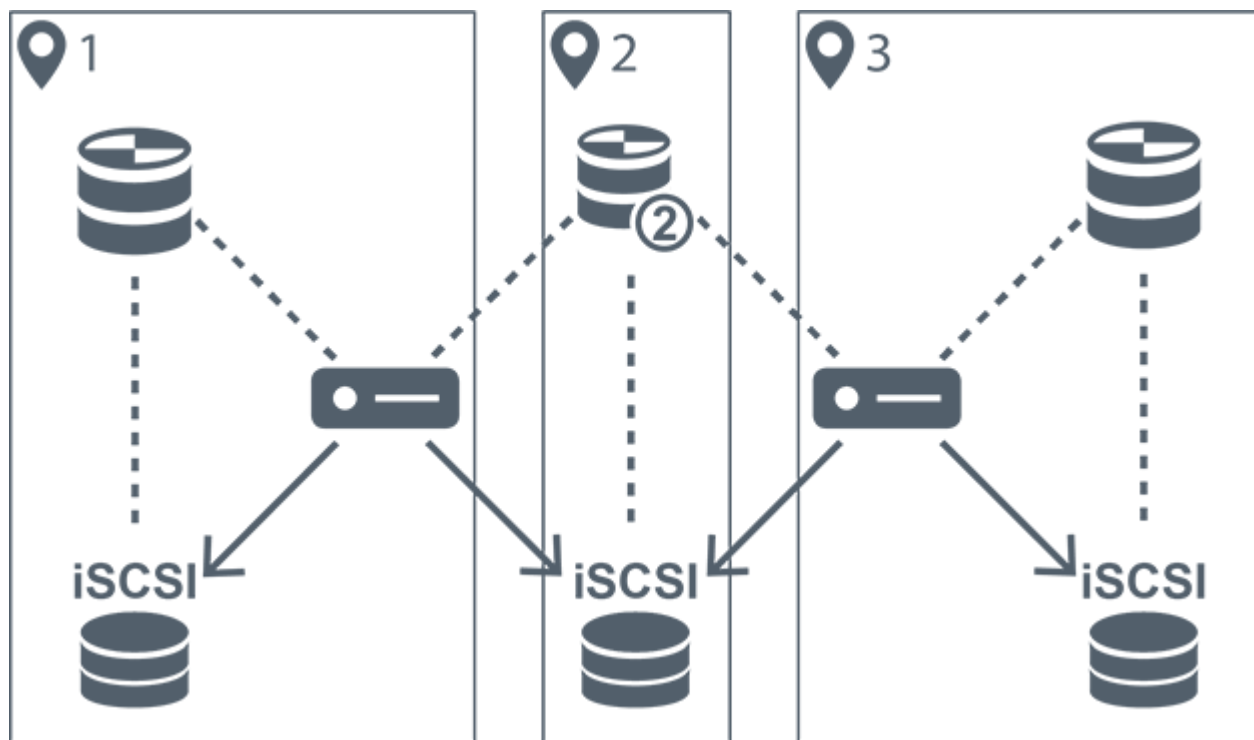
En sekundär VRM-enhet kan hantera den sekundära inspelningen för flera primära VRM-enheter.

Användaren kan välja mellan de inspelningar som hanteras av den primära VRM-enheten och de som hanteras av den sekundära VRM-enheten. För en enskild kamera kan användaren växla till inspelningarna för den sekundära eller primära VRM-enheten. Användaren kan även visa inspelningarna för samma kamera som hanteras av den primära och den sekundära VRM-enheten samtidigt.

För dubbel inspelning måste du installera en sekundär VRM-enhet under installationen.

En reserv-VRM-enhet används för att fortsätta inspelningen när ett fel uppstår i en primär eller sekundär VRM-dator.

I följande diagram visas ett exempel på ett scenario med dubbel strömning:



1	Plats 1		Kodare
2	Central plats		iSCSI-lagringsenhet
3	Plats 2		Styrningsanslutning
	Primär VRM		Videoström
	Sekundär VRM		

Begränsningar

Du kan inte använda dubbel strömning tillsammans med ANR-funktionen. Cameo SDK har endast stöd för uppspelning av primär inspelning.

Se

- Konfigurera dubbel strömning i kameratabellen, sidan 282
- Lägga till en speglad VRM manuellt, sidan 168
- Lägga till en reserv-VRM manuellt, sidan 167
- Sidan Kameror, sidan 266

4.2.3

VRM-inspelningslägen

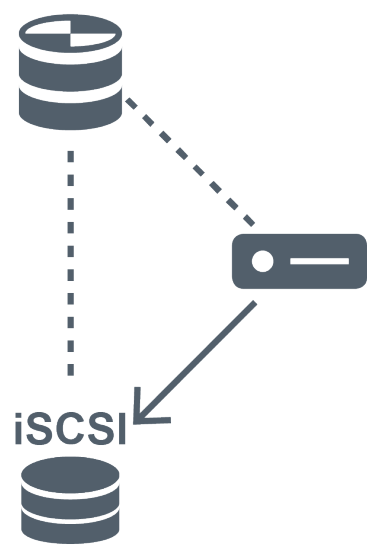
I det här kapitlet visas diagram som illustrerar de möjliga VRM-inspelningslägena.

Lista över möjliga VRM-inspelningslägen:

- Primär VRM-inspelning
- Speglad VRM-inspelning
- Sekundär VRM-inspelning

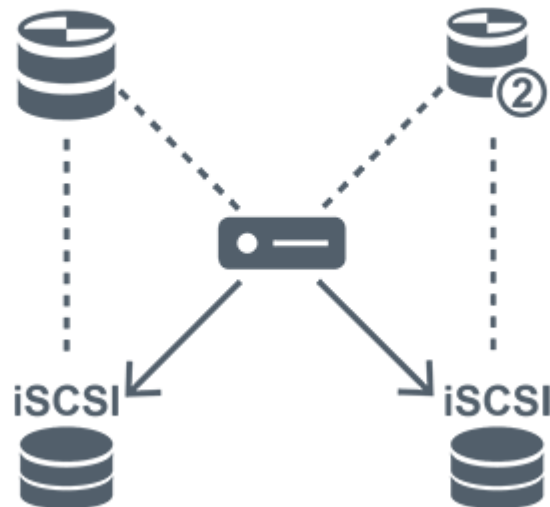
- Reserv-VRM-inspelning
Information om ANR-inspelning finns i kapitlet *ANR (Automated Network Replenishment)*, sidan 27.

Primär VRM-inspelning



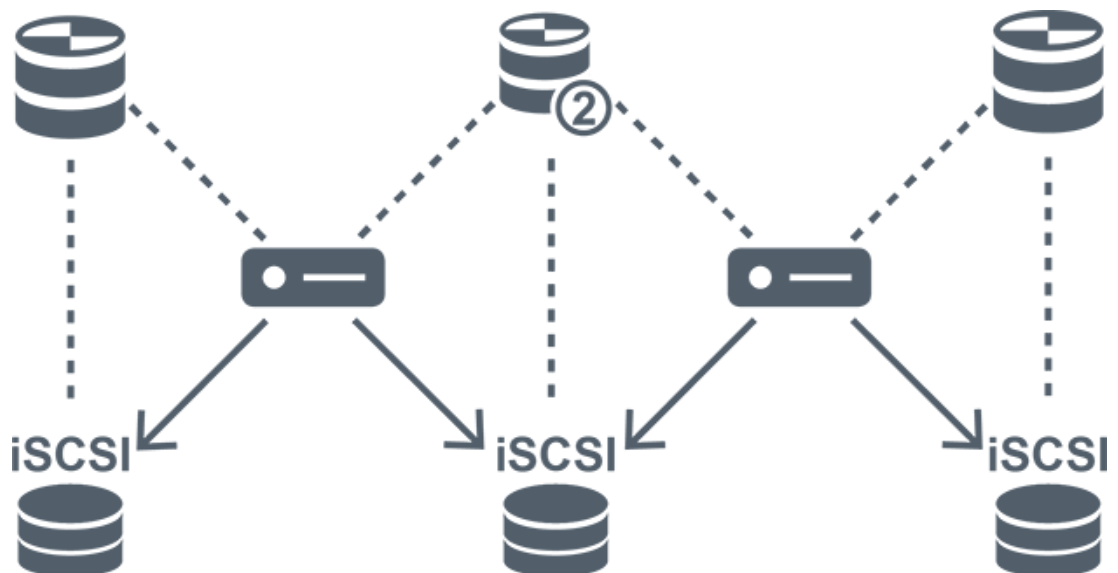
	Primär VRM		Styrningsanslutning
	iSCSI-lagringssenhett	→	Videoström
	Kodare		

Speglad VRM-inspelning



	Primär VRM		Sekundär VRM
	iSCSI-lagringsenhet		Styrningsanslutning
	Kodare	→	Videoström

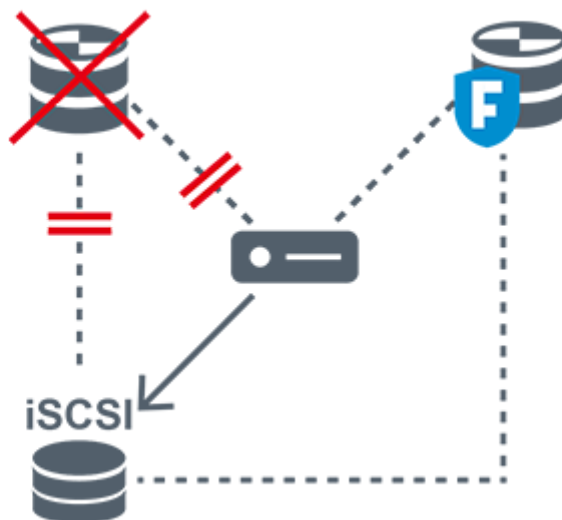
Sekundär VRM-inspelning



	Primär VRM		Sekundär VRM
	iSCSI-lagringsenhet		Styrningsanslutning

	Kodare		Videoström
---	--------	---	------------

Reserv-VRM-inspelning



	Primär VRM		Primär reserv-VRM
	iSCSI-lagringseenhet		Kodare
	Styrningsanslutning		Videoström

4.2.4

Uppspelning av VRM-inspelningskällor

I följande diagram visas bildrutor med uppspelning från alla möjliga VRM-inspelningskällor. I varje diagram visas lagringseenheten, den eventuella VRM-instansen och en del av en bildruta som exempel på uppspelningen. I tillämpliga fall visas inspelningskällan med en ikon på bildrutan.

- Uppspelning av en enskild inspelning, sidan 32
- Uppspelning av dubbel VRM-strömning, sidan 33
- Uppspelning av primär VRM-inspelning med valfri reserv-VRM-enhet, sidan 34
- Uppspelning av sekundär VRM-inspelning med valfri reserv-VRM-enhet, sidan 35
- ANR (Automatic Network Replenishment), sidan 36

Uppspelning av en enskild inspelning

Den här bildrutan visar när endast en primär VRM-enhet har konfigurerats. Du kan inte välja någon annan inspelningskälla.

: Om arbetsstationens konfiguration tillåter det, sker uppspelningen direkt från iSCSI-lagringseenheten.

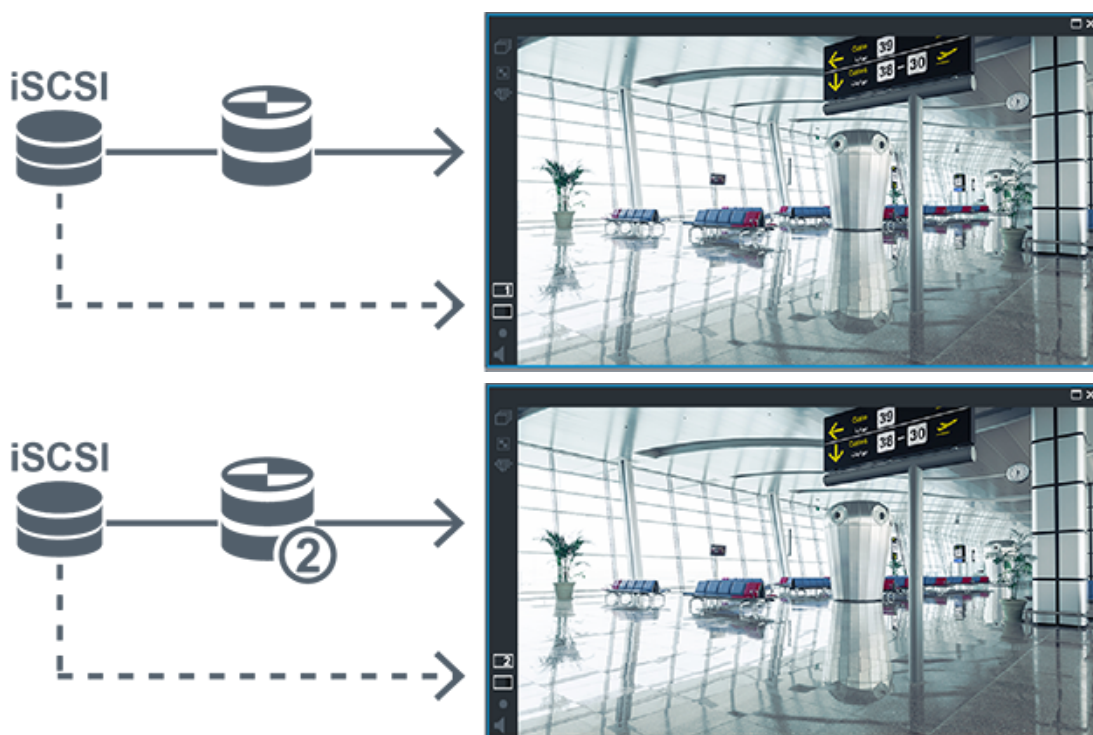


	iSCSI-lagringseenhet
	Primär VRM

Uppspelning av dubbel VRM-strömning

En primär VRM-enhet och en sekundär VRM-enhet har konfigurerats. Klicka på ikonen för inspelningskällan för att visa primär eller sekundär uppspelning.

Om arbetsstationens konfiguration tillåter det, sker uppspelningen direkt från iSCSI-lagringseenheten.



	iSCSI-lagringseenhet
	Primär VRM
	Sekundär VRM

Uppspelning av primär VRM-inspelning med valfri reserv-VRM-enhet

Så länge den primära VRM-enheten fungerar är uppspelning från den möjlig. Reserv-VRM-enheten går i viloläge.

Om arbetsstationens konfiguration tillåter det sker uppspelningen direkt från iSCSI-lagringenheten.

Om en sekundär VRM-enhet eller ANR-inspelning har konfigurerats kan du växla mellan inspelningskällorna.



När det inte finns någon anslutning till den primära VRM-enheten sker uppspelningen från den konfigurerade reserv-VRM-enheten. Stäng bildrutan och visa kameran igen i en bildruta:



När det inte finns någon anslutning till den primära VRM-enheten eller den primära reserv-VRM-enheten sker uppspelningen från kodaren. Stäng bildrutan och visa kameran igen i en bildruta:



	iSCSI-lagringsenhet
	Primär VRM
	Primär reserv-VRM
	Kodare

Med uppspelning från kodare kan endast en begränsad inspelningsperiod visas.

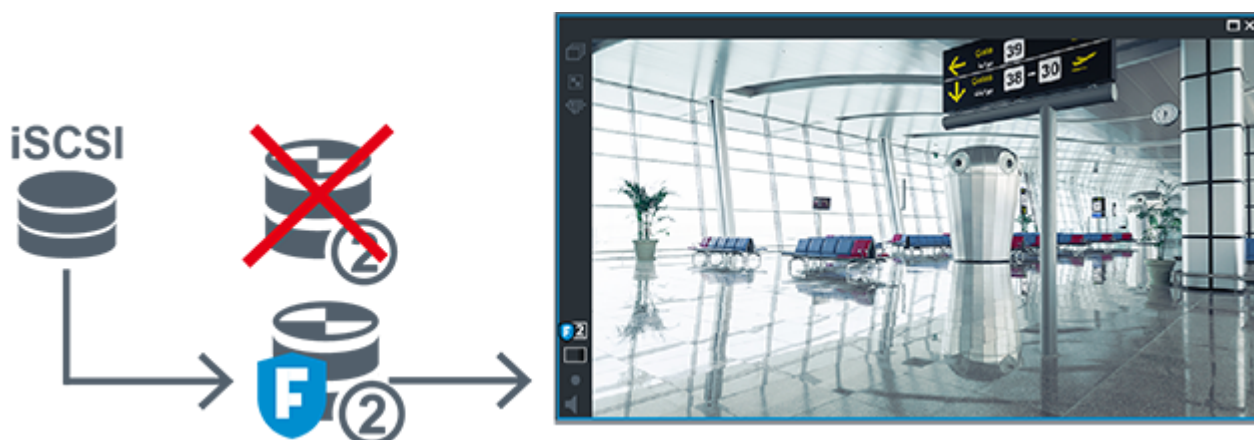
Uppspelning av sekundär VRM-inspelning med valfri reserv-VRM-enhet

Så länge den sekundära VRM-enheten fungerar är uppspelning från den möjlig. Reserv-VRM-enheten går i viloläge.

Om arbetsstationens konfiguration tillåter det sker uppspelningen direkt från iSCSI-lagringsenheten.



När det inte finns någon anslutning till den sekundära VRM-enheten sker uppspelningen från den konfigurerade reserv-VRM-enheten. Stäng bildrutan och visa kameran igen i en bildruta:



När det inte finns någon anslutning till den sekundära VRM-enheten eller den sekundära reserv-VRM-enheten sker uppspelningen från kodaren. Stäng bildrutan och dra kameran igen till en bildruta:



	iSCSI-lagringseenhet
	Primär VRM
	Sekundär reserv-VRM
	Kodare

Med uppspelning från kodare kan endast en begränsad inspelningsperiod visas.

ANR (Automatic Network Replenishment)

ANR har konfigurerats. Klicka på ikonen för inspelningskällan för att visa primär uppspelning (primär reservuppspelning, primär kodaruppspelning) eller ANR-uppspelning.

Om arbetsstationens konfiguration tillåter det sker uppspelningen direkt från iSCSI-lagringseenheten.





	iSCSI-lagringseenhet
	Primär VRM
	SD-kort

4.2.5

Översikt över lagringsrelaterade händelser

Det här kapitlet beskriver olika lagringsrelaterade händelser.

Buffertlagringens tillstånd

Om ett fel uppstår i nätverket eller på den centrala lagringsplatsen ser ANR-funktionen till att kodaren överför den lokalt buffrade inspelningen av den saknade tidsperioden till den centrala lagringsplatsen när felet har åtgärdats.

Buffertlagringstillstånden är:

- **Lagringstillstånd okänt**
- **Lagringstillstånd OK**
- **Lagringstillståndet Kritisk buffertfyllningsnivå**
- **Lagringstillståndsfel**

Buffertöverskridning

Den här händelsen anger att lagringsbufferten redan är full och att registreringen inte längre överförs till den centrala lagringen.

Lagringstillstånd / Läget Sekundär lagring

Lagringstillstånd visar status på anslutningen mellan en kamera och det centrala lagringsutrymmet. Händelsen **Lagringstillståndsfel** utlöses om kameran förlorar anslutningen till det centrala lagringsutrymmet. Om fränkopplingen bara varar en kort stund indikerar den här händelsen inte nödvändigtvis att videodata går förlorade.

Lagringstillståndet är:

- **Lagringstillstånd okänt**
- **Lagringstillstånd OK**
- **Lagringstillståndsfel**

Status för inspelningsmonitor / Status för sekundär inspelningsmonitor

Den här händelsen indikerar en inspelningsövervakning. Så länge kameran kan buffra inspelning i RAM-minnet utlöses inget larm. Händelsen **Status för monitor inspelningsavbrott** utlöses bara om videodata inom de senaste två minuterna inte längre kan buffras i RAM-minnet och går förlorade. Händelsen anger också tidsperioden då videodata förlorades.

Inspelningsövervakarens status är:

- **Okänd status för inspelningsmonitor**
- **Status för inspelningsmonitor OK**
- **Status för monitor inspelningsavbrott**

Se

- *ANR (Automated Network Replenishment), sidan 27*
- *Konfigurera händelser och larm, sidan 297*

4.3

Larmhantering

Larm kan konfigureras separat så att de kan hanteras av en eller flera användargrupper. När ett larm uppstår visas det larmlistan för alla användare i användargrupperna som konfigurerats till att motta detta larm. När någon av dessa användare börjar jobba på larmet försvinner det från larmlistan för alla andra användare.

Larm visas på en arbetsstations larmmonitor. Det här beteendet beskrivs i följande paragrafer.

Larmflöde

1. Ett larm uppstår i systemet.
2. Larmmeddelanden visas i larmlistan för alla användare som konfigurerats för detta larm. Larmvideo visas omedelbart på konfigurerade monitorer. Om det är ett automatiskt visat larm (auto pop-up), visas larmet också automatiskt på Operator Client-arbetsstationens larmmonitorer.
Om larmet är konfigurerat som ett autoclear-larm, tas larmet bort från larmlistan efter autoclear-tiden (konfigurerad i Configuration Client).
På monitorer ersätts alla fyrbildsvyer från VIP XD:er temporärt av helskrämsvisning.
3. En av användarna godkänner larmet. Larmvideon visas då på den användarens arbetsstation (om den inte redan visas via auto pop-up). Larmet tas bort från alla andra larmlistor och larmvideovisningar.
4. Den användare som godkände larmet utlöser ett arbetsflöde som kan inkludera inläsning av en åtgärdsplan samt att skriva in kommentarer. Detta steg är frivilligt – krav på arbetsflöden kan konfigureras av administratören.
5. Slutligen rensar användaren larmet. Det här tar bort larmet från larmlistan och larmdisplayen.
På en monitorgrupp återgår monitorerna till de kameror som visades innan larmet inträffade.

Larmbildsfönster

1. När larmvideo ska visas ersätter larmbildsfönstret live- eller uppspelningsbildfönstret på monitorn som har konfigurerats för larmvisning.
2. Varje larm får en rad med bildrutor. Det går att associera upp till 5 bildrutor med varje larm. Dessa bildrutor kan visa livevideo, uppspelningsvideo eller kartor.
I en skärmgrupp kan varje larm visa kameror på en rad med monitorer. Antalet kameror i raden begränsas av antalet kolumner i monitorgruppen. Monitorer i raden som inte används för larmvideo kan konfigureras till att antingen fortsätta med sin nuvarande visning eller visa en tom skärm.
3. Larm med högre prioritet visas ovanför larm med lägre, både på monitorrader och på larmraderna för Operator Client-arbetsstationsvisningen.
4. Om larmbildfönstret är helt fullt med larmbildsrader och ytterligare ett larm måste visas, staplas larmen med lägst prioritet på den nedersta raden i larmbildfönstret. Du kan stega genom de staplade larmen med kontrollerna på den vänstra sidan av larmraden.

Du kan stega genom larmstaplarna i monitorgrupper med kontrollknapparna i fönstret **Monitorer** på Operator Client-arbetsstationsdisplayen. Monitorer med larm indikeras av röda ikoner med blinkande lysdioder.

Larmnamn, tidpunkt och datum kan visas antingen på alla monitorer eller bara på den första monitorn i larmraden.

5. Administratören kan konfigurera ordningsbeteendet för larm med samma prioritet:
 - Sist-in-först-ut (Last-in-First-out [LIFO])-läge: I denna konfiguration infogas nya larm ovanför äldre larm med samma prioritet.
 - Först-in-först-ut (First-in-First-out (FIFO))-läge: I denna konfiguration infogas nya larm nedanför äldre larm med samma prioritet.
6. Ett larms bildrad kan visas i larmbildfönstret på ett av två sätt:
 - När det genereras (auto pop-up). Det här uppstår när larmprioriteten är högre än visningsprioriteten.
 - När larmet godkänns. Det här uppstår när larmprioriteten är lägre än visningsprioriteten.

Auto pop-up-larm

Larm kan konfigureras så att de automatiskt visas (pop up) i larmbildfönstret baserat på larmprioritet. Varje användargrups live- och uppspelningsdisplayer har också tilldelats prioriteter. När larm tas emot som har en högre prioritet än användarens display, visar larmet automatiskt sin larmrad i larmbildfönstret. Om larmbildfönstret inte visas just då ersätter det automatiskt live- eller uppspelningsbildfönstret på den larmaktiverade monitorn.

Fastän auto pop-up-larm visas i larmbildfönstret godkänns de inte automatiskt. De kan visas på flera användares skärmar samtidigt. När en användare godkänner ett auto pop-up-larm tas det bort från alla andra användares larmlistor och larmvisningar.

Larmhantering vid avstängning

Alla aktiva larm bevaras om servern stängs av. Larmen återställs och visas igen i fönstret

Larmlista när systemet startas om.

Larm i tillståndet **Godkänd** eller **Arbetsflöde** återställs automatiskt till tillståndet **Aktiv** när systemet startas om. Kommentarer som angetts för larm i tillståndet **Arbetsflöde** bevaras.



Obs!

Larmdata sparas automatiskt varje minut. Det betyder att den maximala dataförlusten motsvarar data ackumulerade under en minut.

Se

- *Konfigurera längden på förlarm och efterlarm, sidan 302*

4.4

ONVIF-händelsemappning



Obs!

Observera att den här funktionen snart upphör.

Använd ONVIF Camera Event Driver Tool för enkel ONVIF-händelsemappning.

Se *Starta ONVIF Camera Event Driver Tool från Configuration Client, sidan 197.*

Avsedd användning

Det avsedda bruket är mappning av ONVIF-händelser till BVMS-händelser. ONVIF-händelser kan då utlösa BVMS-larm och inspelning.

Du kan definiera standardhändelsemappningar som bara är giltiga för en specifik ONVIF-enhet, för samtliga ONVIF-enheter med samma modell och tillverkare eller för samtliga ONVIF-enheter från samma tillverkare. Standardhändelsemappningar tilldelas automatiskt alla aktuella ONVIF-kodare som läggs till med sökguiden för BVMS eller manuellt.

När du lägger till en ONVIF-kodare i BVMS-konfigurationen utan en anslutning till denna ONVIF-kodare, tilldelas inga händelsemappningar. Du kan uppdatera en sådan ONVIF-kodare med händelsemappningar från en ONVIF-kodare från samma tillverkare och/eller av samma modell som du redan har lagt till.

Du definierar händelsemappningar som är specifika för var och en av de följande källorna:

- ONVIF-kodare
- Kameror som hör till denna ONVIF-kodare
- Reläer som hör till denna ONVIF-kodare
- Ingångar som hör till denna ONVIF-kodare

Exempel

I en ONVIF-kamera inträffar en rörelseavkänningshändelse. Denna händelse ska utlösa en

Rörelse upptäckt-händelse i BVMS.

För att lyckas med detta konfigurerar du följande för denna ONVIF-kamera:

- ONVIF-ämne (*MotionDetection*)
- ONVIF-dataobjekt (*motion*)
- ONVIF-datatyp (*boolean*)
- ONVIF-datavärde (*true*)

Obs! Det räcker inte att enbart konfigurerar **Rörelse upptäckt**-händelsen. Konfigurerar även **Rörelse stoppad**-händelsen. Du måste alltid konfigurerar ett händelsepar.

Import eller export av en mappningstabell

Du kan exportera en mappningstabell på en dator där du har skapat den och importera den på en annan dator där den mappningstabell som krävs inte finns.

Felsökning

Du kan skapa loggfiler för felsökning.

Se

- *Konfigurerar en ONVIF-mappningstabell, sidan 225*
- *Aktivera loggning för ONVIF-händelser, sidan 349*
- *Sidan ONVIF-kodarhändelser, sidan 221*

4.5

Utloggning vid inaktivitet

Avsedd användning

Utloggning vid inaktivitet används för att skydda en Operator Client eller Configuration Client under operatörens eller administratörens frånvaro.

Du kan konfigurerar per användargrupp att Operator Client ska loggas ut automatiskt efter en viss tidsperiod utan aktivitet.

Inga användargrupper är tillgängliga för Configuration Client. Inställningen för utloggning vid inaktivitet gäller enbart användaren **admin**.

Alla åtgärder med tangentbord, mus och CCTV-tangentbord påverkar den angivna tidsperioden för utloggning vid inaktivitet. Automatiska aktiviteter i Operator Client påverkar inte tidsperioden. Automatiska aktiviteter i Configuration Client såsom överföring av fast programvara eller iSCSI-konfiguration förhindrar utloggning vid inaktivitet.

Du kan även konfigurerar utloggning vid inaktivitet för en BVMS-webbklient.

Strax före en utloggning vid inaktivitet visas en dialogruta som påminner användaren om att aktivt förhindra utloggningen.

I loggboken registreras en inträffad utloggning vid inaktivitet.

Exempel

Om en arbetsstation är placerad på en allmän plats minimerar utloggning vid inaktivitet risken för att obehöriga personer kommer åt en oönskad Operator Client-arbetsstation.

En medlem i administratörsgruppen ska loggas ut automatiskt vid inaktivitet. Däremot kan annan personal (operatörsgruppen) som endast bevakar bildskärmen utan att använda systemet föredra att inte loggas ut vid inaktivitet.

Begränsningar

Client SDK-aktivitet stöder inte utloggning vid inaktivitet, vilket innebär att aktiviteten hos Client SDK inte påverkar den angivna tidsperioden.

Se

- *Dialogrutan Alternativ (menyn Inställningar), sidan 114*
- *Sidan Användarfunktioner, sidan 314*

4.6

Versionsoberoende Operator Client

För kompatibilitetsläget måste både Operator Client och Management Server ha en högre version än 5.5.

Någon som använder Operator Client kan logga in på en Management Server där en tidigare programversion körs.

Om servern tillgängliggör en nyare konfiguration än den som finns på Operator Client-arbetsstationen kopieras den automatiskt till Operator Client-arbetsstationen. Användaren kan bestämma om den nya konfigurationen ska hämtas eller inte.

Operator Client tillhandahåller en begränsad uppsättning funktioner och ansluts till denna Management Server.

De följande funktionerna som är relaterade till Management Server är tillgängliga efter inloggning på en Management Server med en tidigare version:

- Användarinställningar
- Starta manuell inspelning
- Visa enhetstillstånd
- Växla relätillstånd
- Söka i Loggboken
- Det går inte att söka händelser.
- Serversökning
- Fjärreexport

4.6.1

Arbeta med kompatibilitetsläget

Den här funktionen finns i versioner som är senare än 5.5.

En BVMS Operator Client ger feedback om sitt tillstånd i bild och ord.

Följande Operator Client-tillstånd är möjliga:

- : Operator Client är ansluten till Management Server.
- : Operator Client är inte ansluten till Management Server. En anledning kan vara att Management Server har kopplats bort fysiskt från nätverket.

- : Detta tillstånd visas bara efter en återupprättad anslutning till Management Server. Alla berörda funktioner fungerar igen, men konfigurationen av Operator Client är föråldrad eftersom det finns en nyare konfiguration i systemet. Uppdatera konfigurationen genom att logga in igen.
- : Denna tillståndssikonen visas när Management Server har en tidigare version eller vissa Management Server-server inte körs.
- : Denna ikon visas när Management Server har anslutningsproblem. Detaljerad information om servertillståndet finns i verktygstipset.
- : Denna ikon visas när flera inloggningar i Management Server med samma användarnamn nekas.
- : Denna ikon visas när tillståndet är okänt
- : Den här ikonen visas när licensen inte är tillgänglig
- : Den här ikonen visas när Management Server finns i en annan tidszon.

4.7

Visningslägen för en panoreringskamera

I det här kapitlet beskrivs visningslägena för en panoreringskamera som finns i BVMS.

Följande visningslägen är tillgängliga:

- Cirkelvy
- Panoreringsvy
- Beskuren vy

Panoreringsläget och det beskurna visningsläget skapas under kantdistorsionsprocessen i BVMS. Korrigering av kantdistorsion används inte.

Administratören måste konfigurera monteringspositionen för en panoreringskamera i Configuration Client.

Vid behov kan du ändra storleken på en kameras bildruta. Bildrutans bildförhållande är inte begränsat till 4:3 eller 16:9.

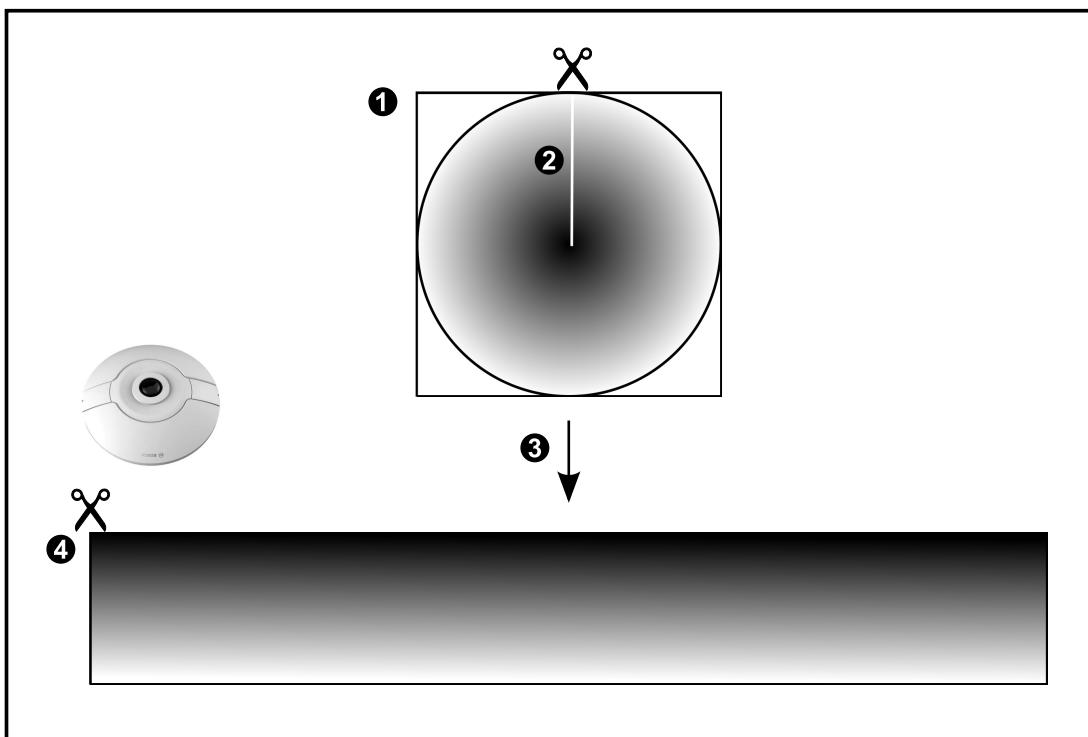
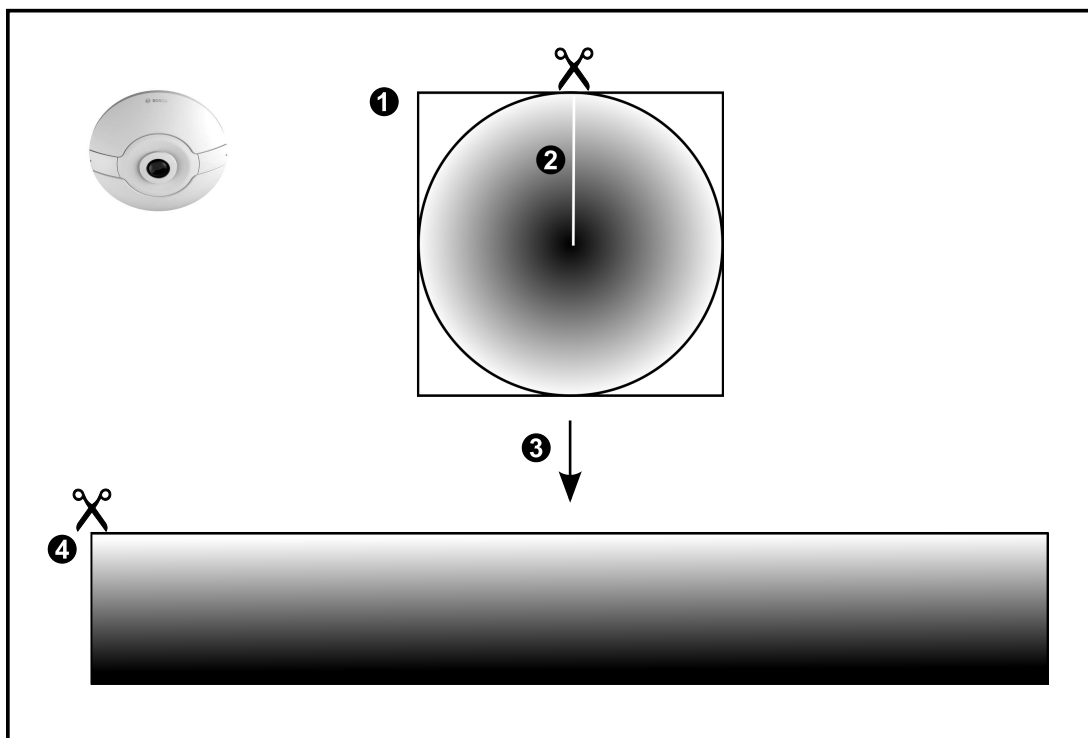
Se

- *Konfigurera fördefinierade positioner och extra kommandon, sidan 279*

4.7.1

360° panoreringskamera – golv- eller takmonterad

I följande bild illustreras distorsionskorrigeringen för en 360° kamera som är golv- eller takmonterad.

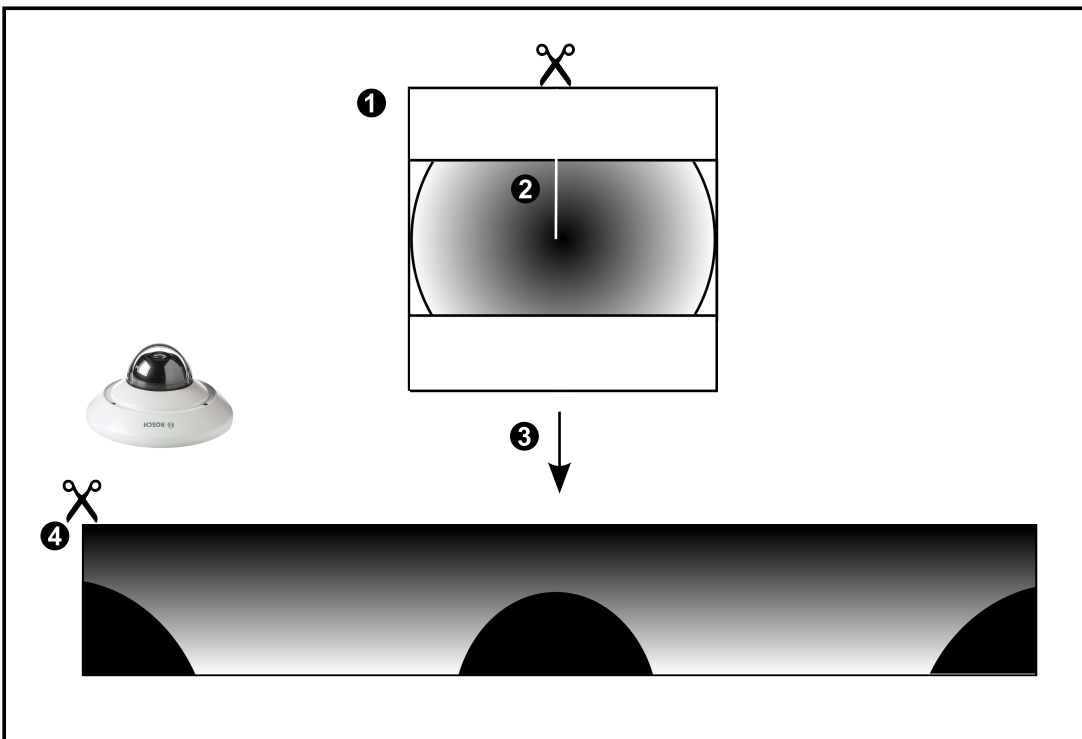
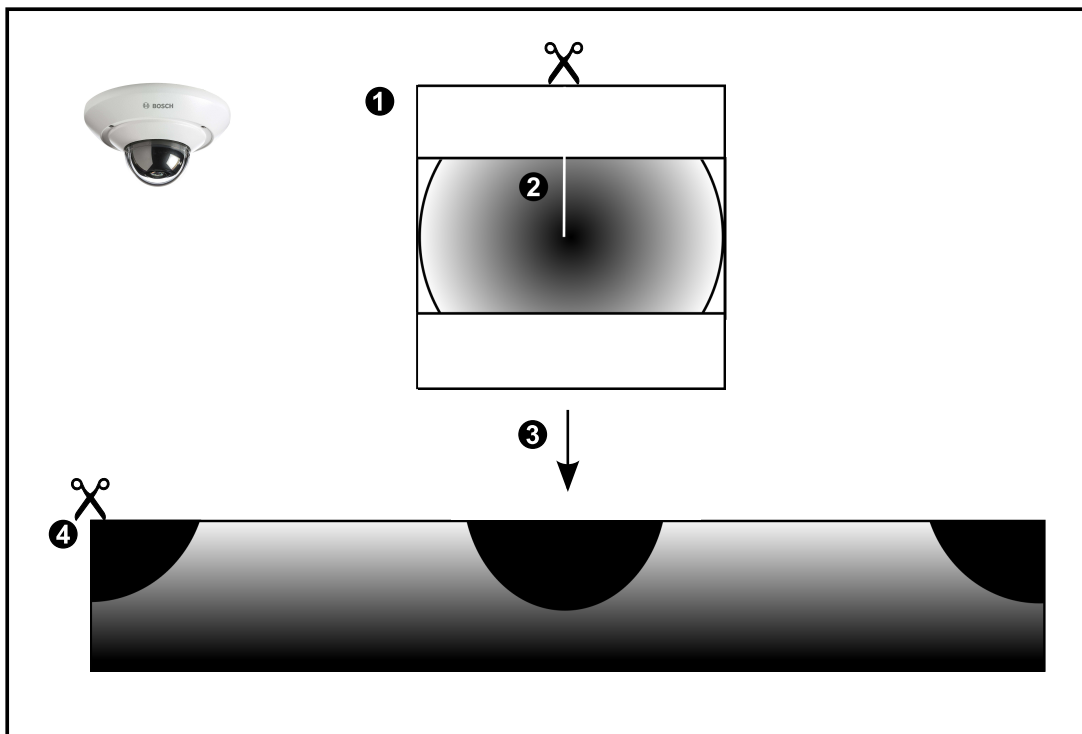


1	Cirkelformad bild	3	Distorsionskorrigering
2	Klipplinje (operatören kan ändra position när bilden inte är inzoomad)	4	Panoreringsvy

4.7.2

180° panoreringskamera – golv- eller takmonterad

I följande bild illustreras distorsionskorrigeringen för en 180° kamera som är golv- eller takmonterad.

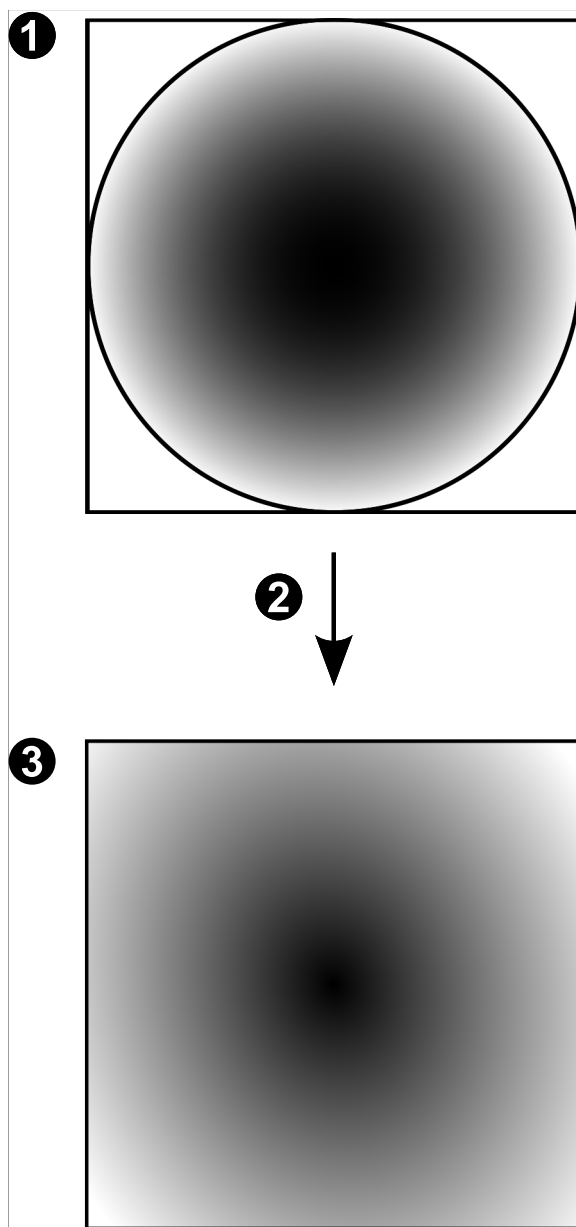


1	Cirkelformad bild	3	Distorsionskorrigering
2	Klipplinje (operatören kan ändra position när bilden inte är inzoomad)	4	Panoreringsvy

4.7.3

360° panoreringskamera – väggmonterad

I följande bild illustreras distorsionskorrigeringen för en 360° kamera som är väggmonterad.

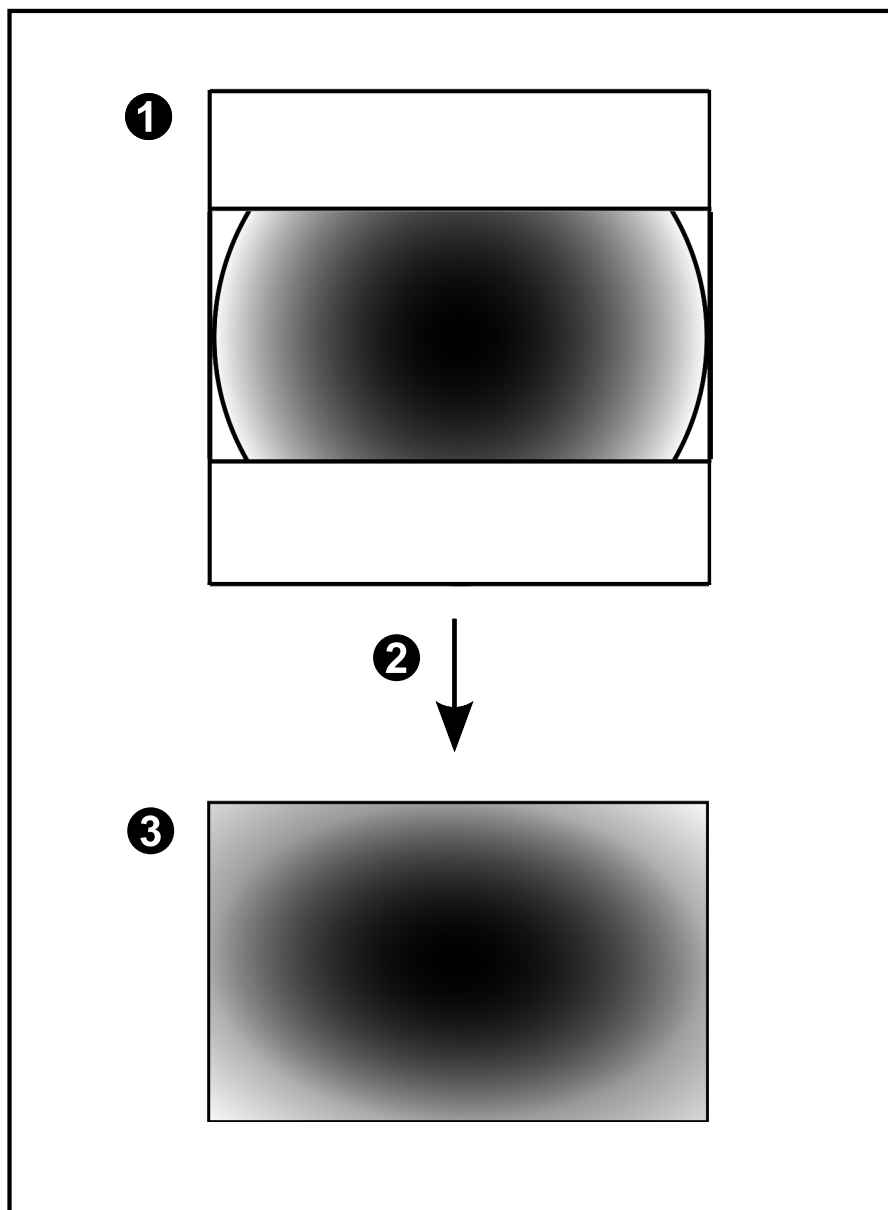


1	Cirkelformad bild	3	Panoreringsvy
2	Distorsionskorrigering		

4.7.4

180° panoreringskamera – väggmonterad

I följande bild illustreras distorsionskorrigeringen för en 180° kamera som är väggmonterad.



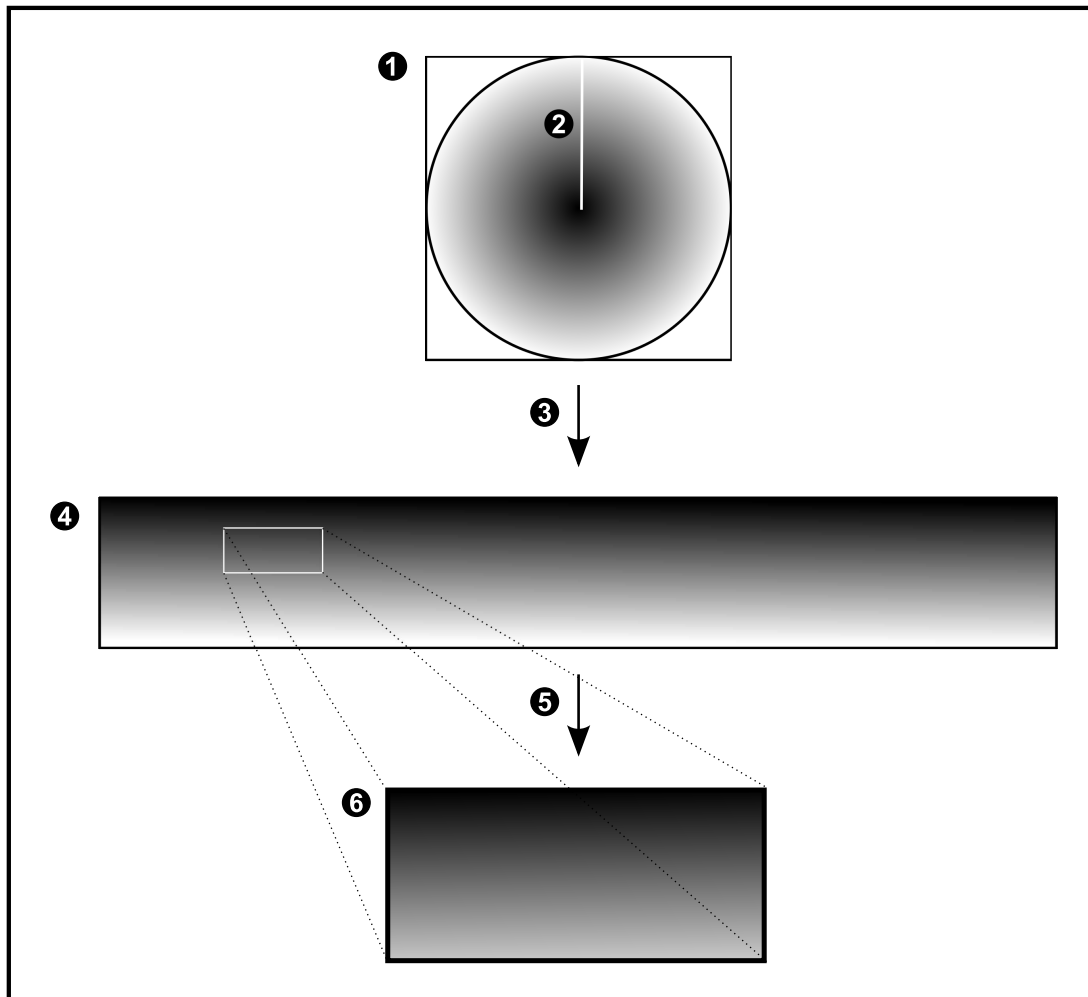
1	Cirkelformad bild	3	Panoreringsvy
2	Distorsionskorrigering		

4.7.5

Beskuren vy på en panoreringskamera

I följande exempelbild illustreras beskärningen för en 360° kamera som är golv- eller takmonterad.

Den rätlinjiga sektionen som används för beskärning är fast. Du kan ändra sektionen i den beskurna bildrutan med de tillgängliga PTZ-kontrollerna.



1	Cirkelformad bild	4	Panoreringsvy
2	Klipplinje (operatören kan ändra position när bilden inte är inzoomad)	5	Beskärning
3	Distorsionskorrigering	6	Beskuren bildruta

4.8 SSH-tunnel

BVMS har fjärranslutningar med SSH-tunnel (Secure Shell).

SSH-tunnlar skapar en krypterad tunnel via en SSH-protokoll/uttagsanslutning. Den krypterade tunneln kan överföra både krypterad och okrypterad trafik. I Bosch SSH-implementeringen används också protokollet Omni-Path som är ett högpresterande kommunikationsprotokoll med låg latens från Intel.

Tekniska aspekter och begränsningar

- SSH-tunnlar använder port 5322. Porten kan inte ändras.
- SSH-tjänsten måste installeras på samma server som BVMS Management Server.
- (Enterprise) användarkonton måste ha konfigurerade lösenord. (Enterprise) användarkonton utan något lösenord kan inte logga in med en SSH-anslutning.
- Kameror med lokal lagring stöder inte SSH-anslutning.
- Configuration Client kan inte fjärransluta via SSH. Configuration Client-anslutningen måste göras via portmappning.
- Operator Client kontrollerar anslutningen med SSH-tjänsten var 15:e sekund. Om anslutningen avbryts testas anslutningen en gång i minuten av Operator Client.

Portmappning

- Konfigurera en vidarekoppling av portar för BVMS Management Server för att port 5322 ska kunna användas både till interna och externa anslutningar. Detta är den enda portmappning du behöver göra i hela systemet. Portmappning för BVMS behövs inte.

Krypterad kommunikation

När anslutningen har upprättats via SSH-tunneln krypteras all kommunikation mellan BVMS Management Server och en fjärrklient.

4.9 Flera sökvägar

BVMS tillhandahåller flera sökvägar för Dual Controller-system. Flera sökvägar (multipath) är en feltoleransteknik som definierar fler än en fysisk sökväg mellan kameran och dess iSCSI-lagringseinheter via redundanta nätverksanslutningar. Flera sökvägar innebär att du kan spela in och spela upp videodata även i händelse av ett iSCSI-styrenhetsfel.

Krav och begränsningar

- En NetApp E2800 Dual Controller iSCSI-enhet är installerad.
- Version 6.43 av den fasta programvaran tillåter att enheter som spelar in till E2800 kan använda alternativa sökvägar.
- VRM 3.71 för övervakning och loggning av enheter med flera sökvägar är aktiverat.
- Två fysiska iSCSI-portar är konfigurerade per styrenhet: 2×2 RJ45 eller 2×2 optisk.
- Länkhastigheten måste vara 10 Gbit/s för att uppnå full kapacitet.
- Dual Simplex-läget som används i E2700 stöds inte längre.

Mer information om installationen av DSA E2800 Full Duplex finns i installationshandboken för DSA E-Series E2800.

5 Maskinvara som kan användas

**Obs!**

Anslut inte en enhet till fler än en BVMS! Detta kan leda till inspelningsluckor och andra oönskade effekter.

Du kan ansluta följande maskinvara till BVMS:

- Mobila videoklienter som iPhone eller iPad via DynDNS
- Olika IP-kameror, kodares och ONVIF-kameror (endast live eller via Video Streaming Gateway)
Ansluten via nätverk
- Endast livekodare med lokal lagring
Ansluten via nätverk
- iSCSI-lagringsenheter
Ansluten via nätverk
- Analoga kameror
Ansluten till kodare,
- Avkodare
Ansluten via nätverk
- Monitorer
Anslutna till en avkodare, till en Bosch Allegiant-matris, till en BVMS-klientarbetsstation
- Bosch Allegiant-matris (version av fast programvara: 8.75 eller senare, MCS-version: 2.80 eller senare)
Ansluten till en COM-port på Management Server eller till en fjärrdator och till en IP kodare i nätverket.
- KBD-Universal XF-tangentbord
Ansluten till en USB-port på en BVMS-arbetsstation.
- Bosch IntuiKey-tangentbord
Ansluten till COM-porten på en BVMS-arbetsstation (version av fast programvara: 1.82 eller senare) eller till en maskinvaruavkodare (VIP XD).
Om du ansluter tangentbordet till en arbetsstation kan användaren styra hela systemet med tangentbordet. Om du ansluter tangentbordet till en VIP XD-avkodare kan användaren endast styra monitorer med tangentbordet.
- SMTP e-postserver
Ansluten via nätverk
- POS
Ansluten via nätverk
- ATM
Ansluten via nätverk
- Nätverksövervaknings enhet
Ansluten via nätverk
- I/O-moduler
Ansluten via nätverk
Endast ADAM-enheter kan hanteras.

Alla enheter som är anslutna via nätverket är anslutna till en switch. Datorerna för BVMS är också anslutna till denna enhet.

5.1 Installation av maskinvara

BVMS har funktioner för följande maskinvarukomponenter:

- KBD-Universal XF-tangentbord
 - Bosch IntuiKey-tangentbord
 - Bosch Allegiant-matrisen med kameror och monitor: anslutna till en COM-port på en av datorerna i nätverket samt till IP-kodare anslutna till nätverket
 - Kodares med analoga kameror
 - Kodare med lokal lagring
 - IP-kameror och IP AutoDomes
 - Monitorer anslutna till en avkodare (monitorgrupper för larmbearbetning är möjliga)
 - DVR-system med kameror
 - ATM / POS -enheter
 - I/O-moduler
- Endast ADAM-enheter kan användas.

5.2

Installera ett KBD Universal XF-tangentbord

**Obs!**

Läs mer i instruktionerna som levereras med KBD-Universal XF-tangentbordet och som finns i onlineproduktkatalogen.

Mer information

För mer information, programvarunedladdningar och dokumentation går du till www.boschsecurity.com och sedan till motsvarande produktsida.

Du kan ansluta följande maskinvara till BVMS:

- Mobila videoklienter som iPhone eller iPad via DynDNS
- Olika IP-kameror, kodares och ONVIF-kameror (endast live eller via Video Streaming Gateway)
Ansluten via nätverk
- Endast livekodare med lokal lagring
Ansluten via nätverk
- iSCSI-lagringsenheter
Ansluten via nätverk
- Analoga kameror
Ansluten till kodare,
- Avkodare
Ansluten via nätverk
- Monitorer
Anslutna till en avkodare, till en Bosch Allegiant-matris, till en BVMS-klientarbetsstation
- Bosch Allegiant-matris (version av fast programvara: 8.75 eller senare, MCS-version: 2.80 eller senare)
Ansluten till en COM-port på Management Server eller till en fjärrdator och till en IP kodare i nätverket.

5.3

Ansluta ett Bosch IntuiKey-tangentbord till BVMS

I det här kapitlet får du information om konfiguration av Bosch IntuiKey-tangentbord.

5.3.1

Scenarion för Bosch IntuiKey-tangentbordsanslutningar

Du kan ansluta ett Bosch IntuiKey-tangentbord till COM-porten på en BVMS-arbetsstation (scenario 1) eller till en maskinvaruavkodare (t.ex. VIP XD, scenario 2).

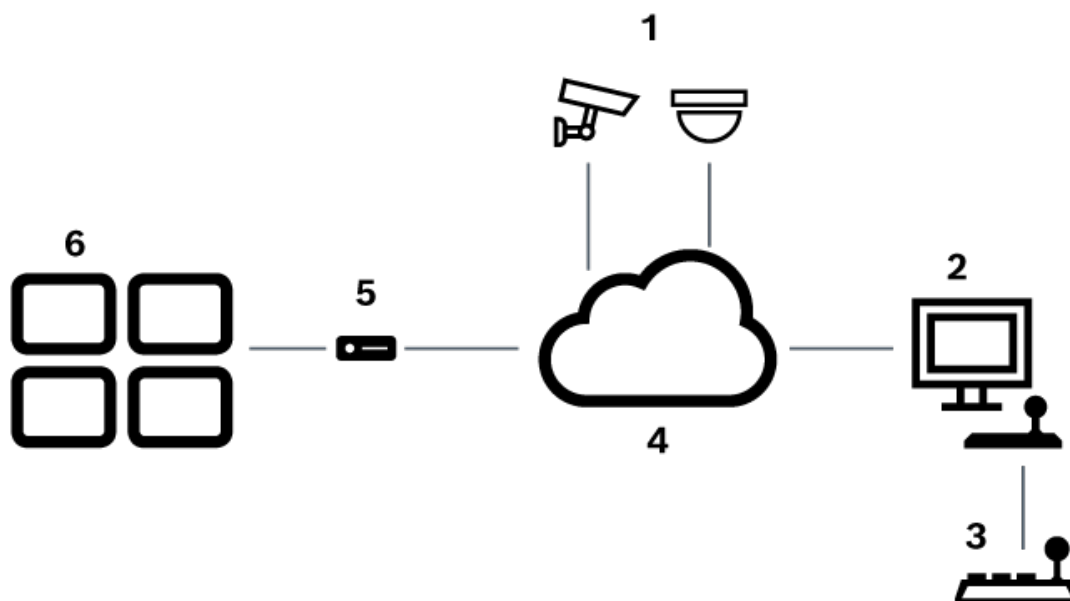
Om du ansluter tangentbordet till en BVMS-arbetsstation kan du styra hela systemet. Om du ansluter tangentbordet till en avkodare kan du endast styra systemets analoga monitorer.

Om du ansluter tangentbordet till en Enterprise Operator Client kan du styra kamerorna för en specifik Management Server genom att först trycka på servertangenten och ange numret på servern och sedan ange kameranumret.

**Obs!**

Använd angiven Bosch-kabel för att ansluta Bosch IntuiKey-tangentbordet till en BVMS-arbetsstation.

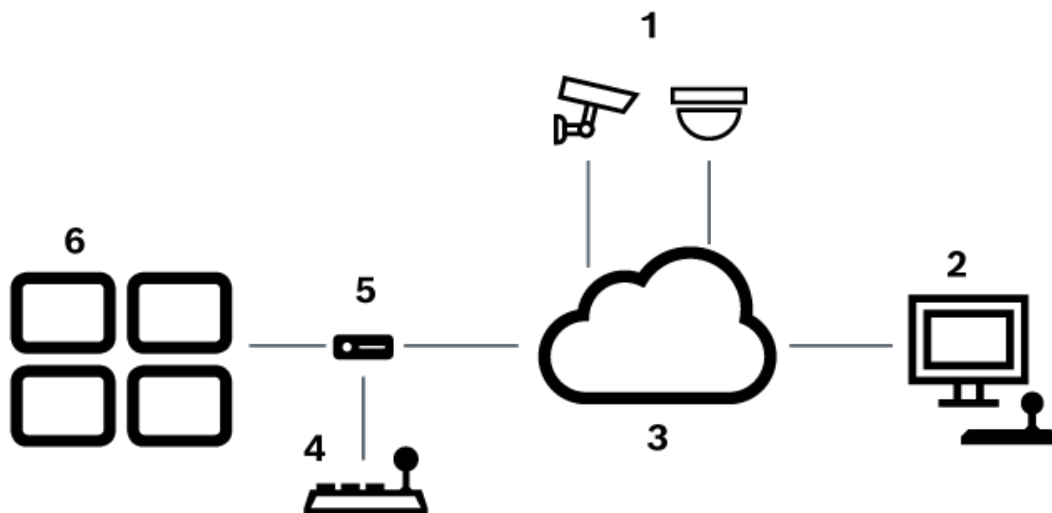
För att ansluta Bosch IntuiKey-tangentbordet till en VIP XD-avkodare behöver du en kabel som ansluter en seriell COM-port på tangentbordet till det seriella gränssnittet på avkodaren. Information om anslutningar finns i Ansluta ett CCTV-tangentbord till en avkodare.

Bosch IntuiKey-tangentbord anslutet till en BVMS-arbetsstation

Figur 5.1: Scenario 1: Bosch IntuiKey-tangentbord anslutet till en Bosch Video Management System-arbetsstation

1	Flera olika kameror är anslutna till nätverket via kodare
2	BVMS-arbetsstation
3	Bosch IntuiKey-tangentbord
4	BVMS-nätverk
5	Avkodare
6	Monitorer

Bosch IntuiKey-tangentbordet är anslutet till en avkodare



Figur 5.2: Scenario 2: Bosch IntuiKey-tangentbordet är anslutet till en avkodare

1	Flera olika kameror är anslutna till nätverket via kodare
2	BVMS-arbetsstation
3	BVMS-nätverk
4	Bosch IntuiKey-tangentbord
5	Avkodare
6	Monitorer

Följ dessa hänvisningar för att få detaljerad information om tillgängliga fönster:

- *Sidan Tilldela tangentbord, sidan 147*

Följ dessa hänvisningar för att få detaljerad information om tillgängliga stegvisa instruktioner:

- *Konfigurera ett Bosch IntuiKey-tangentbord (sidan Inställningar) (arbetsstation), sidan 130*
- *Konfigurera ett Bosch IntuiKey-tangentbord (avkodare), sidan 137*
- *Konfigurera en avkodare för användning med ett Bosch IntuiKey-tangentbord, sidan 137*

Se

- *Sidan Tilldela tangentbord, sidan 147*

5.3.2

Ansluta ett Bosch IntuiKey-tangentbord till en avkodare

Konfigurera avkodaren

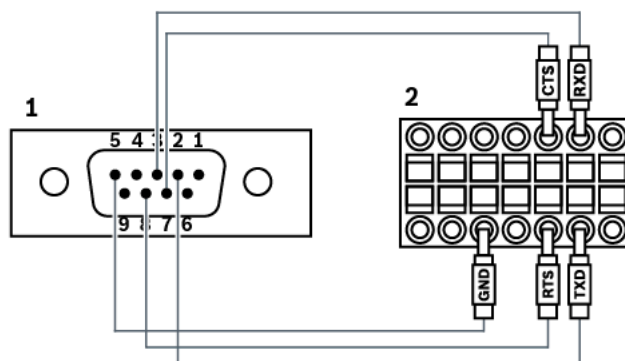
Se *Konfigurera en avkodare för användning med ett Bosch IntuiKey-tangentbord, sidan 137* för information.

Anslutningar mellan COM-port och VIP XD-dekoder

I följande tabell listas anslutningarna mellan en RS232-adapter och ett seriellt gränssnitt till en VIP XD-dekoder:

RS232-adapter	Seriellt gränssnitt till en VIP XD-dekoder
1	
2	TX
3	RX
4	
5	GND
6	
7	CTS
8	RTS
9	

Följande illustration visar stiftkonfigurationen på en standard RS232-adapter (1) och stiftkonfigurationen på avkodarens seriella adapter (2):



5.3.3

Uppdatera Bosch IntuiKey-tangentbordets inbyggda programvara

1. På en PC installerar du IntuiKey-nedladdaren.
2. Starta uppgraderingsverktyget för den inbyggda programvaran för IntuiKey.
3. Anslut tangentbordet med korrekt seriell kabel (kontakta Bosch-support om någon sådan kabel inte finns tillgänglig) till den här PC:n.
4. På tangentbordet, tryck på snabbtangenter Keyboard Control, sedan Firmware Upgrade.
5. Ange lösenordet: 0 och 1 samtidigt.
Tangentbordet är i bootloader-läge.
6. På PC:n, klicka på Browse för att välja filen med den inbyggda programvaran: till exempel kbd.s20
7. Ställ in COM-porten.
8. Klicka på knappen Download för att hämta den fasta programvaran.
På tangentbordsdisplayen visas Programming.
Tryck inte på Clr-tangenten nu. Om du gör det så kan inte tangentbordet användas efter omstart (se Anteckning här nedan).

9. Klicka på Browse för att välja språk: till exempel 8900_EN_..82.s20
På tangentbordsdisplayen visas Programming.
10. Stäng uppgraderingsverktyget för den inbyggda programvaran för IntuiKey.
11. På tangentbordet, tryck på knappen Clr för att avsluta programmet.
Tangentbordet startas om. Vänta några sekunder tills menyn för val av tangentbordsspråk visas.
12. Välj önskat språk med en snabbtangent.
Standardstartdisplayen visas.

**Obs!**

För att direkt starta i boot-läge kan du koppla loss strömförsörjningen från tangentbordet, trycka på 0 och 1 samtidigt, koppla in strömförsörjningen igen, samt släppa 0 och 1.

5.4

Ansluta Bosch Allegiant-matrisen till BVMS

BVMSAllegiant-matrisgränssnittet ger smidig åtkomst till analoga matriskameror i Operator Client-gränssnittet. Allegiant-kameror ser nästan likadana ut som IP-kameror. Den enda skillnaden är en liten rutnätssymbol på kameran som indikerar att det är en Allegiant-kamera. Du kan visa kameror på samma sätt som IP-kameror. De finns med både i det logiska trädet och i anläggningskartorna, och användare kan lägga till dem till sina favoritträd. På video-fönsterstyrning för Allegiant-anslutna PTZ-kameror stöds, och du kan enkelt visa Allegiant-kameror på monitorer som är anslutna till IP-avkodare.

BVMS tillhandahåller ett gränssnitt för matrisväxlaren via programmet Allegiant MCS (Master Control Software). MCS körs, i det här fallet, osynligt i bakgrunden. Den här programvaran ger Allegiant ett effektivt och händelsestyrt gränssnitt. Den ger snabb händelserespons i realtid från Allegiant till BVMS. Om till exempel en defekt koaxialkabel leder till ett videoavbrott i Allegiant, skickas omedelbart ett meddelande till BVMS. Du kan även programmera BVMS att svara på Allegiant-larm.

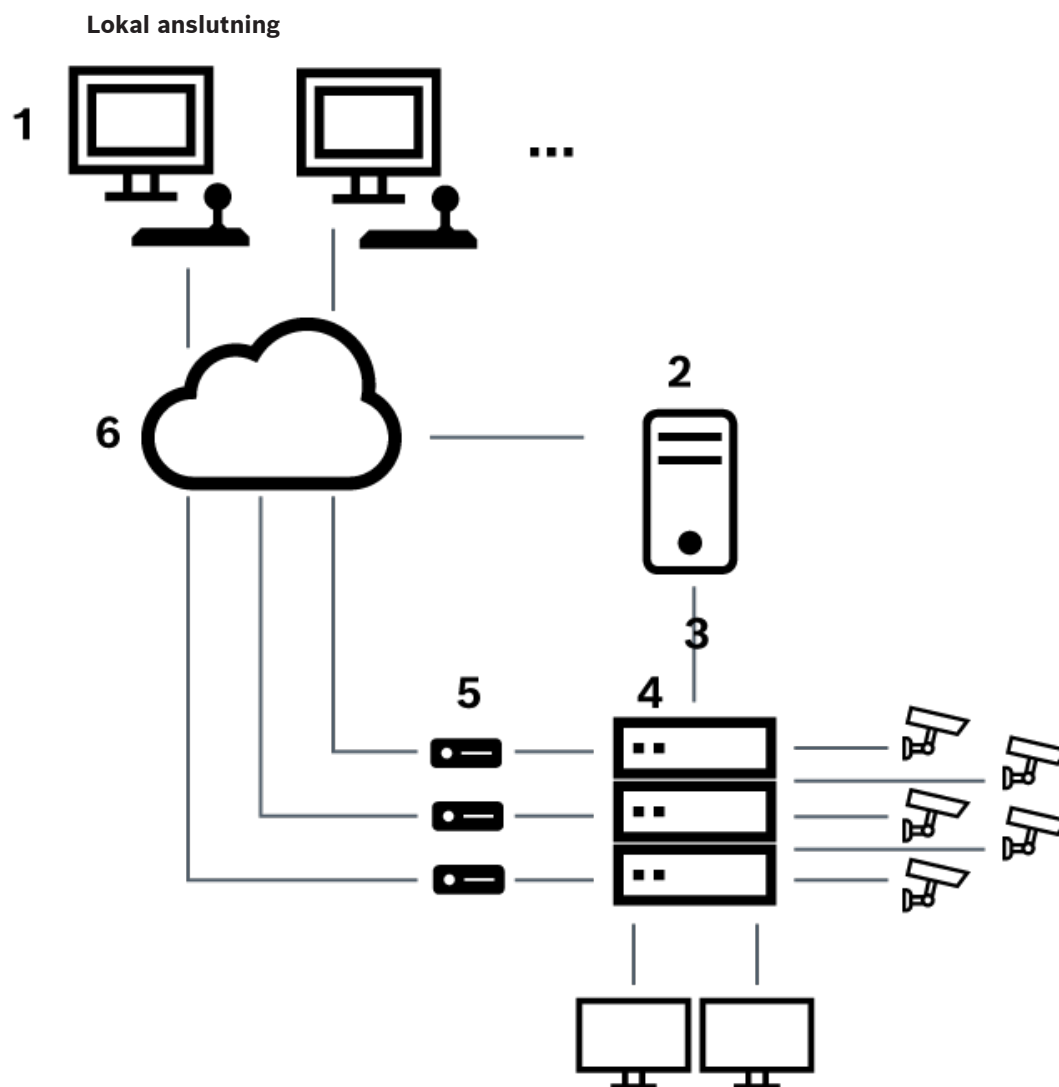
5.4.1

Översikt av Bosch Allegiant-anslutning

Om du vill skapa en anslutning mellan BVMS och ett Allegiant-matrisväxlarsystem kan du konfigurera en styrkanal mellan BVMS och Allegiant-matrisen.

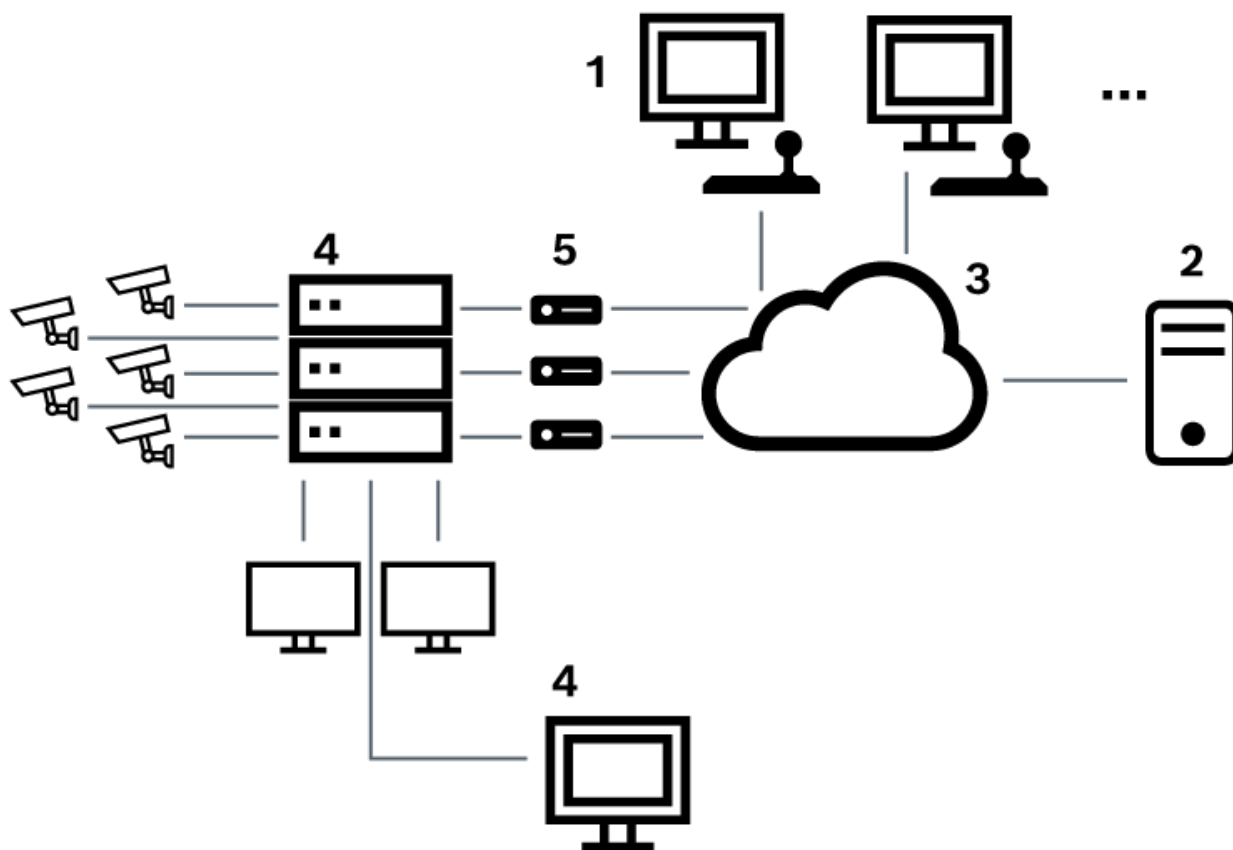
Två scenarier är möjliga:

- Lokal anslutning
Management Server styr Allegiant-matrisen.
- Fjärranslutning
En dedikerad Bosch Allegiant PC, ansluten till nätverket, styr Allegiant-matrisen.



Figur 5.3: Lokal anslutning av Bosch Video Management System till en Bosch Allegiant-matrisswitch

1	BVMS-klientarbetsstationer
2	Management Server med Master Control Software
3	RS-232-anslutning
4	Allegiant-matris
5	kodare
6	Nätverk

Fjärranslutning**Figur 5.4:** Fjärranslutning av Bosch Video Management System till en Bosch Allegiant-matrisswitch

1	BVMS-klientarbetsstationer
2	Management Server med Master Control Software
3	Nätverk
4	Allegiant-PC med Master Control Software
5	RS-232-anslutning
6	kodare
7	Allegiant-matris

5.4.2**Konfigurera kontrollkanalen**

Utför följande uppgifter för att konfigurera kontrollkanalen:

- Anslutningar
- Installera programvaran
- Skapa en Allegiant-konfigurationsfil
- Lägga till Allegiant-matrisen till BVMS
- Konfigurera användarnamn

Anslutningar

Om du vill konfigurera kontrollkanalen mellan BVMS och Allegiant-matrisen ansluter du en dator genom en RS-232-serieport till Allegiants konsolport (använd den specificerade kabeln från Bosch för anslutning). Detta kan vara BVMS Management Server eller vilken dator som helst i nätverket.

Installera Allegiant-Master Control Software

1. Stoppa tjänsten Management Server om den körs (**Start > Kontrollpanelen > Tjänster > Högerklicka på BVMS Management Server > Stoppa**)
2. Installera Allegiant Master Control Software på Management Server och på Allegiant-PC:n (i förekommande fall).
3. Konfigurera en Allegiant-fjärrdator så att programmet Allegiant Network Host (Id_alghw.exe) startas när datorn startas. Detta startar nödvändiga Allegiant-tjänster som gör att andra datorer i nätverket kan komma åt Allegiant. Programvaran arbetar osynligt. Det är inte nödvändigt att ha en dongel ansluten till den här datorn.
Om du vill att tjänsten ska startas automatiskt när datorn startas kopierar du en länk till Id_alghw.exe till startmappen på datorn.

Skapa en Bosch Allegiant-konfigurationsfil

1. Använd Allegiant Master Control Software och skapa en Allegiant-konfigurationsfil som anger vilken dator som är ansluten till Allegiant-matrisen. Denna uppgift kräver en maskinvarunyckel för Master Control Software.
2. På Transfer-menyn klickar du på Communication Setup. På Current Host-listan anger du DNS-namnet för datorn som är ansluten till Allegiant-matrisen och anger serieportparametrarna (COM-portnummer, överföringshastighet o.s.v.) för den Allegiant-anslutna serieporten. Detta gör att Master Control Software på Management Server eller på datorn kan gå online med Allegiant-systemet. Om detta inte fungerar säkerställer du att antingen Master Control Software eller programmet Allegiant Network Host körs på datorn som är kopplad till Allegiant-matrisen och att nätverkssäkerheten är konfigurerad så att den tillåter fjärråtkomst till den här datorn.
3. På Transfer-menyn klickar du på Upload. Välj alla tabeller och klicka på Upload. Om du vill spara konfigurationsfilen väljer du en katalog.
4. Stäng Master Control Software.

Lägga till Bosch Allegiant-matrisen till BVMS

1. Starta BVMSManagement Server-tjänsten, starta Configuration Client och lägg till Allegiant-enheten genom att lägga till denna konfigurationsfil (se Lägga till en enhet för stegvis instruktion).
2. Säkerställ att Allegiant Master Control Software-konfigurationsfilen som används i BVMS motsvarar den aktuella Allegiant-konfigurationen.
BVMS kör de nödvändiga delarna av Master Control Software osynligt i bakgrunden.

Konfigurera användarnamnet för inloggning till Allegiant-tjänsterna

Om Allegiant-matrisen är ansluten till en dator i nätverket och inte till Management Server ska du kontrollera att Allegiant-tjänsterna på denna dator och på Management Server loggar in med samma användarkonto. Den här användaren måste vara medlem av en administratörsgrupp.

Ytterligare noteringar i dokumentationen

Följ dessa hänvisningar för att få detaljerad information om tillgängliga fönster:

- *Sidan Matrisväxlare, sidan 126*

Följ dessa hänvisningar för att få detaljerad information om tillgängliga stegvisa instruktioner:

- *Konfigurera en Bosch Allegiant-enhet, sidan 127*

Se

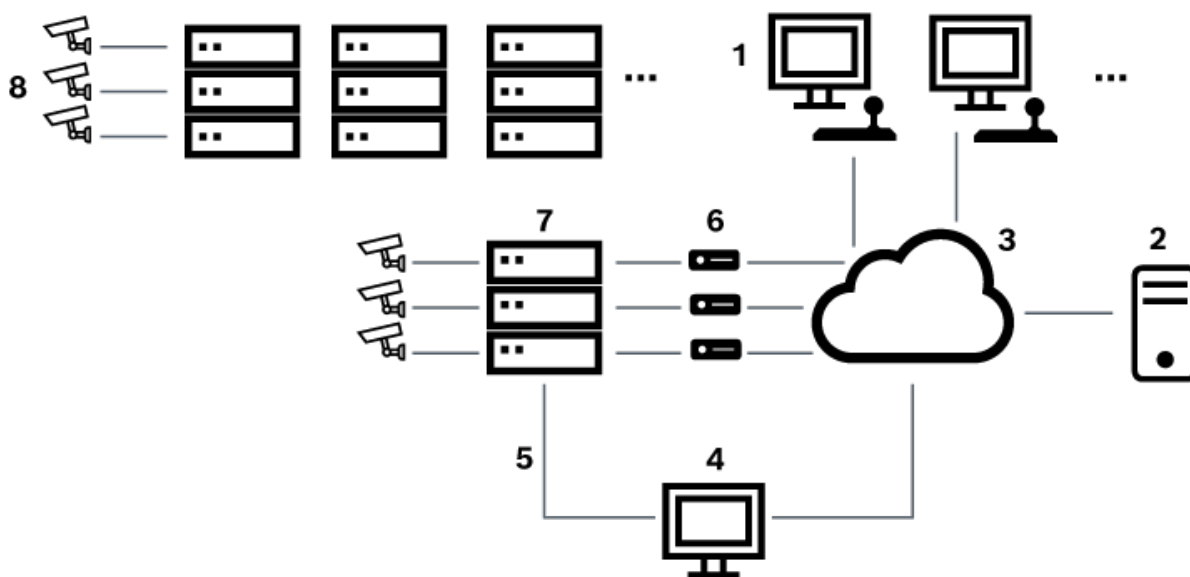
– *Sidan Matrisväxlare, sidan 126*

5.4.3

Bosch Allegiant koncept för satellitsystem

Allegiant-matrisväxlaren gör det möjligt att sammankoppla flera Allegiant-system genom att använda satellitkonceptet. I detta fall kan flera Allegiant-system för BVMS se ut som ett stort system som ger åtkomst till alla systemets kameror.

I ett Allegiant-satellitsystem är monitorutgångarna från en slav-Allegiant kopplade till videoingångarna hos master-Allegiant. Denna anslutning kallas en stamlinje. Dessutom upprättas en kontrollkanal mellan mastern och slaven. När en kamera från en slav-Allegiant begärs av master-Allegiant skickas ett kommando till slaven och instruerar den att växla den begärda kameran till en stamlinje. På samma gång växlar master-Allegiant stamlinjeingångarna till den begärda monitorutgången för master-Allegiant. Detta slutför videoanslutningen från den begärda slavkameran till den önskade mastermonitorn.



Figur 5.5: Bosch Allegiant-system utökat med satellitväxlare

1	BVMS-klientarbetsstationer
2	Management Server med Master Control Software
3	Nätverk
4	Allegiant-PC med Master Control Software
5	RS-232-anslutning
6	kodare
7	Allegiant-matris
8	Allegiant-satellitmatris

Du kan tillämpa satellitkonceptet så att en Allegiant kan vara både en master och en slav. På detta sätt kan varje Allegiant se de andras kameror. Det är endast nödvändigt att ansluta stamlinjen och kontrollledningarna åt båda hållen och att konfigurera Allegiant-tabellerna korrekt.

Konceptet kan utökas ytterligare, utan praktisk gräns, till flera Allegiant-system. En Allegiant kan ha många slavar och den kan vara en slav till många masterenheter. Du kan programmera Allegiant-tabellerna att tillåta eller neka användaråtkomst till kameravyer så som det krävs av platsens regler.

5.5 Allegiant CCL-kommandon som stöds i BVMS

För att kunna använda CCL-kommandon behöver du CCL-användarhandboken. Du hittar handboken i produktkatalogen online, i dokumentavsnittet om respektive LTC Allegiant-matris.

Kommando som stöds	Beskrivning	Anmärkningar
Växling/sekvens		
LCM	Växla logisk kamera till monitor	LCM, LCM+ och LCM- är likvärdiga.
LCMP	Växla logisk kamera till monitor med förpositionering	
MON+CAM	Växla fysisk kamera till monitor	
MON-RUN	Kör sekvens efter monitornummer	
MON-HOLD	Håll sekvens efter monitornummer	
SEQ-REQ	Sekvensbegäran	
SEQ-ULD	Sekvensöverföring	
Mottagare/drivenhet		
R/D	Grundläggande styrkommandon	
REMOTE-ACTION	Styrkommandon för samtidig panorering/lutning/zoomning	
REMOTE-TGL	Växla mellan styrkommandon för panorering/lutning/zoomning	
PREPOS-SET	Ange förprogrammerat läge för kamera	
PREPOS	Anropa förprogrammerat läge för kamera	
AUX-ON AUX-OFF	Styrkommandon för extra enhet – Extra enhet på – Extra enhet av	

Kommando som stöds	Beskrivning	Anmärkningar
Växling/sekvens		
VARSPPEED_PTZ	Kommandon för styrning med variabel hastighet	
Larm		Används för att styra virtuella ingångar. Till exempel stänger "+alarm 1" den virtuella ingången 1 och "-alarm 1" öppnar den virtuella ingången 1
+ALARM	Aktivera ett larm	Öppnar en virtuell ingång i BVMS.
-ALARM	Inaktivera ett larm	Stänger en virtuell ingång i BVMS.
System		
TC8x00>HEX	Ställ in hexadecimalt läge	
TC8x00>DECIMAL	Ställ in decimalläge	

6 Komma igång

I det här kapitlet får du information om hur du kommer i gång med BVMS.

6.1 Installera programvarumodulerna

**Obs!**

Installera alla programvarumoduler på de datorer som är avsedda för användning med respektive modul.

Gör så här:

Stäng Configuration Client innan du startar BVMS-installationen.

1. Starta Setup.exe eller starta BVMS-installationen på välkomstskärmen.
2. Välj de moduler som ska installeras på den här datorn i nästa dialogruta.
3. Följ instruktionerna på skärmen.

6.2 Använda konfigurationsguiden

Config Wizard är avsedd för snabb och enkel konfiguration av mindre system. Med Config Wizard kan du konfigurera ett system med VRM-, iSCSI-system, Mobile Video Service, kameror, inspelningsprofiler och användargrupper.

Du måste lägga till iSCSI-systemen manuellt på en programvaruinstallation av standardtyp. Användargrupper och deras behörigheter konfigureras automatiskt. Du kan lägga till och ta bort användare samt ställa in lösenord.

Config Wizard kan komma åt Management Server endast på den lokala datorn.

Du kan spara en aktiverad konfiguration som säkerhetskopia och importera konfigurationen senare. Du kan ändra den här importerade konfigurationen efter slutförd import.

Med Config Wizard läggs den lokala VRM till automatiskt på både standardinstallationer och på DIVAR IP 3000 och DIVAR IP 7000.

På en DIVAR IP 3000 och en DIVAR IP 7000 läggs även den lokala iSCSI-enheten till automatiskt om den inte redan är tillgänglig.

På en DIVAR IP 3000 och på en DIVAR IP 7000 läggs en lokal Mobile Video Service till automatiskt om den inte redan är tillgänglig.

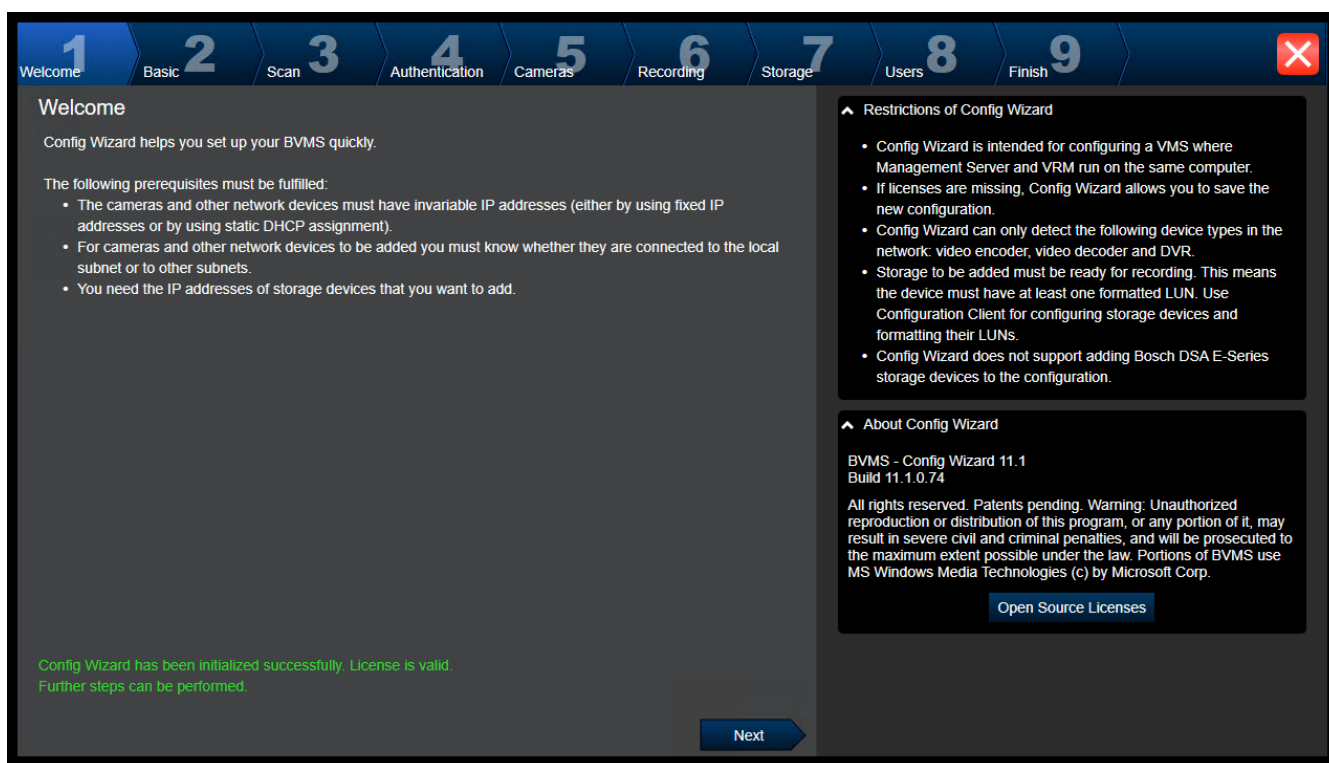
**Obs!**

Om avkodare ska användas i systemet måste samma lösenord för behörighetsnivån user användas för alla kodare.

Så här startar du Config Wizard:

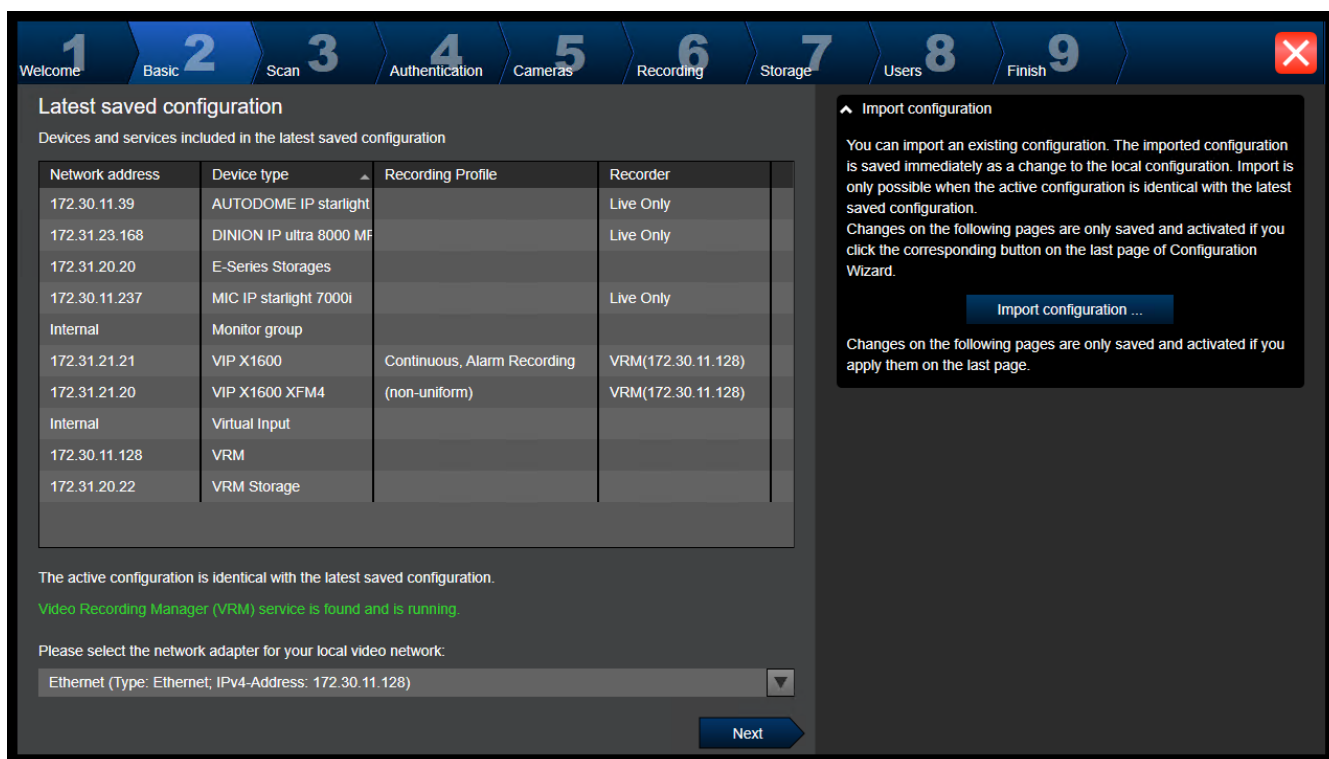
- Klicka på **Start > Alla program > BVMS > Config Wizard**
Sidan Welcome visas.

Sidan Welcome



► Fortsätt genom att klicka på **Next**.

Sidan Basic



På den här sidan visas den senast sparade konfigurationen. Du kan byta ut den befintliga konfigurationen genom att importera en BVMS-fil. Den ändrade konfigurationen sparas men aktiveras inte när du klickar på **Next**.

Du kan välja nätverksadaptorn i den dator som är ansluten till videoenheterna (IP-kameror, kodare, avkodare, iSCSI-lagringsenheter) i systemet. Nätverksadaptorns IP-adress används som IP-adress för VRM, VSG och det lokala iSCSI-lagringssystemet.

Klicka på **Port Mapping** och ange den offentliga IP-adressen eller DNS-namnet om systemet ska vara åtkomligt via internet.

Sidan Scan

Select video devices to be added

Selected 185 of 193

✓	Device name	IP address	MAC address	Device type
☐	DINION IP ultra 8000 MP	172.31.22.240	00-07-5f-95-81-e7	DINION IP ultra 8000 MP
☐	FD IP micro 5000 (172.31.22.217)	172.31.22.217	00-07-5f-84-24-e6	FLEXIDOME IP micro 5000 I
☒	Flexidome IP Dynamic 7000	172.31.22.144	00-07-5f-7a-c2-b6	FLEXIDOME IP dynamic 7000
☒	FlexiDome panorama 5000	172.31.22.62	00-07-5f-88-74-dd	FLEXIDOME IP panoramic 5000
☒	172.30.11.198	172.31.23.202	00-07-5f-c6-71-64	FLEXIDOME multi 7000i
☐	Camera 4	172.31.23.161	00-07-5f-99-2a-4e	DINION IP starlight 7000 HD
☐	Camera 3	172.31.23.160	00-07-5f-99-2f-9f	DINION IP starlight 7000 HD
☒	FLEXIDOME IP starlight 6000	172.31.23.147	00-07-5f-8d-21-a5	FLEXIDOME IP starlight 6000
☒	FLEXIDOME IP panoramik 7000	172.31.23.124	00-07-5f-84-89-e6	FLEXIDOME IP panoramic 7000
☒	FLEXIDOME IP panoramik 7000	172.31.23.123	00-07-5f-84-8a-e1	FLEXIDOME IP panoramic 7000
☒	FLEXIDOME IP panoramik 7000	172.31.23.122	00-07-5f-8b-f8-c1	FLEXIDOME IP panoramic 7000
☐	DINION IP ultra 8000 MP	172.31.23.114	00-07-5f-8d-33-bd	DINION IP ultra 8000 MP
☒	FLEXIDOME IP indoor 5000	172.31.23.113	00-07-5f-7c-64-32	FLEXIDOME IP indoor 5000
☐	DINION IP ultra 8000 MP	172.31.23.102	00-07-5f-98-28-4c	DINION IP ultra 8000 MP
☐	Dinon IP 5000i IR	172.31.23.95	00-07-5f-93-cf-bb	DINION IP 5000i IR
☐	Dinon IP Starlight 6000 HD	172.31.23.145	00-07-5f-8d-21-d3	DINION IP starlight 6000 HD

Scan options

Range of network scan:

☒ Local subnet only (recommended)

☐ Across subnets

Rescan network

Change network addresses

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

Change IP Addresses

Next

Obs!

En avsökning av enheter kan ta tid. Du kan avbryta avsökningen. Alla enheter som redan har avsökts visas i tabellen.

Alla videoenheter som inte ingår i den senast sparade konfigurationen visas på sidan.

Avmarkera kryssrutorna för de enheter som inte ska läggas till i konfigurationen och klicka sedan på **Next**.

Om de valda enheterna inte finns i samma IP-intervall som DIVAR-IP-systemet kan du ändra IP-adressen för enheterna genom att ange en startadress för enheternas IP-intervall.

Sidan Authentication

Enter passwords for devices

Device name	IP address	User name	Password	Status
172.31.23.150	172.31.23.150	service		⚠
Decoder (172.31.21.204)	172.31.21.204	service	*****	🔒
NDC-284-P (172.31.23.15)	172.31.23.15	service		🔒
VIP10 (172.31.23.24)	172.31.23.24	service		🔒
VIPX-1600XFMD (172.31.22.4)	172.31.22.4	service		🔒
VIPX-1600XFMD (172.31.22.5)	172.31.22.5	service		🔒

You must authenticate at the devices of your system. To authenticate, enter the password for the user account of each device. An open green lock indicates a successful authentication. Devices with a status indicated by a yellow warning sign require an initial password; they do not allow logon with an empty password.

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

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

Den här sidan används för autentisering på videoenheter som är lösenordsskyddade. För enkel autentisering på flera enheter med samma lösenord kan du använda urklipp (CTRL+C, CTRL+V):

1. Klicka om du vill aktivera **Show passwords**.
2. Markera en rad med en autentiserad enhet (ett grönt lås visas), tryck på CTRL+C, markera flera rader med röda lås och tryck på CTRL+V).

Lösenordskontrollen utförs automatiskt om du inte har angett ytterligare något tecken i lösenordsfältet inom några sekunder eller om du klickar någonstans utanför fältet.

Du kan ange ett globalt standardlösenord för alla enheter som för närvarande inte är lösenordsskyddade.

Om en enhet kräver ett initialt lösenord visas ⚠.

Ställa in ett initialt lösenord:

1. Skriv det nya lösenordet i fältet **Password**.
2. Klicka på **Set Initial Passwords**.

Det initiala lösenordet ställs in.

Obs! Så länge du inte har angett det initiala lösenordet för alla enheter i listan som kräver en initialt lösenord kan du inte fortsätta.

3. Fortsätt genom att klicka på **Next**.

Sidan Cameras

Specify camera settings

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

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

You can configure recording quality and live quality for each camera. Fractional frame rates (FR) are indicated by the profile names and refer to the fraction of the maximum frame rate of the corresponding camera model.

You can change the settings of the 'Recording quality' and the 'Live quality' columns of multiple cameras simultaneously. To that end select those cameras and change the settings in one of the selected cameras.

If the settings in a column are not identical for all selected cameras, you can click '<no change>' to avoid changing these settings unintentionally.

You can sort cameras in folders. These folders must be created in Configuration Client.

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

Preview

Next

Använd den här sidan när du vill hantera kamerorna i systemet.

Sidan Recording

Specify recording settings

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

Selected 0 of 2

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

You can change the settings for several cameras in parallel: To that end select those cameras and change the settings in one of the selected cameras.

If the settings in a column are not identical for all selected cameras, you can click '<no change>' to avoid changing these settings unintentionally.

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

Motion Alarm Recording in Recording Profiles

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

Next

Bara de kameror som har lagts till nyligen visas på den här sidan. Så fort du aktiverar den här konfigurationen går det inte att ändra dessa kamerors profiltilldelning.

Du kan aktivera rörelseinspelning för inspelningsprofiler när både inspelning och larminspelning är aktiverade. Om det behövs konfigurerar du inspelning och larminspelning i Configuration Client (dialogrutan **Schemalagda inspelningsinställningar**).
VCA aktiveras automatiskt för varje kamera som läggs till.

Sidan Storage

The screenshot displays the 'Storage' configuration page. At the top, a progress bar shows steps 1 through 9, with step 7 ('Storage') currently selected. The page title is 'Add storage'. Below the title, there is a table with two columns: 'IP address' and 'Storage type'. The table is currently empty. To the right of the table, a message reads: 'You can add iSCSI storage devices currently available in the network for storing video recordings. More storage space allows longer storage of the video recordings.' At the bottom right, there is a 'Next' button.

På den här sidan kan ytterligare iSCSI-lagringsenheter läggas till.

Sidan Users

User accounts and passwords

User Groups

- User Groups
 - Admin Group
 - Admin**
 - Operator Group

User Properties

Full name

Description

Password

Strong password policy ☒

Enter new password

Confirm password

Show password

Apply

The password is not set for some of the users, while strong password policy is applied for them.

Next

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

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

For each user, you can enable a strong password policy. The following rules apply:

- Minimum 8 characters
- At least one upper-case letter (A through Z)
- At least one number (0 through 9)
- At least one special character (for example: ! \$ # %)
- Previous password must not be used.

På den här sidan kan du lägga till nya användare till befintliga användargrupper.

- För varje ny användare anger du ett användarnamn och en beskrivning och definierar ett lösenord.

Strong password policy

Kryssrutan **Strong password policy** är förvald för alla nya användargrupper.

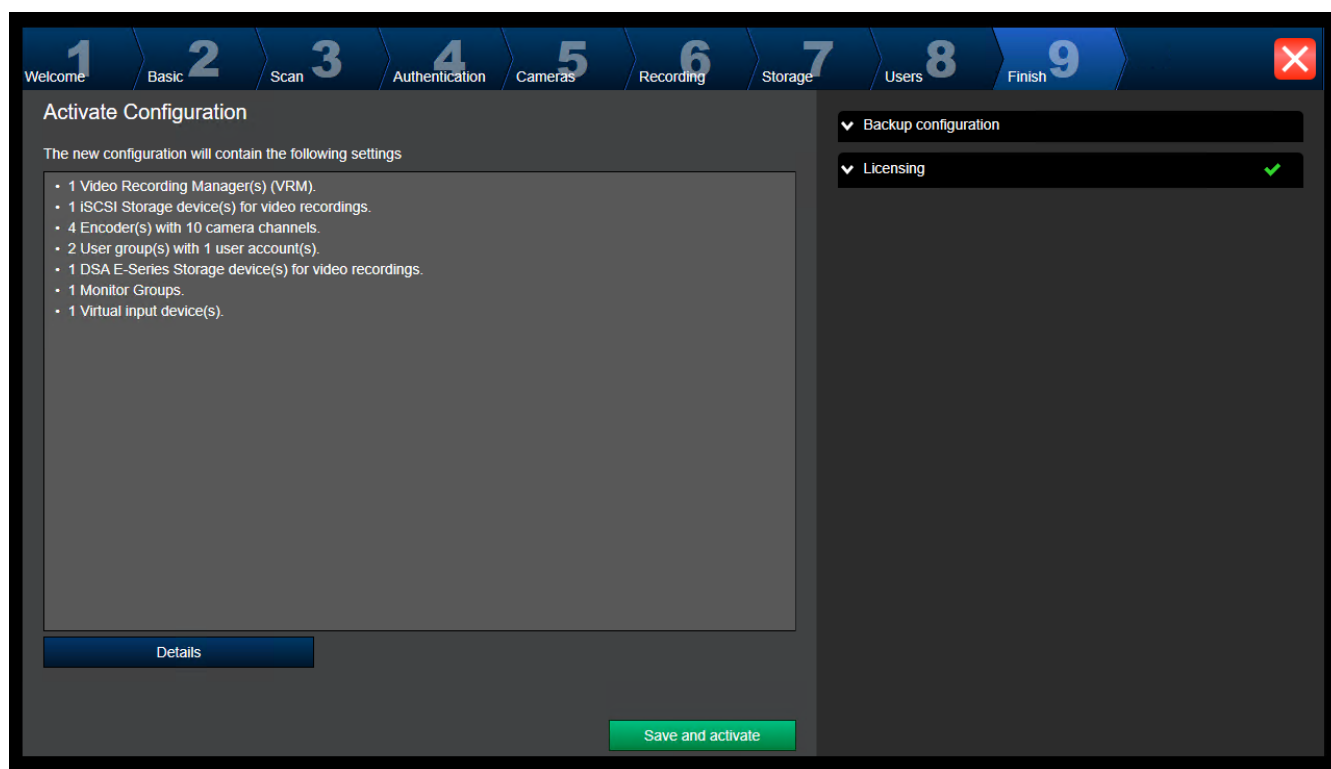
Vi rekommenderar starkt att du behåller den här inställningen för bättre skydd mot obehörig åtkomst.

Följande regler gäller:

- Minsta lösenordslängd enligt inställningen på sidan **Kontopolicyer** för önskad användargrupp.
 - Använd inte någon av de tidigare lösenorden.
 - Använd minst en versal (A–Z).
 - Använd minst en siffra (0–9).
 - Använd minst ett specialtecken (till exempel ! \$ # %).
 - Klicka på **Apply** för att tillämpa inställningarna och klicka sedan på **Next** för att fortsätta.
- Obs!** Om det finns användare som saknar lösenord trots att **Strong password policy** är aktiverat, kan du inte fortsätta. Ange lösenorden som saknas för att fortsätta.

Använd Configuration Client om du vill lägga till användargrupper och ändra behörigheter för användargrupper.

Sidan Finish



Innan du kan aktivera konfigurationen måste du göra detta:

- Ange ett globalt standardlösenord för alla enheter som för närvarande inte är lösenordsskyddade.
- Aktivera ditt licenspaket om så krävs.

Globalt standardlösenord

Om alternativet **Enforce password protection on activation (Inställningar -> Alternativ)** är inaktiverat i Configuration Client tvingas du inte ange ett globalt standardlösenord för att aktivera.

Licensiering

Utvidga **Licensing** och klicka på **License Wizard** om du vill kontrollera eller aktivera ditt licenspaket.

När du klickar på **Save and activate** aktiveras konfigurationen.

Efter lyckad aktivering visas sidan **Finish** igen. Nu kan du lagra en säkerhetskopia av konfigurationen om du vill: Klicka på **Save backup copy**.

När du klickar på **Save and activate** aktiveras konfigurationen.

Efter lyckad aktivering visas sidan **Slutför** igen. Nu kan du lagra en säkerhetskopia av konfigurationen om du vill: Klicka på **Save backup copy**.

6.3

Starta Configuration Client



Obs!

Endast administratörsanvändare kan logga in på Configuration Client.

Den förinställda standardadministratörsanvändaren är användaren som kallas Admin. Det är bara den användaren som kan logga in på Configuration Client när Configuration Client startas första gången.

När du har startat Configuration Client kan du ändra namnet på administratörsanvändaren och byta lösenordet.

Obs!

Du kan inte starta Configuration Client när en annan användare på en annan dator i systemet redan har startat Configuration Client.

Starta Configuration Client:

1. Från menyn **Start** väljer du **Program** > BVMS > Configuration Client.
Dialogrutan för inloggning visas.
2. I fältet **Användarnamn:** anger du ditt användarnamn.
När du startar programmet för första gången anger du Admin som användarnamn. Inget lösenord behövs.
3. Ange ditt lösenord i fältet **Lösenord**.
4. Klicka på **OK**.
Programmet startar.

När administratörsanvändaren startar Configuration Client för första gången visas dialogrutan

Ett brott mot lösenordspolicyn har skett och användaren uppmanas att ställa in ett lösenord för administratörsanvändarkontot. Vi rekommenderar starkt att du använder den här inställningen och att du anger ett starkt lösenord för administratörsanvändarkontot baserat på principreglerna för lösenord.

Se

- *Policy om starka lösenord , sidan 327*
- *Konfigurera den administrativa gruppen, sidan 332*

6.4

Konfigurera språket för Configuration Client

Du konfigurerar språket för Configuration Client oberoende av språket i Windows-installationen.

Så här konfigurerar du språket:

1. På menyn **Inställningar** klickar du på **Alternativ...**
Dialogrutan **Alternativ** visas.
2. Ange önskat språk i listan **Språk**.
Om du väljer posten **Systemspråk**, används språket från din Windows-installation.
3. Klicka på **OK**.
Språket ändras när programmet startas om.

6.5

Konfigurera språket för Operator Client

Du konfigurerar språket för Operator Client oberoende av språket i Windows-installationen och i Configuration Client. Det här steget utförs i Configuration Client.

Så här konfigurerar du språket:

1. Klicka på **Användargrupper** >  . Klicka på fliken **Egenskaper för användargrupper**.
Klicka på fliken **Operatörsbehörigheter**.
2. Välj önskat språk i listan **Språk**.
3. Klicka på  för att spara inställningarna.
4. Klicka på  om du vill aktivera konfigurationen.
Starta om Operator Client.

6.6 Söka efter enheter

Huvudfönster > **Enheter**

Du kan söka efter följande enheter för att lägga till dem i dialogrutan **BVMS Scan Wizard**:

- VRM-enheter
- Kodare
- Endast livekodare
- Endast live-ONVIF-kodare
- Kodare med lokal lagring
- Avkodare
- Video Streaming Gateway-enheter (VSG)
- DVR-enheter

Läs om hur du lägger till enheter genom avsökning i respektive enhetsavsnitt i kapitel *Sidan Enheter, sidan 117*.

Se

- *Lägga till VRM-enheter genom avsökning, sidan 161*
- *Lägga till en endast live-ONVIF-enhet genom avsökning, sidan 220*
- *Lägga till live-enheter från Bosch genom avsökning, sidan 198*
- *Lägga till en enhet, sidan 118*

6.7 Få åtkomst till systemet

Du får åtkomst till systemet genom att utföra följande steg:

1. Utför något av stegen nedan för att ange nätverksadressen för det önskade systemet:
 - Klicka på en förvald listpost.
 - Ange en nätverksadress manuellt.
 - Välj en nätverksadress med hjälp av serversökning.
2. Logga in på de önskade systemen:
 - System med en server
 - Enterprise System

6.8 Använda serversökning

- Med funktionen BVMS Server Lookup kan operatörer ansluta till en BVMS Management Server från en angiven lista med servrar.
- En enskild Configuration Client- eller Operator Client-användare kan ansluta till flera av systemets accesspunkter i följd.
- Systemets accesspunkter kan vara Management Server eller Enterprise Management Server.
- Server Lookup använder en dedikerad Management Server som värd för serverlistan.
- Funktionellt sett kan Server Lookup och Management Server eller Enterprise Management Server köras på en enda dator.
- Server Lookup hjälper dig att hitta systemets accesspunkter med hjälp av deras namn eller beskrivningar.
- När den har anslutits till Management Server tar Operator Client emot händelser och larm från BVMS Management Server och visar direktsänd och inspelad video.

Så här kommer du åt funktionen:

1. Starta Operator Client eller Configuration Client.
Dialogrutan för inloggning visas.

2. Välj **<Adressbok...>** för Configuration Client eller **<Adressbok...>** för Operator Client på listan **Anslutning:**.
Om både privata och offentliga IP-adresser har konfigurerats för en server anges det.
Om du väljer **<Adressbok...>** eller **<Adressbok...>** för första gången visas dialogrutan **Server lookup**.
3. Mata in en giltig nätverksadress för den önskade servern i fältet **(Enterprise) Management Server-adress**.
4. Ange ett giltigt användarnamn och lösenord.
5. Klicka på **Spara inställningar** vid behov.
6. Klicka på **OK**.
Dialogrutan **Server lookup** visas.
7. Välj önskad server.
8. Klicka på **OK**.
9. Om den valda servern har både en privat och en offentlig nätverksadress visas en meddelanderuta med en fråga om du använder en dator inom det privata nätverket för den valda servern.
Servernamnet läggs till i listan **Anslutning:** i dialogrutan för inloggning.
10. Välj den här servern i listan **Anslutning:** och klicka på **OK**.
Om du har markerat kryssrutan **Spara inställningar** kan du välja den här servern direkt när du vill få åtkomst till servern nästa gång.

6.9

Aktivera programvarulicenserna

Första gången du installerar BVMS måste du aktivera licenserna för de programvarupaket som du har beställt, inklusive baspaketet och eventuella tillägg och/eller tillvalsfunktioner.

Så här aktiverar du systemet:

1. Starta BVMS Configuration Client.
2. På menyn **Verktyg** klickar du på **Licenshanterare...**
Dialogrutan **Licenshanterare** visas.
3. Klicka på **Lägg till** för att lägga till licenserna.
Dialogrutan **Lägg till licens** visas.
4. Följ anvisningarna i dialogen.
5. När aktiveringen har lyckats stänger **Lägg till licens** du dialogrutan.
6. Stäng dialogrutan **Licenshanterare**.

För ytterligare information hänvisas till respektive teknisk information om licensen till BVMS.

Se

- *Dialogrutan Licenshanterare (menyn Verktyg), sidan 72*
- *Dialogrutan Licenshanterare (menyn Verktyg), sidan 71*
- *Dialogrutan Lägg till licens, sidan 72*
- *BVMS-licensaktiveringsöversikt, sidan 18*

6.9.1

Dialogrutan Licenshanterare (menyn Verktyg)

Huvudfönster > Menyn **Verktyg** > Kommandot **Licenshanterare...**

Låter dig licensiera BVMS-paket som du har beställt samt uppgradera det med ytterligare funktioner.

Licensstatus

Visar licensstatusen.

Systemets fingeravtryck

För supportändamål rekommenderar vi att du tillhandahåller **Systemets fingeravtryck**.

Installationsplats

När du aktiverar baslicensen i Bosch Remote Portal ger du information om systemets installationsplats. Den här informationen visas här.

Obs! Du kan också tillhandahålla denna information i andra licenser, men endast informationen i baslicensen visas här.

Licenser

1. Klicka på **Lägg till** för att lägga till licenserna.
Dialogrutan **Lägg till licens** visas.
2. Följ anvisningarna i dialogen.

Giltig licens

Visar den gällande baslicensen som du har aktiverat.

Funktioner

- Klicka på **Licenskontroll ...**
Dialogrutan **Licenskontroll** visas.

Visar antalet licensierade funktioner som för närvarande är installerade.

Du kan kontrollera om antalet installerade BVMS-licenser överskrider antalet köpta licenser.

Installerad BVMS-version

Visar den installerade BVMS-versionen, till exempel 11.0.

Licensierade BVMS-versioner

Visar alla BVMS-versioner som ingår och stöds i den aktuella angivna licensfilen.

Till exempel: BVMS 11.0 och alla kommande mindre versioner BVMS 11.x.

Aktiveringsdatum

Visar aktiveringsdatumet för den installerade BVMS-versionen.

Utgångsdatum

Visar utgångsdatumet för den installerade BVMS-versionen. Ett utgångsdatum gäller endast när du installerar en nödlicens eller en försäljningsdemolicens.

Software Maintenance Agreement**Utgångsdatum**

Om du har köpt och aktiverat någon Software Maintenance Agreement, visas utgångsdatumet här.

Se

- Aktivera programvarulicenserna, sidan 71
- Dialogrutan **Lägg till licens**, sidan 72
- Dialogrutan **Licenshanterare (menyn Verktyg)**, sidan 72

6.9.2**Dialogrutan Lägg till licens**

Huvudfönster > menyn **Verktyg** > kommandot **Licenshanterare...** > **Licenser** > **Lägg till**

Gör att du kan lägga till dina köpta licenser eller demolicenser från webbplatsen Bosch Remote Portal remote.boschsecurity.com i ditt BVMS-system.

För att lägga till dina licenser följer du anvisningarna i dialogrutan.

För ytterligare information hänvisas till respektive teknisk information om licensen till BVMS.

6.9.3**Dialogrutan Licenshanterare (menyn Verktyg)**

Huvudfönster > Menyn **Verktyg** > Kommandot **Licenskontroll ...** > Dialogrutan **Licenskontroll**

Visar antalet licensierade funktioner som för närvarande är installerade.

Du kan kontrollera om antalet installerade BVMS-licenser överskrider antalet köpta licenser.
Obs! Om den aktuella systemkonfigurationen överskrider gränserna för de installerade licenserna kan du inte aktivera konfigurationen.

6.10

Underhålla BVMS

Det här kapitlet innehåller information om hur du underhåller ett nyinstallerat eller uppgraderat BVMS.

Utför följande uppgifter för att underhålla systemet:

- Exportera BVMS-konfigurationen och användarinställningarna. Versionshistoriken (alla tidigare aktiverade versioner av konfigurationen) exporteras inte. Vi rekommenderar att du aktiverar konfigurationen innan du exporterar.
 - Anvisningar finns i *Så här exporterar du konfigurationsdata*, sidan 73.

Eller

- Säkerhetskopiera elements.bvms. Detta är nödvändigt om du vill kunna återställa en (Enterprise) Management Server med versionshistorik. Användarinställningarna säkerhetskopieras inte.
 - Anvisningar finns i *Så här utför du en säkerhetskopiering*, sidan 73.
- Spara VRM-konfigurationsfilen (config.xml)
 - Anvisningar finns i *Spara VRM-konfigurationen*, sidan 74.

Den här exporterade konfigurationen innehåller inte systemets historik. Någon återställning är inte möjlig.

Hela systemkonfigurationen inklusive fullständig historik över systemändringar sparas i en fil: C:\ProgramData\Bosch\VMS\Elements.bvms.

Så här exporterar du konfigurationsdata:

1. På menyn **System** väljer du **Exportera konfiguration....**
Dialogrutan **Exportera konfigurationsfil** visas.



Obs! Om den aktuella arbetskopian av konfigurationen inte aktiveras ( är aktiverat) exporterar du arbetskopian i stället för den aktiverade konfigurationen.

2. Klicka på **Spara**.
3. Ange ett filnamn.
Den aktuella konfigurationen har exporterats. En ZIP-fil som innehåller databasen och användardata skapas.

Så här utför du en säkerhetskopiering:

1. Stoppa tjänsten BVMS **Central Server** på (Enterprise) Management Server.
2. Kopiera filen elements.bvms till önskad säkerhetskopieringskatalog.
3. Starta tjänsten BVMS **Central Server** på (Enterprise) Management Server.

VRM-konfigurationen sparas i en krypterad fil, config.xml.

Filen kan kopieras och sparas för säkerhetskopiering medan VRM-tjänsten är i gång.

Filen är krypterad och innehåller alla relevanta VRM-data som:

- Användardata
- Alla systemenheter med respektive VRM-inställningar

Delar av VRM-konfigurationen sparas även i BVMS-konfigurationen. När du ändrar något i dessa data skrivs de till config.xml när BVMS-konfigurationen har aktiverats.

Följande inställningar sparas inte i BVMS-konfigurationen:

- **VRM-inställningar > Huvudinställningar**
- **Nätverk > SNMP**
- **Service > Avancerad**

- **Inspelningsinställningar**
- **Belastningsutjämning**

När du ändrar något på en av dessa sidor skrivs detta direkt till VRM-servern och sparas inte i BVMS-konfigurationen.

Spara VRM-konfigurationen:

- ▶ Kopiera Config.xml till en säker plats.
För en primär VRM-enhet kan du hitta den här filen i följande katalog:
C:\ProgramData\Bosch\VRM\primary
För en sekundär VRM-enhet kan du hitta den här filen i följande katalog:
C:\ProgramData\Bosch\VRM\secondary

6.11 Byta en enhet

I det här kapitlet ges information om hur du reparerar systemet när till exempel enheter slutar fungera och måste bytas ut.

Grundkrav

Underhållet har utförts.

Se

- *Underhålla BVMS, sidan 73*

6.11.1 Byta en MS/EMS

Det är ingen skillnad mellan ett Management Server-byte och ett Enterprise Management Server-byte.

Du kan antingen återställa den gamla Management Server- eller Enterprise Management Server-konfigurationen eller importera den exporterade konfigurationen.

När du återställer konfigurationen förblir server-ID:t oförändrat.

När du importerar konfigurationen används server-ID:t för det nya systemet. Du behöver ett nytt server-ID om du vill skapa ett Enterprise System med en exporterad konfiguration som du importerar i varje Management Server som en mall. Varje Management Server i detta Enterprise System måste ha ett unikt server-ID.

Du kan importera en exporterad konfiguration och användarinställningarna för denna konfiguration. Användarinställningarna innehåller användarna som var tillagda i konfigurationen och deras inställningar i Operator Client såsom fönsterstorlekar och favoriter.

Obs! En konfigurationsimport återställer inte den gamla konfigurationens versionshistorik. När du importerar en konfiguration importeras inte några användarinställningar. Du måste återställa de exporterade användarinställningarna manuellt.

Så här importerar du konfigurationen:

1. På menyn **System** klickar du på **Importera konfiguration....**
Dialogrutan **Importera konfigurationsfil** visas.
2. Markera den file som du vill importera och klicka på **Öppna**.
Dialogrutan **Importera konfiguration...** visas.
3. Ange det aktuella lösenordet och klicka på **OK**.
Configuration Client startas om. Du måste logga in på nytt.
Den importerade konfigurationen är inte aktiverad, men den kan redigeras i Configuration Client.

Så här återställer du en exporterad konfiguration:

Det går bara att komma åt (kopiera, ta bort) den här filen när tjänsten BVMS **Central Server** är stoppad.

1. Stoppa tjänsten BVMS **Central Server** på (Enterprise) Management Server.

2. Om det behövs ändrar du säkerhetskopieringsfilens namn till Elements.bvms.
3. Ersätt den befintliga filen Elements.bvms.
4. Starta tjänsten BVMS **Central Server** på (Enterprise) Management Server.

Obs! Om du vill återställa systemet till en tom konfiguration stoppar du tjänsten och tar bort Elements.bvms.

Fler konfigurationsfiler:

- Elements.bvms.bak (från och med V.2.2): Automatisk säkerhetskopieringsfil med den senaste aktiveringen och historik. Senare ändringar i konfigurationen som inte har aktiverats säkerhetskopieras inte.
- Elements_Backup*****.bvms: Konfiguration från en äldre version. Den här filen skapas efter en programuppdatering.

Återställa exporterade användarinställningar:

1. Extrahera ZIP-filen som skapades under underhållsexporten.
Filen *export.bvms* och katalogen *UserData* extraheras.
2. På önskad (Enterprise) Management Server: Kopiera katalogen *UserData* till C:
`\ProgramData\Bosch\VMS\`.

6.11.2

Byta en VRM

Krav

- Installerat operativsystem med rätt nätverksinställningar och rätt version av VRM.

Så här byter du VRM-enheten inifrån BVMS:

1. Starta BVMS Configuration Client.
2. Välj VRM-enheten i enhetsträdet.
3. Gör inställningarna på följande sidor och spara och aktivera konfigurationen:

- Huvudfönster > **Enheter** > Utvidga  > Utvidga  > 
- Huvudfönster > **Enheter** > Utvidga  > Utvidga  > **VRM-inställningar** > **Huvudinställningar**
- Huvudfönster > **Enheter** > Utvidga  > Utvidga  > **Nätverk** > **SNMP**
- Huvudfönster > **Enheter** > Utvidga  > Utvidga  > **Service** > **Avancerad**
- Huvudfönster > **Enheter** > Utvidga  > Utvidga  >  >  > **Avancerade inställningar** > **Inspelningsinställningar**
- Huvudfönster > **Enheter** > Utvidga  > Utvidga  >  >  >  > **Belastningsutjämning**

Så här byter du VRM-enheten utan BVMS:

Du använder den ursprungliga säkerhetskopieringsfilen config.xml från VRM-enheten, som innehåller alla konfigurationsinställningar (inga fler inställningar behöver göras).

1. Stoppa tjänsten **Video Recording Manager**.
2. Kopiera config.xml till den nya servern.
3. Starta tjänsten **Video Recording Manager**.

Så här byter du en iSCSI-enhet (planerad reserv):

1. Lägg till den nya iSCSI-enheten.

2. I konfigurationshanteraren på den iSCSI-enhet som du ska byta konfigurerar du alla LUN-enheter som skrivskyddade.

Obs! Du kan ta bort den gamla iSCSI-enheten när de gamla inspelningarna inte längre behövs.



Obs!

Vi rekommenderar att du använder samma CHAP-lösenord som för den gamla enheten när du konfigurerar den nya iSCSI-enheten.

Om du använder ett nytt CHAP-lösenord definierar du det nya lösenordet som ett systemövergripande CHAP-lösenord och tilldelar det till alla iSCSI-enheter.

Annars kommer du inte att kunna autentisera på iSCSI eller visa direktuppspelning från iSCSI-enheten.

6.11.3

Byta en kodare eller avkodare



Obs!

Ta inte bort en enhet från enhetsträdet om du vill behålla inspelningarna. Om du ska byta denna enhet måste maskinvaran bytas ut.

Byta kodare/avkodare av samma enhetstyp

För detta krävs en fabriksinställd enhet (IP-adress = 192.168.0.1).

1. Koppla bort den gamla enheten från nätverket.
2. Ta inte bort enheten från enhetsträdet i BVMS Configuration Client. När enheten tas bort från VRM försvinner inspelningen.
3. Anslut den nya enheten av samma typ till nätverket.



Obs!

Följande steg kräver ovanstående standard-IP-adress. Med DHCP-tilldelade IP-adresser kan du inte utföra inledande enhetssökning.

4. Configuration Client: På menyn **Maskinvara** klickar du på **Inledande enhetsskanning....** Dialogrutan **Inledande enhetsskanning** öppnas.
5. Klicka på en cell för att ändra adress. Om du vill ändra adressen på flera enheter väljer du flera rader. Du kan markera flera enheter samtidigt genom att hålla CTRL- eller SKIFT-tangenten nedtryckt. Högerklicka sedan på de valda raderna och klicka på **Ställ in nya IP-adresser...** eller på **Ställ in delnätmask...** för att ändra motsvarande värden. Du måste ange korrekt nätmask och IP-adress. Nätmasken och IP-adressen måste vara identiska med den utbytta enheten.
6. Klicka på **OK**.
7. Inom några sekunder kan du komma åt enhetsinställningar i enhetsträdet.
8. Ändra alla nödvändiga enhetsinställningar som inte styrs av BVMS (se informationen nedan).
9. Spara och aktivera.

Obs!

- Med den inledande enhetssökningen hittar du endast enheter med standard-IP-adresser (192.168.0.1) eller dubbla IP-adresser.
- Använd inte VRM-sökningen för att söka efter enheter som fått standardinställning, eftersom du inte kan ändra IP-adressen efteråt.

Byta en kodare med DHCP-tilldelad IP-adress:

För detta krävs en fabriksinställd kodare (DHCP-tilldelad IP).

1. Anslut kodaren direkt till datorns Ethernet-port.
2. Notera nätverksadapterkonfigurationen för TCP/IPv4 för senare återställning.
3. På datorns nätverksadapter konfigurerar du följande fasta IP-adress och nätmask för nätverksadaptern:
192.168.0.2
255.255.255.0
4. Starta Internet Explorer.
5. I **Adress**-fältet skriver du 192.168.0.1.
Enhetens webbsida visas.
6. Klicka på **Inställningar** och sedan på **Nätverk**.
7. På sidan **Nätverk** i listan **DHCP** väljer du **Av**.
8. I fältet **IP-adress**, i fältet **Nätmask** och i fältet **Gateway-adress** skriver du de värden som krävs för nätverket.
9. Klicka på **Ställ in och starta om**.
10. Återställ nätverksadapterkonfigurationen.

Byta kodare/avkodare av en annan enhetstyp

- Koppla bort den gamla enheten från nätverket.
- Ta inte bort enheten från enhetsträdet i BVMS Configuration Client.
- Anslut den nya typen av enhet till nätverket.

Huvudfönster > **Enheter** > utvidga  > utvidga  > utvidga  > högerklicka på

 > klicka på **Redigera kodare** > dialogrutan **Redigera kodare**
eller

Huvudfönster > **Enheter** > Utvidga  > Högerklicka på  > Klicka på **Redigera kodare** >
Dialogrutan **Redigera kodare**
eller

Huvudfönster > **Enheter** > Utvidga  > Högerklicka på  > Klicka på **Redigera kodare** >
Dialogrutan **Redigera kodare**
eller

Huvudfönster > **Enheter** > Utvidga  > Utvidga  > Högerklicka  > Klicka på
Redigera avkodare > dialogrutan **Redigera avkodare**

När enheten har uppgraderats kan du uppdatera enhetsfunktionerna. Ett meddelande informerar om de hämtade enhetsfunktionerna stämmer med enhetsfunktionerna som finns sparade i BVMS.

Uppdatera:

1. Klicka på **OK**.
En meddelanderuta med följande text visas:
Om du tillämpar enhetsfunktionerna kan det hända att inspelningsinställningarna och händelseinställningarna för enheten ändras. Kontrollera inställningarna för enheten.
2. Klicka på **OK**.
Enhetsfunktionerna uppdateras.

Byta en VSG-kamera

När du byter en VSG-kamera är det viktigt att du kontrollerar att den nya kameran är av samma typ och att den har samma IP-adress och ONVIF-profil som den gamla kameran.

Du måste även göra följande inställningar på en ny AXIS-kamera via VSG-kamerans webbgränssnitt innan du byter ut den gamla AXIS-kameran:

- Ange ett lösenord för användarroten
- Konfigurera tidssynkronisering
- Inaktivera länk till lokal adress
- Skapa en ONVIF-användare
- Inaktivera skydd mot repetitionsattack

Inställningar som kontrolleras av BVMS

Kodare och avkodare som har konfigurerats i ett BVMS-system kontrolleras av BVMS-servern och kan därför inte delas med andra program.

Du kan använda enhetsövervakaren i BVMS för att se vilken enhet som har en konfiguration som avviker från BVMS-konfigurationen.

BVMS Configuration Client har konfigurationssidor för alla BVIP-enheter.

Inställningsskalan beror på den specifika BVIP-modellen (till exempel VIPX 1600 XFM4).

BVMS kontrollerar alla BVIP-inställningar som krävs för en smidig integrering i ett BVMS-system.

Inställningar som kontrolleras av BVMS:

- Kameranamn
- Tidsserverinställningar
- Inspelningshantering (profiler, kvarhållningstider, scheman)
- Definitioner av kvalitetsinställningar
- Lösenord

Lagrade i BVMS-konfigurationen men inte ändrade på enheterna:

- IP-adress (du kan ändra IP-adresser med Konfiguration av IP-enhet i BVMS)
- Relä-/ingångsnamn (skillnaden mellan namnen i enheten och namnen som har konfigurerats i BVMS visas)

Systemhändelser för avvikande enhetskonfiguration

- Systeminformationshändelser genereras när konfigurationen av en enhet har korrigerats under en periodisk kontroll.
- Systemvarningshändelser genereras när en avvikande konfiguration har upptäckts på en enhet för första gången. Efterföljande kontroller rapporterar inte denna händelse förrän konfigurationen har korrigerats genom aktivering eller periodisk korrigering.
- Systemfelshändelser genereras när ett fel som rör konfigurationen har upptäckts under aktivering eller periodiska kontroller. Efterföljande kontroller rapporterar inte denna händelse förrän konfigurationen har korrigerats genom aktivering eller periodisk korrigering.

6.11.4

Byta en operatörsklient

Så här byter du en Operator Client-arbetsstation:

1. Byt ut datorn.
2. Starta BVMS-installationen på den nya datorn.
3. I listan över komponenter som ska installeras väljer du Operator Client.
Välj vid behov ytterligare komponenter som var installerade på den gamla datorn.
4. Installera programvaran.

6.11.5

Sluttester

Kontrollera MS-/EMS-bytet och Operator Client-bytet:

1. Aktivera konfigurationen.
2. Starta Operator Client.

- Kontrollera det logiska trädet i Operator Client.
Det måste vara identiskt med det logiska trädet i Configuration Client.

Kontrollera VRM-byte:

- Starta VRM Monitor och kontrollera de aktiva inspelningarna.

6.11.6 Återställa Divar IP 3000/7000

Mer information finns i installationshandböckerna för DIVAR IP 3000 eller DIVAR IP 7000. Hur du gör detta beskrivs i kapitlet om återställning av enheten.

6.12 Konfigurera tidssynkronisering



Obs!

Kontrollera att tiden på alla datorer i BVMS är synkroniserad med Management Server. Annars kan du förlora inspelningar.

Konfigurera tidsserverprogramvaran på Management Server. På de andra datorerna konfigurerar du IP-adressen för Management Server som en tidsserver enligt standardrutinerna i Windows.

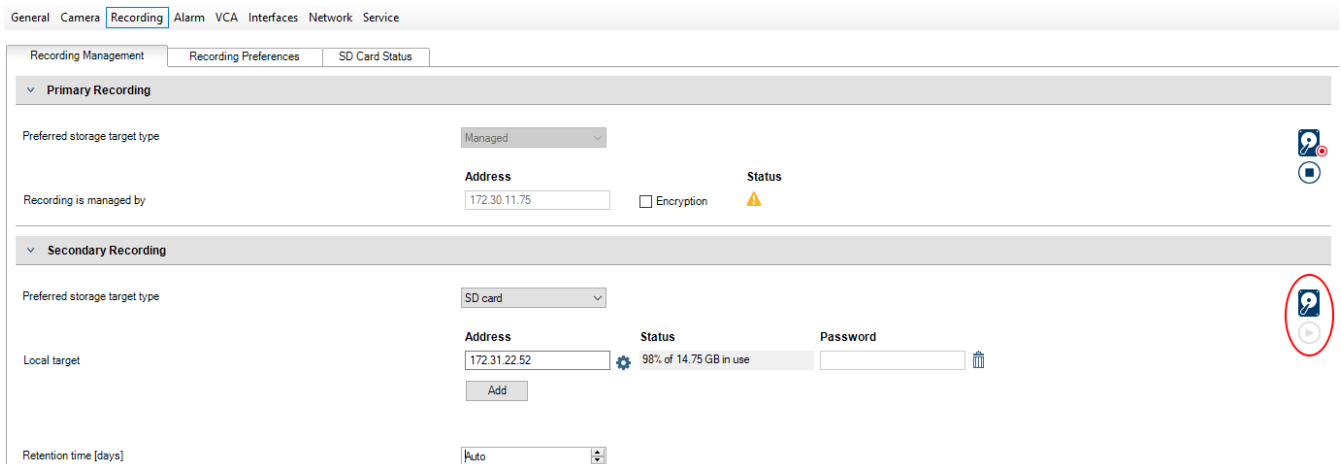
6.13 Konfigurera lagringsmediet för en kodare

Huvudfönster > **Enheter** > Utvidga  > Utvidga  >  > **Avancerade inställningar** > **Inspelningshantering**

Obs! Kontrollera att önskade kameror för kodaren har lagts till i det logiska trädet.

Du måste konfigurera lagringsmediet för en kodare för att kunna använda ANR-funktionen.

Obs! Om du vill konfigurera lagringsmediet för en kodare som redan har lagts till i systemet och spelas in via VRM, ser du till att den andra inspelningen stoppas:



ANR-funktionen fungerar bara på kodare med fast programvara av version 5.90 eller senare. Alla kodartyper har inte stöd för ANR även om rätt version är installerad.

Konfigurera lagringsmediet för en kodare:

- Välj lagringsmediet under **Sekundär inspelning** i listan **Önskad lagringstyp**. Olika medier är tillgängliga beroende på enhetstyp.
- Om det behövs, klickar du på knappen ... och formaterar mediet.
När formateringsprocessen är klar, är lagringsmediet klart för användning med ANR-funktionen.
- Konfigurera ANR-funktionen för den här kodaren på sidan **Kameror och inspelning**.

Se

- *Sidan Inspelningshantering, sidan 217*
- *Konfigurera ANR-funktionen, sidan 282*

7

Skapa ett Enterprise System

Utför följande uppgifter för att skapa ett Enterprise System på en Enterprise Management Server och på flera Management Server-datorer:

1. *Konfigurera serverlistan för Enterprise System, sidan 81*
2. *Skapa en Enterprise User Group, sidan 82*
3. *Skapa ett Enterprise Account, sidan 82*

Du behöver giltiga licenser för att använda ett Enterprise System.

Se

- *Enterprise System, sidan 23*

7.1

Konfigurera serverlistan för Enterprise System

Huvudfönster > **Enheter** > **Enterprise System** > **Serverlista/adressbok**

Du kan konfigurera flera hanteringsserverdatorer i serverlistan för en passande Management Server.

För samtidig åtkomst måste du konfigurera minst en Enterprise User Group. Då ändras den här Management Server till en Enterprise Management Server.

En Operator Client-användare kan logga in med ett användarnamn för en Enterprise User Group för att få samtidig åtkomst till de Management Server-datorer som konfigurerats i serverlistan.

Funktionsbehörigheter konfigureras på Enterprise Management Server i **Användargrupper**, fliken Enterprise User Group.

Enhetsbehörigheter konfigureras på varje Management Server i **Användargrupper**, fliken Enterprise Access.

- Klicka på  för att spara inställningarna.
- Klicka på  om du vill ångra den senaste inställningen.
- Klicka på  för att aktivera konfigurationen.

Så här lägger du till servrar:

1. Klicka på **Lägg till server**.
Dialogrutan **Lägg till server** visas.
2. Ange ett visningsnamn för servern och ange adressen till det privata nätverket (DNS-namn eller IP-adress).
Obs! Om du använder en SSH-anslutning anger du adressen i följande format:
ssh://IP eller servernamn: 5322
3. Klicka på **OK**.
4. Upprepa dessa steg tills du har lagt till alla önskade Management Server-datorer.

Så här lägger du till kolumner:

- ▶ Högerklicka på tabellrubriken och klicka på **Lägg till kolumn**.
Du kan lägga till upp till tio kolumner.
Högerklicka på önskad kolumn och klicka på **Radera kolumn** för att radera den.
- ✓ När du exporterar serverlistan exporteras också de tillagda kolumnerna.
Management Server-datorerna för ditt Enterprise System har konfigurerats.

Se

- *Enterprise System, sidan 23*
- *Sidan Serverlista/adressbok, sidan 121*
- *Sidan Användargrupper, sidan 306*
- *Använda serversökning, sidan 70*

7.2 Skapa en Enterprise User Group

Huvudfönster > **Användargrupper**

Du skapar en Enterprise User Group för ett Enterprise System på Enterprise Management Server.

Du skapar en Enterprise User Group med användare för att konfigurera deras funktionsbehörigheter. Dessa funktionsbehörigheter finns på en Operator Client som är ansluten till Enterprise Management Server. Ett exempel på en funktionsbehörighet är användargränssnittet till larmmonitorn.

Så här skapar du en Enterprise User Group:

1. Klicka på fliken **Enterprise User Groups**.
Obs! Fliken **Enterprise User Groups** är bara tillgänglig om rätt licens är tillgänglig och om en eller flera Management Server-datorer har konfigurerats i **Enheter > Enterprise System > Serverlista/adressbok**.
2. Klicka på .
Dialogrutan **Ny Enterprise-användargrupp** visas.
3. Ange namnet och en beskrivning.
4. Klicka på **OK**.
Enterprise User Group läggs till i motsvarande träd.
5. Högerklicka på den nya Enterprise-gruppen och klicka på **Ändra namn**.
6. Ange önskat namn och tryck på Enter.
7. På sidan **Operatörsbehörigheter** konfigurerar du funktionsbehörigheter och serveråtkomst för de konfigurerade Management Server-datorerna efter behov.

Se

- *Sidan Egenskaper för användargrupper, sidan 308*
- *Sidan Användarfunktioner, sidan 314*
- *Sidan Prioriteringar, sidan 317*
- *Sidan Användargränssnitt, sidan 317*
- *Sidan Serveråtkomst, sidan 319*

7.3 Skapa ett Enterprise Account

Huvudfönster > **Användargrupper**

**Obs!**

Minst en enhet måste konfigureras i enhetsträdet innan du kan lägga till ett Enterprise Account.

Du skapar ett Enterprise Account på en Management Server. Upprepa åtgärden på varje Management Server som ingår i ditt Enterprise System.

Du skapar ett Enterprise Account för att konfigurera enhetsbehörigheterna för en Operator Client som använder ett Enterprise System.

Så här skapar du ett Enterprise Account:

1. Klicka på fliken **Enterprise-åtkomst**.
2. Klicka på .
Dialogrutan **Nytt Enterprise Account** visas.
3. Ange namnet och en beskrivning.
4. Den **Användaren måste ändra sitt lösenord vid nästa inloggning** kryssrutan är förvald för alla nya användarkonton.
Ange nyckeln i enlighet med principreglerna för nycklar och bekräfta nyckeln.
5. Klicka på **OK**.
Ett nytt Enterprise Account läggs till i motsvarande träd.
6. Högerklicka på det nya Enterprise Account-kontot och klicka på **Ändra namn**.
7. Ange önskat namn och tryck på Enter.
8. Konfigurera inloggningsuppgifterna och enhetsbehörigheterna efter behov på sidan **Enhetsbehörigheter**.

Se

- *Policy om starka lösenord*, sidan 327
- *Sidan Inloggningsuppgifter*, sidan 313
- *Sidan Logiskt träd*, sidan 313
- *Sidan Händelser och larm*, sidan 312
- *Sidan Kontrollprioriteter*, sidan 311
- *Sidan Kamerabehörigheter*, sidan 310
- *Sidan Avkodarbehörigheter*, sidan 312

7.4

Tokenbaserad autentisering

Enterprise Account ger Enterprise ledningskunder åtkomst till en Management Server konfigurerad i serveråtkomstlistan för Enterprise Management Server.

Enterprise Account säkras av en nyckel. När du måste byta denna nyckel måste du också ändra den i din Management Server samt i din EnterpriseManagement Server. Dessutom måste du aktivera den ändrade konfigurationen.

Om du har ett stort antal Management Server anslutna till en EnterpriseManagement Server kan detta bli tidskrävande.

Istället för att skydda Enterprise Account med ett användarnamn och en nyckel kan du konfigurera tokenbaserad autentisering.

1. Enterprise Management Server skapar token.
2. Token signeras med hjälp av ett certifikat som heter Token Issuer.
3. Management Server beviljar åtkomst när token är giltig.
Management Server ger endast åtkomst om Management Server är konfigurerad att lita på Token Issuer-certifikatet.

Krav

För att signera och validera token behöver du ett certifikat eller en certifikatskedja.

Obs! Certifikaten genereras eller installeras inte av BVMS. Du måste tillhandahålla och installera dem separat. BVMS kan använda certifikat som finns installerade i Windows Certificate Store.

Det finns olika förutsättningar på maskiner med EnterpriseManagement Server respektive Management Server. Nedan beskrivs vilken miljö som kräver vilka certifikat.

Certifikat

- Enterprise Management Server kräver certifikatet och dess privata nyckel.
- Management Server kräver certifikatet.

Certifikatkedja

En certifikatkedja börjar med ett Root-certifikat som du använder för att signera ett annat certifikat. Du kan sedan använda certifikatet igen för att signera ännu ett certifikat. Du kan själv definiera längden på certifikatkedjorna.

- Enterprise Management Server kräver hela certifikatkedjan.
För det sista certifikatet i kedjan (Token Issuer) krävs en privat nyckel.
- Management Server kräver bara delar av certifikatkedjan, beroende på de konfigurerade inställningarna för åtkomsttoken.

Så här konfigurerar du tokenbaserad autentisering:

1. Konfiguration av Enterprise Management Server
 - Definiera autentisering av åtkomsttoken för Enterprise Accounts
 - Konfigurera inställningarna för åtkomsttoken
2. Konfiguration av Management Server
 - Ange betrodda certifikat
 - Neka åtkomst till Enterprise Account via nyckel

Detaljerad information om respektive avsnitt finns i den tokenbaserade vitboken för autentisering.

Se

- *Dialogrutan Inställningar för åtkomsttoken (menyn Inställningar), sidan 112*
- *Sidan Serveråtkomst, sidan 319*

8 Konfiguration av kommandoskript

I det här kapitlet ges information om hur du konfigurerar kommandoskript. Kommandoskript visas på olika ställen i BVMS.

1. Klicka på  för att spara inställningarna.
2. Klicka på  om du vill ångra den senaste inställningen.
3. Klicka på  om du vill aktivera konfigurationen.



Obs!

Serverskripten aktiveras när tjänsten Management Server startas om även om de inte har aktiverats inifrån Configuration Client.

8.1 Hantera kommandoskript

Huvudfönster

Du kan skapa ett kommandoskript genom att använda följande skriptspråk:

- C#
- VB.Net

Du kan inte ändra skriptspråket för ett befintligt kommandoskript.

Du kan skapa ett klientskript eller ett serverskript.

Du kan lägga till skriptdelar i varje skript.

Klicka på  i dialogrutan **Redigera för kommandoskript** för att få hjälp med att skriva kod. Hjälpen till Bosch Script API visas.

Så här lägger du till en serverskriptdel:

1. Välj kommandot **Redigera för kommandoskript...** på menyn **Verktyg**.
Dialogrutan **Välj skriptspråk** visas om inget kommandoskript har skapats än.
2. Välj den önskade posten på listan **Skriptspråk**.
Dialogrutan **Redigera för kommandoskript** visas.
3. Högerklicka på ServerScript i den vänstra rutan i dialogrutan **Redigera för kommandoskript**. Välj **Ny skriptdel**.
En ny skriptdel läggs till.
4. Ange ditt skript.

Så här lägger du till en klientskriptdel

1. Välj kommandot **Redigera för kommandoskript...** på menyn **Verktyg**.
Dialogrutan **Välj skriptspråk** visas om inget kommandoskript har skapats än.
2. Välj den önskade posten på listan **Skriptspråk**.
Dialogrutan **Redigera för kommandoskript** visas.
3. Högerklicka på ClientScript i den vänstra rutan i dialogrutan **Redigera för kommandoskript**. Välj **Ny skriptdel**.
En ny skriptdel läggs till.
4. Ange ditt skript.

Så här tar du bort en skriptdel:

1. Öppna dialogrutan **Redigera för kommandoskript**.
2. Klicka på fliken **Serverskript** eller på fliken **Klientskript** efter behov.

- Högerklicka på den aktuella händelsen i händelseträdet och välj . Skriptdelen tas bort.

Så här stänger du dialogrutan Redigerare för kommandoskript:

- Klicka på .

Se

- *Redigerare för kommandoskript-dialogrutan, sidan 286*

8.2

Konfigurera ett kommandoskript som startas automatiskt

Huvudfönster > **Larm** > kolumnen  eller  **Larmalternativ** > ...

Du kan konfigurera ett klientkommandoskript så att det startar i följande fall:

- Arbetsstation startas upp.
- Användare accepterar ett larm.

Konfigurera ett kommandoskript vid start av arbetsstation:

Se Konfigurera ett startkommandoskript.

Konfigurera ett kommandoskript efter att en användare har accepterat ett larm:

- Klicka på fliken **Arbetsflöde**.
- I listan **Utför följande klientskript när larm har godkänts**, välj önskat klientskript. Detta skript startar så snart en användare accepterar det valda larmet.

Se

- *Larmalternativ-dialogrutan, sidan 292*
- *Konfigurera ett startkommandoskript (inställningssidan), sidan 87*

8.3

Importera ett kommandoskript

Huvudfönster

Du kan importera kommandoskript som har utvecklats på en annan dator. Filen måste skrivas i samma skriptspråk som du använde i ditt system.

Så här importerar du ett kommandoskript:

- Välj kommandot **Redigerare för kommandoskript...** på menyn **Verktyg**. Dialogrutan **Redigerare för kommandoskript** visas.
- Klicka på .
- Välj skriptfilen som behövs och klicka på **OK**.

Se

- *Redigerare för kommandoskript-dialogrutan, sidan 286*

8.4

Exportera ett kommandoskript

Huvudfönster

Du kan exportera kommandoskript som har utvecklats på en annan dator.

Så här exporterar du ett kommandoskript:

- Välj kommandot **Redigerare för kommandoskript...** på menyn **Verktyg**. Dialogrutan **Redigerare för kommandoskript** visas.

2. Klicka på  .
Dialogrutan för att spara en fil visas.
3. Ange skriptfilen som behövs och klicka på **OK**.

Se

- Redigerare för kommandoskript-dialogrutan, sidan 286

8.5

Konfigurera ett startkommandoskript (inställningssidan)

Huvudfönster > **Enheter** > Utvidga  >  > sidan **Inställningar**

Du konfigurerar ett kommandoskript som ska startas när Operator Client startas på den valda arbetsstationen.

Du måste skapa ett motsvarande kommandoskript.

För att skapa ett kommandoskript se *Hantera kommandoskript, sidan 85*.

Konfigurera ett startskript:

- ▶ I listan **Startskript:**, välj önskat kommandoskript.

Se

- Sidan Arbetsstation, sidan 129

9 Hantera konfigurationsdata

Huvudfönster

Du måste aktivera den aktuella konfigurationen för att den ska gälla för Management Server and Operator Client. Systemet påminner dig om att aktivera när du stänger Configuration Client.

Varje aktiverad konfiguration sparas med ett datum och med en beskrivning om det krävs. Du kan när som helst återställa en konfiguration som nyligen aktiverats. Alla konfigurationer som sparas under tiden går förlorade.

Du kan exportera den aktuella konfigurationen i en konfigurationsfil och importera den filen senare. Detta återställer den exporterade konfigurationen. Alla konfigurationer som sparas under tiden går förlorade.

- Klicka på  för att spara inställningarna.
- Klicka på  om du vill ångra den senaste inställningen.
- Klicka på  för att aktivera konfigurationen.

9.1 Aktivera arbetskonfigurationen

Huvudfönster

Du aktiverar den aktuella arbetskonfigurationen. Operator Client använder den aktiverade konfigurationen efter nästa start om användaren godkänner den. Om aktiveringen tvingas fram avslutas alla instanser av Operator Client i nätverket och startar igen. Användaren av varje Operator Client förekomst behöver normalt inte logga in igen.

Du kan konfigurera en fördröjd aktiveringstid. Om du konfigurerar en fördröjd aktiveringstid aktiveras inte konfigurationen omedelbart, utan vid den tidpunkt som konfigurerats. Om du konfigurerar en annan aktiveringstid senare (om den är fördröjd eller inte spelar någon roll) är den tiden aktiv nu. Den först konfigurerade aktiveringstiden tas nu bort.

När du stänger Configuration Client påminner systemet dig om att aktivera den aktuella arbetskopian av konfigurationen.

Du kan inte aktivera en konfiguration som innehåller en enhet som saknar lösenordsskydd.



Obs!

Om aktiveringen tvingas fram startar alla instanser av Operator Client om när konfigurationen har aktiverats. Undvik onödiga aktiveringar. Gör helst aktiveringar nattetid eller under perioder med låg aktivitet.



Obs!

Om systemet innehåller enheter som inte är lösenordsskyddade måste du säkra dessa enheter innan du kan aktivera konfigurationen. Du kan avaktivera lösenordsskyddet.

Aktivera den aktuella arbetskonfigurationen:

1. Klicka på  .
Dialogrutan **Aktivera konfiguration** visas.
Om konfigurationen innehåller enheter som inte är lösenordsskyddade kan du inte aktivera konfigurationen. I det här fallet visas dialogrutan **Skydda enheter med**

standardlösenord

Följ instruktionerna i den här dialogrutan och klicka på **Verkställ**.

Dialogrutan **Aktivera konfiguration** visas igen.

2. Ange vid behov en fördröjd aktiveringstid. Som standard konfigureras den aktuella tidpunkten som aktiveringstid. Om du inte ändrar den fördröjda aktiveringstiden utförs aktiveringen omedelbart.
Om det är lämpligt kan du klicka här för att markera **Tvinga fram aktivering för alla Operator Clients**.
3. Skriv en beskrivning och klicka på **OK**.
Den aktuella konfigurationen aktiveras.
Alla Operator Client-arbetsstationer som är anslutna till nätverket startas om omedelbart om aktiveringen genomdrivs. Om en arbetsstation inte är ansluten startas den om så snart den återansluts.
Om du har konfigurerat en fördröjd aktiveringstid aktiveras konfigurationen senare.

Obs! Fördröjd aktivering körs inte så länge användaren är inloggad i Configuration Client.

Se

- Skydda enheter med dialogrutan *Globalt standardlösenord (menyn Maskinvara)*, sidan 100
- Aktivera dialogrutan *Konfiguration (menyn System)*, sidan 100

9.2

Aktivera en konfiguration

Huvudfönster

Du kan aktivera en tidigare version av konfigurationen som du har sparat förut.

Så här aktiverar du en konfiguration:

1. På menyn **System** klickar du på **Aktiveringshanteraren....**
Dialogrutan **Aktiveringshanteraren** visas.
2. I listan väljer du den konfiguration som du vill aktivera.
3. Klicka på **Aktivera**.
En meddelanderuta visas.
4. Klicka på **OK**.
Dialogrutan **Aktivera konfiguration** visas.
5. Om det behövs klickar du för att markera **Tvinga fram aktivering för alla Operator Clients**. Varje Operator Client-arbetsstation startas om automatiskt för att aktivera den nya konfigurationen. Användaren kan inte neka den nya konfigurationen.
Om **Tvinga fram aktivering för alla Operator Clients** inte har markerats visas en dialogruta i några sekunder på varje Operator Client-arbetsstation. Användare kan tillbakavisa eller godkänna den nya konfigurationen. Dialogrutan stängs efter några sekunder utan användaraktivitet. Om så är fallet godkänns inte den nya konfigurationen.

Se

- Aktivera dialogrutan *Konfiguration (menyn System)*, sidan 100
- Dialogrutan *Aktiveringshanteraren (menyn System)*, sidan 99

9.3

Exportera konfigurationsdata

Huvudfönster

Du kan exportera enhetens konfigurationsdata för BVMS i en .zip-fil. Den här .zip-filen innehåller databasfilen (*Export.bvms*) och användardata (.dat-filen).

Du kan använda de här filerna för att återställa en systemkonfiguration som exporterats förut på samma (Enterprise) Management Server eller för att importera den till en annan (Enterprise) Management Server. Användardatafilen kan inte importeras, men du kan använda den för att återställa användarkonfigurationen manuellt.

Så här exporterar du konfigurationsdata:

1. På menyn **System** väljer du **Exportera konfiguration....**

Dialogrutan **Exportera konfigurationsfil** visas.



Obs! Om den aktuella arbetskopian av konfigurationen inte aktiveras (är aktiverat) exporterar du arbetskopian i stället för den aktiverade konfigurationen.

2. Klicka på **Spara**.

3. Ange ett filnamn.

Den aktuella konfigurationen har exporterats. En ZIP-fil som innehåller databasen och användardata skapas.

Se

- *Importera konfigurationsdata, sidan 90*

9.4

Importera konfigurationsdata

Huvudfönster

Följande användningssituationer omfattas:

- Importera en konfiguration som har exporterats (säkerhetskopiering har utförts) tidigare på samma server
- Importera en konfigurationsmall som har gjorts i ordning och exporterats på en annan server
- Importera en konfiguration för en tidigare version av BVMS.

Du kan endast importera en konfiguration om de senaste ändringarna för den aktuella arbetskopian har sparats och aktiverats.

För import av konfigurationsdata måste du ha det rätta lösenordet.

Det går inte att importera användardata.

Så här importerar du konfigurationen:

1. På menyn **System** klickar du på **Importera konfiguration....**

Dialogrutan **Importera konfigurationsfil** visas.

2. Markera den file som du vill importera och klicka på **Öppna**.

Dialogrutan **Importera konfiguration...** visas.

3. Ange det aktuella lösenordet och klicka på **OK**.

Configuration Client startas om. Du måste logga in på nytt.

Den importerade konfigurationen är inte aktiverad, men den kan redigeras i Configuration Client.



Obs!

Om du vill fortsätta redigera konfigurationen som har aktiverats för Management Server kan du köra en återställning i dialogrutan **Aktivera konfiguration**.

Se

- *Exportera konfigurationsdata, sidan 89*

9.5 Exportera konfigurationsdata till OPC

Huvudfönster

Du kan exportera enhetskonfigurationsdata i BVMS i en XML-fil och importera den till ett OPC-serverprogram. Filen måste lagras i bin-katalogen för din BVMS-installation.

För att konfigurera en BVMS – BIS-anslutning BVMS – installationshandbok för BIS-anslutningar och BVMS är tekniskt servicemeddelande för OPC Server tillgängligt.



Obs!

Installera BIS-server och BVMS Management Server på separata datorer.

Om båda serverarna körs på samma dator försämras systemens prestanda. Andra allvarliga programfel kan inträffa.

Så här exporterar du konfigurationsdata:

1. På menyn **System** klickar du på **Exportera enhetsinformation för OPC**.
Dialogrutan **Exportera enhetsinformationsfil** visas.
2. Ange ett filnamn och klicka på **Spara**.
Filen sparas.
Du kan importera den här filen i OPC-servertillämpningen.

9.6 Kontrollera status för kodare/avkodare

Huvudfönster > Menyn **Maskinvara** > Kommandot **Enhetsmonitor...** > Dialogrutan **Enhetsmonitor**

Du kan kontrollera status för alla aktiverade kodare/avkodare i enhetsträdet.

Se

- *Dialogrutan Enhetsövervakaren (menyn Maskinvara), sidan 105*

9.7 Konfigurera SNMP-övervakning

Huvudfönster

Så här konfigurerar du:

1. På menyn **Inställningar** klickar du på **SNMP-inställningar**
Dialogrutan **SNMP-inställningar** visas.
2. Gör nödvändiga inställningar och klicka på **OK**.

Avaktivera SNMP GetRequest:

- ▶ Ta bort innehållet i fältet **SNMP GET-port**.
BVMS lyssnar inte längre efter SNMP GetRequest.

Se

- *Dialogrutan SNMP-inställningar (menyn Inställningar), sidan 109*

9.8 Skapa en rapport

Huvudfönster

Du kan skapa rapporter där information om den aktuella konfigurationen samlas.

Så här skapar du en rapport:

1. Välj ett kommando på menyn **Rapporter**.
Motsvarande dialogruta öppnas.
2. Klicka på **CSV-export**.
3. Ange sökväg och filnamn för den nya rapporten.

4. Öppna CSV-filen i Microsoft Excel eller ett annat kalkylbladsprogram för att kontrollera innehållet.

Se

- *Dialogrutan Inspelningsscheman, sidan 107*
- *Dialogrutan Uppgiftsscheman, sidan 107*
- *Dialogrutan Kameror och parametrar för inspelning, sidan 107*
- *Dialogrutan Inställningar för inspelningskvalitet, sidan 107*
- *Dialogrutan Händelseinställningar, sidan 107*
- *Dialogrutan Inställningar för sammansatta händelser, sidan 107*
- *Dialogrutan Larminställningar, sidan 108*
- *Dialogrutan Konfigurerade användare, sidan 108*
- *Dialogrutan Användargrupper och konton, sidan 108*
- *Dialogrutan Funktionsbehörigheter, sidan 108*

10 Konfigurationsexempel

I det här kapitlet finns exempel på hur du konfigurerar vissa enheter i BVMS.

10.1 Lägga till en Bosch ATM/POS-brygga

Det här exemplet beskriver hur du sätter upp en Bosch ATM/POS-brygga.

Konfigurera ATM/POS-bryggan

1. Kontrollera att enheten har strömförsörjning.
2. Om du vill konfigurera enhetens IP-adress och subnätmask ansluter du enheten till en COM-port på datorn med en RS232-kabel (använd den specificerade Bosch-kabeln för anslutning). Se installationshandboken för Bosch ATM/POS-bryggan för mer information.
3. Starta en Hyperterminal-session på datorn (vanligtvis: **Start > Alla program > Tillbehör > Kommunikation > Hyper Terminal**).
4. Skriv in ett namn för sessionen och klicka på **OK**.
5. Välj COM-portnummer och klicka på **OK**.
6. Skriv in följande COM-portinställningar:
 - 9600 bitar/s
 - 8 databitar
 - ingen paritet
 - 1 stoppbit
 - Flödesstyrning för maskinvaraKlicka på **OK**.
7. Tryck på F1 om du vill visa systemalternativsmenyn för enheten.
8. Skriv 1 om du vill ställa in IP-adressen och subnätmaskadressen efter behov.
9. Lämna standardinställningarna för portarna:
 - port1: **4201**
 - port2: **4200**

Lägga till ATM/POS-bryggan till BVMS

1. Ansluta enheten till BVMS-nätverket.
2. Starta Configuration Client.
3. Klicka på **Enheter**, utvidga det logiska trädet, utvidga , högerklicka , klicka på **Lägg till Bosch ATM/POS-brygga**.
Dialogrutan **Lägg till Bosch ATM/POS-brygga** visas.
4. Skriv in önskat namn och inställningarna som du konfigurerade tidigare.
5. Klicka på fliken **Ingångar** och välj önskade ingångar.
6. Klicka på  för att spara inställningarna.
7. Klicka på **Händelser**.

8. Utvidga , utvidga **Ingång för POS-brygga** och klicka på **Dataingång**.
9. I listan **Utlöser larm** ska du välja **Alltid** om denna händelse alltid ska utlösa ett larm. Om du endast vill att händelsen ska utlösa ett larm under en viss tidsperiod väljer du ett schema.
10. Klicka på  för att spara inställningarna.
11. Klicka på **Larm**.
12. Konfigurera önskade larminställningar för den här händelsen.

13. Klicka på  för att spara inställningarna och klicka på  för att aktivera konfigurationen.
14. Utför ett test och kontrollera att larmet fungerar som tänkt.

10.2

Lägga till ett Bosch Allegiant-ingångslarm

När en Bosch Allegiant-enhet har lagts till i BVMS kan du lägga till Allegiant-larvingångar.

1. Klicka på Allegiant-enhetens post i enhetsträdet.
2. Klicka på fliken **Ingångar** och klicka på **Lägg till ingång**.
3. Lägg till önskade ingångslarm.
4. Klicka på **Händelser**.
5. I händelseträdet utvidgar du **Allegiant-enheter**, utvidgar **Allegiant-ingång** och klickar på **Ingång stängd** eller **Ingång öppnad** (beroende på program).
6. I listan **Utlöser larm** väljer du **Alltid** om du vill att en händelse alltid ska utlösa ett larm. Om du endast vill att händelsen ska utlösa ett larm under en viss tidsperiod väljer du ett schema.

7. Klicka på  för att spara inställningarna och klicka på  för att aktivera konfigurationen.
8. Utför ett test och kontrollera att larmet fungerar som tänkt.

10.3

Lägga till och konfigurera 2 Dinion IP-kameror med VRM-inspelning

Det här avsnittet beskriver hur du lägger till 2 Dinion IP-kameror för VRM-inspelning, hur du konfigurerar olika inspelningsinställningar och hur du konfigurerar brottsutredande sökning för dessa kameror.

Grundkrav:

VRM- och iSCSI-enheterna är rätt konfigurerade.

Det innebär att:

- VRM har lagts till i enhetsträdet.
- En iSCSI-enhet med konfigurerat mål och LUN har tilldelats till denna VRM.

Lägga till IP-kameror till en befintlig VRM:

Huvudfönster > **Enheter** > Utvidga 

1. Högerklicka på  och klicka på **Lägg till kodare**. Dialogrutan **Lägg till kodare** visas.
2. Ange IP-adressen för IP-kameran och välj kodartypen (Dinion IP). Klicka på **OK**. Upprepa det här steget för den andra IP-kameran.

Lägga till IP-kameror till det logiska trädet:

Huvudfönster > **Kartor och struktur**

- ▶ Dra kamerorna till det logiska trädet.

Ändra kameraegenskaper:

Huvudfönster > **Kameror och inspelning** >  > -fliken

1. I kolumnen **Live-video** konfigurerar du kvaliteten på live-visningen. För de här enheterna kan du endast ställa in live-kvaliteten per kamera, inte enligt schema.
2. Gör lämpliga inställningar i övriga kolumner.

Konfigurera inspelningsinställningar för kameror:

1. Klicka på .
2. Välj respektive enhetsfamilj.
3. Välj respektive tillgänglig inspelningsinställning.
4. Välj respektive inställningsschema, till exempel **Dag**.
5. Under **Kontinuerlig inspelning eller inspelning före larm** väljer du önskat inspelningsläge, ström och kvalitet.
Om du väljer i inspelningsläge **Före larm** är parametern **Varaktighet** tillgänglig för att välja larminspelningstiden före larmet i sekunder.
6. Under **Larminspelning**, i kolumnen **Varaktighet**, klickar du på en cell och anger önskad inspelningsstid i sekunder efter att larmet har inträffat.
7. Upprepa föregående steg för att konfigurera inspelningsinställningar för den andra kameran i enhetsfamiljen.

Aktivera brottsutredande sökning på en arbetsstation:

Huvudfönster > **Enheter** > Utvidga 

1. Klicka på ikonen  för arbetsstationen.
2. Klicka på fliken **Inställningar**.
3. Klicka för att markera kryssrutan **Aktivera Forensic Search**.

11 Globala Configuration Client-fönster



Obs!

BVMS Viewer har bara grundläggande funktioner. Avancerade funktioner ingår i BVMS Professional. Detaljerad information om de olika BVMS utgåvorna finns på www.boschsecurity.com och BVMS Snabbvalsguiden: [BVMS snabbvalsguide](#).

Det här kapitlet innehåller information om några grundläggande programfönster som är tillgängliga i BVMSConfiguration Client.

11.1 Konfigurationsfönster

Huvudfönster

Låter dig konfigurera ditt system. Knapparna i verktygsfältet representerar de olika sidor som du måste konfigurera för att systemet ska fungera. Deras ordningsföljd illustrerar konfigurationens rekommenderade arbetsflöde.

- Klicka på ett trädobjekt för att visa de tillgängliga egenskapssidorna.

Enheter	Klicka för att visa sidan Enheter med alla enheter som är anslutna till systemet.
Kartor och struktur	Klicka för att visa sidan Kartor och struktur med det logiska trädet, enhetsträdet samt kartor.
Scheman	Klicka för att visa sidan Inspelningsscheman och Uppgiftsscheman .
Kameror och inspelning	Klicka för att visa sidan Kameror och inspelning med kameratabellen och inspelningsinställningarna för alla kameror.
Händelser	Klicka för att visa sidan Händelser .
Larm	Klicka för att visa sidan Larm .
Användargrupper	Klicka för att visa sidan Användargrupper med alla användare.
	Klicka för att spara de ändrade inställningarna i det aktuella fönstret.
	Klicka för att återställa de sparade inställningarna i det aktuella fönstret. Obs! Endast inställningar som utförts i BVMS återställs, inte de inställningar som gjorts direkt på enheten. Detta kan leda till att enheter inte längre är tillgängliga.
	Klicka för att visa dialogrutan Aktivera konfiguration .
	Klicka för att ta bort det markerade objektet. (Inte tillgängligt på alla sidor).

	Klicka för att ändra namnet på det markerade objektet. (Inte tillgängligt på alla sidor).
	Klicka för att visa hjälpinformation för det aktuella fönstret.
	Klicka för att uppdatera tillståndsinformationen för alla enheter och enhetsfunktioner om det behövs (inte tillgängligt på varje sida). Du kan uppdatera tillståndet för en enskild enhet: högerklicka på enheten och klicka på Uppdatera tillståndet . Obs! Om du har ett stort system med flera tusen konfigurerade enheter kan det ta lång tid att uppdatera tillstånd och enhetsfunktioner.

11.2

Menykommandon

System-menykommandon

Spara ändringar	Sparar alla ändringar gjorda på denna sida.
Ångra alla ändringar på sidan	Återställer inställningarna på denna sida sedan de sist sparades.
Aktiveringshanteraren...	Visar dialogrutan Aktiveringshanteraren .
Exportera konfiguration...	Visar dialogrutan Exportera konfigurationsfil .
Importera konfiguration...	Visar dialogrutan Importera konfigurationsfil .
Exportera enhetsinformation för OPC	En dialogruta visas där du kan skapa en konfigurationsfil som du kan importera i ett tredjepartssystem.
Avsluta	Stänger programmet.

Maskinvara-menykommandon

Inledande enhetsskanning...	Visar dialogrutan Inledande enhetsskanning .
Skydda enheter med standardlösenord ...	Visar dialogrutan Skydda enheter med globalt standardlösenord .
Skydda iSCSI-lagringsutrymmen med CHAP-lösenord...	Visar dialogrutan Skydda iSCSI-lagringsutrymmen med CHAP-lösenord .
Ändra enhetslösenord ...	Visar dialogrutan Ändra enhetslösenord .
Uppdatera enhetens fasta programvara ...	Visar dialogrutan Uppdatera enhetens fasta programvara .
Ändra enhetens IP- och nätverksinställningar ...	Visar dialogrutan Ändra enhetens IP- och nätverksinställningar .
Enhetsmonitor...	Visar dialogrutan Enhetsmonitor .

Verktyg-menykommandon

Redigerare för kommandoskript...	Visar dialogrutan Redigerare för kommandoskript
Resurshanteraren...	Visar dialogrutan Resurshanteraren .
Sekvensbyggare...	Visar dialogrutan Sekvensbyggare .
Resurskonverterare	Visar dialogrutan Resurskonverterare om det finns kartresurser tillgängliga.
Licenshanterare...	Visar dialogrutan Licenshanterare .
Licenskontroll ...	Visar dialogrutan Licenskontroll .

Rapporter-menykommandon

Inspelningsscheman ...	Visar rapportdialogrutan Inspelningsscheman .
Schemalagda inspelningsinställningar ...	Visar rapportdialogrutan Schemalagda inspelningsinställningar .
Uppgiftsscheman ...	Visar rapportdialogrutan Uppgiftsscheman .
Kameror och inspelningsparametrar ...	Visar rapportdialogrutan Kameror och inspelningsparametrar .
Kvalitetsinställningar för ström ...	Visar rapportdialogrutan Kvalitetsinställningar för ström .
Händelseinställningar ...	Visar rapportdialogrutan Händelseinställningar .
Inställningar för sammansatt händelse ...	Visar rapportdialogrutan Inställningar för sammansatt händelse .
Larminställningar ...	Visar rapportdialogrutan Larminställningar .
Konfigurerade användare ...	Visar rapportdialogrutan Konfigurerade användare .
Användargrupper och konton ...	Visar rapportdialogrutan Användargrupper och konton .
Enhetsbehörigheter ...	Visar rapportdialogrutan Enhetsbehörigheter .
Operatörsbehörigheter ...	Visar rapportdialogrutan Driftbehörigheter .
Konfigurationsbehörigheter ...	Visar rapportdialogrutan Konfigurationsbehörigheter .
Behörigheter för användargrupp ...	Visar rapportdialogrutan Behörigheter för användargrupp .
Säkerhetsinställningar ...	Visar rapportdialogrutan Säkerhetsinställningar .
Enheter som kringgås ...	Visar rapportdialogrutan Enheter som kringgås .

Inställningar-menykommandon

Larminställningar	Visar dialogrutan Larminställningar .
SNMP-inställningar ...	Visar dialogrutan SNMP-inställningar .
Inställningar för LDAP-server...	Visar dialogrutan Inställningar för LDAP-server .

Definiera LDAP-användargruppens ordning...	Visar dialogrutan Definiera LDAP-användargruppens ordning...
Inställningar för åtkomsttoken...	Visar dialogrutan Inställningar för åtkomsttoken.
Inställningar för betrott certifikat...	Visar dialogrutan Inställningar för betrott certifikat . Obs! Menyn Inställningar för betrott certifikat... är endast tillgänglig om du startar Configuration Client med administratörsbehörigheter och den användare som loggar in har Konfigurera användargrupper/Enterprise Accounts/LDAP-serverinställningar och åtkomsttoken-behörighet.
Ställ in inspelningskvaliteter...	Visar dialogrutan Kvalitetsinställningar för ström.
Alternativ...	Visar dialogrutan Alternativ.

Hjälp-menykommandon

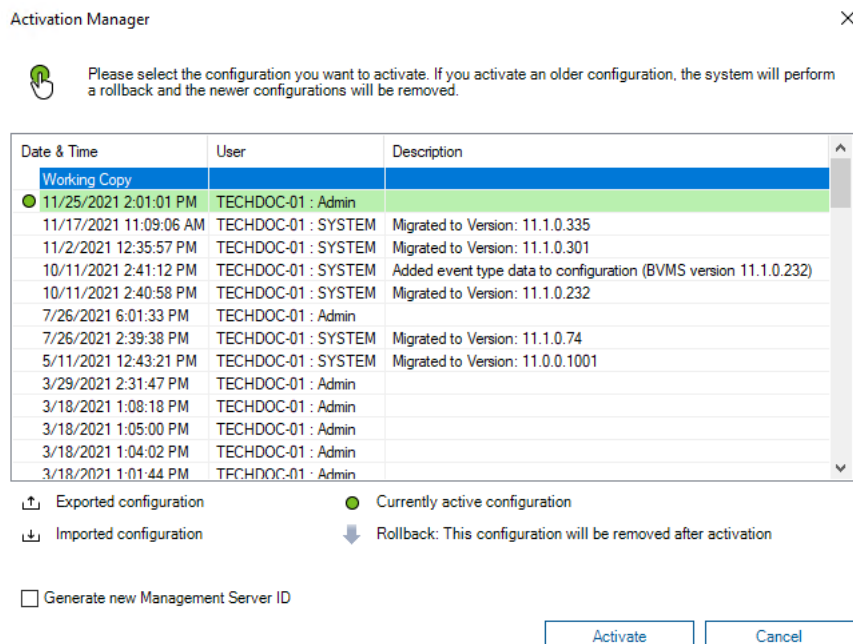
Visa Hjälp	Visar BVMS-programhjälpen.
Om...	Visar en dialogruta som innehåller information om det installerade systemet, t.ex. versionsnumret.

11.3

Dialogrutan Aktiveringshanteraren (menyn System)

Huvudfönster > Menyn **System** > Kommandot **Aktiveringshanteraren...**

Låter dig aktivera en aktuell konfiguration eller återställa en tidigare konfiguration.



Aktivera

Klicka för att visa dialogrutan **Aktivera konfiguration.**

Se

- *Aktivera arbetskonfigurationen, sidan 88*
- *Aktivera en konfiguration, sidan 89*

11.4 Aktivera dialogrutan Konfiguration (menyn System)



Huvudfönster >

Gör att du kan ange en beskrivning för arbetskopian av konfigurationen som ska aktiveras.

Ange fördröjd aktiveringstid

Klicka för att välja en fördröjd aktiveringstid.

Obs! Fördröjd aktivering körs inte så länge användaren är inloggad i Configuration Client.

Tvinga fram aktivering för alla Operator Clients

Om kryssrutan har markerats startas varje Operator Client-arbetsstation om automatiskt för att aktivera den nya konfigurationen. Användare kan inte tillbakavisa den nya konfigurationen.

Om kryssrutan inte har markerats visas en dialogruta i några sekunder på varje Operator Client-arbetsstation. Användare kan tillbakavisa eller godkänna den nya konfigurationen. Dialogrutan stängs efter några sekunder utan användaraktivitet. Om så är fallet godkänns inte den nya konfigurationen.

Se

– *Aktivera arbetskonfigurationen, sidan 88*

11.5 Dialogrutan Inledande enhetsskanning (menyn Maskinvara)

Huvudfönster > Menyn **Maskinvara** > Kommandot **Inledande enhetsskanning...**

Visar enheter som har dubblerade IP-adresser eller standardadress (192.168.0.1).

Här kan du ändra sådana IP-adresser och subnätmaskar.

Du måste ange rätt subnätmask innan du ändrar IP-adress.

11.6 Skydda enheter med dialogrutan Globalt standardlösenord (menyn Maskinvara)

Huvudfönster > Menyn **Maskinvara** > Kommandot **Skydda enheter med standardlösenord ...** eller



Huvudfönster >

I den här dialogrutan visas om en aktivering väntar och om konfigurationen innehåller enheter som inte är lösenordsskyddade. Med hjälp av den kan du ange ett globalt standardlösenord som gäller på alla berörda enheter.

Uppdatera tillstånd och kapaciteter

Klicka här för att avsöka enheter som inte är lösenordsskyddade i nätverket igen.

Global default password

Skriv in ett lösenord som används för alla enheter som för närvarande inte är skyddade.

Visa lösenord

Klicka här om du vill att alla lösenord i dialogrutan ska visas.

Enforce password protection on activation

Klicka här för att markera kryssrutan. Om alternativet har aktiverats måste du använda ett globalt standardlösenord för enheter som inte är lösenordsskyddade.

Verkställ

Klicka här för att använda det globala standardlösenordet.

Dialogrutan **Byta lösenord** visas. Lösenordsändringarna visas i en lista.

Klicka på **OK** om du vill stänga listan.

Om du började med att aktivera konfigurationen visas dialogrutan **Aktiveringshanteraren**.

Se

– *Aktivera arbetskonfigurationen, sidan 88*

11.7

Skydda iSCSI-lagringar med dialogrutan för CHAP-lösenordet (maskinvarumenyn)

Använd den här dialogrutan för att aktivera CHAP-lösenord iSCSI på VRM -enheter. Systemet överför automatiskt dessa lösenord till kontona **Användare** och **Destination** till kodare, avkodare och VSG-enheter.

På nytillagda enheter ställs lösenorden in automatiskt när du aktiverar konfigurationen.

Obs! Om du anger ett tomt CHAP-lösenord tas CHAP-lösenordet bort på iSCSI- och VRM -enheter.



Obs!

- Hos alla DSA E-Series-enheter ställs CHAP-lösenordet in automatiskt.
- VRM-enheter överför CHAP-lösenordet till kodarna. Du måste emellertid ställa in CHAP-lösenordet på respektive iSCSI-enhet för att säkerställa inspelning.
- På samtliga DIVAR IP-enheter måste du manuellt ställa in CHAP-lösenordet. Se respektive DIVAR IP-manual för ytterligare instruktioner. Annars fungerar inte inspelning eller uppspelning.

Globalt CHAP-lösenord

Ange det iSCSI CHAP-lösenord som krävs för att autentisera på iSCSI-lagringsenheten och för att möjliggöra direktuppspelning från iSCSI.

Bekräfta globalt CHAP-lösenord

Bekräfta iSCSI CHAP-lösenordet.

Visa lösenord

Klicka här om du vill att det angivna lösenordet ska visas. Var försiktig så att ingen obehörig kan se lösenordet.

Verkställ

Klicka för att använda CHAP-lösenordet.

Obs! Kontrollera åtgärdsresultatet. Det är möjligt att du måste ställa in CHAP-lösenordet manuellt på vissa iSCSI-enheter.

11.8

Dialogrutan Ändra enhetslösenord (menyn Maskinvara)

Huvudfönster > **Enheter** >  **Ändra enhetslösenord** > Dialogrutan **Ändra enhetslösenord** eller

Huvudfönster > Menyn **Maskinvara** > Kommandot **Ändra enhetslösenord ...** > Dialogrutan **Ändra enhetslösenord**



Klicka för att uppdatera statusinformationen för alla enheter. Du kan uppdatera tillståndet för en enskild enhet: Högerklicka på enheten och klicka på **Uppdatera tillståndet**.

Obs! Om du har ett stort system med flera tusen konfigurerade enheter kan det ta lång tid att uppdatera tillstånd.



Klicka för att välja alla tillgängliga enheter samtidigt.

Visa lösenord

Markera kryssrutan när du vill att de konfigurerade lösenorden ska visas i läsbar form.

Filter...

Skriv in en sträng och tryck på ENTER-tangenten för att filtrera de visade objekten. Endast objekt som innehåller strängen och deras motsvarande föräldraobjekt (endast i träd) visas. Antalet filtrerade objekt och det totala antalet objekt visas. Ett aktivt filter indikeras med . Skriv in strängar inom dubbla citattecken för att hitta dem exakt, till exempel filtrerar "Camera 1" kamerorna med exakt detta namn, inte camera 201.

Avbryt filtreringen genom att klicka på .

Obs! Bara om kryssrutan **Visa lösenord** är markerad går det att söka efter lösenord också.

Tabellen låter dig ställa in följande egenskaper av tillgängliga IP-enheter:

- Servicelösenord
- Användarlösenord
- Lösenord "live"
- Mållösenord

Så här ändrar du lösenordet för IP-enheter:

1. Välj enheten.
2. Högerklicka på den valda enheten och klicka på **Redigera lösenordet ...**. Dialogrutan **Ändra enhetslösenord** visas.
3. Välj lösenordstypen som krävs.
4. Skriv in det nya lösenordet igen.
5. Klicka på **OK**.

Det nya lösenordet uppdateras i den valda enheten.

Så här ändrar du inställningarna för flera enheter:

Se *Konfigurerar flera kodare / avkodare, sidan 215*.

11.9

Dialogrutan Uppdatera enhetens fasta programvara (menyn Maskinvara)

Huvudfönster > Menyn **Maskinvara** > Kommandot **Uppdatera enhetens fasta programvara ...** > Dialogrutan **Uppdatera enhetens fasta programvara**



Klicka för att uppdatera statusinformationen för alla enheter. Du kan uppdatera tillståndet för en enskild enhet: Högerklicka på enheten och klicka på **Uppdatera tillståndet**.

Obs! Om du har ett stort system med flera tusen konfigurerade enheter kan det ta lång tid att uppdatera tillstånd.



Klicka för att välja alla tillgängliga enheter samtidigt.



Klicka för att uppdatera den fasta programvarans version.



Skriv in en sträng och tryck på ENTER-tangenten för att filtrera de visade objekten. Endast objekt som innehåller strängen och deras motsvarande föräldraobjekt (endast i träd) visas. Antalet filtrerade objekt och det totala antalet objekt visas. Ett aktivt filter indikeras med . Skriv in strängar inom dubbla citattecken för att hitta dem exakt, till exempel filtrerar "Camera 1" kamerorna med exakt detta namn, inte camera 201.

Avbryt filtreringen genom att klicka på .

Gör så här för att uppdatera den fasta programvarans version:

1. Välj enheten.
2. Klicka på **Uppdatera den fasta programvaran**.
Ett Configuration Client-informationsfönster visas.
3. Klicka på **OK**.
Filutforskaren öppnas.
4. Välj den fil som innehåller uppdateringen.
5. Klicka på **Öppna**.
Uppladdningsstatus för fast programvara-fönstret öppnas.
6. Klicka på **Starta** för att starta överföringen.
7. Klicka på **Stäng**.
Den fasta programvaran uppdateras.

Så här ändrar du inställningarna för flera enheter:

Se *Konfigurera flera kodare / avkodare, sidan 215*.

11.10

Dialogrutan Ändra enhets-IP och nätverksinställningar (menyn Maskinvara)

Huvudfönster > Menyn **Maskinvara** > Kommandot **Ändra enhetens IP- och nätverksinställningar ...** > Dialogrutan **Ändra enhetens IP- och nätverksinställningar**



Klicka för att uppdatera statusinformationen för alla enheter. Du kan uppdatera tillståndet för en enskild enhet: Högerklicka på enheten och klicka på **Uppdatera tillståndet**.

Obs! Om du har ett stort system med flera tusen konfigurerade enheter kan det ta lång tid att uppdatera tillstånd.



Klicka för att välja alla tillgängliga enheter samtidigt.

Skriv in en sträng och tryck på ENTER-tangenten för att filtrera de visade objekten. Endast objekt som innehåller strängen och deras motsvarande föräldraobjekt (endast i träd) visas. Antalet filtrerade objekt och det totala antalet objekt visas. Ett aktivt filter indikeras med . Skriv in strängar inom dubbla citattecken för att hitta dem exakt, till exempel filtrerar "Camera 1" kamerorna med exakt detta namn, inte camera 201.

Avbryt filtreringen genom att klicka på .

Tabellen låter dig ställa in följande egenskaper av tillgängliga IP-enheter:

- Visningsnamn
- IP-adress
- Nätmask
- Gateway-IP

**Obs!**

I stället för att använda kommandona kan du skriva in lämpliga inställningar i det obligatoriska fältet.

Så här ställer du in visningsnamn för IP-enheter:

1. Välj enheten.
2. Högerklicka på den valda enheten och klicka på **Ställ in visningsnamn**. Dialogrutan **Ställ in visningsnamn** visas.
3. Ange den första strängen i fältet **Startar med:**.
4. Klicka på **Beräkna**. I fältet **Slutar med:** visas den sista strängen i intervallet för den valda enheten.
5. Klicka på **OK**.
6. Gå till dialogrutan **Ändra enhetens IP- och nätverksinställningar** och klicka på **Verkställ**.
Det beräknade namnet uppdateras i den markerade enheten.

Dialogrutan Ange visningsnamn**Startar med:**

Ange det första namnet.

Slutar med:

Visar det sista namnet på valda enheter efter att du har klickat på **Beräkna**.

Beräkna

Klicka för att beräkna intervallet av visningsnamn för valda enheter.

Så här ställer du in IP-adressen för IP-enheter:

1. Välj enheten.
2. Högerklicka på den valda enheten och klicka på **Ställ in nya IP-adresser....** Dialogrutan **Ställ in nya IP-adresser** visas.
3. Ange den första IP-adressen i fältet **Startar med:**.
4. Klicka på **Beräkna**. I fältet **Slutar med:** visas den sista IP-adressen i intervallet för den valda enheten.
5. Klicka på **OK**.
6. I dialogrutan **Ändra enhetens IP- och nätverksinställningar** klickar du på **Verkställ**.
Den nya IP-adressen uppdateras i den markerade enheten.

Dialogrutan Ange IP-adresser

Startar med:

Ange den första IP-adressen.

Slutar med:

Visar den sista IP-adressen för valda enheter efter att du har klickat på **Beräkna**.

Beräkna

Klicka för att beräkna intervallet av IP-adresser för valda enheter.

Så här ställer du in subnätmask/gateway-ID för IP-enheter:

1. Klicka i det önskade fältet.
2. Ange lämpligt värde.
3. Klicka på **Verkställ**.
Det nya värdet uppdateras i den valda enheten.

Verkställ

Klicka för att konfigurera enheterna med angivna värden utan att stänga dialogrutan.

Så här ändrar du inställningarna för flera enheter:

Se *Konfigurera flera kodare / avkodare, sidan 215*.

11.11

Dialogrutan Enhetsövervakaren (menyn Maskinvara)

Huvudfönster > Menyn **Maskinvara** > Kommandot **Enhetsmonitor...** > Dialogrutan

Enhetsmonitor

Gör att du kan kontrollera status för de kodare/avkodare i enhetsträdet som är aktiva i BVMS.

Visningsnamn

Enhetsnamnet som har konfigurerats i BVMS.

Nätverksadress

Enhetens IP-adress.

Tillstånd

Följande status kan visas:

- **Konfigurerad:** Konfigurationen för den här enheten har aktiverats.
- **Konfigurationen stämmer inte:** Konfigurationen för den här enheten har inte aktiverats.
- **Okänd:** Status har inte kunnat fastställas.
- **Inte ansluten:** Inte ansluten.

Senaste kontroll

Datomet och tiden då dialogrutan startades och kontrollen utfördes. Så länge dialogrutan visas kontrolleras inte enheterna igen.

Se

- *Kontrollera status för kodare/avkodare, sidan 91*

11.12

Dialogrutan Licenshanterare (menyn Verktyg)

Huvudfönster > Menyn **Verktyg** > Kommandot **Licenskontroll ...** > Dialogrutan **Licenskontroll**

Visar antalet licensierade funktioner som för närvarande är installerade.

Du kan kontrollera om antalet installerade BVMS-licenser överskrider antalet köpta licenser.

Obs! Om den aktuella systemkonfigurationen överskrider gränserna för de installerade licenserna kan du inte aktivera konfigurationen.

11.13

Dialogrutan Licenshanterare (menyn Verktyg)

Huvudfönster > Menyn **Verktyg** > Kommandot **Licenshanterare...**

Låter dig licensiera BVMS-paket som du har beställt samt uppgradera det med ytterligare funktioner.

Licensstatus

Visar licensstatusen.

Systemets fingeravtryck

För supportändamål rekommenderar vi att du tillhandahåller **Systemets fingeravtryck**.

Installationsplats

När du aktiverar baslicensen i Bosch Remote Portal ger du information om systemets installationsplats. Den här informationen visas här.

Obs! Du kan också tillhandahålla denna information i andra licenser, men endast informationen i baslicensen visas här.

Licenser

1. Klicka på **Lägg till** för att lägga till licenserna.
Dialogrutan **Lägg till licens** visas.
2. Följ anvisningarna i dialogen.

Giltig licens

Visar den gällande baslicensen som du har aktiverat.

Funktioner

- ▶ Klicka på **Licenskontroll ...**
Dialogrutan **Licenskontroll** visas.

Visar antalet licensierade funktioner som för närvarande är installerade.

Du kan kontrollera om antalet installerade BVMS-licenser överskrider antalet köpta licenser.

Installerad BVMS-version

Visar den installerade BVMS-versionen, till exempel 11.0.

Licensierade BVMS-versioner

Visar alla BVMS-versioner som ingår och stöds i den aktuella angivna licensfilen.

Till exempel: BVMS 11.0 och alla kommande mindre versioner BVMS 11.x.

Aktiveringsdatum

Visar aktiveringsdatumet för den installerade BVMS-versionen.

Utgångsdatum

Visar utgångsdatumet för den installerade BVMS-versionen. Ett utgångsdatum gäller endast när du installerar en nödlicens eller en försäljningsdemolicens.

Software Maintenance Agreement

Utgångsdatum

Om du har köpt och aktiverat någon Software Maintenance Agreement, visas utgångsdatumet här.

Se

- *Aktivera programvarulicenserna, sidan 71*
- *Dialogrutan Lägg till licens, sidan 107*
- *Dialogrutan Licenshanterare (menyn Verktyg), sidan 105*

11.14 Dialogrutan Lägg till licens

Huvudfönster > menyn **Verktyg** > kommandot **Licenshanterare...** > **Licenser** > **Lägg till**
Gör att du kan lägga till dina köpta licenser eller demolicenser från webbplatsen Bosch Remote Portal remote.boschsecurity.com i ditt BVMS-system.

För att lägga till dina licenser följer du anvisningarna i dialogrutan.

För ytterligare information hänvisas till respektive teknisk information om licensen till BVMS.

11.15 Dialogrutor för rapporter (menyn Rapporter)

Det här kapitlet omfattar alla dialogrutor för konfigurationsrapporter.

Se

– *Skapa en rapport, sidan 91*

11.15.1 Dialogrutan Inspelningsscheman

Huvudfönster > Menyn **Rapporter** > Kommandot **Inspelningsscheman ...**

Listar de konfigurerade inspelningsschemana.

- ▶ Klicka på **CSV-export** om du vill spara all information i dialogrutan i en CSV-fil.

11.15.2 Dialogrutan Schemalagda inspelningsinställningar

Huvudfönster > Menyn **Rapporter** > Kommandot **Schemalagda inspelningsinställningar ...**

Visar de konfigurerade inställningarna för schemalagda inspelningar.

- ▶ Klicka på **CSV-export** om du vill spara all information i dialogrutan i en CSV-fil.

11.15.3 Dialogrutan Uppgiftsscheman

Huvudfönster > Menyn **Rapporter** > Kommandot **Uppgiftsscheman ...**

Listar de konfigurerade uppgiftsschemana.

- ▶ Klicka på **CSV-export** om du vill spara all information i dialogrutan i en CSV-fil.

11.15.4 Dialogrutan Kameror och parametrar för inspelning

Huvudfönster > Menyn **Rapporter** > Kommandot **Kameror och inspelningsparametrar ...**

Visar de parametrar för inspelning som är konfigurerade i kameratabellen och inspelningstabellen.

- ▶ Klicka på **CSV-export** om du vill spara all information i dialogrutan i en CSV-fil.

11.15.5 Dialogrutan Inställningar för inspelningskvalitet

Huvudfönster > Menyn **Rapporter** > Kommandot **Kvalitetsinställningar för ström ...**

Visar de konfigurerade strömkvalitetsinställningarna för alla kameror.

- ▶ Klicka på **CSV-export** om du vill spara all information i dialogrutan i en CSV-fil.

11.15.6 Dialogrutan Händelseinställningar

Huvudfönster > Menyn **Rapporter** > Kommandot **Händelseinställningar ...**

Visar vilka händelser som ett schema för larmutlösning har ställts in för.

- ▶ Klicka på **CSV-export** om du vill spara all information i dialogrutan i en CSV-fil.

11.15.7 Dialogrutan Inställningar för sammansatta händelser

Huvudfönster > Menyn **Rapporter** > Kommandot **Inställningar för sammansatt händelse ...**

Visar alla sammansatta händelser.

- ▶ Klicka på **CSV-export** om du vill spara all information i dialogrutan i en CSV-fil.

11.15.8**Dialogrutan Larminställningar**

Huvudfönster > Menyn **Rapporter** > Kommandot **Larminställningar**

Visar en lista över alla larminställningar för konfigurerade larm, inklusive inställningarna i dialogrutan **Larmalternativ**.

- Klicka på **CSV-export** om du vill spara all information i dialogrutan i en CSV-fil.

11.15.9**Dialogrutan Konfigurerade användare**

Huvudfönster > Menyn **Rapporter** > Kommandot **Konfigurerade användare ...**

Visar en lista över användare som har behörighet att logga in på Operator Client.

- Klicka på **CSV-export** om du vill spara all information i dialogrutan i en CSV-fil.

11.15.10**Dialogrutan Användargrupper och konton**

Huvudfönster > Menyn **Rapporter** > Kommandot **Användargrupper och konton ...**

Visar en lista över konfigurerade användargrupper, Enterprise Accounts, Enterprise User Groups och grupper med dubbel behörighet.

- Klicka på **CSV-export** om du vill spara all information i dialogrutan i en CSV-fil.

11.15.11**Dialogrutan Enhetsbehörigheter**

Huvudfönster > Menyn **Rapporter** > Kommandot **Enhetsbehörigheter ...**

Visar en lista över behörigheter för att använda konfigurerade enheter för varje användargrupp.

- Klicka på **CSV-export** om du vill spara all information i dialogrutan i en CSV-fil.

11.15.12**Dialogrutan Funktionsbehörigheter**

Huvudfönster > Menyn **Rapporter** > Kommandot **Operatörsbehörigheter ...**

Visar en lista över behörigheter för att använda Operator Client för varje användargrupp.

- Klicka på **CSV-export** om du vill spara all information i dialogrutan i en CSV-fil.

11.15.13**Dialogrutan Konfigurationsbehörigheter**

Huvudfönster > Menyn **Rapporter** > Kommandot **Konfigurationsbehörigheter ...**

Visar en lista över behörigheter för att använda Configuration Client för varje användargrupp.

- Klicka på **CSV-export** om du vill spara all information i dialogrutan i en CSV-fil.

11.15.14**Dialogrutan Behörigheter för användargrupp**

Huvudfönster > Menyn **Rapporter** > Kommandot **Behörigheter för användargrupp ...**

Visar en lista över behörigheter för att konfigurera användargrupper för varje användargrupp.

- Klicka på **CSV-export** om du vill spara all information i dialogrutan i en CSV-fil.

11.15.15**Dialogrutan Säkerhetsinställningar**

Huvudfönster > Menyn **Rapporter** > Kommandot **Säkerhetsinställningar ...**

Visar konfigurerade säkerhetsinställningar för varje användargrupp och Enterprise User Groups.

- Klicka på **CSV-export** om du vill spara all information i dialogrutan i en CSV-fil.

11.15.16**Dialogrutan Enheter som har kringgåtts**

Huvudfönster > Menyn **Rapporter** > Kommandot **Enheter som kringgås ...**

Visar alla konfigurerade enheter och vilka enheter som har kringgåtts.

- Klicka på **CSV-export** om du vill spara all information i dialogrutan i en CSV-fil.

11.16**Dialogrutan Larminställningar (menyn Inställningar)**

Se *Dialogrutan Larminställningar*, sidan 289 för information.

11.17

Dialogrutan SNMP-inställningar (menyn Inställningar)

Huvudfönster > Menyn **Inställningar** > Kommandot **SNMP-inställningar ...**

Gör att du kan konfigurera SNMP-övervakning på Management Server-datorn. Du anger för vilken händelse en SNMP-fälla ska skickas, viss ytterligare information om systemet och IP-adresserna för de datorer som ska ta emot SNMP-fällor från BVMS.

Servern skickar SNMP-fällor när händelserna inträffar. Du kan ta emot dessa fällor med SNMP-mottagaren i Configuration Client som använder verktyget **Loggare av SNMP-fällor**. Du kan också använda annan programvara som kan ta emot SNMP-fällor.

SNMP-agenten i BVMS stöder SNMP GetRequest. När en SNMP-hanteringsprogramvara (till exempel iReasoning MIB Browser) skickar en SNMP GetRequest-förfrågan till BVMS Management Server skickar Management Server ett motsvarande svarsmeddelande.

MIB-filen har följande sökväg:

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

Endast SNMPv1 och SNMPv2 stöds.

Obs! SNMPv1 och SNMPv2 är inte helt kompatibla. Vi rekommenderar därför inte att SNMPv1 och SNMPv2 används tillsammans.

SNMP GET-port

Skriv in ett portnummer för SNMP GetRequest. Det här är den port där SNMP-agenten för BVMS Management Server lyssnar efter SNMP GetRequest.

Obs! BVMS använder inte standardportnumret 161 för SNMP GetRequest eftersom den porten kan användas av SNMP-agenten för datorn som BVMS Management Server har installerats på. Standardvärdet är 12544.

Systemkontakt

Skriv in kontaktdata för BVMS. Den här informationen kan du hämta med en SNMP GetRequest-förfrågan genom att använda OID .1.3.6.1.2.1.1.4.

Systembeskrivning

Skriv in en beskrivning för BVMS. Den här informationen kan du hämta med en SNMP GetRequest-förfrågan genom att använda OID .1.3.6.1.2.1.1.5.

Systemplats

Skriv in platsen för BVMS. Den här strängen ska ange serverdatorns fysiska plats, till exempel byggnad, rumsnummer och racknummer.

Den här informationen kan du hämta med en SNMP GetRequest-förfrågan genom att använda OID .1.3.6.1.2.1.1.6.

Trap-mottagare

Ange IP-adressen för datorn som BVMS ska skicka SNMP-fällor till.

Trap-filter

Klicka här för att välja händelserna i händelseträdet om du vill filtrera de SNMP-fällorna som skickas.

Se

– *Konfigurera SNMP-övervakning, sidan 91*

11.18

Dialogrutan LDAP-inställningar (menyn Inställningar)

Huvudfönster > Menyn **Inställningar** > Kommandot **Inställningar för LDAP-server...**

Du anger LDAP-serverinställningarna som konfigurerats utanför BVMS. Du kommer att behöva hjälp av din IT-administratör som installerade LDAP-servern för de följande posterna.

Alla fält är obligatoriska utom fälten i grupp-rutan **Testanvändare/användargrupp**.

Inställningar för LDAP-server

LDAP-server

Skriv in namnet eller IP-adressen till LDAP-servern.

Port

Ange portnumret för LDAP-servern (standard HTTP: 389, HTTPS: 636)

Säker anslutning

Markera kryssrutan för att aktivera säker dataöverföring.

Autentiseringsmekanism

Med förhandling väljs rätt autentiseringsprotokoll automatiskt.

Med enkelt skickas inloggningsuppgifterna okrypterade som ren text.

Proxy-autentisering

Anonym

Använd för att logga in som gäst. Välj det här alternativet om LDAP-servern har stöd för det och du inte kan konfigurera en specifik proxy-användare.

Använd följande autentiseringsuppgifter

Användarnamn

Ange det unika namnet för proxy-användaren. Den här användaren måste ge användarna av den här BVMS-användargruppen åtkomst till LDAP-servern.

Lösenord

Ange proxy-användarens lösenord.

Test

Klicka för att testa huruvida proxy-användaren har åtkomst till LDAP-servern.

LDAP-bas för användare

Ange det unika namnet (DN = distinguished name) på LDAP-sökvägen där du kan söka efter en användare.

Exempel på ett DN för LDAP-bas: CN=Users,DC=Security,DC=MyCompany,DC=com

Filter för användare

Välj ett filter som används för att söka efter ett unikt användarnamn. Exempel är fördefinierade. Ersätt %username% med det faktiska användarnamnet.

LDAP-bas för grupp

Ange det unika namnet för LDAP-sökvägen i vilken du kan söka efter grupper.

Exempel på ett DN för LDAP-bas: CN=Users,DC=Security,DC=MyCompany,DC=com

Filter för sökning av gruppmedlem

Välj ett filter som används för att söka efter en gruppmedlem.

Exempel är fördefinierade. Ersätt %usernameDN% med det faktiska användarnamnet och dess DN.

Gruppsokningsfilter

Lämna inte det här fältet tomt. Om det inte finns någon registrering så kan du inte tilldela en LDAP-grupp till en BVMS-användargrupp.

Välj ett filter för att hitta en användargrupp.

Exempel är fördefinierade.

Testanvändare/användargrupp

Posterna i den här grupp-rutan sparas inte efter klick på **OK**. De fungerar endast för testningen.

Användarnamn

Ange namnet på en testanvändare. Uteslut DN:et.

Lösenord

Ange testanvändarens lösenord.

Testanvändare

Klicka för att testa om kombinationen av användarnamn och lösenord är korrekt.

Grupp (DN)

Ange det unika gruppnamnet med vilket användaren är associerad.

Testgrupp

Klicka för att testa associeringen av användaren med gruppen.

Se

– *Välja en associerad LDAP-grupp, sidan 333*

11.18.1**Associera en LDAP-grupp**

Du kan associera en LDAP-grupp med en BVMS-användargrupp för att ge användarna av denna LDAP-grupp åtkomst till Operator Client. Användarna i LDAP-gruppen får användargruppens åtkomstbehörigheter på de ställen där du konfigurerar LDAP-gruppen.

Du behöver förmodligen hjälp av en IT-administratör som är ansvarig för LDAP-servern.

Du konfigurerar LDAP-grupper i vanliga användargrupper eller Enterprise User Groups.

**Obs!**

Om en LDAP-grupp är associerad med en BVMS-användargrupp kan användare av den här LDAP-gruppen starta Operator Client med enkel inloggning.

**Obs!**

En LDAP-användare kan associeras med fler än en LDAP-användargrupp, vilken i sin tur är associerad med en särskild BVMS-användargrupp.

LDAP-användaren får de behörigheter för BVMS-användargruppen som beställts utöver övriga LDAP-användargrupper, som associeras med den här LDAP-användaren.

Associera en LDAP-grupp:

1. Klicka på **Inställningar för LDAP-server...**
Dialogrutan **Inställningar för LDAP-server** visas.
2. Ange inställningarna för din LDAP-server och klicka på **OK**.
För detaljerad information om olika fält, följ länken till lämpligt programfönster.

Se

- *Dialogrutan LDAP-inställningar (menyn Inställningar), sidan 109*
- *Sidan Egenskaper för användargrupper, sidan 308*

11.19**Definiera LDAP-användargruppens ordning i dialogruta (menyn Inställningar)**

Visar **Ändra ordning på LDAP-användargruppen** listan. I listan visas LDAP-användargrupperna med tillhörande BVMS-användargrupper och Enterprise User Groups. Genom att dra och släppa eller använda upp- och ner-pilarna kan du ändra ordningen på grupperna.

**Obs!**

En LDAP-användare kan associeras med fler än en LDAP-användargrupp, vilken i sin tur är associerad med en särskild BVMS-användargrupp.

LDAP-användaren får de behörigheter för BVMS-användargruppen som beställts utöver övriga LDAP-användargrupper som associeras med den här LDAP-användaren.

11.20

Dialogrutan Inställningar för åtkomsttoken (menyn Inställningar)

Huvudfönster >menyn **Inställningar** > kommandot **Inställningar för åtkomsttoken...**

Om du har konfigurerat inloggningen till Management Server med hjälp av en åtkomsttoken måste du först definiera tokeninställningarna.

En token skapas av Enterprise Management Server och måste signeras av ett certifikat från ett certifikatarkiv på den lokala datorn. Du måste identifiera certifikatet för att veta vilket certifikat som ska användas.

Obs! BVMS stöder inte certifikat som använder en secure hash-algoritm SHA-1 och har en nyckellängd som understiger 2 048 bitar.

Egenskaper för signeringscertifikat

Ange en egenskapssträng för att identifiera respektive certifikat.

Obs! Om mer än ett certifikat matchar villkoren används det senaste giltiga certifikatet.

Skriv en giltig egenskapssträng i fältet genom att följa reglerna i **Egenskaper för signeringscertifikat**-fältet:

- Strängen består av ett eller flera villkor.
- Förhållandena separeras av semikolon (;).
- Villkoren är par med certifikategenskapsnamn och förväntat värde, avgränsade med ett likhetstecken (=).
- Certifikategenskapsnamn kan bestå av en eller flera delar, avgränsade av en punkt (.).
- Certifikategenskapsnamn och förväntade värden är inte skiftlägeskänsliga.

Exempel:

SubjectName.CN=BVMS Token Issuer;Parent.SubjectName.CN=BVMS Intermediate

- Den gemensamma namndelen (CN) i certifikatets ämnesnamn måste vara lika med *BVMS Token Issuer*.
- Dessutom måste den gemensamma namndelen av ämnesnamnet för certifikatets överordnade certifikat vara lika med *BVMS Intermediate*. Det överordnade certifikatet är det certifikat som användes för att signera det aktuella certifikatet.

Parent.Thumbprint=A95FF7C6EC374127174D3AFA8EA67C94E8E66C3F

- Tumavtrycket för certifikatets överordnade certifikat måste vara som angivet.

Lista över certifikategenskapsnamn som stöds:

Namn	Returtyp
Tumavtryck	Sträng
Serienummer	Sträng
Ämnesnamn	Unikt ämnesnamn

Namn	Returtyp
Utfärdarnamn	Unikt namn på utfärdare
Överordnad	Certifikat som användes för att signera det aktuella certifikatet (CA-utfärdare)

Lista över egenskapsnamn som stöds på det unika namnet:

Namn	Returtyp
CN	Sträng: Vanligt namn
OU	Sträng: Namn på organisationsenhet
O	Sträng: Organisationsnamn
L	Sträng: Ortnamn
S	Sträng: Namn på delstat eller provins
C	Sträng: Landsnamn

Exempel på användning av unikt namn:

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

Certifikatkedja

Markera kryssrutan om du vill inkludera certifikatkedjan.

Obs! Om Management Server har exakt samma certifikat installerat behöver du inte nödvändigtvis inkludera certifikatkedjan.

Antal inkluderade certifikat

Ange det exakta antalet certifikat som ingår i åtkomsttoken.

Obs! Du får inte inkludera Root-certifikatet.

Åtkomsttokens livstid

Ange tiden i timmar för att definiera hur länge tokens är giltiga efter att de har skapats av Enterprise Management Server.

Se

- *Tokenbaserad autentisering, sidan 83*

11.21

Dialogrutan Inställningar för betrodda certifikat (menyn Inställningar)

Huvudfönster >menyn **Inställningar** > kommandot **Inställningar för betrott certifikat...**

Med den här dialogrutan kan du introducera certifikatets tumavtryck som används av Management Server för att autentisera åtkomsttoken.

Obs! Menyn **Inställningar för betrott certifikat...** är endast tillgänglig om du startar Configuration Client med administratörsbehörighet och användaren som loggar in har behörigheten **Konfigurera användargrupper/Enterprise Accounts/LDAP-serverinställningar och åtkomsttoken**.

Tumavtryck av betrott certifikat

Visar ett redan konfigurerat tumavtryck eller ett tomt tumavtryck om ingen konfiguration kan hittas i registret. Ange eller ändra tumavtrycket för rotcertifikatet.

Det medföljande tumavtrycket skrivs till sökvägen `HKEY_LOCAL_MACHINE\SOFTWARE\Bosch Sicherheitssysteme GmbH\Bosch Video Management System\TrustedCertificates`, till nyckeln "BvmsTrustedCertificate".

Obs! Tumavtrycket ingår inte i exporten när konfigurationen exporteras.

Obs! BVMS stöder inte certifikat som använder en secure hash-algoritm SHA-1 och har en nyckellängd som understiger 2 048 bitar.

11.22**Dialogrutan Alternativ (menyn Inställningar)**

Obs! Vissa funktioner kräver att du köper respektive licens.

Huvudfönster > Menyn **Inställningar** > Kommandot **Alternativ...**

Configuration Client**Språk**

Här kan du konfigurera språket för Configuration Client. Om du väljer **Systemspråk** används samma språk som i Windows.

Den här inställningen aktiveras efter omstart av Configuration Client.

Automatisk utloggning

Här kan du konfigurera automatisk utloggning av Configuration Client. Configuration Client loggar ut efter den konfigurerade tidsperioden.

Ändringar på konfigurationssidorna för följande enheter på sidan **Enheter** sparas inte automatiskt och går förlorade vid utloggning på grund av inaktivitet:

- Kodare
- Avkodare
- VRM-enheter
- iSCSI-enheter
- VSG-enheter

Alla andra väntande konfigurationsändringar sparas automatiskt.

Obs! Ändringar i dialogrutor som du inte bekräftar genom att klicka på **OK** sparas inte.

Scan options

Här kan du konfigurera huruvida det går att söka efter enheter i respektive subnät eller mellan subnät.

Operator Client**Flera inloggningar****Tillåt flera inloggningar för samma användare**

Gör att du kan ange att en användare med BVMS SDK, webbklienten BVMS, mobilappen BVMS eller Operator Client kan göra flera inloggningar samtidigt med samma användarnamn.

Serverinställningar**Databasanslutningssträng**

Här kan du konfigurera anslutningssträngen för loggboks-databasen.

**Obs!**

Ändra endast denna sträng när du vill konfigurera en fjärr-SQL-server för loggboken och bara när du är bekant med SQL-serverteknik.

Kvarhållningsperiod

Du kan också definiera den längsta kvarhållningstiden för posterna i loggboken. När den definierade arkiveringstiden går ut tas posterna bort automatiskt. Den här inställningen aktiveras när konfigurationen har aktiverats.

Enheter**Monitorgrupp**

Gör att du kan ange att användarna ska kunna styra alla -skärmgrupper med alla BVMS-klientdatorer. Den här datorn behöver då inte konfigureras som en arbetsstation i enhetsträdet.

Välj avkodarström

Låter dig konfigurera att alla avkodare i ditt system använder en kompatibel ström och inte nödvändigtvis liveström. Den här inställningen aktiveras när konfigurationen har aktiverats.

Tidsserver för kodare

Tillåter att du kan konfigurera tidsserverinställningar för kodare. Som standard används IP-adressen för Central-Server.

Systemfunktioner**Kartor****Kundspecifik API-nyckel**

Ange din API-nyckel för att använda (Here) onlinemappningar.

Visa API-nyckel

Markera kryssrutan om du vill visa API-tangenten.

Typ av bakgrundskarta*

Låter dig välja typ av bakgrundskarta för den globala kartan. Följande karttyper är tillgängliga om du har tillgång till Internet (onlineläge):

- **HERE stadskarta**
- **HERE mörk stadskarta**
- **HERE satellitkarta**

Om du inte har tillgång till Internet (offlineläge) väljer du **Inga**.

**Obs!**

Om du byter typ av bakgrundskarta från online (kartor Here) till offline (**Inga**) eller tvärtom förlorar du alla placerade kamerahotspots och kartvyportar.

Du kan bara definiera en bakgrund för den globala kartan. Den här bakgrunden gäller för alla kartvyportar.

Map-based tracking assistant**Aktivera systemfunktion**

Låter dig konfigurera att en Operator Client-användare kan använda Map-based tracking assistant.

Inaktivera färgning av aktiva punkter på kartor

Här kan du inaktivera blinkande aktiveringspunkter på kartor.

Aktivera avancerad statusvisning (färgning av aktiva punkter på kartor beroende på status)

Här kan du för alla tillståndsrelaterade händelser ange att aktiveringspunkterna för enheterna som hör till den här händelsen ska visas med en bakgrundsfärg och blinka när den konfigurerade händelsen inträffar.

Aktivera avancerad larmvisning (färgning av aktiva punkter på kartor beroende på larm)

Här kan du för alla larm ange att aktiveringspunkterna för enheterna som hör till det här larmet ska visas med en bakgrundsfärg och blinka när det konfigurerade larmet utlöses.

Du kan konfigurera den avancerade tillståndsvisningen när du har sparat konfigurationen.

Aktiveringspunkterna visas på en karta i Operator Client när du har aktiverat konfigurationen.

12

Sidan Enheter

Huvudfönster > **Enheter**



Obs!

BVMS Viewer stöder inte avkodarenheter.

Visar enhetsträdet och konfigurationssidorna.

Antalet objekt nedanför en post visas inom hakparenteser.

Du kan konfigurera tillgängliga enheter, som mobila videotjänster ONVIF-kodare, Bosch Video Streaming Gateway-enheter, kodare, avkodare, VRM-enheter, lokala lagringskodare, analoga matriser eller kringutrustning som ATM/POS-bryggor.

Obs!

Enheterna är representerade i ett träd och indelade enligt fysisk nätverksstruktur samt enhetskategorier.

Videokällor, såsom kodare, är grupperade under VRM-enheter.

Skriv in en sträng och tryck på ENTER-tangenten för att filtrera de visade objekten. Endast objekt som innehåller strängen och deras motsvarande föräldraobjekt (endast i träd) visas. Antalet filtrerade objekt och det totala antalet objekt visas. Ett aktivt

filter indikeras med . Skriv in strängar inom dubbla citattecken för att hitta dem exakt, till exempel filtrerar "Camera 1" kamerorna med exakt detta namn, inte camera 201.

Avbryt filtreringen genom att klicka på .

- Klicka på ett trädobjekt för att visa motsvarande sida.

12.1

Uppdatera tillstånd och funktioner för enheter

Huvudfönster > **Enheter**

Efter en uppdatering av den fasta programvaran kan det vara nödvändigt att synkronisera funktionerna för alla konfigurerade avkodare, kodare och VSG. Med den här funktionen jämförs funktionerna från varje enhet med de funktioner som redan har lagrats i BVMS. Du kan uppdatera enhetsfunktionerna för alla enheter i enhetsträdet samtidigt.

Det är också möjligt att kopiera en lista över de enheter vars funktioner har ändrats till Urklipp. Du kan sedan klistra in listan, till exempel i en textredigerare för att undersöka ändringarna i närmare detalj.

Enhetslistan från Urklipp formateras som CSV och innehåller följande information:

- Enhet
- Enhetstyp
- IP-adress

Obs! Om du har ett stort system med flera tusen konfigurerade enheter kan det ta lång tid att uppdatera enheternas tillstånd och funktioner.



Obs!

Funktionerna hämtas endast för tillgängliga enheter. Om du vill se om en enhet inte kan nås måste du kontrollera enhetens tillstånd.

Så här uppdaterar du enhetens tillstånd och funktioner:

1. Klicka på .
Dialogrutan **Uppdatera enhetsfunktioner** visas. Tillståndsinformationen för alla enheter uppdateras och enhetsfunktionerna hämtas.
Endast om enhetsfunktionerna inte är uppdaterade visas lämpliga enheter i en lista och knappen **Uppdatera** är aktiverad.
 2. Klicka på **Kopierar enhetslistan till Urklipp** vid behov.
 3. Klicka på **Uppdatera**.
 4. Klicka på **OK**.
- ✓ Enhetsfunktionerna har uppdaterats.

**Obs!**

Tillståndsinformationen för alla enheter uppdateras alltid, även om du avbryter dialogrutan **Uppdatera enhetsfunktioner**.

12.2**Ändra lösenordet för IP-enheter**

Huvudfönster > **Enheter** >  **Ändra enhetslösenord** > Dialogrutan **Ändra enhetslösenord** eller

Huvudfönster > Menyn **Maskinvara** > Kommandot **Ändra enhetslösenord ...** > Dialogrutan **Ändra enhetslösenord**

Så här ändrar du lösenordet för IP-enheter:

1. Välj enheten.
2. Högerklicka på den valda enheten och klicka på **Redigera lösenordet ...**
Dialogrutan **Ändra enhetslösenord** visas.
3. Välj lösenordstypen som krävs.
4. Skriv in det nya lösenordet igen.
5. Klicka på **OK**.

Det nya lösenordet uppdateras i den valda enheten.

Se *Dialogrutan Ändra enhetslösenord (menyn Maskinvara)*, sidan 101 för mer information.

Så här ändrar du inställningarna för flera enheter:

Se *Konfigurera flera kodare / avkodare*, sidan 215.

Se

- *Dialogrutan Ändra enhetslösenord (menyn Maskinvara)*, sidan 101

12.3**Lägga till en enhet**

Huvudfönster > **Enheter**

Du lägger till följande enheter i enhetsträdet manuellt, vilket innebär att du måste känna till nätverksadressen för enheten för att kunna lägga till den:

- Video IP-enhet från Bosch
- Analog matris
För att kunna lägga till en Bosch Allegiant-enhet behöver du en giltig Allegiant-konfigurationsfil.
- BVMS-arbetsstation
En arbetsstation måste ha Operator Client-programvaran installerad.
- Kommunikationsenhet

- Bosch ATM/POS Bridge, DTP-enhet
- Virtuellt ingång
- Nätverksövervaknings -enhet
- Bosch IntuiKey-tangentbord
- KBD-Universal XF-tangentbord
- Monitorgrupp
- I/O-modul
- Allegiant CCL-emulering
- Inbrottspanel från Bosch
- Serverbaserad analysenhet
- Passersystem från Bosch

Du kan söka efter följande enheter för att lägga till dem i dialogrutan **BVMS Scan Wizard**:

- VRM-enheter
- Kodare
- Endast livekodare
- Endast live-ONVIF-kodare
- Kodare med lokal lagring
- Avkodare
- Video Streaming Gateway-enheter (VSG)
- DVR-enheter



Obs!

När du har lagt till en enhet, klicka på  för att spara inställningarna.



Obs!

Lägg till DVR-enheten med hjälp av administratörskontot för enheten. Med ett DVR-användarkonto med begränsade behörigheter kan resultatet bli att det inte går att använda funktioner i BVMS, till exempel använda kontrollen för en PTZ-kamera.

Dialogrutan BVMS Scan Wizard

Huvudfönster > **Enheter** > Utvidga  > Högerklicka på  > Klicka på **Sök efter kodare** > Dialogrutan **BVMS Scan Wizard**

Huvudfönster > **Enheter** > Utvidga  > Högerklicka på  > Klicka på **Sök efter Video Streaming Gateways** > Dialogrutan **BVMS Scan Wizard**

Huvudfönster > **Enheter** > Högerklicka på  > Klicka på **Sök efter endast live-kodare** > Dialogrutan **BVMS Scan Wizard**

Huvudfönster > **Enheter** > Högerklicka på  > Klicka på **Sök efter kodare med lokal lagring** > Dialogrutan **BVMS Scan Wizard**

Huvudfönster > **Enheter** > Utvidga  > Utvidga  > Högerklicka på  > Klicka på **Sök efter avkodare** > Dialogrutan **BVMS Scan Wizard**

I den här dialogrutan kan du avsöka tillgängliga enheter i nätverket, konfigurera dem och lägga till dem i systemet i en enda process.

Använd

Klicka här för att välja en enhet som ska läggas till i systemet.

Typ (inte tillgänglig för VSG-enheter)

Visar enhetens typ.

Visningsnamn

Visar enhetsnamnet som har angetts i enhetsträdet.

Nätverksadress

Visar enhetens IP-adress.

Användarnamn

Visar användarnamnet som har konfigurerats på enheten.

Lösenord

Autentisera dig med enheten genom att skriva in lösenordet.

Status

Visar statusen för autentisering.



: Lyckades



: Misslyckades

Huvudfönster > **Enheter** > Högerklicka på  > Klicka på **Sök efter VRM-enheter** > Dialogrutan BVMS Scan Wizard



Obs!

Om du vill konfigurera en sekundär VRM-enhet måste du först installera lämplig programvara på datorn. Kör Setup.exe och välj **Sekundär VRM**.

Roll

Välj önskat värde i listan.

I följande tabell visas vilka roller som varje VRM-typ kan ha:

Roll/typ	Primär VRM	Sekundär VRM
Primär (normal)	X	
Sekundär (normal)		X
Primär reserv	X	
Sekundär reserv		X
Spegglad		X

För en primär VRM kan du lägga till en VRM-enhet med följande roller:

- Reserv-VRM
- Spegglad VRM

För en sekundär VRM kan du lägga till VRM-enheter med följande roll:

- Reserv-VRM

VRM-master

Välj önskat värde i listan.

Användarnamn

Visar användarnamnet som har konfigurerats på VRM-enheten.
Du kan skriva in ett annat användarnamn vid behov.

Se

- *Lägga till VRM-enheter genom avsökning, sidan 161*
- *Lägga till en kodare till en VRM-pool, sidan 205*
- *Lägga till en kodare för endast live video, sidan 206*
- *Lägga till en kodare för lokal lagring, sidan 206*
- *Söka efter enheter, sidan 70*

12.4**Sidan Serverlista/adressbok**

Huvudfönster > **Enheter** > **Enterprise System** > **Serverlista/adressbok**

Du kan lägga till flera Management Server-datorer för samtidig åtkomst i BVMS Enterprise System. Du kan också lägga till flera Management Server-datorer för sekventiell åtkomst i Server Lookup.

Du kan lägga till ytterligare kolumner i serverlistan. Det gör att du kan lägga till ytterligare information som användaren kan söka efter med Server Lookup. De tillagda kolumnerna visas också på sidan **Serveråtkomst** (huvudfönster > **Användargrupper** > fliken **Enterprise User**

Groups >  > fliken **Serveråtkomst**).

Lägg till server

Klicka för att visa dialogrutan **Lägg till server**.

Ta bort server

Klicka här för att ta bort Management Server-objekten.

Management Server

Här visas namnen på alla tillagda Management Server-datorer. Du kan ändra alla poster.

Obs! Om du använder en SSH-anslutning anger du adressen i följande format:

ssh://IP eller servernamn:5322

Privat nätverksadress

Här visas de privata nätverksadresserna för alla tillagda Management Server-datorer. Du kan ändra alla poster.

Servernummer

Här visas de logiska numren för alla tillagda Management Server-datorer. Du kan ändra alla poster.

Serverbeskrivning

Skriv in en beskrivning för Management Server. Du behöver den här beskrivningen när du ska hitta den i listan över tillgängliga servrar när du vill ha åtkomst endast till Management Server, t.ex. om du ska utreda ett larm som kommer från ett annat hanteringssystem.

Klicka här för att få stegvisa instruktioner:

- *Konfigurera serverlistan för Enterprise System, sidan 81*
- *Konfigurera Server Lookup, sidan 122*
- *Exportera serverlistan, sidan 122*
- *Importera en serverlista, sidan 123*

Se

- *SSH-tunnel, sidan 48*

12.4.1**Dialogrutan Lägg till server**

Huvudfönster > **Enheter** > **Enterprise System** > **Serverlista/adressbok**

Servernamn

Ange displaynamnet för Management Server.

Obs! Om du använder en SSH-anslutning anger du adressen i följande format:

ssh://IP eller servernamn:5322

Privat nätverksadress

Ange den privata IP-adressen eller DNS-namnet för Management Server.

Publik nätverksadress

Ange den offentliga nätverksadressen.

Serverbeskrivning

Skriv in en beskrivning för Management Server.

12.4.2**Konfigurera Server Lookup**

För serversökning kan användare av Operator Client eller Configuration Client logga in med användarnamnet för en normal användargrupp, inte som en användare för en Enterprise User Group.

Se

- *Server Lookup, sidan 24*
- *Sidan Serverlista/adressbok, sidan 121*
- *Använda serversökning, sidan 70*

12.4.3**Konfigurera serverlistan**

Huvudfönster > **Enheter** > **Enterprise System** > **Serverlista/adressbok**

Så här lägger du till servrar:

1. Klicka på **Lägg till server**.
Dialogrutan **Lägg till server** visas.
2. Ange ett visningsnamn för servern och ange adressen till det privata nätverket (DNS-namn eller IP-adress).
Obs! Om du använder en SSH-anslutning anger du adressen i följande format:
ssh://IP eller servernamn: 5322
3. Klicka på **OK**.
4. Upprepa dessa steg tills du har lagt till alla önskade Management Server-datorer.

Så här lägger du till kolumner:

- ▶ Högerklicka på tabellrubriken och klicka på **Lägg till kolumn**.
Du kan lägga till upp till tio kolumner.
Högerklicka på önskad kolumn och klicka på **Radera kolumn** för att radera den.
- ✓ När du exporterar serverlistan exporteras också de tillagda kolumnerna.

Se

- *Konfigurera serverlistan för Enterprise System, sidan 81*

12.4.4**Exportera serverlistan**

Huvudfönster > **Enheter** > **Enterprise System** > **Serverlista/adressbok**

Du kan exportera serverlistan med alla konfigurerade egenskaper för redigering och senare import.

När du redigerar den exporterade CSV-filen i ett externt redigeringsprogram är det viktigt att du noterar de begränsningar som beskrivs i kapitlet Serverlista.

Så här exporterar du:

1. Högerklicka på tabellrubriken och klicka på **Exportera serverlista...**
 2. Ange ett namn på exportfilen och klicka på **Spara**.
- ✓ Alla kolumner i serverlistan exporteras som en csv-fil.

Närliggande ämnen

- *Server Lookup, sidan 24*
- *Serverlista*
- *Sidan Serverlista/adressbok, sidan 121*

12.4.5

Importera en serverlista

Huvudfönster > **Enheter** > **Enterprise System** > **Serverlista/adressbok**

När du redigerar den exporterade CSV-filen i ett externt redigeringsprogram är det viktigt att du noterar de begränsningar som beskrivs i kapitlet Serverlista.

Så här importerar du:

1. Högerklicka på tabellrubriken och klicka på **Importera serverlista...**
2. Klicka på önskad fil och klicka på **Öppna**.

Närliggande ämnen

- *Server Lookup, sidan 24*
- *Serverlista*
- *Sidan Serverlista/adressbok, sidan 121*

12.5

Sidan DVR (digital videoinspelare)

Huvudfönster > **Enheter** >  > 

Visar egenskapssidorna för vald DVR-enhet.

Låter dig integrera en DVR-enhet i ditt system.

- Klicka på en flik för att visa motsvarande egenskapssida.



Obs!

Du konfigurerar inte själva DVR-enheten utan integreringen av DVR-enheten i BVMS.



Obs!

Lägg till DVR-enheten med hjälp av administratörskontot för enheten. Med ett DVR-användarkonto med begränsade behörigheter kan resultatet bli att det inte går att använda funktioner i BVMS, till exempel använda kontrollen för en PTZ-kamera.

Se

- *DVR-enheter, sidan 123*
- *Konfigurera integreringen för en DVR-enhet, sidan 126*

12.5.1

DVR-enheter

Det här kapitlet innehåller bakgrundsinformation om de DVR-enheter som du kan integrera i BVMS.

Vissa DVR-modeller (t.ex. DHR-700) har funktioner för inspelning från kodare/IP-kameror. Andra DVR-modeller har endast funktioner för analoga kameror.

En kodare/IP-kamera ska inte integreras i konfigurationen för de två videosystemen (DVR-enheter eller videohanteringssystem).

Om kodare/IP-kameror är anslutna till en DVR som redan har integrerats i BVMS, så upptäcks inte de här kodarna/IP-kamerorna av BVMS-nätverkets enhetssökning. Det här stämmer för nätverkssökningen som inleddes från Configuration Client eller från Config Wizard.

Om en DVR-enhet med anslutna kodare/IP-kameror har integrerats i BVMS och de här kodarna/IP-kamerorna redan har lagts till i BVMS, så visas en varning. Ta bort de här kodarna/IP-kamerorna från DVR-enheten eller från BVMS.

Config Wizard lägger inte till DVR-enheter som har IP kameror som orsakar en konflikt i konfigurationen.

DVR-enheter kan hantera ett begränsat antal samtidiga anslutningar. Det här antalet anger det maximala antalet Operator Client-användare som kan visa videor från den här DVR-enheten samtidigt utan att svarta bildrutor visas.

**Obs!**

Lägg till DVR-enheten med hjälp av administratörskontot för enheten. Med ett DVR-användarkonto med begränsade behörigheter kan resultatet bli att det inte går att använda funktioner i BVMS, till exempel använda kontrollen för en PTZ-kamera.

**Obs!**

DIVAR AN 3000/5000: När du tar bort videodata från DVR:en, raderas alltid minst en hel timme videodata. Om du väljer en tidsperiod från till exempel 6:50 till 7:05, raderas alla videodata från 6:00 till 8:00.

Bosch HD hybrid- och nätverksinspelare i 700-serien: Borttagningen börjar alltid i början av inspelningarna för alla kameror som visas i Operator Client, och avslutas vid den tidpunkt du anger.

Se

- *Sidan DVR (digital videoinspelare), sidan 123*
- *Konfigurera integreringen för en DVR-enhet, sidan 126*

12.5.2

Lägga till en DVR-enhet genom avsökning

Så här lägger du till DVR-enheter genom avsökning:



1. Högerklicka på  och klicka på **Sök efter DVR-enheter**. Dialogrutan **BVMS Scan Wizard** visas.
2. Markera önskade kryssrutor för de enheter som du vill lägga till.
3. Klicka på **Nästa >>**. Dialogrutan **Autentisera enheter** i guiden visas.
4. Ange lösenordet för varje enhet som skyddas med ett lösenord. Lösenordskontrollen sker automatiskt om du inte skriver något i lösenordsfältet inom ett par sekunder, eller om du klickar utanför lösenordsfältet. Om samtliga enheter har samma lösenord kan du ange det i det första **Lösenord**-fältet.

Högerklicka sedan på detta fält och klicka på **Kopiera cell till kolumn.**



I kolumnen **Status** anges lyckade inloggningar med .



Misslyckade inloggningsförsök anges med .

5. Klicka på **Slutför.**
Enheten läggs till i enhetsträdet.

12.5.3

Dialogrutan Lägg till DVR



Huvudfönster > **Enheter** > expandera  >  > **Lägg till DVR-inspelare**

Kan användas för att lägga till en DVR-enhet manuellt.

Nätverksadress/port

Ange IP-adressen för din DVR-enhet. Ändra portnumret om det behövs.

Användarnamn:

Ange användarnamnet som du vill använda för att ansluta till DVR-enheten.

Lösenord:

Ange lösenordet som du vill använda för att ansluta till DVR-enheten.

Säkerhet

Kryssrutan **Säker anslutning** är markerad som standard.

Om det inte går att ansluta via en säker anslutning, visas ett meddelande. Klicka för att ta bort markeringen.



Obs!

Om kryssrutan **Säker anslutning** har markerats är kommando- och kontrollanslutningar säkra. Strömning av videodata är inte säker.

Se

- *Lägga till en enhet, sidan 118*

12.5.4

Fliken inställningar



Huvudfönster > **Enheter** >  >  > fliken **Inställningar**

Visar nätverksinställningarna för DVR-enheten som är ansluten till ditt system. Låter dig ändra inställningarna om det behövs:

12.5.5

Fliken Kameror



Huvudfönster > **Enheter** >  >  > fliken **Kameror**

Visar alla videokanaler i DVR-enheten som kameror. Låter dig ta bort kameror.

En videoingång som är inaktiverad i DVR-enheten visas som en aktiv kamera i BVMS eftersom det kan finnas tidigare inspelningar för ingången.

12.5.6

Fliken Ingångar



Huvudfönster > **Enheter** >  >  > fliken **Ingångar**

Här visas alla ingångar på DVR-enheten.

Låter dig ta bort objekt.

12.5.7 Fliken Reläer

Huvudfönster > **Enheter** >  >  > fliken **Reläer**
Här visas alla reläer på DVR-enheten. Låter dig ta bort objekt.

12.5.8 Konfigurera integreringen för en DVR-enhet

Huvudfönster > **Enheter** > Utvidga  > 



Obs!

Lägg till DVR-enheten med hjälp av administratörskontot för enheten. Med ett DVR-användarkonto med begränsade behörigheter kan resultatet bli att det inte går att använda funktioner i BVMS, till exempel använda kontrollen för en PTZ-kamera.



Obs!

Du konfigurerar inte själva DVR-enheten utan integreringen av DVR-enheten i BVMS.

Så här tar du bort ett objekt:

1. Klicka på fliken **Inställningar, Kameror, Ingångar** eller **Reläer**.
2. Högerklicka på ett objekt och klicka på **Ta bort**. Objektet tas bort.



Obs!

Du kan återställa ett borttaget objekt genom att högerklicka på DVR-enheten och välja **Skanna DVR-enhet igen**.

Ändra namn på en DVR-enhet:

1. Högerklicka på en DVR-enhet och välj **Ändra namn**.
2. Ange objektets nya namn.

Se

- *Lägga till en enhet, sidan 118*
- *Sidan DVR (digital videoinspelare), sidan 123*

12.6 Sidan Matrisväxlare

Huvudfönster > **Enheter** >  > 

Visar egenskapssidorna för Bosch Allegiant-enheten.
Du konfigurerar inte själva Bosch Allegiant-enheten utan endast BVMS-relaterade egenskaper. Information om hur du ansluter en Allegiant-enhet med BVMS finns i kapitlet **Koncept** i den här onlinehjälp. I det här kapitlet ges bakgrundsinformation om valda frågor.
Du kan även konfigurera kontrollprioriteter för Allegiant-trunkledning.
► Klicka på en flik för att visa motsvarande egenskapssida.

Se

- *Konfigurera en Bosch Allegiant-enhet, sidan 127*
- *Ansluta Bosch Allegiant-matrisen till BVMS, sidan 54*

12.6.1 Lägga till en Bosch Allegiant-enhet

Lägga till en Bosch Allegiant-enhet:

1. Högerklicka på  och klicka på **Lägg till Allegiant**. Dialogrutan **Öppna** visas.
2. Välj lämplig Allegiant-konfigurationsfil och klicka på **OK**. Bosch Allegiant-enheten läggs till i systemet.

Obs! Du kan endast lägga till en Bosch Allegiant-matris.

12.6.2 Konfigurera en Bosch Allegiant-enhet

Huvudfönster > **Enheter** > expandera  > 

Du konfigurerar inte själva Bosch Allegiant-enheten utan endast BVMS-relaterade egenskaper.

Tilldela en utgång till en kodare:

1. Klicka på fliken **Utgångar**.
2. I kolumnen **Användning**, klicka på **Digitalledningar** i de önskade cellerna.
3. Välj den önskade kodaren i kolumnen **Encoder**.

Lägga till en ingång till en Bosch Allegiant-enhet:

1. Klicka på fliken **Ingångar**.
2. Klicka på **Lägg till ingångar**. En ny rad läggs till i tabellen.
3. Ange nödvändiga inställningar i cellerna.

Ta bort en ingång:

1. Klicka på fliken **Ingångar**.
2. Klicka på den tabellrad som behövs.
3. Klicka på **Ta bort ingång**. Raden tas bort från tabellen.

Se

- *Ansluta ett Bosch IntuiKey-tangentbord till BVMS, sidan 50*
- *Sidan Anslutning, sidan 128*
- *Sidan Kameror, sidan 129*
- *Sidan Utgångar, sidan 127*
- *Sidan Ingångar, sidan 128*

12.6.3 Sidan Utgångar

Huvudfönster > **Enheter** > Utvidga  >  > fliken **Utgångar**

Låter dig konfigurera användningen av en Bosch Allegiant-enhetsutgång och tilldela en kodare till en utgång.

Om du vill lagra videodata för en Bosch Allegiant-enhetsutgång i BVMS måste du tilldela en kodare till utgången. Den här kodaren måste anslutas till utgången.

Antal

Visar utgångens nummer.

Allegiant-logiskt nr.

Visar utgångens logiska nummer inom Allegiant.

Logiskt BVMS-nummer

Gör att du kan ändra det logiska numret på utgången inom BVMS. Om du anger ett nummer som redan använts visas ett meddelande.

Namn

Visar utgångens namn.

Användning

Gör att du kan ändra utgångens användning.

Om du väljer **Digitalledningar** så kan du tilldela en kodare till den här utgången i fältet **Kodare**. Allegiant-utgången blir nätverkskompatibel.

Om du väljer **Allegiant-monitor** kan Operator Client-användaren tilldela en bildskärm kamerasygnalen. Om kameran konfigurerats som en PTZ-kamera är PTZ-styrning möjlig. I Operator Client kan inte användaren dra den här kameran på bildrutan.

Om du väljer **Används inte** kan användaren inte tilldela en bildskärm till en Allegiant-kamera.

Kodare

Gör att du kan tilldela en utgång till en kodare. Du kan bara välja en kodare när du har markerat **Digitalledningar**. Kodaren är låst för det logiska trädets. Om du tilldelar en kodare som redan finns i det logiska trädets tas den bort därifrån. I Operator Client kan användaren dra kameran till en bildruta.

Se

– *Konfigurera en Bosch Allegiant-enhet, sidan 127*

12.6.4**Sidan Ingångar**

Huvudfönster > **Enheter** > Utvidga  >  > fliken **Ingångar**

Låter dig lägga till ingångar till en Bosch Allegiant-enhet.

Lägg till ingång

Klicka för att lägga till en ny rad i tabellen för att specificera en ny ingång.

Ta bort ingång

Klicka för att ta bort en rad från tabellen.

Ingång nr.

Ange numret som krävs för ingången. Om du anger ett nummer som redan använts visas ett meddelande.

Ingångsnamn

Ange namnet som krävs för ingången.

Se

– *Konfigurera en Bosch Allegiant-enhet, sidan 127*

12.6.5**Sidan Anslutning**

Huvudfönster > **Enheter** > Utvidga  >  > fliken **Anslutning**

Visar namnet för Bosch Allegiant-konfigurationsfilen.

BVMS kan utläsa en konfigurationsfil i ett strukturerat lagringsformat med namn och konfigurationsinformation för alla kameror som är anslutna till Bosch Allegiant-enheten.

Uppdateringskonfiguration

Klicka för att välja en uppdaterad konfigurationsfil för Bosch Allegiant.

Se

– *Konfigurera en Bosch Allegiant-enhet, sidan 127*

12.6.6

Sidan Kameror

Huvudfönster > **Enheter** > Utvidga  >  > fliken **Kameror**

Visar en kameratabell för de kameror som är anslutna till Bosch Allegiant-enheten.

Antal

Visar kamerans löpande nummer.

Allegiant-logiskt nr.

Visar kamerans logiska nummer.

Kameranamn

Visar kamerans namn.

Se

- *Konfigurera en Bosch Allegiant-enhet, sidan 127*

12.7

Sidan Arbetsstation

Huvudfönster > **Enheter** > Utvidga  > 

En arbetsstation måste ha Operator Client-programvaran installerad.

Gör att du kan konfigurera följande inställningar för en arbetsstation:

- Lägg till ett CCTV-tangentbord som är anslutet till en arbetsstation med Bosch Video Management System.
- Tilldela ett kommandoskript som körs när arbetsstationen startas.
- Välj standardströmmen för livevisning. Du kan välja strömmar för kameror med dubbla strömmar och för multiströmskameror.
- Aktivera brottsutredande sökning.

Obs! Du kan inte konfigurera ett CCTV-tangentbord för en standardarbetsstation. Det är bara möjligt för specifika konfigurerade arbetsstationer.

Lägg till ett Bosch IntuiKey-tangentbord som är anslutet till en kodare genom att utöka 

och sedan klicka på .

Se

- *Lägga till en arbetsstation manuellt, sidan 129*
- *Konfigurera ett startkommandoskript (inställningssidan), sidan 130*

12.7.1

Lägga till en arbetsstation manuellt

Lägga till en BVMS-arbetsstation:

1. Högerklicka på .
2. Klicka på **Lägg till arbetsstation**.
Dialogrutan **Lägg till arbetsstation** visas.
3. Ange det passande värdet.
4. Klicka på **OK**.

Arbetsstationen  läggs till i systemet.

Lägga till en BVMS-standardarbetsstation:

- ▶ Högerklicka på 

Klicka på **Lägg till standardarbetsstation**.

Arbetsstationen  läggs till i systemet.

**Obs!**

Du kan bara lägga till en enda standardarbetsstation.

Om en standardarbetsstation har konfigurerats gäller inställningarna för varje arbetsstation som är ansluten till den här servern och inte har konfigurerats separat.
Om en arbetsstation har konfigurerats gäller inställningarna för den här specifika arbetsstationen och inte inställningarna för standardarbetsstationen.

12.7.2**Konfigurera ett Bosch IntuiKey-tangentbord (sidan Inställningar) (arbetsstation)**

Huvudfönster > **Enheter**> utvidga  > 

Konfigurera ett Bosch IntuiKey-tangentbord som anslutits till en arbetsstation:

1. Klicka på fliken **Inställningar**.
 2. Gör nödvändiga inställningar i fältet **Tangentbordsinställningar**.
- För detaljerad information om olika fält, se onlinehjälpens för lämpligt programfönster.

Se

– *Sidan Arbetsstation, sidan 129*

12.7.3**Aktivera brottsutredande sökningar på arbetsstationen (sidan Inställningar)**

Huvudfönster > **Enheter** > expandera  >  > Sidan **Inställningar**
Du måste aktivera Forensic Search på en arbetsstation.

Obs!

Aktivera videoinnehållsanalys på varje kodare. Använd sidan VCA för kodaren i enhetsträdet.

Aktivera Forensic Search:

- ▶ Klicka för att markera kryssrutan **Aktivera Forensic Search**'.

12.7.4**Konfigurera ett startkommandoskript (inställningssidan)**

Huvudfönster > **Enheter** > Utvidga  >  > sidan **Inställningar**

Du konfigurerar ett kommandoskript som ska startas när Operator Client startas på den valda arbetsstationen.

Du måste skapa ett motsvarande kommandoskript.

För att skapa ett kommandoskript se *Hantera kommandoskript, sidan 85*.

Konfigurera ett startskript:

- ▶ I listan **Startskript:**, välj önskat kommandoskript.

Se

– *Sidan Arbetsstation, sidan 129*

12.7.5

Sidan Inställningar

Huvudfönster > **Enheter** > Utvidga  >  > fliken **Inställningar**

Gör att du kan konfigurera ett skript som utförs när Operator Client i arbetsstationen startas.

Gör att du kan konfigurera TCP eller UDP som det överföringsprotokoll som ska användas för alla kameror som visas i liveläge på arbetsstationen.

Gör att du kan konfigurera vilken ström från en IP-enhet som används för live-visning.

Gör att du kan aktivera brottsutredande sökningar för arbetsstationen.

Du kan också konfigurera tangentbordet som är anslutet till den här arbetsstationen.

Nätverksadress:

Ange DNS-namnet eller IP-adressen för din arbetsstation.

Startskript:

Välj önskat skript som du vill ska startas när arbetsstationens Operator Client startas. Du skapar eller importerar detta skript från sidan **Händelser**.

Standardprotokoll för kamera:

Välj det fabriksinställda överföringsprotokollet som används för alla kameror som är tilldelade det logiska trädets på den här arbetsstationen.

Åsidosätt inspelningsinställningar från sidan Kameror och inspelning

Markera kryssrutan för att aktivera val av önskad ström för livevisning.

Obs! För DVR-enheter som erbjuder mer än en ström (till exempel DIVAR AN 3000/5000) ändras också liveströminställningen här. Liveströminställningar för DVR-enheter inte är tillgängliga på sidan **Kameror och inspelning**.

Live-ström

Välj dataströmmen för livevisning. Du kan välja strömmar för kameror med dubbla strömmar och för multiströmskameror.

När du väljer **Bildrutans storlek har optimerats** justeras upplösningen för varje kamera som visas automatiskt till samma storlek som bildrutan beroende på upplösningen på monitorn som används. Det är praktiskt när du vill visa flera kameror med hög upplösning, exempelvis 4K ultra HD-kameror. Endast kameror med strömmar vars upplösning kan konfigureras oberoende av varandra kan justera upplösningen efter bildrutan. Användaren av Operator Client kan ändra strömvalet för varje kamera enskilt.

Dubbelströmskameror

Välj standardström för livevisning för kameror med dubbla strömmar.

Flerströmskameror

Välj standardström för livevisning för kameror med flera strömmar.

Använd omkodad ström istället, om tillgänglig

Markera kryssrutan om du vill aktivera användningen av en omkodad ström, om den är tillgänglig. Den omkodade strömmen används i stället för den valda strömmen för livevisning. För en omkodad ström som finns i BVMS måste antingen MVS installeras eller också måste datorn VRM innehålla en inbyggd maskinvaruomkodare.

När en kamera visas i liveläget används standardströmmen som har angetts för arbetsstationen. Om kameran inte har ström 2 eller om omkodningstjänsten (SW och HW) inte är tillgänglig används ström 1, även om en annan inställning har gjorts i inställningarna för arbetsstationen.

Aktivera Forensic Search'

Klicka om du vill aktivera brottsutredande sökningar på arbetsstationen.

Använd direktuppspelning från lagring

Markera kryssrutan för att sända videoströmmen direkt från lagringsenheten till den här arbetsstationen. Nu sänds strömmen inte via VRM. Arbetsstationen behöver fortfarande en anslutning till VRM för att säkerställa en korrekt uppspelning.

Obs! Du kan endast använda direktuppspelning från iSCSI-lagringsenheten om du har ställt in det globala iSCSI CHAP-lösenordet.

Hämta livevideo från Video Streaming Gateway i stället för från kameran

Visar listan med Video Streaming Gateway-enheter. Välj önskade poster för att aktivera överföringen av videodata via låga bandbreddssegment mellan videokällan och arbetsstationen.

Obs! Om du väljer en Video Streaming Gateway-enhet för att hämta livevideo blir **Live-video – Profil** på sidan **Kameror och inspelning** inaktuell. Istället används inställningen **Inspelning – Profil** även för livevideo.

Tangentbordstyp:

Välj typen av tangentbord som är anslutet till din arbetsstation.

Port

Välj den COM-port som används för att ansluta tangentbordet.

Överföringshastighet:

Välj maximal hastighet, i bits per sekund (bps), med vilken du vill att data överförs via denna port. Vanligtvis är denna inställd på den maximala hastighet som stöds av datorn eller enheten som du kommunicerar med.

Databitar:

Visar antalet databitar som du vill använda för varje tecken som överförs och mottas.

Stoppbitar:

Visar tiden som går mellan varje tecken som överförs (där tid mäts i bitar).

Paritet:

Visar vilken sorts felkontroll du vill använda för den valda porten.

Porttyp:

Visar anslutningstypen som används för att ansluta Bosch IntuiKey-tangentbordet till arbetsstationen.

Se

- *Konfigurera ett startkommandoskript (inställningssidan), sidan 130*
- *Aktivera brottsutredande sökningar på arbetsstationen (sidan Inställningar), sidan 130*

12.7.6

Ändra nätverksadressen för en arbetsstation

Huvudfönster > **Enheter** > Utvidga 

Ändra IP-adressen:

1. Högerklicka på  och klicka på **Byt nätverksadress**. Dialogrutan **Byt nätverksadress** visas.
2. Ändra värdet i fältet efter önskemål.

12.8 Sidan Avkodare

Huvudfönster > **Enheter** > utvidga  > 
Här kan du lägga till och konfigurera avkodare.



Obs!

BVMS Viewer stöder inte avkodarenheter.



Obs!

Om avkodare ska användas i systemet måste samma lösenord för behörighetsnivån user användas för alla kodare.

Se

- *Söka efter enheter, sidan 70*
- *Sidan Bosch-kodare/-avkodare/-kamera, sidan 204*

12.8.1 Lägga till en kodare/avkodare manuellt

Huvudfönster > **Enheter** > Utvidga  > Utvidga  > Högerklicka  > Klicka på **Lägg till kodare** > dialogrutan **Lägg till kodare**
eller

Huvudfönster > **Enheter** > Högerklicka  > Klicka på **Lägg till kodare** > dialogrutan **Lägg till kodare**
eller

Huvudfönster > **Enheter** > Högerklicka  > Klicka på **Lägg till kodare** > dialogrutan **Lägg till kodare**
eller

Huvudfönster > **Enheter** > Utvidga  > Högerklicka på  > Klicka på **Lägg till avkodare** > dialogrutan **Lägg till kodare**

Här kan du lägga till en kodare eller avkodare manuellt. Detta är särskilt användbart när du vill lägga till en Video IP-enhet från Bosch (endast för VRM).

Obs!

För att du ska kunna lägga till en Video IP-kodare eller -avkodare från Bosch med alternativet **<Uptäck automatiskt>** måste enheten finnas i nätverket.

Så här lägger du till en Video IP-enhet från Bosch:

1. Utvidga , utvidga , högerklicka på ,
eller

högerklicka på ,
eller

högerklicka på .

2. Klicka på **Lägg till kodare**.
Dialogrutan **Lägg till kodare** visas.
3. Ange IP-adressen.
4. Välj **<Upptäck automatiskt>** i listan.
5. Klicka på **OK**.
Enheten läggs till i systemet.

-ikonen anger ett fel som du måste åtgärda. Mer information om det specifika felet finns i knappbeskrivningen.

Dialogrutan **Lägg till kodare**

IP-adress:

Ange en giltig IP-adress.

Kodartyp:/Avkodartyp:

För en enhet med känd enhetstyp väljer du lämplig post. Enheten behöver inte vara tillgänglig i nätverket.

Om du vill lägga till en Video IP-enhet från Bosch väljer du **<Upptäck automatiskt>**. Enheten måste vara tillgänglig i nätverket.

Om du vill lägga till en kamera för offlinekonfiguration väljer du **<Enkel platshållarkamera>**.

12.8.2

Dialogruta för redigering av kodare/avkodare

Huvudfönster > **Enheter** > utvidga  > utvidga  > utvidga  > högerklicka på

 > klicka på **Redigera kodare** > dialogrutan **Redigera kodare**
eller

Huvudfönster > **Enheter** > Utvidga  > Högerklicka på  > Klicka på **Redigera kodare** > Dialogrutan **Redigera kodare**
eller

Huvudfönster > **Enheter** > Utvidga  > Högerklicka på  > Klicka på **Redigera kodare** > Dialogrutan **Redigera kodare**
eller

Huvudfönster > **Enheter** > Utvidga  > Utvidga  > Högerklicka  > Klicka på **Redigera avkodare** > dialogrutan **Redigera avkodare**

Gör att du kan kontrollera och uppdatera en enhets funktioner. När du öppnar dialogrutan ansluts enheten. Lösenordet kontrolleras och enhetens enhetsfunktioner jämförs med de enhetsfunktioner som finns sparade i BVMS.

Namn

Visar enhetens namn. När du lägger till en Video IP-enhet från Bosch genereras ett enhetsnamn. Ändra posten om det behövs.

Nätverksadress/port

Ange enhetens nätverksadress. Ändra portnumret om det behövs.

Användarnamn

Visar det användarnamn som används för verifiering på enheten.

Lösenord

Ange lösenordet för autentisering på enheten.

Visa lösenord

Klicka här om du vill att det angivna lösenordet ska visas. Var försiktig så att ingen obehörig kan se lösenordet.

Autentisera

Verifiera dig på enheten med de uppgifter som angavs ovan.

Säkerhet

Kryssrutan **Säker anslutning** är markerad som standard.

Om det inte går att ansluta via en säker anslutning, visas ett meddelande. Klicka för att ta bort markeringen.

Följande avkodare har stöd för säker anslutning:

- VJD 7000
- VJD 8000
- VIP XD HD

**Obs!**

Anslutningen mellan en avkodare och en kodare är bara säker om båda har konfigurerats med säker anslutning.

Videoström

UDP: Aktiverar krypterad multicast-strömning för avkodarenheter som stöds.

TCP: Aktiverar krypterad unicast-strömning för avkodarenheter som stöds.

Ons! Om ingen multicast-adress har konfigurerats för en kodare hämtar avkodaren strömmen via unicast.

**Obs!**

BVMS stöder inte Bosch kameror anslutna till en VSG.

BVMS stöder endast UDP-kryptering för plattformar äldre än CPP13.

Enhetsfunktioner

Du kan sortera visningen av enhetsfunktionerna i bokstavsordning eller efter kategori. Ett meddelande anger om de upptäckta enhetsfunktionerna stämmer med de aktuella enhetsfunktionerna.

Klicka på **OK** om du vill använda de ändrade enhetsfunktionerna efter det att enheten har uppdaterats.

Se

- *Kryptering av live-video (Redigera kodare), sidan 206*
- *Uppdatera enhetsfunktioner (Redigera kodare), sidan 207*

12.8.3**Ändra lösenordet för en kodare/avkodare (Byt lösenord/Ange lösenord)**

Huvudfönster > **Enheter** > utvidga  > utvidga  >  > 

Huvudfönster > **Enheter** >  > 

Huvudfönster > **Enheter** >  > 

Huvudfönster > **Enheter** > Utvidga  > Utvidga  > 

Definiera och ändra ett separat lösenord för varje nivå. Ange lösenordet (högst 19 tecken och inga specialtecken) för den valda nivån.

Så här ändrar du lösenord:

1. Högerklicka på  och klicka på **Byt lösenord....**
Dialogrutan **Ange lösenord** visas.
 2. Välj användaren du vill ändra lösenordet för i listan **Ange användarnamn.**
 3. Skriv det nya lösenordet i fältet **Ange lösenord för användare.**
 4. Klicka på **OK.**
- ✓ Lösenordet ändras på enheten direkt.

Ett lösenord förhindrar obehörig åtkomst till enheten. Du kan använda olika behörighetsnivåer för att begränsa åtkomsten.

Korrekt lösenordsskydd kan endast garanteras när även alla behörigheter på högre nivå är skyddade av lösenord. När du ska tilldela lösenord måste du därför alltid börja på den högsta behörighetsnivån.

Du kan ange och ändra ett lösenord för varje behörighetsnivå när du har loggat in på användarkontot service.

Enheten har tre behörighetsnivåer: service, user och live.

- service är högsta behörighetsnivån. När du har angett korrekt lösenord har du tillgång till alla funktioner och kan ändra alla konfigurationsinställningar.
- user är mellanbehörighetsnivån. På den här nivån kan du till exempel manövrera enheten, spela upp inspelningar och styra kameran men du kan inte ändra configurationen.
- live är lägsta behörighetsnivån. På den här nivån kan du endast visa videobilder och växla mellan olika live-bildskärmar.

För en avkodare ersätter följande behörighetsnivå behörighetsnivån live:

- destination password (endast tillgänglig för avkodare)
Används för åtkomst till en kodare.

Se

- *Ange mållösenord för en avkodare (Autentisera ...), sidan 200*

12.8.4

Avkodarprofil

Låter dig välja olika alternativ för visning av videobilder på en VGA-monitor.

Bildskärmsnamn

Ange namnet på monitorn. Monitornamnet underlättar identifieringen av fjärrmonitorplatsen. Ange ett namn som gör det så lätt som möjligt att snabbt identifiera platsen.

Klicka på  för att uppdatera namnet i enhetsträdet.

Standard

Välj videoutgångssignal för den monitor som du använder. Det finns åtta förkonfigurerade inställningar för VGA-monitörer tillgängliga, förutom PAL- och NTSC-alternativen för analoga videomonitörer.



Obs!

Valet av en VGA-inställning med värden som ligger utanför den tekniska specifikationen för monitorn, kan resultera i allvarliga skador på monitorn. Se den tekniska dokumentationen för monitorn som du använder.

Fönsterlayout

Välj standardbildlayouten för monitorn.

VGA-skärmstorlek

Ange skärmens bildförhållanden (exempelvis 4 x 3) eller skärmens fysiska storlek i millimeter. Enheten använder de här uppgifterna till att bättre kunna skala videobilden för distorsionsfri visning.

12.8.5**Monitorvisning**

Enheten känner igen överföringsavbrott och visar en varning på monitorn.

Visa överföringsstörning

Välj **På** om du vill visa en varning i händelse av överföringsavbrott.

Störningskänslighet

Flytta skjutreglaget för att justera nivån på det avbrott som utlöser varningen.

Aviseringstext för störning

Skriv textmeddelandet som monitorn ska visa om anslutningen bryts. Texten får inte vara längre än 31 tecken.

12.8.6**Konfigurera ett Bosch IntuiKey-tangentbord (avkodare)**

Huvudfönster > **Enheter** > Utvidga  > 

**Obs!**

Det går inte att ansluta ett KBD-Universal XF-tangentbord till en avkodare.

Konfigurera ett Bosch IntuiKey-tangentbord som anslutits till en avkodare:

1. Klicka på en cell i kolumnen **Anslutning** och välj en lämplig avkodare.
Du kan även välja en arbetsstation om Bosch IntuiKey-tangentbordet är anslutet till den.



En arbetsstation måste ha konfigurerats på sidan

2. Gör nödvändiga inställningar i fältet **Anslutningsinställningar**.
För detaljerad information om olika fält, se onlinehjälpen för lämpligt programfönster.

Se

- *Sidan Tilldela tangentbord, sidan 147*
- *Scenarion för Bosch IntuiKey-tangentbordsanslutningar, sidan 50*
- *Ansluta ett Bosch IntuiKey-tangentbord till en avkodare, sidan 52*

12.8.7**Konfigurera en avkodare för användning med ett Bosch IntuiKey-tangentbord**

Huvudfönster > **Enheter** > Utvidga  > Utvidga 

Med följande steg konfigurerar du en VIP XD-avkodare som är ansluten till ett Bosch IntuiKey-tangentbord.

Konfigurera en avkodare:

1. Klicka på lämplig avkodare som används för anslutning till ett Bosch IntuiKey-tangentbord.
2. Klicka på fliken **Kringutrustning**.
3. Kontrollera att följande inställningar används:

- Funktion hos seriell port: **Genomskinlig**
- Överföringshastighet (baud): **19200**
- Stoppbitar: **1**
- Paritetskontroll: **Ingen**
- Gränssnittsläge: **RS232**
- Halvduplexläge: **Av**

Se

- *Scenarion för Bosch IntuiKey-tangentbordsanslutningar, sidan 50*
- *Ansluta ett Bosch IntuiKey-tangentbord till en avkodare, sidan 52*
- *Uppdatera Bosch IntuiKey-tangentbordets inbyggda programvara, sidan 53*

12.8.8**Ta bort avkodarlogo**

Klicka för att ta bort den logotyp som konfigurerats på avkodarens webbplats.

12.9**Sidan Monitorgrupper**

Huvudfönster > **Enheter** > Utvidga  > 

Gör att du kan lägga till och konfigurera monitorgrupper. En analog monitorgrupp tilldelar du

en BVMS arbetsstation i .

**Obs!**

Du kan inte styra en analog monitorgrupp från Operator Client om anslutningen till Management Server bryts.

Se

- *Lägga till en monitorgrupp manuellt, sidan 138*
- *Konfigurera en monitorgrupp, sidan 139*
- *Konfigurera fördefinierade positioner och extra kommandon, sidan 279*
- *Konfigurera ett larm, sidan 301*
- *Larmalternativ-dialogrutan, sidan 292*
- *Dialogrutan Välj bildruteinnehåll (MG), sidan 291*

12.9.1**Lägga till en monitorgrupp manuellt**

Huvudfönster > **Enheter** > utvidga  > högerklicka på  > klicka på **Lägg till en monitorgrupp**

1. Klicka på **Lägg till en monitorgrupp**.
Dialogrutan **Lägg till en monitorgrupp** visas. Ange namnet på din nya monitorgrupp.
2. Klicka på OK
Monitorgruppen läggs till i ditt system.
3. Klicka på **Kartor och struktur**.
4. Dra monitorgruppen till det logiska träd.

12.9.2 Konfigurera en monitorgrupp

Huvudfönster > **Enheter** > utvidga  >  > 



Obs!

Du kan inte styra en analog monitorgrupp från Operator Client om anslutningen till Management Server bryts.

Monitorerna i en monitorgrupp konfigureras logiskt i rader och kolumner. Denna ordning behöver inte motsvara hur monitorerna är arrangerade rent fysiskt.

Så här konfigurerar du en monitorgrupp:

1. Dra lämpliga monitorer från fliken **Ikke tildelade monitorer** till monitorgruppfället.
2. På fliken **Layout** väljer du lämplig layout.
3. Dra valfri tillgänglig kamera från fliken **Kameror** till en monitorruta till vänster. Kamerans logiska nummer visas som en siffra i svart på monitorrutan och färgen på denna ruta ändras.
4. Ändra vid behov de logiska numren för bildrutorna. Om du anger ett nummer som redan använts visas en meddelanderuta.
5. På fliken **Alternativ** kan du välja om kamerans namn och nummer ska visas på monitorrutan. Du kan även välja var denna information ska placeras.

Monitorbild

Den svarta, fetstilta siffran, om sådan finns, visar det logiska numret för den initiala kameran.

Den svarta smala siffran visar det logiska numret för monitorn.

För att upphäva tilldelningen av en kamera högerklickar du på monitorrutan och klickar sedan på **Rensa rutan** eller drar kameran utanför bildrutan.

Se

- *Lägga till en monitorgrupp manuellt, sidan 138*

12.10 Sidan Kommunikationsenheter

Huvudfönster > **Enheter** > Utvidga  > 

Gör att du kan lägga till eller konfigurera en kommunikationsenhet.

Du kan konfigurera följande kommunikationsenhet:

- E-post

Se

- *Konfigurera en kommunikationsenhet, sidan 140*

12.10.1 Lägga till en E-post-/SMTP-server

Lägga till en kommunikationsenhet:

1. Utvidga , högerklicka på  och klicka på **Lägg till e-post-/SMTP-enhet**. Dialogrutan för **Lägg till e-post-/SMTP-enhet** visas.
2. Ange lämpliga inställningar.
3. Klicka på **OK**.
Kommunikationsenheten läggs till i systemet.

Dialogrutan Lägga till e-post-/SMTP-enhet

Namn:

Ange displaynamnet för e-postservern.

12.10.2

Sidan SMTP-server

Huvudfönster > **Enheter** > Utvidga  > Utvidga  > 

Gör att du kan konfigurera e-postinställningarna i systemet. På sidan **Händelser** kan du tilldela en händelse till ett e-postmeddelande. När denna händelse inträffar skickar systemet ett e-postmeddelande. Du kan inte ta emot e-postmeddelanden i BVMS.

SMTP-servernamn

Ange namnet på e-postservern. Informationen för uppgiften som krävs får du från din operatör. Vanligen är det IP-adressen eller DNS-namnet på din e-postserver.

Sändaradress

Skriv e-postadressen som används som avsändaradress när systemet skickar ett e-postmeddelande, exempelvis vid larm.

SSL/TLS

Markera kryssrutan för att aktivera användningen av en säker SSL/TLS-anslutning. I det här fallet växlar nätverksporten automatiskt till 587.

Port

Ange nödvändigt nätverksportnummer för utgående e-post. Informationen för uppgiften som krävs får du från din operatör.

Port 25 väljs automatiskt när du inaktiverar inställningen **SSL/TLS**.

Du kan välja en annan port, om det behövs.

Anslutningstidsgräns [s]

Ange antalet sekunder av inaktivitet som får gå innan anslutningen avbryts.

Behörighetskontroll

Markera en kryssruta för den verifieringsmetod som krävs. Informationen för uppgiften som krävs får du från din operatör.

Användarnamn

Ange användarnamnet för verifiering hos e-postservern. Informationen för uppgiften som krävs får du från din operatör.

Lösenord

Ange lösenordet för verifiering hos e-postservern. Informationen för uppgiften som krävs får du från din operatör.

Skicka testmeddelande

Klicka för att visa dialogrutan **Skicka testmeddelande**.

Se

– Konfigurera en kommunikationsenhet, sidan 140

12.10.3

Konfigurera en kommunikationsenhet

Huvudfönster > **Enheter** > Utvidga  > Utvidga 

Konfigurera en kommunikationsenhet:

1. Klicka på .
2. Gör lämpliga inställningar.

För detaljerad information om olika fält, se onlinehjälpn för lämpligt programfönster.

Se

- *Lägga till en E-post-/SMTP-server, sidan 139*
- *Sidan SMTP-server, sidan 140*

12.10.4

Skicka testmeddelande-dialogrutan

Huvudfönster > **Enheter** > Utvidga  > Utvidga  >  > Knappen **Skicka testmeddelande**

Gör att du kan skicka ett test-e-postmeddelande.

Från:

Ange avsändarens e-postadress.

Till

Ange mottagarens e-postadress.

Ämne

Ange e-postmeddelandets ämne.

Meddelande

Skriv meddelandet.

Skicka testmeddelande

Klicka för att skicka e-postmeddelande.

Se

- *Konfigurera en kommunikationsenhet, sidan 140*

12.11

Bankomat/kassasida

Huvudfönster > **Enheter** > Utvidga  > 

Gör att du kan lägga till och konfigurera kringutrustningsenheter, till exempel en Bosch ATM/POS-brygga.

Om du vill lägga till flera bryggor till en server måste du använda olika portar.

Se

- *Lägga till en Bosch ATM/POS-brygga, sidan 93*
- *Konfigurera kringutrustning, sidan 142*

12.11.1

Lägga till en Bosch ATM/POS-brygga manuellt

Huvudfönster > **Enheter** > Utvidga  > Högerklicka på  > **Lägg till Bosch ATM/POS-brygga.**

Gör att du kan lägga till en Bosch ATM/POS-brygga.

Lägga till kringutrustning:

1. Utvidga , högerklicka på  och klicka på **Lägg till Bosch ATM/POS-brygga**. Dialogrutan för **Lägg till Bosch ATM/POS-brygga** visas.
2. Ange lämpliga inställningar.
3. Klicka på **OK**.
Kringutrustningsenheten läggs till i systemet.

Dialogrutan Lägga till Bosch ATM/POS-brygga**Namn:**

Ange ett lämpligt namn för enheten.

IP-adress:

Ange enhetens IP-adress.

Port 1

Ange portnumret som används som avlyssningsport på ATM/POS-bryggan.

Port 2

Ange portnumret som används som avlyssningsport på BVMS Management Server.

**Obs!**

När du lägger till flera ATM/POS-bryggor i systemet ska du se till att numren på port 2 på enheterna inte är samma. Samma nummer på port 2 flera gånger kan leda till dataförluster på ATM/POS.

Se

- *Lägga till en Bosch ATM/POS-brygga, sidan 93*

12.11.2**Sidan Bosch ATM/POS-brygga**

Huvudfönster >  **Enheter** > Utvidga  > Utvidga  >  > fliken **Bosch ATM/POS-brygga**

Låter dig konfigurera en Bosch ATM/Pos Bridge.

IP-adress:

Ange enhetens IP-adress.

Port 1

Ange portnumret som används som avlyssningsport på ATM/POS-bryggan.

Port 2

Ange portnumret som används som avlyssningsport på BVMS Management Server.

**Obs!**

När du lägger till flera ATM/POS-bryggor i systemet ska du se till att numren på port 2 på enheterna inte är samma. Samma nummer på port 2 flera gånger kan leda till dataförluster på ATM/POS.

Se

- *Konfigurera kringutrustning, sidan 142*
- *Lägga till en Bosch ATM/POS-brygga, sidan 93*

12.11.3**Konfigurera kringutrustning**

Huvudfönster >  **Enheter** > Utvidga  > Utvidga  >  **Bosch ATM/POS-brygga**
eller

Huvudfönster >  **Enheter** > Utvidga  > Utvidga  >  **DTP-enhet** > 

Konfigurera kringutrustning:

- ▶ Ändra nödvändiga inställningar.

För detaljerad information om olika fält, följ länken till lämpligt programfönster.

Se

- Sidan ATM-inställningar, sidan 143
- Sidan Bosch ATM/POS-brygga, sidan 142
- Sidan DTP-inställningar, sidan 143

12.11.4

Sidan DTP-inställningar

Huvudfönster >  **Enheter** > Utvidga  > Utvidga  > 

Gör att du kan konfigurera en DTP-enhet med upp till 4 uttagsautomater anslutna till DTP-enheten.

Serieport

Välj lämplig port från listan.

Se

- Sidan ATM-inställningar, sidan 143
- Konfigurera kringutrustning, sidan 142

12.11.5

Sidan ATM-inställningar

Huvudfönster >  **Enheter** > Utvidga  > Utvidga  >  > 

Gör att du kan konfigurera en uttagsautomat som är ansluten till en DTP-enhet.

Ingångsnummer för DTP-enheten

Välj önskat ingångsnummer. Om numret redan används av en annan uttagsautomat kan du byta ingångsnummer.

Tidsgräns för anslutning [timmar]

Ange önskat antal timmar. När uttagsautomaten inte har skickat några transaktionsdata under den här tidsperioden antar BVMS att anslutningen har brutits. En motsvarande händelse utlöses. Händelsen **Ej behörig** är tillgänglig för en uttagsautomat men är inte relevant. Inställningen **0** innebär att ingen anslutningskontroll utförs.

Dataingångar

Klicka här för att aktivera önskade ingångar och ge ingångarna namn.

Se

- Konfigurera kringutrustning, sidan 142

12.11.6

Sidan Ingångar

Huvudfönster >  **Enheter** > Utvidga  > Utvidga  >  > Fliken **Ingångar**

Gör att du kan konfigurera ingångarna för en Bosch ATM/Pos Bridge.

Se

- Konfigurera kringutrustning, sidan 142
- Lägga till en Bosch ATM/POS-brygga, sidan 93

12.12**Nyckelkortsläsare**

Huvudfönster > **Enheter** > Utvidga  >  > Fliken **Globala inställningar för nyckelkortsläsare**

Du kan konfigurera inställningarna som är giltiga för alla nyckelkortsläsare i systemet.

Serieport

Välj den serieport som nyckelkortsläsaren ska ansluta till.

Utelåst

Gör att du kan lägga till bankroutingkoder för spärrning. Detta innebär att kort med de låsegenskaper som anges här inte har tillträdesbehörighet. Tillträde nekas av nyckelkortsläsaren. Nyckelkortsläsarens standardläge för elektrisk dörrupplåsning måste vara inställt på: **Automatiskt**

Listan kan innehålla poster med jokertecken:

?: Anger valfritt eller inget tecken.

*: Anger en följd (ett eller flera tecken) av valfria eller inga tecken (undantag: * ensamt innebär att alla banksorteringskoder är spärrade).

Ignorera landskod på EC-kort

Klicka här om du vill att BVMS inte ska analysera kortdata som används för att identifiera i vilket land som kortet har utfärdats. Tillträde är möjligt med kort som har annan landskod.

12.12.1**Dialogrutan Lägg till nyckelkortsläsare**

Huvudfönster > **Enheter** > Utvidga  > Högerklicka på  > Kommandot **Lägg till nyckelkortsläsare**

Du kan lägga till en nyckelkortsläsare.

Namn

Skriv in ett namn för enheten.

Enhetsidentifierare

Välj ett unikt nummer för enheten. Om inga nummer finns tillgängliga har maximalt antal nyckelkortsläsare redan lagts till i systemet.

12.12.2**Inställningar för sidan för nyckelkortsläsare**

Huvudfönster > **Enheter** > Utvidga  >  >  > Fliken **Inställningar för nyckelkortsläsare**

Du kan konfigurera en nyckelkortsläsare.

Enhetsidentifierare

Visar enhetens unika nummer.

Aktivera skimmingsskydd

Klicka här om du vill att BVMS ska utlösa en händelse när en inkopplad skimmingsenhet upptäcker ett skimmingsförsök. Detta stöds inte av alla typer av nyckelkortsläsare.

Standardläge för öppning av elektriskt dörrlås

Öppna: Dörren är öppen och alla kan få tillträde utan kort.

Stängd: Dörren är stängd oavsett vilket kort som sätts i.

Automatiskt: Dörren öppnas när ett kort med tillträdesbehörighet sätts i läsaren.

Aktivera schemabaserad styrning

Klicka här om du vill kunna tilldela dörrlåsets valda upplåsningsläge ett schema.

När ett schema blir aktivt växlar BVMS nyckelkortsläsaren till motsvarande upplåsningsläge.

Om valda scheman överlappar varandra har upplåsningslägena följande prioritetsordning: 1.

Öppna 2. Stängd 3. Automatiskt

12.13

Sidan Virtuella ingångar

Huvudfönster > **Enheter** > utvidga  > 

Visar de virtuella ingångarna som är konfigurerade i systemet.

Gör att du kan lägga till nya virtuella ingångar samt ta bort befintliga sådana ingångar.

Lägg till ingångar

Klicka för att visa en dialogruta där du lägger till nya virtuella ingångar.

Ta bort ingångar

Klicka för att ta bort en vald virtuell ingång.

Antal

Visar den virtuella ingångens nummer.

Namn

Klicka på en cell för att modifiera namnet på den virtuella ingången.

12.13.1

Lägga till virtuella ingångar manuellt

Huvudfönster > **Enheter** > Utvidga  > Knappen **Lägg till ingångar**

Gör att du kan lägga till nya virtuella ingångar.

Så här lägger du till en virtuell ingång:

1. Utvidga  och klicka på .
Motsvarande sida visas.
2. Klicka på **Lägg till ingångar**.
En ny rad läggs till i tabellen.
3. Gör lämpliga inställningar.
4. Klicka på **Lägg till**.
Den virtuella ingången läggs till i systemet.

Dialogrutan Lägg till ingångar

Start

Välj det första numret för de nya virtuella ingångarna.

Slut

Välj det sista numret för de nya virtuella ingångarna.

Namn:

Skriv in namnet för varje ny virtuell ingång. Ett löpande nummer läggs till.

Lägg till

Klicka här för att lägga till nya virtuella ingångar.

12.14

Sidan RMon och Snmp

Huvudfönster > **Enheter** > Utvidga  > 

Gör att du kan lägga till eller konfigurera SNMP-mätvärden så att du kan underhålla nätverkskvaliteten.

Se

- Konfigurera mottagare för SNMP-fälla (sidan Mottagare för SNMP-fälla), sidan 146

12.14.1**Lägga till en SNMP manuellt**

Huvudfönster > **Enheter** > Utvidga  > Högerklicka på  > Kommandot **Lägg till SNMP**
Gör att du kan lägga till ett nätverksövervakningssystem till BVMS.

Lägga till en nätverksövervakningsenhet:

1. Utvidga , högerklicka på  och klicka på **Lägg till SNMP**.
Dialogrutan för **Lägg till SNMP** visas.
2. Skriv ett namn för SNMP-enheten.
Nätverksövervakningsenheten läggs till i systemet.

Dialogrutan Lägg till SNMP**Namn:**

Skriv in ett namn på nätverksövervakningsenheten.

Se

- Konfigurera mottagare för SNMP-fälla (sidan Mottagare för SNMP-fälla), sidan 146

12.14.2**Konfigurera mottagare för SNMP-fälla (sidan Mottagare för SNMP-fälla)**

Huvudfönster > **Enheter** > Utvidga 

Konfigurera SNMP trap receiver:

1. Klicka på  för att visa sidan **Mottagare för SNMP-fälla**.
2. Gör de nödvändiga inställningarna.

För detaljerad information om olika fält, se onlinehjälpens för lämpligt programfönster.

Sidan Mottagare för SNMP-fälla.

Huvudfönster > **Enheter** > Utvidga  > Utvidga 

Gör att du kan välja enheter för övervakning samt välja SNMP-fälla-OID:er som utlöser en händelse för den valda enheten när de tas emot.

**Obs!**

Du måste ange IP-adressen för Bosch Video Management System Management Server som mottagare för fälla i enheterna som du vill övervaka.

Sändenheter för SNMP-fällor

Gör att du kan ange ett intervall av IP-adresser för de övervakade nätverksenheterna. Om du bara vill övervaka en enhet anger du motsvarande IP-adress i cellen **Intervall från**.

Var försiktig när du ändrar de här adresserna. Om du anger fel adress slutar nätverksövervakningen för denna enhet.

Filterregler för SNMP-fällor

Gör att du kan ange OID:er och motsvarande värden. Du kan använda jokertecknen * och ? för att utöka filterintervallet. Om du anger OID:er och värden i fler än en rad måste dessa filterregler överensstämma om en händelse ska utlösas. I båda kolumnerna kan du ange ett reguljärt uttryck i {}. Om det finns tecken utanför klammarna utvärderas inte det reguljära uttrycket.

Visa verktyget för loggning av fällor

Klicka för att visa dialogrutan **Loggare av SNMP-fällor** där du kan spåra OID:er för SNMP-fällor.

12.14.3

Loggare av SNMP-fällor-dialogrutan

Huvudfönster > **Enheter** > Utvidga  > Utvidga  > Välj en generisk mottagare för SNMP-fälla > Klicka på **Visa verktyget för loggning av fällor**

Gör att du kan spåra OID:er för SNMP-fälla. Du kan ta emot fällor från alla enheter i nätverket eller endast från utvalda enheter. Du kan filtrera fällorna som ska tas emot och du kan lägga till OID:er och värden för valda fällor i tabellen **Filterregler för SNMP-fällor**.

Start/paus

Klicka om du vill starta eller stoppa en spårningsprocess.

Endast fällor från sändare

Skriv in IP-adressen eller DNS-namnet för en enhet. Endast fällor från denna enhet spåras.

Endast fällor som innehåller

Skriv in en sträng som en fälla kan innehålla. Du kan använda * och ? som jokertecken. Strängar inom {} behandlas som reguljära uttryck. Endast fällor som innehåller en sådan sträng spåras.

Mottagna fällor

Visar de fällor som har tagits emot med en spårningsprocess.



Klicka om du vill ta bort alla poster i fältet **Mottagna fällor**.

Detaljer om fällor

Visar detaljerna om fällan. Du kan kopiera OID och värdet till tabellen **Filterregler för SNMP-fällor**.

Se

– *Konfigurera mottagare för SNMP-fälla (sidan Mottagare för SNMP-fälla), sidan 146*

12.15

Sidan Tilldela tangentbord

Huvudfönster > **Enheter** > utvidga  > 

Här kan du lägga till ett KBD-Universal XF-tangentbord (som är anslutet till en BVMS-arbetsstation) eller ett Bosch IntuiKey-tangentbord (som är anslutet till en BVMS-arbetsstation eller till en avkodare).

Så här lägger du till ett CCTV-tangentbord:

OBS! För att du ska kunna lägga till ett tangentbord måste det finnas en arbetsstation tillagd.

1. Utvidga  och klicka på .
Motsvarande sida visas.

2. Klicka på **Lägg till tangentbord**.
En ny rad läggs till i tabellen.
3. I motsvarande fält i kolumnen **Tangentbordstyp** väljer du önskad tangentbordstyp:
IntuiKey-tangentbord
KBD-Universal XF Keyboard
4. I motsvarande fält i kolumnen **Anslutning** väljer du den arbetsstation som är ansluten till tangentbordet.
5. Gör de önskade inställningarna.
Tangentbordet läggs till i systemet.

Lägg till tangentbord

Klicka för att lägga till en rad i tabellen för konfiguration av tangentbordet.

Ta bort tangentbord

Klicka för att ta bort den valda raden.

Tangentbordstyp

Visar vilken typ av tangentbord som är anslutet till din arbetsstation eller avkodare.

Klicka på en cell för att välja önskad tangentbordstyp.

- **IntuiKey**
Välj den här typen om du har anslutit ett IntuiKey-tangentbord från Bosch.
- **KBD-Universal XF Keyboard**
Välj den här typen om du har anslutit ett KBD-Universal XF-tangentbord.

Anslutning

I en cell väljer du den enhet som ditt tangentbord är anslutet till. Om du väljer en

arbetsstation läggs även tangentbordet till på  > sidan .

Port

I en cell väljer du önskad COM-port.

Överföringshastighet

I en cell väljer du maximal hastighet, i bitar per sekund (bps), med vilken du vill att data överförs via denna port. Vanligtvis är detta inställt på den maximala hastighet som stöds av datorn eller enheten som du kommunicerar med.

Databitar

Visar antalet databitar du vill använda för varje tecken som överförs och mottas.

Stoppbitar

Visar tiden som går mellan varje tecken som överförs (där tid mäts i bitar).

Paritet

Visar vilken sorts felkontroll du vill använda för den valda porten.

Porttyp

Visar anslutningstypen som används för att ansluta Bosch IntuiKey-tangentbordet till arbetsstationen.

Se

- *Konfigurera en avkodare för användning med ett Bosch IntuiKey-tangentbord, sidan 137*
- *Konfigurera ett Bosch IntuiKey-tangentbord (sidan Inställningar) (arbetsstation), sidan 130*
- *Konfigurera ett Bosch IntuiKey-tangentbord (avkodare), sidan 137*

12.16 Sidan I/O-moduler

Huvudfönster > **Enheter** > Utvidga



Gör att du kan lägga till eller konfigurera en I/O-modul.

För tillfället kan endast ADAM-enheter hanteras.

Se

– *Konfigurera en I/O-modul, sidan 149*

12.16.1 Lägga till en I/O-modul manuellt

Lägga till en I/O-modul:



1. Utöka , högerklicka på och klicka på **Lägg till ny ADAM-enhet**. Dialogrutan **Lägg till ADAM** visas.
2. Ange enhetens IP-adress.
3. Välj enhetstyp.
Motsvarande sida visas.
4. Klicka på fliken **ADAM** för att vid behov ändra displaynamnen ingångar.
5. Klicka på fliken **Namn** för att ändra displaynamnen för reläerna om det behövs.



Obs!

Du kan också genomföra skanning efter ADAM-enheter (**Sök efter ADAM-enheter**). Enheternas IP-adresser upptäcks. Om den är tillgänglig förväljs enhetstypen. Du måste bekräfta valet.

12.16.2 Konfigurera en I/O-modul

Huvudfönster > **Enheter**> expandera



> expandera



Konfigurera en I/O-modul:



Obs!

Undvik att ändra enhetstyp.

Om du minskar antalet ingångar eller reläer raderas alla konfigurationsdata för de borttagna ingångarna eller reläerna.

1. Klicka på fliken **ADAM**.
2. Välj lämplig enhetstyp i listan **ADAM-typ:**.
3. Klicka på fliken **Ingångar**.
4. Ändra visningsnamnet för en ingång i kolumnen **Namn** om det behövs.
5. Klicka på fliken **Reläer**.
6. Ändra namnet på ett relä i kolumnen **Reläer** om det behövs.

Så här ändrar du en IP-adress:

1. Högerklicka på en ADAM-enhet i enhetsträdet.
2. Välj **Byt nätverksadress**.
3. Ange den nya IP-adressen och klicka på **OK**.
4. Aktivera konfigurationen.
- ✓ Den nya IP-adressen används för åtkomst till enheten.

Se

– *Sidan I/O-moduler, sidan 149*

12.16.3

Sidan ADAM

Huvudfönster > **Enheter** > expandera  >  >  > fliken **ADAM**

Visar information om vald ADAM-enhet.

Låter dig ändra displaynamnet för en ADAM-enhet.

ADAM-typ:

Välj lämplig enhetstyp.

Totalt antal ingångar:

Visar det totala antalet ingångar som är tillgängliga för denna enhetstyp.

Totalt antal reläer/utgångar:

Visar det totala antalet reläer som är tillgängliga för denna enhetstyp.

12.16.4

Sidan Ingångar

Huvudfönster > **Enheter** > expandera  >  >  > fliken **Ingångar**

Låter dig ändra displaynamnen för ingångarna för vald ADAM-enhet.

Antal

Visar ingångens logiska nummer.

Namn

Klicka på en cell för att ändra ingångens visningsnamn.

12.16.5

Sidan Reläer

Huvudfönster > **Enheter** > expandera  >  >  > fliken **Reläer**

Låter dig ändra displaynamnen för reläerna för vald ADAM-enhet.

Antal

Klick på en cell för att ändra det logiska numret för ett relä.

Namn

Ange reläets visningsnamn.

12.17

Sidan Allegiant-CCL-emulering

Huvudfönster > **Enheter** > Utvidga  > 

Gör att du kan aktivera emuleringen av Allegiant CCL.

Allegiant CCL-kommandon som stöds i BVMS, sidan 59 visar en lista över CCL-kommandon som stöds i Bosch Video Management System.

Obs!

Konfigurera inte Allegiant CCL-emuleringen och en Allegiant-enhet till samma COM-port. Om samma COM-port konfigureras för båda enheterna prioriteras Allegiant-enheten. Åtkomsten för Allegiant CCL-emuleringsenheten misslyckas och ett felmeddelande genereras.

För att lösa problemet måste antingen hanteringsservern ha två olika COM-portar eller Allegiant-enheten anslutas till en annan dator.

Aktivera Allegiant-CCL-emulering.

Markera kryssrutan för att aktivera emuleringen.

Överföringshastighet (baud)

Välj värdet för överföringshastigheten i bit/s.

Stoppbitar

Välj antalet stoppbitar per tecken.

Paritetskontroll

Välj typ av paritetskontroll.

Handskakning

Välj önskad metod för flödesstyrning.

Modell

Markera den Allegiant-modell som du vill emulera.

Se

– *Konfigurera en Allegiant-CCL-emulering, sidan 151*

12.17.1**Lägga till en Allegiant-CCL-emulering manuellt**

Så här lägger du till en Allegiant-CCL-emulering:

1. Utvidga , klicka på .
Fliken **Allegiant-CCL-emulering** visas.
2. Klicka och markera **Aktivera Allegiant-CCL-emulering**.
3. Gör nödvändiga inställningar.
Emuleringstjänsten Allegiant CCL startas på Management Server.

12.17.2**Allegiant CCL-kommandon**

Du använder CCL-kommandon för att växla IP-kameror eller kodare till IP-avkodare som båda konfigurerats i BVMS. Du kan inte använda CCL-kommandon för att direkt styra analoga kameror eller själva Allegiant-matrisen.

Allegiant CCL-emuleringen startar en intern BVMS-tjänst som översätter CCL-kommandon i matrisväxlaren till BVMS. Du kan konfigurera en COM-port för Management Server så att den lyssnar till CCL-kommandona. CCL-emuleringen gör det enklare att byta ut befintliga Allegiant-enheter mot Bosch Video Management System eller att använda Bosch Video Management System med program som har stöd för Allegiant CCL-kommandona. Gammla Allegiant-maskinvara som har konfigurerats i BVMS kan inte styras med dessa kommandon.

12.17.3**Konfigurera en Allegiant-CCL-emulering**

> **Enheter**> utvidga  > 

Du behöver CCL Användarhandbok för att använda CCL-kommandona. Denna handbok finns tillgänglig i produktkatalogen online i dokumentavsnittet hos varje LTC Allegiant-matris. Avsnittet *Allegiant CCL-kommandon som stöds i BVMS, sidan 59* innehåller en lista över CCL-kommandon som stöds i Bosch Video Management System.

Så här konfigurerar du en Allegiant-CCL-emulering:

1. Klicka på **Aktivera Allegiant-CCL-emulering**.
 2. Konfigurera kommunikationsinställningarna efter behov.
- För detaljerad information om olika fält, se onlinehjälpfen för lämpligt programfönster.

Se

– *Sidan Allegiant-CCL-emulering, sidan 150*

12.18 Sidan Mobil videotjänst



Huvudfönster > **Enheter** >

Gör att du kan lägga till en eller flera kodkonverteringstjänster i BVMS. Den här kodkonverteringstjänsten anpassar videoströmmen från en kamera konfigurerad i BVMS till den tillgängliga nätverksbandbredden. Gör att mobila videoklienter som iPhone, iPad eller webbklienter kan ta emot direktsända eller uppspelade videodata via opålitliga nätverksanslutningar med begränsad bandbredd.

Se

- *Lägga till en Mobile Video Service (mobil videotjänst) manuellt, sidan 152*

12.18.1

Mobila videotjänster

Mobile Video Service kodkonverterar videoströmmar från källan till den ursprungliga bandbredden för anslutna klienter. Gränssnitten för Mobile Video Service har utformats för hantering av klienter på flera plattformar, t.ex. mobila enheter (IOS, iPad, iPhone) och en HTML-klient för Windows Internet Explorer.

Mobile Video Service bygger på Microsoft Internet Information Service.

En mobil tjänst kan hantera flera klienter samtidigt.

Begränsningar finns angivna på databladet och den tekniska kommentaren Mobile Video Service som finns tillgänglig i produktkatalogen online för BVMS.

Internet Information Service

Konfigurera inställningarna för Internet Information Service på den dator där du ska installera MVS för BVMS.

Installationskommentarer

Du kan inte lägga till en Mobile Video Service (MVS) i Configuration Client om tiden mellan Configuration Client-datorn och Mobile Video Service-datorn inte är synkroniserad. Kontrollera att tiden är synkroniserad mellan de berörda datorerna.

Installera och konfigurerar Internet Information Service (IIS) innan du installerar Mobile Video Service. Om IIS inte har installerats avbryts BVMS-installationen av Mobile Video Service.

Välj Mobile Video Service-komponenten för installation under BVMS-installationen.

Du kan inte installera VRM och Mobile Video Service på samma dator.

Vi rekommenderar att du inte installerar Mobile Video Service på samma dator där du installerade Management Server.

Med mobilappen kan du göra följande:

- Visa video
 - Fas
 - Uppspelning
- Övervaka nätverk och server

Se

- *Lägga till en Mobile Video Service (mobil videotjänst) manuellt, sidan 152*

12.18.2

Lägga till en Mobile Video Service (mobil videotjänst) manuellt



Huvudfönster > **Enheter** > Högerklicka på > Klicka på **Lägg till mobil videotjänst**

Du kan lägga till en eller flera Mobile Video Service poster i din BVMS.

Så här lägger du till:

1. Ange URI för din Mobile Video Service.

2. Klicka på **OK**.
- ✓ Mobile Video Service och Management Server känner nu igen varandra, och Mobile Video Service kan ta emot konfigurationsdata från Management Server.

Dialogrutan Lägg till mobil videotjänst

URI

Ange URI för din Mobile Video Service. Följ syntaxen i exemplet:

<https://www.MyDomain.org/mvs>

Du måste alltid börja posten med https://, även när du inte konfigurerade någon krypterad åtkomst till webbservern.

12.19

Sidan Inbrottspaneler

Huvudfönster > **Enheter** > Utvidga  > 

Här kan du lägga till och konfigurera inbrottspaneler från Bosch. Enheten måste vara ansluten och tillgänglig.

När du har lagt till en inbrottspanel visas områdena, punkterna, dörrarna och reläerna hierarkiskt i enhetsträdet.

Du kan ta bort eller ändra namn på panelen och varje område, punkt, dörr och relä.

Sök igenom enheten på nytt om konfigurationen av inbrottspanelen ändras för att ändringarna ska visas i BVMS.



Obs!

Alla larmhändelser som kan inträffa i en punkt konfigureras automatiskt som ett BVMS-larm. Exempel: brandlarm



Obs!

Om en dörr inte är tilldelad en punkt i konfigurationen för en inbrottspanel som läggs till i BVMS utlöser ett larm från denna dörr inte en BVMS-händelse och därmed inget BVMS-larm.

12.19.1

Lägga till en inbrottspanel manuellt

Huvudfönster > **Enheter** > Utvidga  > Högerklicka  > kommandot **Lägg till en panel**
Här kan du lägga till en inbrottspanel från Bosch.

Så här lägger du till en inbrottspanel:

1. Utvidga , högerklicka på  och klicka på **Lägg till en panel**.
Dialogrutan för **Lägg till inbrottspanel** visas.
2. Ange passande värden.
3. Klicka på **OK**.
Inbrottspanelen läggs till i systemet.

Dialogrutan Lägg till inbrottspanel

Nätverksadress

Ange enhetens IP-adress.

Nätverksport

Välj portnumret som har konfigurerats i enheten.

Lösenord för automatisering

Ange lösenordet för autentisering på enheten.

12.19.2**Sidan Inställningar**

Huvudfönster > **Enheter** > Utvidga  > Utvidga  >  > fliken **Inställningar**
Här kan du ändra inbrottspanelens anslutningsinställningar.

12.20**Sidan Passersystem**

Huvudfönster > **Enheter** > Utvidga  > 

Gör att du kan lägga till och konfigurera passersystem från Bosch. Enheten måste vara ansluten och tillgänglig. När du har lagt till ett passersystem visas styrenheten, ingångar, läsare och dörrar hierarkiskt i enhetsträdet.

Du kan ta bort eller ändra namn på styrenheten, ingångar, läsare och dörrar på sidan **Kartor och struktur**.

När konfigurationen eller hierarkin för styrenheter, läsare eller dörrar i passersystemet ändras måste du göra en ny avsökning av enheten för att visa ändringarna i BVMS.

HTTPS-certifikat för klient

För att säkra anslutningen mellan passersystemet och BVMS behöver du exportera ett klientcertifikat från passersystemet och importera det till BVMS. Denna process beskrivs i avsnittet **HTTPS-certifikat för klient** i passersystemets dokumentation.

**Obs!**

Om du inte lägger till certifikatet kan systemen inte utbyta information med varandra.

12.20.1**Lägga till ett passersystem**

Huvudfönster > **Enheter** > Utvidga  > 

Så här lägger du till ett passersystem:

1. Högerklicka på .
2. Klicka på **Lägg till åtkomstkontrollsystem**.
Dialogrutan **Lägg till åtkomstkontrollsystem** visas.

Obs! När du lägger till ett passersystem visas konfigurerade dörrar, läsare, ingångar och reläer i enhetsträdet på sidan **Kartor och struktur**.

Dialogrutan Lägg till åtkomstkontrollsystem**Nätverksadress/HTTPS-port**

Ange enhetens nätverksadress. Ändra portnumret om det behövs.

Användarnamn

Visar det användarnamn som används för verifiering på enheten.

Lösenord

Ange lösenordet för autentisering på enheten.

Så här testas du anslutningen:

1. Klicka på Anslut.
BVMS Configuration Client försöker att ansluta till passersystemet och hämta den relevanta informationen.
2. Klicka på OK.
Passersystemet läggs till i systemet utifrån den visade informationen.

12.20.2

Redigera ett passersystem

Huvudfönster > **Enheter** > Utvidga  >  > 

Så här redigerar du ett passersystem:

1. Högerklicka på .
2. Klicka på **Redigera åtkomstkontrollsystem**.
Dialogrutan **Redigera åtkomstkontrollsystem** visas.

12.20.3

Sidan Inställningar

Huvudfönster > **Enheter** > Utvidga  >  >  > Fliken **Inställningar**
Gör att du kan ändra passersystemets anslutningsinställningar.

12.21

Videoanalyssida

Huvudfönster > > **Enheter** > Utvidga  > 

Gör att du kan lägga till videoanalyser, Person Identification-enheter (PID) och LPR-enheter.

12.21.1

Inställningssida för Video Analytics

Huvudfönster > > **Enheter** > expandera  > expandera  >  **Video Analytics** > sidan **Inställningar för Video Analytics**

Du kan lägga till en enhet för serverbaserad videoanalys.

Användaruppgifterna och installationssökvägen till analysvisningsprogrammet som används för videoanalysenheten måste finnas tillgänglig.

Nätverksadress

Ange IP-adressen för videoanalysenheten. DNS-namn är inte tillåtna.

Användarnamn

Ange användarnamnet som konfigurerats i videoanalysenheten.

Lösenord

Ange lösenordet som konfigurerats i den serverbaserade analysenheten.

Sökväg för analysvisare

Ange den relativa sökvägen för installationssökvägen till analysvisningsprogrammet. Sökvägen är relativ till *C:\Program Files (x86)* på datorn där visningsprogrammet används.

Exempel: Analysvisningsprogrammet (*AnalyticsViewer.exe*) är installerat i följande katalog:

C:\Program Files (x86)\VideoAnalytics

Konfigurera följande sökväg i fältet **Sökväg för analysvisare**:

VideoAnalytics\AnalyticsViewer.exe

12.21.2

Lägga till en Video Analytics-enhet

Huvudfönster > > **Enheter** > högerklicka på  > kommando **Lägg till Video Analytics-enhet** > dialogrutan **Lägg till Video Analytics-enhet**

När du lägger till en serverbaserad analysenhet anger du inloggningsuppgifterna för den nya enheten.

Lägga till en serverbaserade analysenhet:

1. Expandera , högerklicka på  och klicka på **Lägg till Video Analytics-enhet**. Dialogrutan **Lägg till Video Analytics-enhet** visas.
2. Ange passande värden.
3. Klicka på **OK**.
Enheten läggs till i systemet.

Dialogrutan Lägg till Video Analytics-enhet

Nätverksadress

Ange IP-adressen för videoanalysenheten. DNS-namn är inte tillåtna.

Användarnamn

Ange användarnamnet som konfigurerats i videoanalysenheten.

Lösenord

Ange lösenordet som konfigurerats i den serverbaserade analysenheten.

12.21.3

Sidan Person Identification-enheter

Huvudfönster > > **Enheter** > Utvidga  > Utvidga  > sidan  Person Identification

Gör att du kan lägga en Person Identification-enhet. Enheten måste vara ansluten och tillgänglig. Du kan lägga till kameror till din Person Identification-enhet och konfigurera Person Identification-händelser och larm.

Persongrupper

Under fliken **Persongrupper** kan du lägga till och konfigurera persongrupper.

Kameror

På fliken **Kameror** kan du lägga till kameror till din Person Identification-enhet. De tillagda kamerorna visas i en lista.

Obs! Lägg först till lämpliga kameror i det logiska trädet.

12.21.4

Lägga till en Person Identification device (PID)



Obs!

I händelse av ett centralserveravbrott måste du återställa BVMS-konfigurationen och certifikatet Bosch VMS CA. Annars kan du inte använda en befintlig PID utan återställning, vilket innebär att alla lagrade personer tas bort. Vi rekommenderar att du skapar en säkerhetskopia av BVMS-konfigurationen och certifikatet Bosch VMS CA.

När du lägger till en Person Identification-enhet måste du se till att certifikatet visas i dialogrutan **Lägg till Person Identification-enhet** som motsvarar det PID som du vill lägga till. Från BVMS 10.1 du kan lägga till flera PID-enheter.

Den första PID-enheten du lägger till är den ledande enheten som är ansluten till BVMS-systemet. Den första PID-enheten upprättar anslutningen till de andra PID-enheterna och persondatabasen lagras på den.

Obs! Innan du kan ta bort den första PID-enheten måste du ta bort alla andra konfigurerade PID-enheter.

Så här lägger du till en Person Identification-enhet:

1. Expandera .
2. Högerklicka på .
3. Klicka på **Lägg till Person Identification-enhet**.
Dialogrutan **Lägg till Person Identification-enhet** visas.
4. Ange passande värden.
5. Klicka på **Visa certifikatet ...** för att kontrollera om certifikatet motsvarar PID.
6. Bekräfta genom att klicka på **OK**.
7. Klicka på **OK**.
Enheten läggs till i systemet.

Lägg till Person Identification-enhet -dialogrutan

Nätverksadress

Ange enhetens IP-adress.

Portnummer

Skriv in enhetens portnummer.

Se

- Återställa åtkomst till ett PID efter ett BVMS-centralserveravbrott, sidan 157
- Så här exporterar du konfigurationsdata:, sidan 90

12.21.5

Sidan PID

Huvudfönster > **Enheter** > Utvidga  > Utvidga  > sidan  Person Identification-enheter >  PID sida

Anslutning

Anslutning-fliken visar nätverksadressen och portnumret för Person Identification-enheten. Anslutningsinställningarna för en Person Identification-enhet är skrivskyddade.

12.21.6

Återställa åtkomst till ett PID efter ett BVMS-centralserveravbrott



Obs!

I händelse av ett centralserveravbrott måste du återställa BVMS-konfigurationen och certifikatet Bosch VMS CA. Annars kan du inte använda en befintlig PID utan återställning, vilket innebär att alla lagrade personer tas bort.

Vi rekommenderar att du skapar en säkerhetskopia av BVMS-konfigurationen och certifikatet Bosch VMS CA.

Mer information om hur du sparar BVMS-konfigurationen finns i *Så här exporterar du konfigurationsdata*, sidan 73. Certifikat hanteras utanför BVMS i Windows-programmet **Hantera datorcertifikat**.

**Obs!**

Certifikat innehåller konfidentiell information. Skydda dem genom att göra följande:

- Ange ett starkt lösenord.
- Lagra certifikatet i ett begränsat område, till exempel en icke-offentlig server.
- Se till att endast behörig personal har åtkomst till certifikatet.

Så här skapar du en säkerhetskopia av Bosch VMS CA-certifikatet:

1. Öppna Windows-programmet **Hantera datorcertifikat**.
2. I mappen **Betrodda rotcertifikatutfärdare** väljer du certifikatet Bosch VMS CA.
3. Exportera certifikatet med den privata nyckeln genom att välja **Ja, exportera den privata nyckeln**.
4. Använd formatet Personal Information Exchange.
5. Ange ett starkt lösenord.
6. Spara certifikatet som en PFX-fil.

Så här återställer du åtkomsten till PID från en nyligen installerad BVMS-centralserver:

1. Öppna Windows-programmet **Hantera datorcertifikat**.
2. Importera PFX-filen som innehåller certifikatet Bosch VMS CA till mappen **Betrodda rotcertifikatutfärdare** för den nya centralservern. Ta med alla utökade egenskaper.
3. Importera BVMS-konfigurationssäkerhetskopian.

Se

- *Exportera konfigurationsdata*, sidan 89

12.21.7**Lägga till kameror i en Person Identification device (PID)**

Du kan lägga till kameror till Person Identification-enheten, om de redan har lagts till i det logiska trädet.

Så här lägger du till en Person Identification-enhet:

1. Utvidga .
2. Utvidga .
3. Klicka på .
4. Klicka på **Kameror** -fliken.
5. Dra lämpliga kameror från **Logiskt träd**-fönstret till **Kameror** -fönstret.

Du kan även

dubbelklicka på lämpliga kameror i **Logiskt träd**-fönstret.

Kamerorna läggs till i Person Identification-enheten och visas i **Kameror**-listan.

12.21.8**Konfigurera kameraparametrar för Person Identification-larm**

För varje tillgänglig kamera kan du konfigurera kameraparametrar för Person Identification-larm för att minska falsklarm.

Kameraparameter

Namn	Värdeinformation	Beskrivning
Tröskelsannolikhet (%)	Standard: 55 % Min: 0 % Max: 100 %	Minsta sannolikhet för positiv identifiering av ett ansikte för att generera en Person Identification-händelse.
Ansiktsstorlek (%)	Standard: 7,5 % Min: 5 % Max: 100 %	Minsta storlek av ett ansikte som ska identifieras jämfört med storleken på hela bildrutan.
Min. bildantal	Standard: 4 Min: 1	Minsta antalet bildrutor i följd där ett ansikte måste visas för att kunna identifieras.
Bildrutor som ska analyseras (%)	Standard: 100 % Min: 10 % Max: 100 %	Den procentandel av ramar som analyseras för att identifiera personer. Ett värde på 50 % betyder att varannan bildruta analyseras.

12.21.9**Konfigurera persongrupper**

Huvudfönster > > **Enheter** > Utvidga  > 

Så här konfigurerar du persongrupper:

1. Välj **Persongrupper** -fliken.
2. Klicka på  för att lägga till en ny persongrupp.
3. Ange passande värden.
4. Klicka på  för att ta bort en persongrupp.

**Obs!**

Du kan inte ta bort eller ändra värdena i standardgruppen.

Persongruppstabell

Persongrupp	Ange namnet på persongruppen.
Larmfärg	Dubbelklicka för att välja larmfärg.
Larmtitel	Ange titeln för larmet som ska visas i Operator Client.

Så här ändrar du värdena för persongruppstabellen:

1. Dubbelklicka i lämpligt tabellfält.
2. Ändra värdet.

Larmprioritet

Du kan ställa in larmprioritet för Person Identification-larm på **Larm**-sidan.

**Obs!**

Du kan ställa in olika larmprioriteter för varje kamera i lämplig persongrupp. Du kan också ändra larmprioriteten för standardpersongruppen.

Se

– *Sidan Larm, sidan 289*

12.21.10**Lägga till en LPR-enhet**

Huvudfönster > > **Enheter** > Utvidga  >  > 

LPR-enheterna identifierar och detekterar registreringsnummer. Du kan konfigurera LPR-händelser och larm i enlighet med detta.

Om LPR-enheten ska detektera specifika registreringsnummer måste du först konfigurera en lista med tillämpliga registreringsnummer direkt i LPR-enheten. Mer information finns i användardokumentationen för enheten.

**Obs!**

Enheten måste vara ansluten och tillgänglig.

BVMS ansluter bara om autentisering är aktiverad på LPR-enheten och användarnamn och lösenord anges. Användarnamn och lösenord får inte vara tomma.

Så här lägger du till en LPR-enhet:

1. Högerklicka på 
2. Klicka på **Lägg till LPR-enhet**.
Dialogrutan **Lägg till LPR-enhet** visas.
3. Ange passande värden.
4. Klicka på **Autentisera**.
5. Klicka på **OK**.
Enheten läggs till i systemet.

**Obs!**

Du måste ange IP-adressen för BVMS Management Server i LPR-enhetens konfiguration. Annars hämtar inte BVMS-systemet händelser från LPR-enheten.

Dialogrutan Lägg till LPR-enhet**Nätverksadress**

Ange enhetens IP-adress.

Portnummer

Skriv in enhetens portnummer.

Användarnamn

Skriv in det giltiga användarnamnet som används för autentisering på enheten.

Lösenord

Ange lösenordet för autentisering på enheten.

Autentisera

Verifiera dig på enheten med de uppgifter som angavs ovan.

12.22**Sidan VRM-enheter**

Huvudfönster > **Enheter** > utvidga  > 
 Låter dig lägga till och konfigurera VRM-enheter. En VRM-enhet behöver minst en kodare, en iSCSI-enhet, en LUN tilldelad till iSCSI-enheten samt en lagringspool. Se versionskommentarerna och databladet för aktuella versioner på fast programvara.

**Obs!**

Efter att du har lagt till en iSCSI-enhet med respektive kodare till BVMS, måste du lägga till IQN för varje kodare till den här iSCSI-enheten (gäller vissa typer av iSCSI-enheter).
 Se *Konfigurera en iSCSI-enhet, sidan 183* för mer information.

**Obs!**

Se till att tidsinställningen på VRM-datorn är synkroniserad med den Management Server. Annars kan du förlora inspelningar.
 Konfigurera tidsserverprogramvaran på Management Server. På VRM-datorn konfigurerar du IP-adressen för Management Server som en tidsserver enligt standardprocedurer i Windows.

Se

- *Konfigurera multicast, sidan 218*
- *Synkronisera BVMS-konfigurationen, sidan 170*
- *Sidan VRM-inställningar, sidan 164*
- *Poolsidan, sidan 170*
- *Sidan för iSCSI-enhet, sidan 179*
- *Ändra lösenordet för en VRM-enhet, sidan 166*

12.22.1**Lägga till VRM-enheter genom avsökning**

Huvudfönster > **Enheter** > 
 I nätverket behöver du en VRM-tjänst som körs på en dator och en iSCSI-enhet.

**Obs!**

Starta en standardkonfiguration och lägg till IQN för varje kodare till den här iSCSI-enheten när du lägger till en iSCSI-enhet utan mål och utan LUN-enheter konfigurerade.
 När du lägger till en iSCSI-enhet med mål och LUN-enheter förkonfigurerade lägger du till IQN för varje kodare till den här iSCSI-enheten.
 Se *Konfigurera en iSCSI-enhet, sidan 183* för mer information.

Så här lägger du till VRM-enheter genom avsökning:

1. Högerklicka på  och klicka på **Sök efter VRM-enheter**. Dialogrutan **BVMS Scan Wizard** visas.
2. Markera önskade kryssrutor för de enheter som du vill lägga till.
3. I listan **Roll** väljer du önskad roll.
 Vilken roll du kan välja beror på den aktuella typen av VRM-enhet.
 Om du väljer **Speglad** eller **Reserv** krävs även nästa konfigurationssteg.

4. Välj önskad roll i listan **Roll**.
Vilken ny roll du kan välja beror på den aktuella typen av VRM-enhet.
5. Klicka på **Nästa >>**
6. Välj huvud-VRM för den valda speglade VRM:en eller VRM-reserven på listan **VRM-master**.
7. Klicka på **Nästa >>**.
Dialogrutan **Autentisera enheter** i guiden visas.
8. Ange lösenordet för varje enhet som skyddas med ett lösenord.
Lösenordskontrollen sker automatiskt om du inte skriver något i lösenordsfältet inom ett par sekunder, eller om du klickar utanför lösenordsfältet.
Om samtliga enheter har samma lösenord kan du ange det i det första **Lösenord**-fältet.
Högerklicka sedan på detta fält och klicka på **Kopiera cell till kolumn**.



I kolumnen **Status** anges lyckade inloggningar med .



Misslyckade inloggningsförsök anges med .

9. Klicka på **Slutför**.
Enheten läggs till i enhetsträdet.
- Obs!** Alla VRM-enheter läggs till med säker anslutning som standard.

Så här ändrar du säker/osäker anslutning:



1. Högerklicka på .
2. Klicka på **Redigera VRM-enhet**.
Dialogrutan **Redigera VRM-enhet** visas.
3. Markera kryssrutan **Säker anslutning**.
Den använda porten ändras automatiskt till HTTPS-porten.
Eller
avmarkera kryssrutan **Säker anslutning**.
Den använda porten ändras automatiskt till rcpp-porten.

Se

- *Lägga till en enhet, sidan 118*
- *Sidan VRM-enheter, sidan 161*
- *Konfigurera en iSCSI-enhet, sidan 183*
- *Dubbel strömning/reservinspelning, sidan 28*

12.22.2

Lägga till en primär eller sekundär VRM manuellt



Huvudfönster > **Enheter** > Högerklicka på  > Klicka på **Lägg till VRM-enhet** > Dialogrutan **Lägg till VRM-enhet**

Gör att du kan lägga till en VRM-enhet. Du kan välja enhetens typ och ange inloggningsuppgifterna.

En reserv-VRM-enhet kan endast tilldelas en huvud-VRM-enhet när båda enheterna är online och kan autentiseras. Då synkroniseras lösenorden.

Du kan lägga till en primär VRM-enhet manuellt om du vet IP-adressen och lösenordet.

Så här lägger du till en primär VRM-enhet:

1. Gör nödvändiga inställningar för din VRM-enhet.
 2. I listan **Typ** väljer du **Primär**.
 3. Klicka på **OK**.
- VRM-enheten läggs till.

Du kan lägga till en sekundär VRM-enhet manuellt om du vet IP-adressen och lösenordet.

**Obs!**

Om du vill konfigurera en sekundär VRM-enhet måste du först installera lämplig programvara på datorn. Kör Setup.exe och välj **Sekundär VRM**.

Så här lägger du till en sekundär VRM-enhet:

1. Gör nödvändiga inställningar för din VRM-enhet.
2. I listan **Typ** väljer du **Sekundär**.
3. Klicka på **OK**.

VRM-enheten läggs till.

Nu kan du konfigurera den sekundära VRM-enheten som vilken primär VRM-enhet som helst.

Dialogrutan Lägg till VRM-enhet**Namn**

Ange ett visningsnamn för enheten.

Nätverksadress/port

Skriv in enhetens IP-adress.

Om kryssrutan **Säker anslutning** är markerad ändras porten automatiskt till HTTPS-porten.

Du kan ändra portnumret om inga standardportar används.

Typ

Välj önskad enhetstyp.

Användarnamn

Skriv in användarnamnet för autentisering.

Lösenord

Skriv in lösenordet för autentisering.

Visa lösenordet

Klicka här om du vill att lösenordet ska visas.

Säkerhet

Kryssrutan **Säker anslutning** är markerad som standard, om HTTPS stöds.

**Obs!**

Om du migrerar till BVMS-version 10.0 och senare är kryssrutan **Säker anslutning** inte markerad som standard och anslutningen är osäker (rcpp).

Om du vill ändra säker eller osäker anslutning använder du kommandot **Redigera VRM-enhet** och markerar eller avmarkerar kryssrutan **Säker anslutning**.

Test

Klicka här för att kontrollera om enheten är ansluten och autentiseringen lyckades.

Egenskaper

Ändra portnumren för HTTP-porten och för HTTPS-porten vid behov. Detta är endast möjligt när du lägger till eller redigerar en VRM-enhet som inte är ansluten. Om VRM-enheten är ansluten hämtas värdena och du kan inte ändra dem.

Tabellraden **VRM-master** visar den valda enheten i förekommande fall.

Se

- Redigera en VRM-enhet, sidan 164
- Lägga till en speglad VRM manuellt, sidan 168
- Lägga till en reserv-VRM manuellt, sidan 167

12.22.3**Redigera en VRM-enhet**Huvudfönster > **Enheter**

Gör att du kan redigera en VRM-enhet.

Så här ändrar du säker/osäker anslutning:

1. Högerklicka på .
2. Klicka på **Redigera VRM-enhet**.
Dialogrutan **Redigera VRM-enhet** visas.
3. Markera kryssrutan **Säker anslutning**.
Den använda porten ändras automatiskt till HTTPS-porten.
Eller
avmarkera kryssrutan **Säker anslutning**.
Den använda porten ändras automatiskt till rcpp-porten.

**Obs!**

När du har uppgraderat till en nyare version rekommenderar vi att du ändrar till säker anslutning.

Detaljerad information om parametern i dialogrutan **Redigera VRM-enhet** finns i kapitlet Lägga till en primär eller sekundär VRM manuellt.

Se

- Lägga till en primär eller sekundär VRM manuellt, sidan 162

12.22.4**Sidan VRM-inställningar**

Huvudfönster > **Enheter** > Utvidga  >  > **Huvudinställningar** > **VRM-inställningar**

Serverinitiatörsnamn

Visar iSCSI-initiatörsnamnet för VRM Server.

12.22.5**Sidan SNMP**

Huvudfönster > **Enheter** > Utvidga  > Utvidga  > **Nätverk** > **SNMP**

1. SNMP-värddress 2. SNMP-värddress

VRM stöder SNMP (Simple Network Management Protocol) för hantering och övervakning av nätverkskomponenter och kan skicka SNMP-meddelanden (fällor) till IP-adresser. Enheten stöder SNMP MIB II i den enhetliga koden. Om du vill skicka SNMP-fällor (traps) anger du IP-adresser till en eller två önskade målenheter här.

Vissa händelser skickas bara som SNMP-fällor. Mer information finns i MIB-filen.

12.22.6**Sidan Konton**

Om du vill ställa in bildöverföring och exportera video i filformatet MP4 måste du skapa ett konto där du kan spara och öppna objekten. Du kan skapa högst fyra (4) konton.

Typ

Välj typ av konto: **FTP** eller **Dropbox**.

IP-adress

Ange IP-adress till den server där du vill spara bilderna.

Användarnamn

Ange servers användarnamn.

Lösenord

Ange det lösenord som ger dig tillgång till servern. Verifiera lösenordet genom att klicka på knappen **Kontrollera** till höger.

Kontrollera

Klicka när du vill verifiera lösenordet.

Sökväg

Ange den exakta sökvägen för överföringen av bilderna och videor till servern.

12.22.7**Sidan Avancerad**

Huvudfönster > **Enheter** > Utvidga  > Utvidga  > **Service** > **Avancerad**

RCP+-loggning / Felsökningsloggning / Återuppspelningsloggning / VDP-loggning / Prestandaloggning

Aktivera de olika loggarna för VRM Server och Configuration Manager.

Loggfilerna för VRM Server sparas på den dator där VRM Server startades, och de kan visas eller hämtas med VRM Monitor.

Loggfilerna för Configuration Manager lagras lokalt i följande katalog:

%USERPROFILE%\My Documents\Bosch\Video Recording Manager\Log

Kvarhållningstid (dagar):

Ange kvarhållningstiden för loggfiler i dagar.

Fullständig minnesdumpningsfil

Välj endast den här kryssrutan om det är nödvändigt, till exempel om, om den tekniska supporten begär en fullständig sammanställning av huvudminnet.

Telnet-stöd

Välj den här kryssrutan om åtkomst med Telnet-protokollet ska stödjas. Välj enbart om det är nödvändigt.

**Obs!**

Omfattande loggning kräver betydande processorkraft och hårddiskutrymme. Använd inte omfattande loggning kontinuerligt.

12.22.8**Kryptera inspelning för VRM**

Krypterad inspelning för VRM-kodare är inte aktiverat som standard.

Du måste aktivera krypterad inspelning för primär och sekundär VRM separat.

**Obs!**

Du måste skapa en redundansnyckel (säkerhetskopieringscertifikat) innan du aktiverar krypterad inspelning första gången. Du behöver bara skapa en redundansnyckel en gång för varje VRM-enhet.

Om du inte har tillgång till den vanliga krypteringsnyckeln kan du dekryptera inspelningarna med redundansnyckeln.

Vi rekommenderar att du behåller en kopia av redundansnyckeln på en säker plats (t.ex. i ett kassaskåp).

Så här skapar du en redundansnyckel:

1. Välj lämplig VRM-enhet.
2. Välj **Service**-fliken.
3. Välj **Inspelningskryptering** -fliken.
4. Klicka på **Redundansnyckel**.
5. Välj en plats för lagring av certifikat.
6. Ange ett lösenord som uppfyller kraven på lösenordskomplexitet och bekräfta.
7. Klicka på **Skapa**.

Redundansnyckeln (säkerhetskopieringscertifikat) skapas.

Så här aktiverar/inaktiverar du krypterad inspelning:

1. Välj lämplig VRM-enhet.
2. Välj **Service**-fliken.
3. Välj **Inspelningskryptering** -fliken.
4. Markera/avmarkera kryssrutan **Aktivera krypterad inspelning**.

5. Klicka på  .

Obs! Kryptering aktiveras först efter nästa blockändring. Det här kan ta en stund. Kontrollera att kodarna krypterar.

Så här kontrollerar du de VRM-kodare som krypterar:

1. Välj lämplig VRM-enhet.
2. Välj **Service**-fliken.
3. Välj **Inspelningskryptering** -fliken.

Obs! Du kan även se fliken **Monitoring** på VRM-monitorn.

**Obs!**

Alla VRM-kodare som stöder kryptering krypterar automatiskt inspelningen när kryptering har aktiverats i VRM.

Kryptering kan inaktiveras för en enskild kodare.

VSG-kodare krypteras alltid om kryptering har aktiverats i VRM.

Så här aktiverar/inaktiverar du krypterad inspelning för en enda VRM-kodare:

1. Välj lämplig VRM-kodare.
2. Välj **Inspelning**-fliken.
3. Klicka på fliken **Inspelningshantering**.
4. Markera/avmarkera kryssrutan **Kryptering**.

5. Klicka på  .

12.22.9**Ändra lösenordet för en VRM-enhet**

Huvudfönster > **Enheter** > Utvidga  > 

Så här ändrar du lösenordet:

1. Högerklicka på  och klicka på **Ändra VRM-lösenord**. Dialogrutan **Byt lösenord** visas.
2. I fältet **Gammalt lösenord** skriver du lämpligt lösenord.
3. I fältet **Nytt lösenord** skriver du det nya lösenordet och klickar och upprepar inmatningen i det andra **Nytt lösenord** -fältet.

Klicka på **OK**.

- ▶ Bekräfta i nästa dialogruta.
- ✓ Lösenordet ändras på enheten direkt.

12.22.10

Lägga till en VRM-pool

Huvudfönster > **Enheter** > Utvidga



Så här lägger du till en VRM-pool:

- ▶ Högerklicka på  eller  och välj **Lägg till pool**.
En ny pool läggs till i systemet.

Se

- *iSCSI-lagringspool, sidan 179*

12.22.11

Lägga till en reserv-VRM manuellt

Huvudfönster > **Enheter** > Utvidga



> Högerklicka på



> Klicka på **Lägg till VRM-reservenhet** > Dialogrutan **Lägg till VRM-reservenhet**



Obs!

Om du vill konfigurera en sekundär VRM-enhet måste du först installera lämplig programvara på datorn. Kör Setup.exe och välj **Sekundär VRM**.

Det är bara en primär VRM-enhet eller en sekundär VRM-enhet som kan ha rollen som reserv-VRM. Du lägger till en primär reserv-VRM för en primär VRM-enhet eller en sekundär reserv-VRM för en sekundär VRM-enhet.

Du kan lägga till en reserv-VRM-enhet manuellt om du vet IP-adressen och lösenordet. Den VRM-enhet som valdes först blir huvud-VRM för reserv-VRM-enheten.

Du kan lägga till en reserv-VRM-enhet. Du kan antingen lägga till den manuellt eller välja en enhet i en lista över avsökta VRM-enheter.

En reserv-VRM-enhet kan endast tilldelas en huvud-VRM-enhet när båda enheterna är online och kan autentiseras. Då synkroniseras lösenorden.

Så här lägger du till en reserv-VRM-enhet:

1. Gör nödvändiga inställningar för din VRM-enhet.
 2. Kontrollera att rätt huvud-VRM har valts. I annat fall avbryter du åtgärden.
 3. Klicka på **OK**.
- ✓ Reserv-VRM-enheten läggs till för den valda huvud-VRM-enheten.

Dialogrutan Lägg till VRM-reservenhet

Nätverksadress

Skriv in enhetens IP-adress eller välj en nätverksadress i listan **Avsökta VRM-enheter**.

Avsökta VRM-enheter

Visar en lista över avsökta VRM-datorer. Om du vill göra en ny avsökning stänger du dialogrutan och öppnar den på nytt.



Obs!

Reserv-VRM-enheten får inställningarna som konfigureras i huvud-VRM. Om inställningarna för huvud-VRM ändras, ändras inställningarna för reserv-VRM-enheten därefter.

Se

– *Dubbel strömning/reservinspelning, sidan 28*

12.22.12

Lägga till en speglad VRM manuellt

Huvudfönster > **Enheter** > Utvidga  > Högerklicka på  > Klicka på **Lägg till speglad VRM** > Dialogrutan **Lägg till VRM-enhet**



Obs!

Om du vill konfigurera en sekundär VRM-enhet måste du först installera lämplig programvara på datorn. Kör Setup.exe och välj **Sekundär VRM**.

Det är bara en sekundär VRM som kan överta rollen som en speglad VRM. Du lägger till en speglad VRM i en primär VRM.

Du kan lägga till en speglad VRM-enhet manuellt om du känner till IP-adressen och lösenordet. Den VRM som väljs först är huvud-VRM för denna speglade VRM.

Så här lägger du till en speglad VRM-enhet:

1. Gör nödvändiga inställningar för din VRM-enhet.
2. Kontrollera att rätt huvud-VRM har valts. I annat fall avbryter du åtgärden.
3. Klicka på **OK**.

Den speglade VRM-enheten läggs till i den valda primära VRM-enheten.

Dialogrutan **Lägg till VRM-enhet**

Namn

Ange ett visningsnamn för enheten.

Nätverksadress/port

Skriv in enhetens IP-adress.

Om kryssrutan **Säker anslutning** är markerad ändras porten automatiskt till HTTPS-porten.

Du kan ändra portnumret om inga standardportar används.

Typ

Välj önskad enhetstyp.

Användarnamn

Skriv in användarnamnet för autentisering.

Visa lösenordet

Klicka här om du vill att lösenordet ska visas.

Lösenord

Skriv in lösenordet för autentisering.

Säkerhet

Kryssrutan **Säker anslutning** är markerad som standard, om HTTPS stöds.



Obs!

Om du migrerar till BVMS-version 10.0 och senare är kryssrutan **Säker anslutning** inte markerad som standard och anslutningen är osäker (rcpp).

Om du vill ändra säker eller osäker anslutning använder du kommandot **Redigera VRM-enhet** och markerar eller avmarkerar kryssrutan **Säker anslutning**.

Test

Klicka här för att kontrollera om enheten är ansluten och autentiseringen lyckades.

Egenskaper

Ändra portnumren för HTTP-porten och för HTTPS-porten vid behov. Detta är endast möjligt när du lägger till eller redigerar en VRM-enhet som inte är ansluten. Om VRM-enheten är ansluten hämtas värdena och du kan inte ändra dem.

Tabellraden **VRM-master** visar den valda enheten i förekommande fall.

Se

- *Lägga till en primär eller sekundär VRM manuellt, sidan 162*
- *Dubbel strömning/reservinspelning, sidan 28*

12.22.13

Lägga till kodare genom avsökning

Så här lägger du till kodare genom avsökning:

1. Högerklicka på  och klicka på **Sök efter kodare**.
Dialogrutan **BVMS Scan Wizard** visas.
2. Välj de kodare som krävs, välj önskad VRM-pool och klicka på **Tilldela** för att tilldela dem till poolen.
3. Klicka på **Nästa >>**.
Dialogrutan **Autentisera enheter** i guiden visas.
4. Ange lösenordet för varje enhet som skyddas med ett lösenord.
Lösenordskontrollen sker automatiskt om du inte skriver något i lösenordsfältet inom ett par sekunder, eller om du klickar utanför lösenordsfältet.
Om samtliga enheter har samma lösenord kan du ange det i det första **Lösenord**-fältet.
Högerklicka sedan på detta fält och välj **Kopiera cell till kolumn**.

- I kolumnen **Status** indikeras lyckade inloggningsförsök med .
- Misslyckade inloggningsförsök indikeras med .
5. Klicka på **Slutför**.
Enheten läggs till i enhetsträdet.

-ikonen anger ett fel som du måste åtgärda. Mer information om det specifika felet finns i knappbeskrivningen.

12.22.14

Lägga till VSG-enheter genom avsökning

Så här lägger du till VSG-enheter genom avsökning:

1. Högerklicka på  och klicka på **Sök efter Video Streaming Gateways**.
Dialogrutan **BVMS Scan Wizard** visas.
2. Välj de VSG-enheter som krävs, välj önskad VRM-pool och klicka på **Tilldela** för att tilldela dem till VRM-poolen.
3. Klicka på **Nästa >>**.
Dialogrutan **Autentisera enheter** i guiden visas.
4. Ange lösenordet för varje enhet som skyddas med ett lösenord.
Lösenordskontrollen sker automatiskt om du inte skriver något i lösenordsfältet inom ett par sekunder, eller om du klickar utanför lösenordsfältet.
Om samtliga enheter har samma lösenord kan du ange det i det första **Lösenord**-fältet.

Högerklicka sedan på detta fält och klicka på **Kopiera cell till kolumn.**



I kolumnen **Status** anges lyckade inloggningar med .



Misslyckade inloggningsförsök anges med .

5. Klicka på **Slutför.**

Enheten läggs till i enhetsträdet.

12.22.15

Synkronisera BVMS-konfigurationen



Huvudfönster > **Enheter** > expandera > högerklicka på > kommandot **Synkronisera BVMS-konfigurationen**

Från BVMS 6.0 stöds VRM 3.50. Om du inte uppgraderar VRM till version 3.50 under uppgraderingen till BVMS 6.0, fortsätter inspelningen men du kan inte ändra konfigurationen för den gamla VRM.

Om du har uppgraderat din VRM-programvara till version 3.50, måste du synkronisera BVMS-konfigurationen manuellt.

12.22.16

Importerar konfiguration från VRM



Huvudfönster > **Enheter** > utvidga

>

Om du måste byta ut en primär VRM enhet kan du importera konfigurationen av den tidigare primära VRM -enheten.

Obs! Detta är endast möjligt för primära VRM enheter.

Förutsättning: En säkerhetskopia av den tidigare VRM enhetskonfigurationsfilen (config.xml) utfördes. Så här utför du en säkerhetskopia, se *Underhålla BVMS, sidan 73*.

Så här kan du importera konfiguration från VRM:

1. Kopiera säkerhetskopiering för VRM konfigurationsfilen (config.xml) till C:\ProgramData\Bosch\VRM\primary.



2. Högerklicka på .

3. Välj **Importera konfiguration från VRM.**

Den tidigare konfigurationen VRM är importerad.



Obs!

Endast kodaren VSG och iSCSI konfigurationen importeras.

Du måste göra om alla andra konfigurationer, till exempel lägga till de enheter som krävs för att **Logiskt träd**, konfigurera larm eller inspelningsinställningar.

12.23

Poolsidan



Huvudfönster > **Enheter** > Utvidga

> Utvidga

>

Gör att du kan konfigurera inspelningsinställningar som gäller för alla enheter som samlats i lagringspoolen.

Poolidentifiering

Visar poolnumret.

Inspelningsinställningsläge

– **Reserv**

Inspelningar sparas endast på primärt mål. Om det inte går att spara till det primära målet sparas inspelningen på den målenhet som angivits under sekundärt mål. Den här situationen inträffar om det primära målet inte uppger lagringsblock av någon orsak, exempelvis systemfel, nätverksfel eller slut på kapacitet.

Den andra mållistan kan lämnas tom. I det här fallet kan ingen failover utföras, men antalet nödvändiga iSCSI-sessioner minskas och inget diskutrymme på det sekundära målet allokeras. Detta minskar systemets omkostnader och förlänger systemets kvarhållningstid.

Obs! För varje kamera och kodare måste du sedan konfigurera det primära och sekundära målet.

- **inspelningsläge Automatiskt**

Lastbalansering konfigureras automatiskt. Det **automatiska** läget försöker automatiskt optimera kvarhållningstiden för de tillgängliga iSCSI-målen. För att allokera blocken för det andra iSCSI-målet väljer du **På** i listan **Användning av sekundärt mål**.

Sanitetskontrollperiod (dagar)

Ange önskad tidsperiod. Efter denna tidsperiod Video Recording Manager gör programmet en analys av om lagringsdistributionen i **automatiskt** läge fortfarande är optimal. Och om inte, Video Recording Manager gör programmet ändringar.

Användning av sekundärt mål

Gör att du kan välja om block ska distribueras från ett andra mål.

Välj **På** eller **Av** aktivera användningen av ett sekundärt mål.

- **På:** Välj **På** för att använda ett sekundärt mål för att minska inspelningsgapet i händelse av primärt målfel. Om det primära målet är tillgängligt används inte blocken på det sekundära målet, men lagringen är tilldelad. Den här redundansen minskar systemets kvarhållningstid.
- **Av:** Välj **Av** om du inte vill använda något sekundärt mål. Vid händelse av primärt målfel Video Recording Manager behöver programmet mer tid för att omorganisera. Det innebär att inspelningsgapet är större.

Blockera reservering för nertid

Ange det antal dagar som de tilldelade kodarna spelas in även om VRM Server är ur funktion. Om du till exempel anger 4, så spelas kodarna in under ungefär 4 dagar under VRM Server driftsavbrottet.

Om ditt system har kodare med låg bithastighet kan du minska det i förväg tilldelade diskutrymme avsevärt. På så sätt säkerställs en korrekt fördelning av lagringskapacitet, och kvarhållningstiderna förlängs.

Tillåt LUN:er som är större än 2 TB

Klicka för att aktivera användning av LUN-enheter större än 2 TB.

LUN-enheter större än 2 TB ("stora LUN-enheter") stöds inte av följande enheter:

- VRM-enheter före 3.60
- VSG-enheter med fast programvara före version 6.30
- Kodare med fast programvara före version 6.30

BVMS gör att du inte kan göra följande:

- Lägg till eller flytta enheter med fast programvara före version 6.30 i en pool som tillåter stora LUN-enheter.
- Lägg till eller flytta enheter som för närvarande inte är anslutna till nätverket till en pool som tillåter stora LUN-enheter.
- Lägg till eller flytta en iSCSI-enhet som innehåller stora LUN-enheter till en pool som inte tillåter stora LUN-enheter.

- Tillåta stora LUN-enheter i en pool som innehåller enheter med fast programvara före version 6.30.
- Avaktivera stora LUN-enheter i en pool med en iSCSI-enhet som innehåller stora LUN-enheter.

Flytta enheter med fast programvara före version 6.30 till en pool som inte tillåter stora LUN-enheter.

Se

- *Lägga till LUN, sidan 187*
- *Lägga till en VRM-pool, sidan 167*

12.23.1

Konfigurera automatiskt inspelningsläge för en pool

Huvudfönster > **Enheter** > Utvidga  > Utvidga  > 

OBS!

Om du har konfigurerat ett reservinspelningsläge tidigare skrivs den konfigurationen över.

Så här konfigurerar du:

- ▶ I listan **Läge för inspelningsinställning** väljer du **Automatiskt**.

När konfigurationen har aktiverats är inspelningsläget **Automatiskt** aktivt. På sidan **Inspelningsinställningar** för en kodare visas listorna med primära och sekundära mål.

Närliggande ämnen

- *Konfigurera reservinspelningsläge på en kodare, sidan 217*

12.23.2

Lägga till en kodare/avkodare manuellt

Huvudfönster > **Enheter** > Utvidga  > Utvidga  > Högerklicka  > Klicka på **Lägg till kodare** > dialogrutan **Lägg till kodare** eller

Huvudfönster > **Enheter** > Högerklicka  > Klicka på **Lägg till kodare** > dialogrutan **Lägg till kodare** eller

Huvudfönster > **Enheter** > Högerklicka  > Klicka på **Lägg till kodare** > dialogrutan **Lägg till kodare** eller

Huvudfönster > **Enheter** > Utvidga  > Högerklicka på  > Klicka på **Lägg till avkodare** > dialogrutan **Lägg till kodare**

Här kan du lägga till en kodare eller avkodare manuellt. Detta är särskilt användbart när du vill lägga till en Video IP-enhet från Bosch (endast för VRM).

Obs!

För att du ska kunna lägga till en Video IP-kodare eller -avkodare från Bosch med alternativet **<Upptäck automatiskt>** måste enheten finnas i nätverket.

Så här lägger du till en Video IP-enhet från Bosch:

1. Utvidga  , utvidga  , högerklicka på  , eller
högerklicka på  ,

eller

högerklicka på  .

2. Klicka på **Lägg till kodare**.
Dialogrutan **Lägg till kodare** visas.
3. Ange IP-adressen.
4. Välj **<Upptäck automatiskt>** i listan.
5. Klicka på **OK**.
Enheten läggs till i systemet.

-ikonen anger ett fel som du måste åtgärda. Mer information om det specifika felet finns i knappbeskrivningen.

Dialogrutan Lägg till kodare

IP-adress:

Ange en giltig IP-adress.

Kodartyp:/Avkodartyp:

För en enhet med känd enhetstyp väljer du lämplig post. Enheten behöver inte vara tillgänglig i nätverket.

Om du vill lägga till en Video IP-enhet från Bosch väljer du **<Upptäck automatiskt>**. Enheten måste vara tillgänglig i nätverket.

Om du vill lägga till en kamera för offlinekonfiguration väljer du **<Enkel platshållarkamera>**.

12.23.3

Lägga till en iSCSI-enhet manuellt

Huvudfönster > **Enheter** >  > Utvidga  > Högerklicka på  > **Lägg till iSCSI-enhet** > Dialogrutan **Lägg till iSCSI-enhet**

Låter dig lägga till iSCSI-enheter i en VRM.

Lägga till en iSCSI-enhet:

1. Högerklicka på  och klicka på **Lägg till iSCSI-enhet**.
Dialogrutan **Lägg till iSCSI-enhet** visas.
2. Skriv in önskat visningsnamn, nätverksadress till en iSCSI-enhet samt enhetstyp och klicka på **OK**.
iSCSI-enheten läggs till i den valda VRM-poolen.
Lägg till mål och LUN-enheter om vid behov.

Dialogrutan Lägg till iSCSI-enhet

Namn

Ange ett visningsnamn för enheten.

Nätverksadress

Skriv in en giltig nätverksadress för enheten.

iSCSI-enhetstyp

Välj lämplig enhetstyp.

Användarnamn

Skriv in användarnamnet för autentisering.

Lösenord

Skriv in lösenordet för autentisering.

Aktivera övervakning

Om en DIVAR IP-enhet är markerad som iSCSI-enhetstyp och all SNMP (Simple Network Management Protocol) övervakning stöds för den typen av DIVAR IP-enhet, **Aktivera övervakning** aktiveras kryssrutan.

Markera kryssrutan för att aktivera övervakning av hälsotillståndet på DIVAR IP-enheten. BVMS tar nu emot och analyserar automatiskt SNMP-meddelanden på DIVAR IP-enheten och aktiverar hälsoövervakningshändelser och larm (till exempel CPU, lagring, fläkt ...). Som standard utlöses endast kritiska larm.

Obs! Se till att konfigurera SNMP på DIVAR IP-enheten först.

Obs! Den här inställningen är endast tillgänglig för enheter som stöds.

Mer information om hur du konfigurerar SNMP på en DIVAR IP-enhet, se respektive DIVAR IP dokumentation.

Närliggande ämnen

- *Lägga till VRM-enheter genom avsökning, sidan 161*

Se

- *Sidan RMon och Snmp, sidan 145*
- *Konfigurera SNMP-övervakning, sidan 91*

12.23.4

Lägga till en Video Streaming Gateway manuellt

Huvudfönster > **Enheter** > Utvidga  > 

Du kan lägga till VSG-enheter i en VRM-pool.

Lägga till en VSG-enhet manuellt:

1. Högerklicka på  och klicka på **Lägg till Video Streaming Gateway**. Dialogrutan **Lägg till Video Streaming Gateway** visas.
 2. Gör nödvändiga inställningar för din VSG-enhet.
 3. Klicka på **Lägg till**.
- ✓ VSG-enheten läggs till i systemet. De kameror som den här VSG-enheten har tilldelats spelas in.

Dialogrutan Lägg till Video Streaming Gateway

Högerklicka på dialogrutan  > **Lägg till Video Streaming Gateway** > **Lägg till Video Streaming Gateway**

Namn

Ange ett önskat visningsnamn för enheten.

Användarnamn

Skriv in användarnamnet som används för autentisering på enheten. Vanligtvis: service

Nätverksadress/port

Skriv in enhetens IP-adress.

Om kryssrutan **Säker anslutning** är markerad ändras porten automatiskt till HTTPS-porten.

Du kan ändra portnumret om inga standardportar används eller om VSG-instanserna konfigureras i en annan ordning.

Standardportar

VSG-instans	rcpp-port	HTTPS-port
1	8756	8443

VSG-instans	rcpp-port	HTTPS-port
2	8757	8444
3	8758	8445
4	8759	8446
5	8760	8447
6	8761	8448
7	8762	8449

Lösenord

Skriv in lösenordet för autentisering på enheten.

Show password

Klicka här om du vill att det angivna lösenordet ska visas. Var försiktig så att ingen obehörig kan se lösenordet.

Säkerhet

Kryssrutan **Säker anslutning** är markerad som standard, om HTTPS stöds.

Från VSG-version 7.0 har VSG stöd för säker anslutning.



Obs!

Om du migrerar till BVMS-version 10.0 och senare är kryssrutan **Säker anslutning** inte markerad som standard och anslutningen är osäker (rcpp).

Om du vill ändra säker eller osäker anslutning använder du kommandot **Redigera Video Streaming Gateway** och markerar eller avmarkerar kryssrutan **Säker anslutning**.

Test

Verifiera dig på enheten med de uppgifter som angavs ovan.

Se

- *Redigera Video Streaming Gateway, sidan 191*

12.23.5

Lägga till en DSA E-Series iSCSI-enhet manuellt

Huvudfönster > **Enheter** >  > utvidga  > 

Du kan antingen lägga till en E-Series iSCSI-enhet som redan har initierats eller en som inte har initierats.

Du kan lägga till LUN-enheter större än 2 TB om poolen har aktiverats för stora LUN-enheter. LUN-enheter större än 2 TB ("stora LUN-enheter") stöds inte av följande enheter:

- VRM-enheter före 3.60
- VSG-enheter med fast programvara före version 6.30
- Kodare med fast programvara före version 6.30

BVMS gör att du inte kan göra följande:

- Lägga till eller flytta enheter med fast programvara före version 6.30 i en pool som tillåter stora LUN-enheter.
- Lägga till eller flytta enheter som för närvarande inte är anslutna till nätverket till en pool som tillåter stora LUN-enheter.
- Lägga till eller flytta en iSCSI-enhet som innehåller stora LUN-enheter till en pool som inte tillåter stora LUN-enheter.

- Tillåta stora LUN-enheter i en pool som innehåller enheter med fast programvara före version 6.30.
- Avaktivera stora LUN-enheter i en pool med en iSCSI-enhet som innehåller stora LUN-enheter.

Flytta enheter med fast programvara före version 6.30 till en pool som inte tillåter stora LUN-enheter.

Så här lägger du till en initierad iSCSI-enhet:

1. Högerklicka på  och klicka på **Lägg till DSA E-Series-enhet**. Dialogrutan **Lägg till DSA E-Series-enhet** visas.
2. Ange IP-adressen för hanteringen och lösenordet.
3. Klicka på **Anslut**. Om anslutningen upprättas fylls fälten i gruppen **Styrenhet** eller **2:a styrenhet** i.
4. Klicka på **OK**. Enheten läggs till i systemet. De tillgängliga målen skannas automatiskt och LUN-enheterna visas. Du kan använda iSCSI-enheten. Om poolen har aktiverats för stora LUN-enheter och iSCSI-enheten har konfigurerats för stora LUN-enheter innehåller kolumnen **Stor LUN** en markering för de berörda LUN-enheterna.

Så här lägger du till en iSCSI-enhet som inte har initierats:

1. Högerklicka på  och klicka på **Lägg till DSA E-Series-enhet**. Dialogrutan **Lägg till DSA E-Series-enhet** visas.
2. Ange IP-adressen för hanteringen och lösenordet.
3. Klicka på **Anslut**. Om anslutningen upprättas fylls fälten i gruppen **Styrenhet** eller **2:a styrenhet** i.
4. Klicka på **OK**. Enheten läggs till i systemet.
5. Klicka på  och sedan på .
6. Klicka på fliken **Grundkonfiguration**.
7. Ange önskad LUN-kapacitet. Om du skriver in ett värde större än 2 TB måste du aktivera din pool för LUN-enheter som är större än 2 TB.
8. Klicka på **Initiera**. LUN-enheterna skapas.
9. Klicka på **Stäng**.
10. Högerklicka på iSCSI-enheten och klicka sedan på **Sök efter mål**. LUN-enheterna visas med ett okänt tillstånd.
11. Spara och aktivera konfigurationen.
12. Formatera alla LUN-enheter.
13. Om du har lagt till en iSCSI-enhet med dubbel styrenhet tar du först bort önskade LUN-enheter från den första styrenheten. Högerklicka sedan på den andra styrenheten och lägg därefter till LUN-enheterna genom att klicka på **Sök efter mål**.

Dialogrutan Lägg till DSA E-Series-enhet

Huvudfönster > **Enheter** >  > Utvidga  > Högerklicka på  > **Lägg till DSA E-Series-enhet** > Dialogrutan **Lägg till DSA E-Series-enhet**

Används för att lägga till en DSA E-Series iSCSI-enhet. Den här enhetstypen har en IP-adress för hantering som skiljer sig från IP-adressen för iSCSI-lagringen. Via IP-adressen för hantering kan enheten upptäckas och konfigureras automatiskt.

Namn

Ange ett visningsnamn för enheten.

Hanteringsadress

Ange IP-adressen för automatisk konfiguration av enheten.

Lösenord:

Ange enhetens lösenord.

DSA E-Series-typ

Visar enhetstypen.

Nätverksadress iSCSI-kanal

Visar IP-adressen för enhetens iSCSI-port. Du kan välja en annan IP-adress om en sådan finns tillgänglig.

Hanteringsadress

Visar IP-adressen för automatisk konfiguration av den andra styrenheten, om en sådan finns tillgänglig. Du kan välja en annan IP-adress om en sådan finns tillgänglig.

Nätverksadress iSCSI-kanal

Visar IP-adressen för iSCSI-porten på den andra styrenheten, om en sådan finns tillgänglig. Du kan välja en annan IP-adress om en sådan finns tillgänglig.

Anslut

Klicka här för att söka efter enhetens inställningar.

Om anslutningen upprättas fylls fälten i gruppen **Styrenhet** och gruppen **2:a styrenhet**.

Se

- *Sidan Standardkonfiguration, sidan 184*
- *Formatera ett LUN, sidan 188*

12.23.6

Lägga till kodare genom avsökning

Så här lägger du till kodare genom avsökning:

1. Högerklicka på  och klicka på **Sök efter kodare**. Dialogrutan **BVMS Scan Wizard** visas.
2. Välj de kodare som krävs, välj önskad VRM-pool och klicka på **Tilldela** för att tilldela dem till poolen.
3. Klicka på **Nästa >>**. Dialogrutan **Autentisera enheter** i guiden visas.
4. Ange lösenordet för varje enhet som skyddas med ett lösenord. Lösenordskontrollen sker automatiskt om du inte skriver något i lösenordsfältet inom ett par sekunder, eller om du klickar utanför lösenordsfältet. Om samtliga enheter har samma lösenord kan du ange det i det första **Lösenord**-fältet.

Högerklicka sedan på detta fält och välj **Kopiera cell till kolumn**.



I kolumnen **Status** indikeras lyckade inloggningsförsök med .



Misslyckade inloggningsförsök indikeras med .

5. Klicka på **Slutför**.

Enheten läggs till i enhetsträdet.

-ikonen anger ett fel som du måste åtgärda. Mer information om det specifika felet finns i knappbeskrivningen.

12.23.7

Lägga till VSG-enheter genom avsökning

Så här lägger du till VSG-enheter genom avsökning:



1. Högerklicka på och klicka på **Sök efter Video Streaming Gateways**. Dialogrutan **BVMS Scan Wizard** visas.
2. Välj de VSG-enheter som krävs, välj önskad VRM-pool och klicka på **Tilldela** för att tilldela dem till VRM-poolen.
3. Klicka på **Nästa >>**. Dialogrutan **Autentisera enheter** i guiden visas.
4. Ange lösenordet för varje enhet som skyddas med ett lösenord. Lösenordskontrollen sker automatiskt om du inte skriver något i lösenordsfältet inom ett par sekunder, eller om du klickar utanför lösenordsfältet. Om samtliga enheter har samma lösenord kan du ange det i det första **Lösenord**-fältet. Högerklicka sedan på detta fält och klicka på **Kopiera cell till kolumn**.



I kolumnen **Status** anges lyckade inloggningar med .



Misslyckade inloggningsförsök anges med .

5. Klicka på **Slutför**.

Enheten läggs till i enhetsträdet.

12.23.8

Konfigurera dubbel strömning i enhetsträdet



Huvudfönster > **Enheter** > Utvidga



Du måste avaktivera ANR-funktionen för att kunna konfigurera dubbel strömning.

Om du konfigurerar dubbel strömning för en kamera i en flerkanalskodare kontrollerar systemet att samma inspelningsmål konfigureras för kodarens samtliga kameror.

Du kan konfigurera dubbel strömning genom att tilldela en sekundär VRM-enhet kodare som spelas in av en primär VRM-enhet. Detta är användbart till exempel när du vill tilldela endast en del av kodarna som spelas in av en primär VRM-enhet.

En sekundär VRM-enhet måste redan vara tillagd.

Så här konfigurerar du:



1. Högerklicka på och klicka på **Lägg till kodare från primär VRM**. Dialogrutan **Lägg till kodare** visas.
2. Klicka för att välja önskade kodare. När du väljer en pool eller en VRM-enhet väljs även alla underordnade poster automatiskt.
3. Klicka på **OK**.

De valda kodarna läggs till för den sekundära VRM-enheten.

Se

- Konfigurera dubbel strömning i kameratabellen, sidan 282
- Konfigurera ANR-funktionen, sidan 282
- Dubbel strömning/reservinspelning, sidan 28

12.24 Sidan Bosch-kodare/-avkodare

Läs mer om hur du konfigurerar en Bosch-kodare/-avkodare här: *Sidan Bosch-kodare/-avkodare/-kamera, sidan 204.*

12.25 Sidan för iSCSI-enhet



Du kan antingen lägga till en E-Series iSCSI-enhet eller en annan iSCSI-enhet som stöds.

Se

- Lägga till en iSCSI-enhet manuellt, sidan 180
- Lägga till en DSA E-Series iSCSI-enhet manuellt, sidan 181
- Konfigurera en iSCSI-enhet, sidan 183
- Lägga till LUN, sidan 187
- Formatera ett LUN, sidan 188

12.25.1 iSCSI-lagringspool

En lagringspool kan användas för att ha en logisk mappning av nätverkstopologin till Video Recording Manager systemet. Till exempel: 2 byggnader, båda med lagring och enheter, där du vill undvika att dirigera nätverkstrafiken från en byggnad till den andra.

Lagringspooler kan dessutom användas för att gruppera kameror och lagringssystem efter någon viktig egenskap i vyn. Ta t.ex. ett system som innehåller några få mycket viktiga kameror och ett stor antal mindre viktiga kameror. I det här fallet går det att gruppera dem i två lagringspooler, en med många redundanta funktioner och en med mindre redundans.

Följande lastbalanseringsegenskaper kan konfigureras för en lagringspool:

- Inspelningsinställningar (**Automatiska** eller **Reserv**)
- Användning av sekundärt mål
Det sekundära målet används om **Reserv**-läget används och det tilldelade primära målet misslyckas. Om det här alternativet är inaktiverat så stoppas inspelningen på alla målenheter som tilldelats det primära målet som misslyckades.
Om läget **Automatisk** används: om ett av målen misslyckas, så tilldelar VRM Server automatiskt om de tillhörande enheterna till andra lagringar. Om VRM Server ligger nere när ett mål misslyckas, stoppas inspelningen på de enheter som spelar in på det misslyckade målet.
- Blockreservation för stilleståndstid
- Sanitetskontrollperiod

Du kan ange att varje pool kan tillåta LUN-enheter som är större än 2 TB.

LUN-enheter större än 2 TB ("stora LUN-enheter") stöds inte av följande enheter:

- VRM-enheter före 3.60
- VSG-enheter med fast programvara före version 6.30

- Kodare med fast programvara före version 6.30
- BVMS gör att du inte kan göra följande:
- Lägga till eller flytta enheter med fast programvara före version 6.30 i en pool som tillåter stora LUN-enheter.
 - Lägga till eller flytta enheter som för närvarande inte är anslutna till nätverket till en pool som tillåter stora LUN-enheter.
 - Lägga till eller flytta en iSCSI-enhet som innehåller stora LUN-enheter till en pool som inte tillåter stora LUN-enheter.
 - Tillåta stora LUN-enheter i en pool som innehåller enheter med fast programvara före version 6.30.
 - Avaktivera stora LUN-enheter i en pool med en iSCSI-enhet som innehåller stora LUN-enheter.

Flytta enheter med fast programvara före version 6.30 till en pool som inte tillåter stora LUN-enheter.

Om en primär VRM har en pool som tillåter stora LUN-enheter, får motsvarande speglad VRM samma inställning och du kan inte markera eller avmarkera kryssrutan **Tillåt LUN:er som är större än 2 TB** i den speglade VRM:ens motsvarande pool. Om du har lagt till en iSCSI-enhet med stora LUN-enheter i en speglad VRM kan du inte avmarkera kryssrutan **Tillåt LUN:er som är större än 2 TB** på den primära VRM:ens motsvarande pool.

Se

- *Poolsidan, sidan 170*

12.25.2

Lägga till en iSCSI-enhet manuellt

Huvudfönster > **Enheter** >  > Utvidga  > Högerklicka på  > **Lägg till iSCSI-enhet** > Dialogrutan **Lägg till iSCSI-enhet**

Låter dig lägga till iSCSI-enheter i en VRM.

Lägga till en iSCSI-enhet:

1. Högerklicka på  och klicka på **Lägg till iSCSI-enhet**. Dialogrutan **Lägg till iSCSI-enhet** visas.
2. Skriv in önskat visningsnamn, nätverksadress till en iSCSI-enhet samt enhetstyp och klicka på **OK**.
iSCSI-enheten läggs till i den valda VRM-poolen.
Lägg till mål och LUN-enheter om vid behov.

Dialogrutan Lägg till iSCSI-enhet

Namn

Ange ett visningsnamn för enheten.

Nätverksadress

Skriv in en giltig nätverksadress för enheten.

iSCSI-enhetstyp

Välj lämplig enhetstyp.

Användarnamn

Skriv in användarnamnet för autentisering.

Lösenord

Skriv in lösenordet för autentisering.

Aktivera övervakning

Om en DIVAR IP-enhet är markerad som iSCSI-enhetstyp och all SNMP (Simple Network Management Protocol) övervakning stöds för den typen av DIVAR IP-enhet, **Aktivera övervakning** aktiveras kryssrutan.

Markera kryssrutan för att aktivera övervakning av hälsotillståndet på DIVAR IP-enheten. BVMS tar nu emot och analyserar automatiskt SNMP-meddelanden på DIVAR IP-enheten och aktiverar hälsoövervakningshändelser och larm (till exempel CPU, lagring, fläkt ...). Som standard utlöses endast kritiska larm.

Obs! Se till att konfigurera SNMP på DIVAR IP-enheten först.

Obs! Den här inställningen är endast tillgänglig för enheter som stöds.

Mer information om hur du konfigurerar SNMP på en DIVAR IP-enhet, se respektive DIVAR IP-dokumentation.

Närliggande ämnen

- *Lägga till VRM-enheter genom avsökning, sidan 161*

Se

- *Sidan RMon och Snmp, sidan 145*
- *Konfigurera SNMP-övervakning, sidan 91*

12.25.3

Lägga till en DSA E-Series iSCSI-enhet manuellt

Huvudfönster > **Enheter** >  > utvidga  > 

Du kan antingen lägga till en E-Series iSCSI-enhet som redan har initierats eller en som inte har initierats.

Du kan lägga till LUN-enheter större än 2 TB om poolen har aktiverats för stora LUN-enheter. LUN-enheter större än 2 TB ("stora LUN-enheter") stöds inte av följande enheter:

- VRM-enheter före 3.60
- VSG-enheter med fast programvara före version 6.30
- Kodare med fast programvara före version 6.30

BVMS gör att du inte kan göra följande:

- Lägga till eller flytta enheter med fast programvara före version 6.30 i en pool som tillåter stora LUN-enheter.
- Lägga till eller flytta enheter som för närvarande inte är anslutna till nätverket till en pool som tillåter stora LUN-enheter.
- Lägga till eller flytta en iSCSI-enhet som innehåller stora LUN-enheter till en pool som inte tillåter stora LUN-enheter.
- Tillåta stora LUN-enheter i en pool som innehåller enheter med fast programvara före version 6.30.
- Avaktivera stora LUN-enheter i en pool med en iSCSI-enhet som innehåller stora LUN-enheter.

Flytta enheter med fast programvara före version 6.30 till en pool som inte tillåter stora LUN-enheter.

Så här lägger du till en initierad iSCSI-enhet:

1. Högerklicka på  och klicka på **Lägg till DSA E-Series-enhet**. Dialogrutan **Lägg till DSA E-Series-enhet** visas.
2. Ange IP-adressen för hanteringen och lösenordet.
3. Klicka på **Anslut**

Om anslutningen upprättas fylls fälten i gruppen **Styrenhet** eller **2:a styrenhet** i.

4. Klicka på **OK**.
 Enheten läggs till i systemet.
 De tillgängliga målen skannas automatiskt och LUN-enheter visas.
 Du kan använda iSCSI-enheten.
 Om poolen har aktiverats för stora LUN-enheter och iSCSI-enheten har konfigurerats för stora LUN-enheter innehåller kolumnen **Stor LUN** en markering för de berörda LUN-enheterna.

Så här lägger du till en iSCSI-enhet som inte har initierats:

1. Högerklicka på  och klicka på **Lägg till DSA E-Series-enhet**.
 Dialogrutan **Lägg till DSA E-Series-enhet** visas.
2. Ange IP-adressen för hanteringen och lösenordet.
3. Klicka på **Anslut**
 Om anslutningen upprättas fylls fälten i gruppen **Styrenhet** eller **2:a styrenhet** i.
4. Klicka på **OK**.
 Enheten läggs till i systemet.
5. Klicka på  och sedan på .
6. Klicka på fliken **Grundkonfiguration**.
7. Ange önskad LUN-kapacitet.
 Om du skriver in ett värde större än 2 TB måste du aktivera din pool för LUN-enheter som är större än 2 TB.
8. Klicka på **Initiera**.
 LUN-enheterna skapas.
9. Klicka på **Stäng**.
10. Högerklicka på iSCSI-enheten och klicka sedan på **Sök efter mål**.
 LUN-enheterna visas med ett okänt tillstånd.
11. Spara och aktivera konfigurationen.
12. Formatera alla LUN-enheter.
13. Om du har lagt till en iSCSI-enhet med dubbel styrenhet tar du först bort önskade LUN-enheter från den första styrenheten. Högerklicka sedan på den andra styrenheten och lägg därefter till LUN-enheterna genom att klicka på **Sök efter mål**.

Dialogrutan Lägg till DSA E-Series-enhet

Huvudfönster > **Enheter** >  > Utvidga  > Högerklicka på  > **Lägg till DSA E-Series-enhet** > Dialogrutan **Lägg till DSA E-Series-enhet**

Används för att lägga till en DSA E-Series iSCSI-enhet. Den här enhetstypen har en IP-adress för hantering som skiljer sig från IP-adressen för iSCSI-lagringen. Via IP-adressen för hantering kan enheten upptäckas och konfigureras automatiskt.

Namn

Ange ett visningsnamn för enheten.

Hanteringsadress

Ange IP-adressen för automatisk konfigurerings av enheten.

Lösenord:

Ange enhetens lösenord.

DSA E-Series-typ

Visar enhetstypen.

Nätverksadress iSCSI-kanal

Visar IP-adressen för enhetens iSCSI-port. Du kan välja en annan IP-adress om en sådan finns tillgänglig.

Hanteringsadress

Visar IP-adressen för automatisk konfiguration av den andra styrenheten, om en sådan finns tillgänglig. Du kan välja en annan IP-adress om en sådan finns tillgänglig.

Nätverksadress iSCSI-kanal

Visar IP-adressen för iSCSI-porten på den andra styrenheten, om en sådan finns tillgänglig. Du kan välja en annan IP-adress om en sådan finns tillgänglig.

Anslut

Klicka här för att söka efter enhetens inställningar.

Om anslutningen upprättas fylls fälten i gruppen **Styrenhet** och gruppen **2:a styrenhet**.

Se

- *Sidan Standardkonfiguration, sidan 184*
- *Formatera ett LUN, sidan 188*

12.25.4**Konfigurera en iSCSI-enhet**

Huvudfönster > **Enheter** > utvidga  > utvidga  > 

Efter att du har lagt till VRM-enheter, iSCSI-enheter och kodare gör du följande för att säkerställa att kodarnas videodata lagras på iSCSI-enheterna eller för att hämta videodata från iSCSI-enheterna:

- Kör standardkonfigurationen för att skapa LUN-enheter på varje mål i iSCSI-enheten. Steget är valfritt. Du behöver inte utföra det här steget på en iSCSI-enhet med LUN-enheter förkonfigurerade.
- Sök igenom iSCSI-enheten för att lägga till mål och LUN-enheter i enhetsträdet efter standardkonfigurationen.

Obs!

Inte alla iSCSI-enheter stöder standardkonfigurationen och automatisk IQN mapping.

Grundkrav:

iSCSI-enheten måste konfigureras med giltiga IP-adresser.

Så här ställer du in grundkonfigurationen på en DSA E-Series iSCSI-enhet:

- Expandera lämplig VRM-enhet  och  och klicka sedan på lämplig iSCSI-enhet .

1. Klicka på fliken **Grundkonfiguration**.
2. Ange önskad LUN-kapacitet.
Om du skriver in ett värde större än 2 TB måste du aktivera din pool för LUN-enheter som är större än 2 TB.
3. Klicka på **Initiera**.
LUN-enheterna skapas.
4. Klicka på **Stäng**.
5. Högerklicka på iSCSI-enheten och klicka sedan på **Sök efter mål**.
LUN-enheterna visas med ett okänt tillstånd.
6. Spara och aktivera konfigurationen.
7. Formatera alla LUN-enheter.

- Om du har lagt till en iSCSI-enhet med dubbel styrenhet tar du först bort önskade LUN-enheter från den första styrenheten. Högerklicka sedan på den andra styrenheten och lägg därefter till LUN-enheterna genom att klicka på **Sök efter mål**.

Så här ställer du in grundkonfigurationen på andra iSCSI-enheter:

- Klicka på fliken **Grundkonfiguration**.
- Ange önskat antal LUN-enheter.
- Klicka på **Ställ in**.
LUN-enheterna skapas.
- Klicka på **Stäng**.
- Högerklicka på iSCSI-enheten och klicka sedan på **Sök efter mål**.
LUN-enheterna visas med ett okänt tillstånd.
- Spara och aktivera konfigurationen.
- Formatera alla LUN-enheter.

IQN-mappa för andra iSCSI-enheter så här:

- Expandera lämplig VRM-enhet  och  och klicka sedan på lämplig iSCSI-enhet .
- Högerklicka på  och välj **Kart-IQN**.
Dialogrutan iqn-Mapper visas och processen startas.
Kodarna som tilldelas de valda VRM-enheterna utvärderas och deras IQN:er läggs till i den här iSCSI-enheten.
- Klicka på  för att spara inställningarna.
- Klicka på  om du vill aktivera konfigurationen.

Se

- *Sidan Standardkonfiguration, sidan 184*
- *Dialogrutan Belastningsutjämning, sidan 185*
- *iqn-Mapper-dialogrutan, sidan 188*
- *Formatera ett LUN, sidan 188*

12.25.5

Sidan Standardkonfiguration

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  > klicka på  > fliken **Grundkonfiguration**

De visade alternativen kan variera beroende på vilken typ av iSCSI-lagringssystem som används.

Låter dig utföra en grundkonfiguration av iSCSI-enheten. Du skapar LUN-enheter på iSCSI-hårddisken och formaterar dessa LUN-enheter.

Visas bara om enheten är en av de iSCSI-lagringssystem som stöds av Bosch, t.ex. DSA eller DLS 1x00.

**Obs!**

Efter den grundläggande konfigurationen av en enhet i E-serien tar det flera timmar (eller till och med dagar) för systemet att starta. Under den här fasen är inte fullständiga prestanda tillgängliga, och i fas 1.5 kan formateringen misslyckas.

Fysisk kapacitet [GB]

Information om lagringssystemets totala kapacitet.

Antal LUN-enheter

Du kan ändra antalet LUN-enheter.

**Obs!**

Om du ändrar antalet LUN:er omorganiserar hela iSCSI-systemet och alla sekvenser som sparas på systemet går förlorade.

Innan du gör ändringar kontrollerar du därför inspelningarna och säkerhetskopierar viktiga sekvenser.

Kapacitet för nya LUN-enheter [GB]

Eftersom 256 är det maximala antalet LUN för en lagringsmatris bör LUN-storleken inte anges till ett för litet värde. Annars kan inga fler LUN skapas i framtiden, om ytterligare en hylla installeras.

Målreservdiskar

Antal reservdiskar som användaren vill att systemet ska ha.

Faktiska reservdiskar

Antalet reservdiskar som finns i systemet för närvarande. Det här antalet kan skilja sig från antalet ovan, till exempel om lagringssystemet har konfigurerats om manuellt eller om det finns trasiga diskar.

Initieringsstatus (%)

Ytterligare information visas under initieringen. När initieringen är klar (100 %), får du också möjligheten att ta bort alla LUN-enheter igen.

RAID-DP (tillförlitlighet fokuserad)

Aktivera det här alternativet om du inte vill använda den angivna RAID-typen RAID-4, utan i stället använda den mer tillförlitliga RAID-typen RAID-DP.

RAID 6 (tillförlitlighet fokuserad)

Välj det här alternativet om du inte vill använda den angivna RAID-typen RAID 5, utan i stället använda den mer tillförlitliga RAID-typen RAID 6.

Ytterligare information

Ytterligare information visas, till exempel information om att lagringssystemet inte har konfigurerats på rätt sätt och att ingen installation därför kan utföras.

Se

– *Lägga till en DSA E-Series iSCSI-enhet manuellt, sidan 181*

12.25.6**Dialogrutan Belastningsutjämning**

Huvudfönster > **Enheter** > Utvidga  > Utvidga  > Utvidga  > Högerklicka på  > Kommandot **Belastningsutjämnar ...** > Dialogrutan **Belastningsutjämning**

Förutsättning: Läget för **automatisk** inspelning har konfigurerats.

Ange den övre gränsen för tillåten bithastighet och antalet samtidiga iSCSI-anslutningar för varje iSCSI-system. Om dessa gränser överskrids skrivs inga data längre till iSCSI-systemet och förloras.

Använd standardvärden för system som stöds (till exempel Bosch RAID, NetApp, DLA). Mer information om andra enheter finns i dokumentationen för respektive enhet. Börja testa med små värden.

12.25.7

Flytta ett iSCSI-system till en annan pool (Ändra pool ...)

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  > 

Du kan flytta en enhet från en pool till en annan inom samma VRM-enhet utan att någon inspelning går förlorad.

Så här gör du för att flytta:

1. Högerklicka på  /  /  och klicka på **Ändra pool ...**.
Dialogrutan **Ändra pool** visas.
2. Välj önskad pool i listan **Ny pool:**.
3. Klicka på **OK**.
Enheten flyttas till vald pool.

12.25.8

Sidan för LUN-enheter

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  > expandera  > 

Gör att du kan lägga till, ta bort och formatera LUN-enheter, och visa information om LUN-enheterna.

Lägg till

Klicka för att visa dialogrutan **Lägg till LUN**.

Ta bort

Klicka för att ta bort de valda raderna. Välj en rad genom att klicka på radrubriken till vänster. Varje rad representerar LUN-enhet. En meddelanderuta visas.

Formatera LUN

Klicka när du vill formatera den valda LUN-enheten. En meddelanderuta visas.

Format

Markera kryssrutan när du vill välja LUN-enheten och klicka sedan på **Formatera LUN**.

LUN

Visar LUN-enhetens namn.

Storlek [GB]

Visar LUN-enhetens maximala kapacitet.

Stor LUN

Varje cell visar om det här är en LUN-enhet som är större än 2 TB.

Tillstånd

Visar LUN-enhetens status.

Förlopp

Visar formateringsprocessens förlopp.

Se

- *Poolsidan, sidan 170*
- *Lägga till LUN, sidan 187*
- *Lägga till VRM-enheter genom avsökning, sidan 161*

12.25.9

Lägga till LUN

Huvudfönster > **Enheter** > utvidga  > utvidga  > 

Oftast lägger nätverkssökningen automatiskt till önskade iSCSI-enheter med deras mål och LUN. Om nätverkssökningen inte fungerade korrekt eller om du vill konfigurera iSCSI-enheten offline innan den integreras i nätverket kan du konfigurera målet i iSCSI-enheten och på detta mål konfigurerar du ett eller flera LUN.

Du kan lägga till LUN-enheter större än 2 TB om poolen har aktiverats för stora LUN-enheter. LUN-enheter större än 2 TB ("stora LUN-enheter") stöds inte av följande enheter:

- VRM-enheter före 3.60
- VSG-enheter med fast programvara före version 6.30
- Kodare med fast programvara före version 6.30

BVMS gör att du inte kan göra följande:

- Lägg till eller flytta enheter med fast programvara före version 6.30 i en pool som tillåter stora LUN-enheter.
- Lägg till eller flytta enheter som för närvarande inte är anslutna till nätverket till en pool som tillåter stora LUN-enheter.
- Lägg till eller flytta en iSCSI-enhet som innehåller stora LUN-enheter till en pool som inte tillåter stora LUN-enheter.
- Tillåta stora LUN-enheter i en pool som innehåller enheter med fast programvara före version 6.30.
- Avaktivera stora LUN-enheter i en pool med en iSCSI-enhet som innehåller stora LUN-enheter.

Flytta enheter med fast programvara före version 6.30 till en pool som inte tillåter stora LUN-enheter.

Så här lägger du till:

1. Markera **Tillåt LUN:er som är större än 2 TB** vid behov.

2. Högerklicka på  och klicka på **Sök efter mål**.

Målet  läggs till.

3. Klicka på målet.
Sidan **LUN-enheter** visas.

4. Klicka på **Lägg till**.
Dialogrutan **Lägg till LUN** visas.

5. Skriv in ett LUN-nummer och klicka på **OK**.
LUN-enheten läggs till som en ny rad i tabellen.
Upprepa det här steget för varje LUN-enhet.

Obs!

- Klicka på **Ta bort** om du vill ta bort ett LUN.
Videodata finns kvar på detta LUN.

- Klicka på **Formatera LUN** om du vill formatera ett LUN.
Alla data på detta LUN tas bort!

Dialogrutan Lägg till LUN

Huvudfönster > **Enheter** > utvidga  > utvidga  > utvidga  > utvidga  >  > klicka på **Lägg till**
Låter dig lägga till ett LUN.

Id

Ange ID för önskat LUN.

Se

- *Poolsidan, sidan 170*
- *Sidan för LUN-enheter, sidan 186*

12.25.10

Formatera ett LUN

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  > expandera  > 

Du förbereder ett LUN för den första användningen genom att formatera det.



Obs!

All data på detta LUN går förlorad vid formateringen.

Så här konfigurerar du:

1. Välj önskad LUN och klicka för att markera i kolumnen **Format**.
2. Klicka på **Formatera LUN**.
3. Läs det visade meddelande noga och bekräfta vid behov.
Vald LUN-enhet formateras. Alla data på LUN-enheten går förlorade.

Se

- *Sidan för LUN-enheter, sidan 186*

12.25.11

iqn-Mapper-dialogrutan

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  >  > **Kart-IQN**
Låter dig starta IQN-mappningsprocessen.

Se

- *Lägga till VRM-enheter genom avsökning, sidan 161*
- *Konfigurera en iSCSI-enhet, sidan 183*

12.26

Sidan Video Streaming Gateway-enhet

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  > 

I det här kapitlet ges information om hur du konfigurerar VSG-enheten i systemet.

Gör att du kan lägga till och konfigurerar följande kodartyper:

- Kodare från Bosch
- ONVIF-kodare
- JPEG-kodare
- RTSP-kodare

Så här lägger du till VSG-enheter genom avsökning:

1. Högerklicka på  och klicka på **Sök efter Video Streaming Gateways**. Dialogrutan **BVMS Scan Wizard** visas.
2. Välj de VSG-enheter som krävs, välj önskad VRM-pool och klicka på **Tilldela** för att tilldela dem till poolen.
3. Klicka på **Nästa >>**. Dialogrutan **Autentisera enheter** i guiden visas.
4. Ange lösenordet för varje enhet som skyddas med ett lösenord. Lösenordskontrollen sker automatiskt om du inte skriver något i lösenordsfältet inom ett par sekunder, eller om du klickar utanför lösenordsfältet. Om samtliga enheter har samma lösenord kan du ange det i det första **Lösenord**-fältet. Högerklicka sedan på detta fält och klicka på **Kopiera cell till kolumn**.

I kolumnen **Status** anges lyckade inloggningar med .

Misslyckade inloggningsförsök anges med .

5. Klicka på **Slutför**. Enheten läggs till i enhetsträdet.

Om du lägger till en ny VSG-version 7.0 eller senare är kryssrutan **Säker anslutning** markerad som standard.

Om du vill ändra säker eller osäker anslutning använder du kommandot **Redigera Video Streaming Gateway** och markerar eller avmarkerar kryssrutan **Säker anslutning**.

Se

- *Redigera Video Streaming Gateway, sidan 191*
- *Sidan ONVIF, sidan 220*

12.26.1

Lägga till en Video Streaming Gateway manuellt

Huvudfönster > **Enheter** > Utvidga  > 

Du kan lägga till VSG-enheter i en VRM-pool.

Lägga till en VSG-enhet manuellt:

1. Högerklicka på  och klicka på **Lägg till Video Streaming Gateway**. Dialogrutan **Lägg till Video Streaming Gateway** visas.
2. Gör nödvändiga inställningar för din VSG-enhet.
3. Klicka på **Lägg till**.
 - ✓ VSG-enheten läggs till i systemet. De kameror som den här VSG-enheten har tilldelats spelas in.

Dialogrutan Lägga till Video Streaming Gateway

Högerklicka på dialogrutan  > **Lägg till Video Streaming Gateway** > **Lägg till Video Streaming Gateway**

Namn

Ange ett önskat visningsnamn för enheten.

Användarnamn

Skriv in användarnamnet som används för autentisering på enheten. Vanligtvis: service

Nätverksadress/port

Skriv in enhetens IP-adress.

Om kryssrutan **Säker anslutning** är markerad ändras porten automatiskt till HTTPS-porten.

Du kan ändra portnumret om inga standardportar används eller om VSG-instanserna konfigureras i en annan ordning.

Standardportar

VSG-instans	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

Lösenord

Skriv in lösenordet för autentisering på enheten.

Show password

Klicka här om du vill att det angivna lösenordet ska visas. Var försiktig så att ingen obehörig kan se lösenordet.

Säkerhet

Kryssrutan **Säker anslutning** är markerad som standard, om HTTPS stöds.

Från VSG-version 7.0 har VSG stöd för säker anslutning.



Obs!

Om du migrerar till BVMS-version 10.0 och senare är kryssrutan **Säker anslutning** inte markerad som standard och anslutningen är osäker (rcpp).

Om du vill ändra säker eller osäker anslutning använder du kommandot **Redigera Video Streaming Gateway** och markerar eller avmarkerar kryssrutan **Säker anslutning**.

Test

Verifiera dig på enheten med de uppgifter som angavs ovan.

Se

- *Redigera Video Streaming Gateway, sidan 191*

12.26.2

Redigera Video Streaming Gateway

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  > 

Så här ändrar du säker/osäker anslutning:

1. Högerklicka på .
2. Klicka på **Redigera Video Streaming Gateway**.
Dialogrutan **Redigera Video Streaming Gateway** visas.
3. Markera kryssrutan **Säker anslutning**.
Den använda porten ändras automatiskt till HTTPS-porten.
Eller
avmarkera kryssrutan **Säker anslutning**.
Den använda porten ändras automatiskt till rcpp-porten.

**Obs!**

När du har uppgraderat till en nyare version rekommenderar vi att du ändrar till säker anslutning.

Se

- *Lägga till en Video Streaming Gateway manuellt, sidan 189*

12.26.3

Lägga till en kamera för en VSG-enhet

Huvudfönster > **Enheter** > Utvidga  > Utvidga  > Utvidga  > 

Du kan lägga till följande enheter för VSG-enheten:

- Kodare från Bosch
- ONVIF-kameror
- JPEG-kameror
- RTSP-kodare

Om du lade till VSG-kodare offline kan du uppdatera deras tillstånd.

Så här lägger du till:

1. Högerklicka på , peka på **Lägg till kodare/kamera** och klicka på önskat kommando.
2. Gör nödvändiga inställningar i dialogrutan för att lägga till enheten.
3. Klicka på **OK**.

Enheten läggs till.

Så här uppdaterar du:

- ▶ Högerklicka på den aktuella kodaren och välj **Uppdatera tillståndet**.
Enhetens egenskaper hämtas.

Se

- *Dialogrutan Lägg till kodare från Bosch, sidan 192*
- *Dialogrutan Lägg till ONVIF-kodare, sidan 193*
- *Dialogrutan Lägg till JPEG-kameror, sidan 194*
- *Dialogrutan Lägg till RTSP-kodare, sidan 195*

12.26.4

Dialogrutan Lägga till kodare från Bosch

Huvudfönster > **Enheter** > Utvidga  > Utvidga  > Utvidga  > Högerklicka på



> **Lägg till kodare/kamera** > Kommandot **Kodare från Bosch**

Du kan lägga till en kodare från Bosch för VSG-enheten.

Namn

Ange ett önskat visningsnamn för enheten.

Nätverksadress

Ange enhetens nätverksadress.

Typ

Visar den identifierade enhetstypen, om den stöds.

Användarnamn

Skriv in användarnamnet som används för autentisering på enheten. Vanligtvis: service

Lösenord

Skriv in lösenordet för autentisering på enheten.

Show password

Klicka här om du vill att det angivna lösenordet ska visas. Var försiktig så att ingen obehörig kan se lösenordet.

Test

Verifiera dig på enheten med de uppgifter som angavs ovan.

Egenskaper

Klicka här för att aktivera önskade funktioner som är tillgängliga för enheten.

Ljud	Klicka för att aktivera ljudet om enheten kan tillhandahålla ljud.
PTZ	Klicka för att aktivera PTZ om enheten kan tillhandahålla det.
Kameraprotokoll	TCP Används för överföring via Internet och/eller för förlustfri dataöverföring. Säkerställer att inga datapaket förloras. Bandbreddskraven kan vara höga. Använd om enheten finns bakom en brandvägg. Stöder inte multicast. UDP Används för anslutningsfri och smidig dataöverföring i privata nätverk. Datapaket kan förloras. Bandbreddskraven kan vara låga. Stöd för multicast.
Använd videoingång 1 – Använd videoingång 4	Klicka här för att välja videoingångarna om du konfigurerar en flerkanalsenhet.

Se

- *Lägga till en kamera för en VSG-enhet, sidan 191*

12.26.5

Dialogrutan Lägg till ONVIF-kodare

Huvudfönster > **Enheter** > Utvidga  > Utvidga  > Utvidga  > Högerklicka på  > **Lägg till kodare/kamera** > Kommandot **Lägg till ONVIF-kodare** eller

Huvudfönster > **Enheter** > Högerklicka på  > kommandot **Lägg till ONVIF-kodare**

Du kan lägga till en ONVIF-kodare i din VSG-enhet eller som en livekodare.

Du måste konfigurera profilen som används för inspelning och livebilder i kameratabellen.

Från BVMS 10.0 kan ONVIF-kodarhändelser hämtas från VSG- eller ONVIF-kodaren direkt. Om du lägger till en ny ONVIF-kodare är kryssrutan **hämta ONVIF-händelser från VSG (Profil S, T)** markerad som standard och profil T stöds.

Följande funktioner stöds endast om en ONVIF-kodare läggs till i systemet via en VSG-enhet:

- Om ONVIF-kodarhändelser hämtas från VSG är standard-ONVIF-händelser redan mappade.
- Operatören kan slå på eller av reläer i Operator Client.



Obs!

Det går bara att hämta ONVIF-händelser från VSG från VSG version 7.0. Om du migrerar till BVMS version 10.0 hämtas befintliga ONVIF-kodarhändelser från ONVIF-kodaren direkt. Du måste uppdatera VSG till version 7.0.

Namn

Ange ett önskat visningsnamn för enheten.

Nätverksadress/port

Ange enhetens nätverksadress. Ändra portnumret om det behövs.

Användarnamn

Skriv in användarnamnet som används för autentisering på enheten. Vanligtvis: service

Lösenord

Skriv in lösenordet för autentisering på enheten.

Show password

Klicka här om du vill att det angivna lösenordet ska visas. Var försiktig så att ingen obehörig kan se lösenordet.

Test

Verifiera dig på enheten med de uppgifter som angavs ovan.

Säker anslutning

Du kan aktivera säker anslutning för en live-video som överförs från en ONVIF-kodare till din VSG-enhet.

Obs!

När den är aktiverad kan användaren av Operator Client inte byta en ström till UDP och UDP-multicast.

När den är aktiverad fungerar inte ANR för den berörda enheten.

När den är aktiverad fungerar inte kodaråteruppspelning på kodare med fast programvara före version 6.30.

**Obs!**

Port 443 är inställd som standard. Du kan redigera portnumret så att det matchar den konfigurerade HTTPS-porten på kodaren.
Det konfigurerade portnumret glöms.

Egenskaper

Enhetstyp	Visar den hämtade enhetstypen.
Tillverkare	Visar det hämtade namnet på tillverkaren.
Modell	Visar det hämtade namnet på modellen.
Version av fast programvara	Visar vilken version av fast programvara som har hämtats.
Extrakommandon	Om kryssrutan är markerad stöds extrakommandon.
Antal videoingångskanaler	Ange antalet önskade videoingångar.
Antal ljudingångskanaler	Ange antalet önskade ljudingångar.
Antal larmingångar	Ange antalet önskade larmingångar.
Antal reläer	Ange antalet önskade reläer.
Tilldelade gateway-kanaler	Ange antalet önskade gatewaykanaler.
Kameraprotokoll	Välj önskat kameraprotokoll.
Använd videoingång {0}	Markera kryssrutan för att använda lämplig videoingång.
ONVIF-profil	Om det finns stöd för det väljer du den profil som du vill konfigurera.

**Obs!**

Alternativen för **Inställningar för Video Streaming Gateway** är inte tillgängliga för ONVIF-kodare som läggs till som endast live-kodare.

Se

– *Lägga till en kamera för en VSG-enhet, sidan 191*

12.26.6**Dialogrutan Lägg till JPEG-kameror**

Huvudfönster > **Enheter** > Utvidga  > Utvidga  > Utvidga  > Högerklicka på



> **Lägg till kodare/kamera** > Kommandot **JPEG-kamera**

Du kan lägga till en JPEG-kamera i VSG-enheten.

Namn

Ange ett önskat visningsnamn för enheten.

URL

Ange JPEG-kamerans/RTSP-kamerans URL.

Ange följande sträng för en JPEG-kamera från Bosch:

`http://<ip-address>/snap.jpg?jpegCam=<channel_no.>`

Ange följande sträng för en RTSP-kamera från Bosch:

`rtsp://<ip-address>/rtsp_tunnel`

Användarnamn

Skriv in användarnamnet som används för autentisering på enheten. Vanligtvis: service

Lösenord

Skriv in lösenordet för autentisering på enheten.

Show password

Klicka här om du vill att det angivna lösenordet ska visas. Var försiktig så att ingen obehörig kan se lösenordet.

Test

Verifiera dig på enheten med de uppgifter som angavs ovan.

Egenskaper

Antal videoingångskanaler	Ange antalet tillgängliga videoingångar.
Bildrutefrekvens [bilder/s]	Ange den önskade bildrutehastigheten.

Se

– *Lägga till en kamera för en VSG-enhet, sidan 191*

12.26.7

Dialogrutan Lägg till RTSP-kodare

Huvudfönster > **Enheter** > Utvidga  > Utvidga  > Utvidga  > Högerklicka på



> **Lägg till kodare/kamera** > Kommandot **RTSP-kamera**

Du kan lägga till en RTSP-kodare i VSG-enheten.

Namn

Ange ett önskat visningsnamn för enheten.

URL

Ange JPEG-kamerans/RTSP-kamerans URL.

Ange följande sträng för en JPEG-kamera från Bosch:

`http://<ip-address>/snap.jpg?jpegCam=<channel_no.>`

Ange följande sträng för en RTSP-kamera från Bosch:

`rtsp://<ip-address>/rtsp_tunnel`

Användarnamn

Skriv in användarnamnet som används för autentisering på enheten. Vanligtvis: service

Lösenord

Skriv in lösenordet för autentisering på enheten.

Show password

Klicka här om du vill att det angivna lösenordet ska visas. Var försiktig så att ingen obehörig kan se lösenordet.

Test

Verifiera dig på enheten med de uppgifter som angavs ovan.

Egenskaper

Antal videoingångskanaler	Ange antalet tillgängliga videoingångar.
----------------------------------	--

Se

- *Lägga till en kamera för en VSG-enhet, sidan 191*

12.26.8**Flytta en VSG till en annan pool (Ändra pool)**

Huvudfönster > **Enheter** > Utvidga  > Utvidga  >  > 

Du kan flytta en enhet från en pool till en annan inom samma VRM-enhet utan att någon inspelning går förlorad.

Så här gör du för att flytta:

1. Högerklicka på  /  /  och klicka på **Ändra pool ...**.
Dialogrutan **Ändra pool** visas.
2. Välj önskad pool i listan **Ny pool:**.
3. Klicka på **OK**.
Enheten flyttas till vald pool.

12.26.9**Konfigurera multicast (fliken Multicast)**

Huvudfönster > **Enheter** > Utvidga  > Utvidga  > Utvidga  > 

För varje kamera som tilldelas till en Video Streaming Gateway-enhet kan du konfigurera en multicastadress och port.

Konfigurera multicast:

1. Markera önskad kryssruta för att aktivera multicast.
2. Skriv in en giltig multicastadress och ett portnummer.
3. Om det behövs konfigurerar du fortlöpande multicaststreaming.

Fliken Flersändning (multicasting)

Huvudfönster > **Enheter** > utvidga  > utvidga  > utvidga  >  > fliken

Nätverk > fliken Flersändning (multicasting)

Här kan du konfigurera multicast för de tilldelade kamerorna.

Aktivera

Klicka för att aktivera multicast för den här kameran.

Multicast-adress

Infoga en giltig multicast-adress (i intervallet 224.0.0.0 - 239.255.255.255).

Ange 1.0.0.0. En unik multicast-adress infogas automatiskt baserat på enhetens MAC-adress.

Port

När en brandvägg används anger du ett portvärde som är konfigurerat som en oblockerad port i brandväggen.

Strömmande

Klicka för att aktivera kontinuerlig multicast-strömning till växeln. Det innebär att multicast-anslutningen inte föregås av en RCP+-registrering. Kodaren strömmar alltid alla data till växeln. Växeln skickar i sin tur (om ingen IGMP-multicastfiltrering stöds eller är konfigurerad) dessa data till alla portar, med resultatet att växeln svämmar över.

Du behöver strömning när du använder en icke-Bosch-enhet för att ta emot en multicast-ström.

12.26.10

Konfigurera loggning (fliken Avancerat)

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  >  > fliken **Service** > fliken **Avancerad**

Här kan du aktivera loggning för Video Streaming Gateway.

Loggfilerna lagras normalt under följande sökväg:

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

Från VSG version 7.0 lagras loggfilerna normalt under följande sökväg:

```
C:\ProgramData\Bosch\VSG\log
```

Obs! Om du uppgraderar till VSG 7.0 eller senare flyttas tidigare loggfiler automatiskt till den här platsen.

Loggfiler från äldre VSG-versioner lagras vanligtvis under följande sökväg:

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

Fliken Avancerad

RCP+-loggning

Klicka här för att aktivera RCP+-loggning.

Felsökningsloggning

Klicka här för att aktivera felsökningsloggning.

RTP-loggning

Klicka här för att aktivera RTP-loggning.

Kvarhållningstid (dagar):

Välj önskat antal dagar.

Fullständig minnesdumpningsfil

Välj endast den här kryssrutan om det är nödvändigt, till exempel om, om den tekniska supporten begär en fullständig sammanställning av huvudminnet.

Telnet-stöd

Välj den här kryssrutan om åtkomst med Telnet-protokollet ska stödjas. Välj enbart om det är nödvändigt.



Obs!

Omfattande loggning kräver betydande processorkraft och hårddiskutrymme. Använd inte omfattande loggning kontinuerligt.

12.26.11

Starta ONVIF Camera Event Driver Tool från Configuration Client

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  > 

Du kan starta ONVIF Camera Event Driver Tool direkt från Configuration Client för de valda VSG.

Obs! Du kan också starta verktyget från Start-menyn i Windows.

ONVIF Camera Event Driver Tool gör att du kan mappa ONVIF händelser till VSG BVIP-händelser. Du kan ansluta till ONVIF-kameror och hämta ONVIF-händelserna för mappning.

Så här startar du ONVIF Camera Event Driver Tool från Configuration Client:

1. Högerklicka på lämplig VSG.

2. Klicka på **Starta ONVIF Camera Event Driver Tool**.
ONVIF Camera Event Driver Tool visas.

**Obs!**

ONVIF Camera Event Driver Tool har bara stöd för säker anslutning till VSG.

Så här använder ONVIF Camera Event Driver Tool:

Se [Hur man video](#).

12.27**Sidan Endast live**

Huvudfönster > **Enheter** > Utvidga > >

Gör att du kan lägga till och konfigurera kodare som används för endast live. Du kan lägga till Bosch-kodare och videosändare för ONVIF-nätverk.

Läs mer om hur du lägger till, redigerar och konfigurerar en endast live-ONVIF-kodare här:
Sidan ONVIF, sidan 220.

Se

- *Lägga till en kodare för endast live video, sidan 206*
- *Söka efter enheter, sidan 70*
- *Sidan Bosch-kodare/-avkodare/-kamera, sidan 204*
- *Sidan ONVIF, sidan 220*
- *Konfigurera multicast, sidan 218*

12.27.1**Lägga till live-enheter från Bosch genom avsökning**

Så här lägger du till live-enheter från Bosch genom avsökning:

1. Högerklicka på och klicka på **Sök efter endast live-kodare**.
Dialogrutan **BVMS Scan Wizard** visas.
2. Markera önskade kryssrutor för de enheter som du vill lägga till.
3. Klicka på **Nästa >>**.
Dialogrutan **Autentisera enheter** i guiden visas.
4. Ange lösenordet för varje enhet som skyddas med ett lösenord.
Lösenordskontrollen sker automatiskt om du inte skriver något i lösenordsfältet inom ett par sekunder, eller om du klickar utanför lösenordsfältet.
Om samtliga enheter har samma lösenord kan du ange det i det första **Lösenord**-fältet.
Högerklicka sedan på detta fält och välj **Kopiera cell till kolumn**.

I kolumnen **Status** indikeras lyckade inloggningsförsök med .
Misslyckade inloggningsförsök indikeras med .
5. Klicka på **Slutför**.
Enheten läggs till i enhetsträdet.

-ikonen anger ett fel som du måste åtgärda. Mer information om det specifika felet finns i knappbeskrivningen.

12.27.2

Lägga till en kodare/avkodare manuellt

Huvudfönster > **Enheter** > Utvidga  > Utvidga  > Högerklicka  > Klicka på **Lägg till kodare** > dialogrutan **Lägg till kodare** eller

Huvudfönster > **Enheter** > Högerklicka  > Klicka på **Lägg till kodare** > dialogrutan **Lägg till kodare** eller

Huvudfönster > **Enheter** > Högerklicka  > Klicka på **Lägg till kodare** > dialogrutan **Lägg till kodare** eller

Huvudfönster > **Enheter** > Utvidga  > Högerklicka på  > Klicka på **Lägg till avkodare** > dialogrutan **Lägg till kodare**

Här kan du lägga till en kodare eller avkodare manuellt. Detta är särskilt användbart när du vill lägga till en Video IP-enhet från Bosch (endast för VRM).

Obs!

För att du ska kunna lägga till en Video IP-kodare eller -avkodare från Bosch med alternativet **<Upptäck automatiskt>** måste enheten finnas i nätverket.

Så här lägger du till en Video IP-enhet från Bosch:

1. Utvidga , utvidga , högerklicka på ,
eller
högerklicka på ,
eller
högerklicka på .
2. Klicka på **Lägg till kodare**.
Dialogrutan **Lägg till kodare** visas.
3. Ange IP-adressen.
4. Välj **<Upptäck automatiskt>** i listan.
5. Klicka på **OK**.
Enheter läggs till i systemet.

-ikonen anger ett fel som du måste åtgärda. Mer information om det specifika felet finns i knappbeskrivningen.

Dialogrutan Lägg till kodare**IP-adress:**

Ange en giltig IP-adress.

Kodartyp:/Avkodartyp:

För en enhet med känd enhetstyp väljer du lämplig post. Enheten behöver inte vara tillgänglig i nätverket.

Om du vill lägga till en Video IP-enhet från Bosch väljer du **<Upptäck automatiskt>**. Enheten måste vara tillgänglig i nätverket.

Om du vill lägga till en kamera för offlinekonfiguration väljer du **<Enkel platshållarkamera>**.

12.27.3

Ange mållösenord för en avkodare (Autentisera ...)

Huvudfönster > **Enheter** > utvidga  > utvidga  > högerklicka på  > klicka på **Autentisera...** > dialogrutan **Ange lösenord**

För att aktivera en lösenordsskyddad kodares åtkomst till en avkodare måste du ange lösenordet för kodarens användarbehörighetsnivå som mållösenord i avkodaren.

Gör så här:

1. I listan **Ange användarnamn** väljer du destination password.
2. I fältet **Ange lösenord för användare** skriver du det nya lösenordet.
3. Klicka på **OK**.
- ✓ Lösenordet ändras på enheten direkt.

Se

- *Ändra lösenordet för en kodare/avkodare (Byt lösenord/Ange lösenord), sidan 135*

12.28

Sidan Lokal lagring

Huvudfönster > **Enheter** > utvidga  > 

Medger tillägg och konfigurering av kodare med lokal lagring.

Så här lägger du till kodare för lokal lagring genom avsökning:

1. Högerklicka på  i enhetsträdet och klicka på **Sök efter kodare med lokal lagring**. Dialogrutan **BVMS Scan Wizard** visas.
2. Markera önskade kryssrutor för de enheter som du vill lägga till.
3. Klicka på **Nästa >>**. Dialogrutan **Autentisera enheter** i guiden visas.
4. Ange lösenordet för varje enhet som skyddas med ett lösenord. Lösenordskontrollen sker automatiskt om du inte skriver något i lösenordsfältet inom ett par sekunder, eller om du klickar utanför lösenordsfältet. Om samtliga enheter har samma lösenord kan du ange det i det första **Lösenord**-fältet. Högerklicka sedan på detta fält och välj **Kopiera cell till kolumn**.

I kolumnen **Status** indikeras lyckade inloggningsförsök med .

Misslyckade inloggningsförsök indikeras med .

5. Klicka på **Slutför**. Enheten läggs till i enhetsträdet.

-ikonen anger ett fel som du måste åtgärda. Mer information om det specifika felet finns i knappbeskrivningen.

Se

- *Konfigurera multicast, sidan 218*
- *Lägga till en kodare för lokal lagring, sidan 206*
- *Sidan Bosch-kodare/-avkodare/-kamera, sidan 204*
- *Söka efter enheter, sidan 70*

12.29

Sidan Unmanaged Site

Huvudfönster > **Enheter** > utvidga



Du kan lägga till en videonätverksenhet i **Unmanaged Sites**-objektet i enhetsträdet.

Det förutsätts att alla ohanterade nätverksenheter i en unmanaged site finns i samma tidszon.

Platsnamn

Visar namnet på den plats som angavs när det här objektet skapades.

Beskrivning

Skriv in en beskrivning för detta site.

Tidszon

Välj en tidszon för unmanaged site.

Se

- *Unmanaged site, sidan 25*
- *Lägga till en unmanaged site manuellt, sidan 201*
- *Importera ohanterade platser, sidan 201*
- *Konfigurera tidszonen, sidan 203*

12.29.1

Lägga till en unmanaged site manuellt

Huvudfönster > **Enheter** >



Så här skapar du:

1. Högerklicka på  och klicka på **Lägg till Unmanaged Site**. Dialogrutan **Lägg till Unmanaged Site** visas.
2. Ange ett webbplatsnamn och en beskrivning.
3. Välj ett värde i listan **Tidszon**.
4. Klicka på **OK**.
En ny unmanaged site läggs till i systemet.

Se

- *Unmanaged site, sidan 25*
- *Sidan Unmanaged Site, sidan 201*

12.29.2

Importera ohanterade platser

Huvudfönster > **Enheter** >



Du kan importera en CSV-fil som innehåller en konfiguration av en DVR-enhet eller en annan BVMS som du vill importera i din BVMS som en ohanterad plats.

Så här importerar du:

1. Högerklicka på  och klicka på **Importera Unmanaged Sites**.
2. Klicka på önskad fil och klicka på **Öppna**.
En eller flera ohanterade platser läggs till i systemet.
Nu kan du lägga till dessa ohanterade platser i det logiska trädet.
Obs! Om det uppstår ett fel och det inte går att importera filen visas ett felmeddelande.

12.29.3

Sidan Unmanaged Site**Platsnamn**

Visar namnet på den plats som angavs när det här objektet skapades.

Beskrivning

Skriv in en beskrivning för detta site.

Tidszon

Välj en tidszon för unmanaged site.

12.29.4

Lägga till en ohanterad nätverksenhet

Huvudfönster > **Enheter** >  > 

1. Högerklicka på objektet och klicka sedan på **Lägg till ohanterad nätverksenhet**.

Dialogrutan **Lägg till ohanterad nätverksenhet** visas.

2. Välj önskad enhetstyp.
3. Ange en giltig IP-adress eller ett giltigt värddamn och inloggningsuppgifter för enheten.
4. Klicka på **OK**.

En ny **Unmanaged nätverksenhet** läggs till i systemet.

Nu kan du lägga till denna unmanaged site i det logiska trädet.

Observera att endast platsen visas i det logiska trädet, men inte nätverksenheter som hör till den här platsen.

5. Skriv användarnamnet för den här nätverksenheten, om det är tillgängligt.
6. Skriv lösenordet, om det är tillgängligt.

Dialogrutan Lägg till ohanterad nätverksenhet

Huvudfönster > **Enheter** > Utvidga  > Högerklicka på  > Klicka på **Lägg till ohanterad nätverksenhet**

Enhetstyp:

Markera den post som gäller för den här enheten.

Tillgängliga poster:

- **DIVAR AN / DVR**
- **DIVAR IP 3000/7000 / BVMS**
- **Bosch IP-kamera/kodare**

Nätverksadress:

Ange en IP-adress eller ett värddamn. Ändra portnumret om det behövs.

Obs! Om du använder en SSH-anslutning anger du adressen i följande format:

ssh://IP eller servernamn:5322

Säkerhet

Kryssrutan **Säker anslutning** är markerad som standard.

**Obs!**

Om du lägger till DVR och kryssrutan **Säker anslutning** är markerad, är kommando- och kontrollanslutningarna säkra. Strömning av videodata är inte säker.

Användarnamn:

Skriv användarnamnet för den här nätverksenheten, om det är tillgängligt. Se *Unmanaged site, sidan 25* för mer information.

Lösenord:

Skriv lösenordet, om det är tillgängligt. Se *Unmanaged site, sidan 25* för information om användarbehörighet.

Se

- *Unmanaged site, sidan 25*

12.29.5**Konfigurera tidszonen**

Huvudfönster > **Enheter** > utvidga  > 

Du kan konfigurera tidszonen för en unmanaged site. Detta är användbart när en användare av Operator Client vill få åtkomst till en unmanaged site med hjälp av en dator med Operator Client som finns i en annan tidszon än denna unmanaged site.

Så här konfigurerar du tidszon:

- ▶ Välj ett värde i listan **Tidszon**.

Se

- *Sidan Unmanaged Site, sidan 201*

13

Sidan Bosch-kodare/-avkodare/-kamera

I det här kapitlet ges information om hur du konfigurerar kodarna och avkodarna i systemet.

**Obs!**

BVMS Viewer stöder inte avkodarenheter.

Du hittar mer detaljerad information om kodarens, avkodarens eller kamerans inställningar, till exempel Video Content Analysis (VCA), eller nätverksinställningar i handboken för motsvarande enhet.

Antalet objekt nedanför en post visas inom hakparenteser.

Så här konfigurerar du en kodare:

Huvudfönster > **Enheter** > utvidga > utvidga > >

eller

Huvudfönster > **Enheter** > Utvidga > Utvidga > Utvidga > >

eller

Huvudfönster > **Enheter** > >

eller

Huvudfönster > **Enheter** > >

Konfigurera en avkodare:

Huvudfönster > **Enheter** > Utvidga > Utvidga >

På -sidorna i onlinehjälpn finns mer information.

Konfigurera en kamera:

Huvudfönster > **Enheter** > utvidga > utvidga > >

Huvudfönster > **Enheter** > Utvidga > Utvidga > > >

eller

Huvudfönster > **Enheter** > Utvidga > Utvidga > Utvidga > >

eller

Huvudfönster > **Enheter** > > >

eller

Huvudfönster > **Enheter** > > >

– Klicka på för att spara inställningarna.

– Klicka på om du vill ångra den senaste inställningen.



- Klicka på för att aktivera konfigurationen.

De flesta av inställningarna på sidorna för kodare/avkodare/kamera är aktiva omedelbart efter



att du klickar på . Om du klickar på en annan flik utan att klicka på och ändringar har gjorts, visas två motsvarande meddelanderutor. Bekräfta dem båda om du vill spara. Ändra lösenord för en kodare genom att högerklicka på enhetsikonen och klicka på **Byt lösenord...**

Visa enheten i en webbläsare genom att högerklicka på enhetsikonen och klicka på **Visa webbsidan i webbläsaren**.

Obs!

Beroende på vald kodare eller kamera är inte alla sidorna som beskrivs här tillgängliga för alla enheter. Ordalydelsen som används här för att beskriva fältnamn kan avvika från din programvara.

- Klicka på en flik för att visa motsvarande egenskapssida.

Så här lägger du till kodare genom avsökning:



1. Högerklicka på och klicka på **Sök efter kodare**. Dialogrutan **BVMS Scan Wizard** visas.
2. Välj de kodare som krävs, välj önskad VRM-pool och klicka på **Tilldela** för att tilldela dem till poolen.
3. Klicka på **Nästa >>**. Dialogrutan **Autentisera enheter** i guiden visas.
4. Ange lösenordet för varje enhet som skyddas med ett lösenord. Lösenordskontrollen sker automatiskt om du inte skriver något i lösenordsfältet inom ett par sekunder, eller om du klickar utanför lösenordsfältet. Om samtliga enheter har samma lösenord kan du ange det i det första **Lösenord**-fältet. Högerklicka sedan på detta fält och välj **Kopiera cell till kolumn**.



I kolumnen **Status** indikeras lyckade inloggningsförsök med .



Misslyckade inloggningsförsök indikeras med .

5. Klicka på **Slutför**. Enheten läggs till i enhetsträdet.

⚠-ikonen anger ett fel som du måste åtgärda. Mer information om det specifika felet finns i knappbeskrivningen.

Se

- *Söka efter enheter, sidan 70*

13.1

Lägga till en kodare till en VRM-pool

Läs mer om att lägga till kodare i en VRM-pool här: *Lägga till kodare genom avsökning, sidan 169*.

Se

- *Lägga till en enhet, sidan 118*

13.2 Lägga till en kodare för endast live video

Läs mer om att lägga till en endast live-kodare här: *Lägga till live-enheter från Bosch genom avsökning, sidan 198.*

Se

- *Lägga till en enhet, sidan 118*
- *Sidan Endast live, sidan 198*

13.3 Lägga till en kodare för lokal lagring

Läs mer om att lägga till kodare för lokal lagring genom avsökning här: *Sidan Lokal lagring, sidan 200*

Se

- *Lägga till en enhet, sidan 118*
- *Sidan Lokal lagring, sidan 200*

13.4 Lägga till en kamera med en enda platshållare

Om du vill lägga till och konfigurera en kamera som för närvarande är offline kan du lägga till kamera med en enda platshållare istället. Du kan lägga till kameran med en enda platshållare i det logiska trädet för att mappa och konfigurera händelser och larm.

Så här lägger du till en kamera med en enda platshållare

1. Högerklicka på enhetsträdeobjektet där du vill lägga till platshållarkameran.
2. Klicka på **Lägg till kodare**.
Dialogrutan **Lägg till kodare** visas.
3. Ange en tillhörande IP-adress som för närvarande är offline.
4. Välj kodartypen **<Enkel platshållarkamera>**.
5. Konfigurera alla lämpliga inställningar för platshållarkameran.

Så här ersätter du en kamera med en enda platshållare

1. Högerklicka på respektive platshållarkamera.
2. Klicka på **Redigera kodare**.
Dialogrutan **Redigera kodare** visas.
3. Ange ersättningskamerans nätverksadress.
4. Ange rätt lösenord för ersättningskameran.
5. Klicka på **OK**.
Dialogrutan **Uppdaterar enhetsnamn** visas.
6. Klicka på **OK**.

Obs! När ersättningskamerans enhetsfunktioner är uppdaterade måste du kontrollera inställningarna du gjorde i tabellen för kameror och inspelningar.

13.5 Redigera en kodare

13.5.1 Kryptering av live-video (Redigera kodare)

Huvudfönster > **Enheter** > Utvidga  > Utvidga  > Utvidga  > Klicka på  > dialogrutan **Redigera kodare**

Huvudfönster > **Enheter** > Utvidga  > Högerklicka på  > dialogrutan **Redigera kodare**

Huvudfönster > **Enheter** > Utvidga  > Klicka på  > dialogrutan **Redigera kodare**

Du kan aktivera den säkra anslutningen av en live-video som överförs från en kodare till följande enheter om HTTPS-port 443 är konfigurerad på kodaren:

- Operator Client-dator
- Management Server-dator
- Configuration Client-dator
- VRM-dator
- Avkodare

Obs!

När den är aktiverad fungerar inte ANR för den berörda enheten.

När den är aktiverad fungerar inte kodaråteruppspelning på kodare med fast programvara före version 6.30.

Endast kodare med version 7.0 av den fasta programvaran eller senare har stöd för säker UDP. Om en säker anslutning har aktiverats i det här fallet kan användaren av Operator Client växla en ström till UDP och till UDP-multicast.

Aktivera så här:

1. Markera kryssrutan **Säker anslutning**.
2. Klicka på **OK**.

Säker anslutning har aktiverats för den här kodaren.

Se

- *Konfigurera multicast, sidan 218*
- *Dialogruta för redigering av kodare/avkodare, sidan 208*

13.5.2

Uppdatera enhetsfunktioner (Redigera kodare)

Huvudfönster > **Enheter** > utvidga  > utvidga  > utvidga  > högerklicka på

 > klicka på **Redigera kodare** > dialogrutan **Redigera kodare**
eller

Huvudfönster > **Enheter** > Utvidga  > Högerklicka på  > Klicka på **Redigera kodare** > Dialogrutan **Redigera kodare**
eller

Huvudfönster > **Enheter** > Utvidga  > Högerklicka på  > Klicka på **Redigera kodare** > Dialogrutan **Redigera kodare**
eller

Huvudfönster > **Enheter** > Utvidga  > Utvidga  > Högerklicka  > Klicka på **Redigera avkodare** > dialogrutan **Redigera avkodare**

När enheten har uppgraderats kan du uppdatera enhetsfunktionerna. Ett meddelande informerar om de hämtade enhetsfunktionerna stämmer med enhetsfunktionerna som finns sparade i BVMS.

Uppdatera:

1. Klicka på **OK**.

En meddelanderuta med följande text visas:

Om du tillämpar enhetsfunktionerna kan det hända att inspelningsinställningarna och händelseinställningarna för enheten ändras. Kontrollera inställningarna för enheten.

2. Klicka på **OK**.

Enhetsfunktionerna uppdateras.

Se

- Dialogruta för redigering av kodare/avkodare, sidan 208

13.5.3**Dialogruta för redigering av kodare/avkodare**

Huvudfönster > **Enheter** > utvidga  > utvidga  > utvidga  > högerklicka på

 > klicka på **Redigera kodare** > dialogrutan **Redigera kodare**
eller

Huvudfönster > **Enheter** > Utvidga  > Högerklicka på  > Klicka på **Redigera kodare** > Dialogrutan **Redigera kodare**
eller

Huvudfönster > **Enheter** > Utvidga  > Högerklicka på  > Klicka på **Redigera kodare** > Dialogrutan **Redigera kodare**
eller

Huvudfönster > **Enheter** > Utvidga  > Utvidga  > Högerklicka  > Klicka på **Redigera avkodare** > dialogrutan **Redigera avkodare**

Gör att du kan kontrollera och uppdatera en enhets funktioner. När du öppnar dialogrutan ansluts enheten. Lösenordet kontrolleras och enhetens enhetsfunktioner jämförs med de enhetsfunktioner som finns sparade i BVMS.

Namn

Visar enhetens namn. När du lägger till en Video IP-enhet från Bosch genereras ett enhetsnamn. Ändra posten om det behövs.

Nätverksadress/port

Ange enhetens nätverksadress. Ändra portnumret om det behövs.

Användarnamn

Visar det användarnamn som används för verifiering på enheten.

Lösenord

Ange lösenordet för autentisering på enheten.

Visa lösenord

Klicka här om du vill att det angivna lösenordet ska visas. Var försiktig så att ingen obehörig kan se lösenordet.

Autentisera

Verifiera dig på enheten med de uppgifter som angavs ovan.

Säkerhet

Kryssrutan **Säker anslutning** är markerad som standard.

Om det inte går att ansluta via en säker anslutning, visas ett meddelande. Klicka för att ta bort markeringen.

Följande avkodare har stöd för säker anslutning:

- VJD 7000
- VJD 8000
- VIP XD HD



Obs!

Anslutningen mellan en avkodare och en kodare är bara säker om båda har konfigurerats med säker anslutning.

Videoström

UDP: Aktiverar krypterad multicast-strömning för avkodarenheter som stöds.

TCP: Aktiverar krypterad unicast-strömning för avkodarenheter som stöds.

Ons! Om ingen multicast-adress har konfigurerats för en kodare hämtar avkodaren strömmen via unicast.



Obs!

BVMS stöder inte Bosch kameror anslutna till en VSG.

BVMS stöder endast UDP-kryptering för plattformar äldre än CPP13.

Enhetsfunktioner

Du kan sortera visningen av enhetsfunktionerna i bokstavsordning eller efter kategori. Ett meddelande anger om de upptäckta enhetsfunktionerna stämmer med de aktuella enhetsfunktionerna.

Klicka på **OK** om du vill använda de ändrade enhetsfunktionerna efter det att enheten har uppgraderats.

Se

- *Kryptering av live-video (Redigera kodare), sidan 206*
- *Uppdatera enhetsfunktioner (Redigera kodare), sidan 207*

13.6

Hantera autentiseringskontroll

Så här aktiverar du en kodares autentiseringskontroll:

- Konfigurera autentiseringen på kodaren.
- Hämta ett certifikat från kodaren.
- Installera kodarcertifikatet på arbetsstationen som används till autentiseringskontrollen.

Se

- *Kontroll av äkthet , sidan 209*

13.6.1

Kontroll av äkthet

Användaren av Operator Client kan verifiera inspelningarnas äkthet. Exportautentiseringen görs automatiskt.

Administratören måste följa de här stegen för att kunna säkerställa ett obrutet certifikat. För större system (över 30 kameror) rekommenderar vi följande:

- Låt certifieringsorganisationen utfärda ett certifikat för varje kodare.
- Ladda upp det utfärdade certifikatet (inklusive den privata nyckeln) på ett säkert sätt på varje kodare.

- Installera certifieringsorganisationens certifikat på de Operator Client-arbetsstationer där du vill genomföra autentiseringskontroll, eller på andra datorer där du vill genomföra exporter.

För små system (färre än 30 kameror) rekommenderar vi följande:

- Hämta *HTTPS Server*-certifikatet från varje kodare.
- Installera certifikaten på de Operator Client-arbetsstationer där du vill utföra verifieringskontroll.

Mer information får du av ditt företags IT-support.

Administratören måste göra följande för att kunna aktivera en säker kontroll av äktheten:

- Aktivera autentiseringen på varje önskad kamera.
- För större system: överför och tilldela certifikat till varje önskad kamera.
- För små system: hämta ett certifikat från varje kodare. Installera certifikatet som möjliggör kontroll på en arbetsstation.

Begränsningar

Fast programvara version 6.30 eller senare krävs.

Vi rekommenderar att verifiera äktheten på maximalt fyra kameror åt gången.

En användare av Operator Client kan inte verifiera äktheten på en livevideo.

Obs! Ändra inte certifikatet när inspelningen pågår. Om du behöver ändra certifikatet ska du först stoppa inspelningen, sedan ändra certifikatet och därefter starta inspelningen igen.

En inspelnings äkthet kontrolleras genom att inspelningen spelas upp i en bakgrundsprocess med maximal hastighet. I nätverk med låg bandbredd kan uppspelningen blir långsam.

Verifieringen kan sedan ta så lång tid som den valda verifieringstiden. Exempel: Du väljer en tidsperiod på en timme. Verifieringen kan ta så lång tid som en timme.

Användaren kan endast verifiera att en inspelning är autentiskt. Om verifieringen inte lyckas, behöver det inte innebära att videon har manipulerats. Det kan finnas många andra orsaker, exempelvis en manuell borttagning. Användaren av Operator Client kan inte skilja mellan en avsiktlig, tillåten ändring och en otillåten manipulering av inspelningen.

Videoautentisering gäller bara metoder för verifiering av en videos äkthet. Videoautentisering gäller inte överföring av video eller data på något sätt.

Vattenstämpelfunktionen för verifiering av äkthet i tidigare BVMS-versioner ersätts. Den nya äkthetskontroll blir automatiskt tillgänglig efter uppgraderingen den senaste BVMS-versionen. Äkthetskontroller som tidigare lyckades, kan nu inte verifieras eftersom inspelningarna inte innehåller den nödvändiga informationen.

Verifiering av äkthet stöds inte i följande fall:

- Omkodning
- Lokal inspelning
- VSG
- Digital videoinspelare
- Bosch Recording Station
- ANR

Se

- *Konfigurera autentisering, sidan 210*
- *Ladda upp ett certifikat, sidan 211*
- *Hämta ett certifikat, sidan 211*
- *Installera ett certifikat på en arbetsstation, sidan 211*

13.6.2

Konfigurera autentisering

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  > 

eller

Huvudfönster > **Enheter** > utvidga  > 

Du kan aktivera autentiseringskontrollen på en kodare.

Så här konfigurerar du:

1. Klicka på **Kamera** och klicka sedan på **Videoingång**.
2. Gå till listan **Videoverifiering** och välj **SHA-256**.
3. Välj ett värde i listan **Signaturintervall**.
Ett lågt värde ökar säkerheten, ett högt värde minskad belastning på kodaren.

4. Klicka på  .

13.6.3

Ladda upp ett certifikat

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  > 

eller

Huvudfönster > **Enheter** > utvidga  > 

Du kan ladda upp ett härlett certifikat till en kodare.

Ladda upp så här:

1. Klicka på **Service** och klicka sedan på **Certifikat**.
2. Klicka på **Ladda upp certifikat**.
3. Välj filen som innehåller certifikatet för den här kodaren. Filen måste innehålla den privata nyckeln, till exempel *.pem.
Kontrollera att dataöverföringen är säker.
4. Klicka på **Öppna**.
5. Välj **HTTPS-server** i listan **Användning** för att kunna koppla det uppladdade certifikatet till posten för **HTTPS-server**.
6. Klicka på  .

13.6.4

Hämta ett certifikat

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  > 

eller

Huvudfönster > **Enheter** > utvidga  > 

Du kan hämta en certifikat från en kodare.

Hämta så här:

1. Klicka på **Service** och klicka sedan på **Certifikat**.
 2. Välj certifikatet och klicka på ikonen *Save*.
 3. Välj en katalog där certifikatfilen ska sparas.
 4. Byt namn på certifikatfilens filtyp till *.cer.
- Nu kan du installera certifikatet på arbetsstationen där du vill göra autentiseringskontrollen.

13.6.5

Installera ett certifikat på en arbetsstation

Du kan installera certifikatet som du hämtade från en kodare på en arbetsstation där du vill utföra en autentiseringskontroll.

1. Starta *Microsoft Management Console* på arbetsstationen.

2. Lägga till *Certificates* -sna-pinmodulen på datorn och markera alternativet *Computer account*.
3. Utvidga *Certificates (Local computer)*, utvidga *Trusted Root Certification Authorities*.
4. Högerklicka på *Certificates*, peka på *All Tasks* och klicka sedan på *Import... Certificate Import Wizard* visas.
Alternativet *Local Machine* är markerat och går inte att ändra.
5. Klicka på *Next*.
6. Välj certifikatfilet du hämtade från kodaren.
7. Klicka på *Next*.
8. Ändra inga inställningar. Klicka på *Next*.
9. Ändra inga inställningar. Klicka på *Finish*.

13.7

Ange mållösenord för en avkodare (Autentisera ...)

Huvudfönster > **Enheter** > utvidga  > utvidga  > högerklicka på  > klicka på **Autentisera...** > dialogrutan **Ange lösenord**

För att aktivera en lösenordsskyddad kodares åtkomst till en avkodare måste du ange lösenordet för kodarens användarbehörighetsnivå som mållösenord i avkodaren.

Gör så här:

1. I listan **Ange användarnamn** väljer du destination password.
 2. I fältet **Ange lösenord för användare** skriver du det nya lösenordet.
 3. Klicka på **OK**.
- ✓ Lösenordet ändras på enheten direkt.

Se

- Ändra lösenordet för en kodare/avkodare (Byt lösenord/Ange lösenord), sidan 212

13.8

Ändra lösenordet för en kodare/avkodare (Byt lösenord/Ange lösenord)

Huvudfönster > **Enheter** > utvidga  > utvidga  >  > 
eller

Huvudfönster > **Enheter** >  > 
eller

Huvudfönster > **Enheter** >  > 
eller

Huvudfönster > **Enheter** > Utvidga  > Utvidga  > 

Definiera och ändra ett separat lösenord för varje nivå. Ange lösenordet (högst 19 tecken och inga specialtecken) för den valda nivån.

Så här ändrar du lösenord:

1. Högerklicka på  och klicka på **Byt lösenord....**
Dialogrutan **Ange lösenord** visas.
2. Välj användaren du vill ändra lösenordet för i listan **Ange användarnamn**.
3. Skriv det nya lösenordet i fältet **Ange lösenord för användare**.

4. Klicka på **OK**.
- ✓ Lösenordet ändras på enheten direkt.

Ett lösenord förhindrar obehörig åtkomst till enheten. Du kan använda olika behörighetsnivåer för att begränsa åtkomsten.

Korrekt lösenordsskydd kan endast garanteras när även alla behörigheter på högre nivå är skyddade av lösenord. När du ska tilldela lösenord måste du därför alltid börja på den högsta behörighetsnivån.

Du kan ange och ändra ett lösenord för varje behörighetsnivå när du har loggat in på användarkontot service.

Enheten har tre behörighetsnivåer: service, user och live.

- service är högsta behörighetsnivån. När du har angett korrekt lösenord har du tillgång till alla funktioner och kan ändra alla konfigurationsinställningar.
- user är mellanbehörighetsnivån. På den här nivån kan du till exempel manövrera enheten, spela upp inspelningar och styra kameran men du kan inte ändra konfigurationen.
- live är lägsta behörighetsnivån. På den här nivån kan du endast visa videobilder och växla mellan olika live-bildskärmar.

För en avkodare ersätter följande behörighetsnivå behörighetsnivån live:

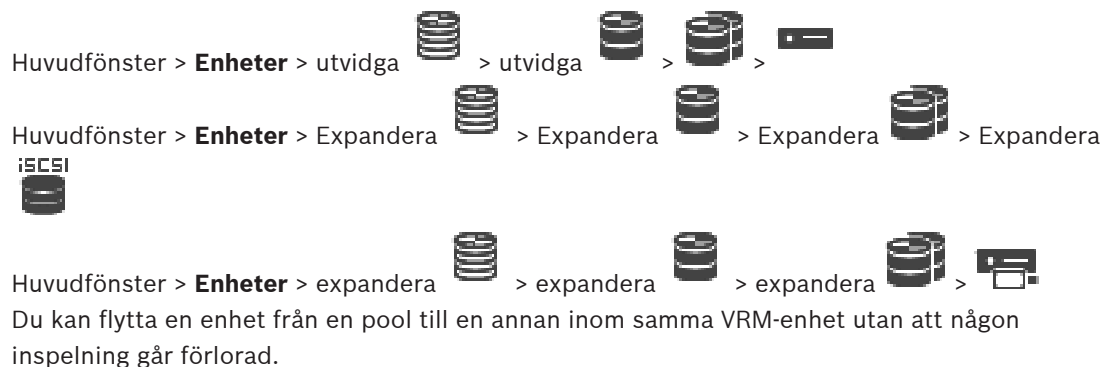
- destination password (endast tillgänglig för avkodare)
Används för åtkomst till en kodare.

Se

- *Ange mållösenord för en avkodare (Autentisera ...), sidan 212*

13.9

Flytta en kodare till en annan pool (Ändra pool)



Så här gör du för att flytta:

1. Högerklicka på / / och klicka på **Ändra pool**
Dialogrutan **Ändra pool** visas.
2. Välj önskad pool i listan **Ny pool:.**
3. Klicka på **OK**.
Enheten flyttas till vald pool.

Dialogrutan Ändra pool

Här kan du ändra en enhets pooltilldelning.

Aktuell pool:

Visar numret på den pool som den valda enheten för tillfället är tilldelad till.

Ny pool:

Välj önskat poolnummer.

13.10 Återställa inspelningar från en utbytt kodare (Associera med inspelningar på tidigare enhet)

Huvudfönster > **Enheter** > Utvidga  > Utvidga  >  > 

Om du behöver byta en defekt kodare är inspelningarna från den utbytta kodaren tillgängliga för den nya kodaren när du väljer den nya kodaren i Operator Client.



Obs!

En kodare kan endast bytas ut mot en kodare med samma antal kanaler.

Så här återställer du inspelningar från en utbytt kodare



Obs!

Använd inte kommandot **Redigera kodare**.

1. Högerklicka på kommandot  > **Associera med inspelningar från föregångaren**
2. Dialogrutan **Associera med inspelningar från föregångaren ...** visas.
3. Ange nätverksadressen och ett giltigt lösenord för den nya enheten.
4. Klicka på **OK**.

5. Klicka på  för att spara inställningarna.

6. Klicka på  för att aktivera konfigurationen.

Dialogrutan Associera med inspelningar från föregångaren ...

Du kan återställa inspelningar från en kodare som bytts ut. När du har konfigurerat inställningarna i dialogrutan är inspelningarna från den utbytta kodaren tillgängliga för den nya kodaren när du väljer den nya kodaren i Operator Client.

Nätverksadress/port

Ange enhetens nätverksadress.

Användarnamn

Visar det användarnamn som används för verifiering på enheten.

Lösenord

Ange lösenordet för autentisering på enheten.

Autentisera

Autentisera på enheten med de uppgifter som angavs ovan.

13.11 Konfigurera kodare/avkodare

13.11.1 Konfigurera lagringsmediet för en kodare

Huvudfönster > **Enheter** > Utvidga  > Utvidga  >  >  > **Avancerade inställningar** > **Inspelningshantering**

Obs! Kontrollera att önskade kameror för kodaren har lagts till i det logiska trädet.

Du måste konfigurera lagringsmediet för en kodare för att kunna använda ANR-funktionen.

Obs! Om du vill konfigurera lagringsmediet för en kodare som redan har lagts till i systemet och spelas in via VRM, ser du till att den andra inspelningen stoppas:

The screenshot shows the 'Recording' configuration page in the BVMS interface. The 'Secondary Recording' section is expanded, showing settings for a secondary storage target. The 'Preferred storage target type' is set to 'SD card'. The 'Address' field contains '172.31.22.52', and the 'Status' shows '98% of 14.75 GB in use'. A red circle highlights the 'Add' button next to the address field. The 'Retention time [days]' is set to 'Auto'.

ANR-funktionen fungerar bara på kodare med fast programvara av version 5.90 eller senare. Alla kodartyper har inte stöd för ANR även om rätt version är installerad.

Konfigurera lagringsmediet för en kodare:

1. Välj lagringsmediet under **Sekundär inspelning** i listan **Önskad lagringstyp**. Olika medier är tillgängliga beroende på enhetstyp.
2. Om det behövs, klickar du på knappen ... och formaterar mediet.
När formateringsprocessen är klar, är lagringsmediet klart för användning med ANR-funktionen.
3. Konfigurera ANR-funktionen för den här kodaren på sidan **Kameror och inspelning**.

Se

- Sidan *Inspelningshantering*, sidan 217
- Konfigurera ANR-funktionen, sidan 282

13.11.2

Konfigurera flera kodare / avkodare

Huvudfönster

Du kan ändra följande egenskaper för flera kodare och avkodare på samma gång:

- Enhetslösenord
- IP-adresser
- Visningsnamn
- Nätmask
- Gateway-ID
- Version av fast programvara

Så här väljer du flera enheter:

- Markera de nödvändiga enheterna genom att trycka på CTRL- eller SKIFT-tangenten.

Så här väljer du alla tillgängliga enheter:

- Klicka på kommandot  **Markera allt.**

Så här ändrar du lösenord för flera enheter:

1. I huvudfönstret **Enheter** klickar du på kommandot  **Ändra enhetslösenord**.
Eller
på menyn **Maskinvara** klickar du på **Ändra enhetslösenord ...**
Dialogrutan **Ändra enhetslösenord** visas.
2. Välj enheterna.
3. Högerklicka på de valda enheterna.
4. Klicka på **Redigera lösenordet** Dialogrutan **Byta lösenord** visas.
5. Gör lämpliga inställningar.

**Obs!**

Du kan endast välja de lösenordstyper som är tillgängliga för alla valda enheter.

Konfigurera flera visningsnamn:

1. På **Maskinvara**-menyn klickar du på **Ändra enhetens IP- och nätverksinställningar**
Dialogrutan **Ändra enhetens IP- och nätverksinställningar** visas.
2. Välj enheterna.
3. Högerklicka på de valda enheterna.
4. Klicka på **Ställ in visningsnamn**.
Dialogrutan **Ställ in visningsnamn** visas.
5. Gör lämpliga inställningar.

Konfigurera flera IP-adresser:**Obs!**

Om du ändrar IP-adressen för en IP-enhet kan den bli oåtkomlig.

1. På **Maskinvara**-menyn klickar du på **Ändra enhetens IP- och nätverksinställningar**
Dialogrutan **Ändra enhetens IP- och nätverksinställningar** visas.
2. Välj enheterna.
3. Högerklicka på de valda enheterna.
4. Klicka på **Ange IP-adresser**
Dialogrutan **Ställ in nya IP-adresser** visas.
5. Gör lämpliga inställningar.

Så här ändrar du subnätmask/gateway-ID för flera enheter:

1. Klicka i det obligatoriska fältet för en av enheterna som du vill ändra värdet för.
2. Ange lämpligt värde.
3. Välj alla nödvändiga enheter.
4. Högerklicka på det obligatoriska fältet för enheten som du redan har ändrat värdet för.
5. Klicka på kommandot **Kopiera cell till** och kommandot **Urval i kolumn**.
Eller klicka på kommandot **Fullständig kolumn**, om det behövs.

**Obs!**

Du kan även kopiera hela rader för att ändra IP-adresser, visningsnamn, subnätmasker och gateway-ID:n för flera enheter.

Uppdatera fast programvara för flera enheter:

1. På menyn **Maskinvara** klickar du på **Uppdatera enhetens fasta programvara**
Dialogrutan **Uppdatera enhetens fasta programvaravisas.**
2. Välj enheterna.
3. Klicka på kommandot **Uppdatera den fasta programvaran.**
4. Välj den fil som innehåller uppdateringen.
5. Klicka på **OK.**

Åtgärdsresultat

Visar rätt status för de enheter som påverkas.

13.11.3**Konfigurera reservinspelningsläge på en kodare**

Huvudfönster > **Enheter** > utvidga  > utvidga  >  > 

förutsättningar: På sidan **Pool** i listan **Läge för inspelningsinställning** väljer du **Reserv.** Om du väljer **Automatiskt** görs inställningarna automatiskt och går inte att konfigurera.

Om du vill använda ett sekundärt mål för både automatiskt läge och reservläge: På sidan **Pool** i listan **Användning av sekundärt mål** väljer du **På.**

Vi rekommenderar att du konfigurerar minst två iSCSI-enheter för reservläget.

Så här konfigurerar du:

1. Klicka på **Avancerade inställningar.**
 2. Klicka på **Inspelningsinställningar.**
 3. Under **Primärt mål** väljer du posten för önskat mål. Alla lagringssystem som finns angivna under **Lagringssystem** visas då i listan.
 4. Under **Sekundärt mål** väljer du posten för önskat mål. Alla lagringssystem som anges under **Lagringssystem** visas i listan.
- Ändringarna börjar omedelbart att gälla. Någon aktivering behövs inte.

Närliggande ämnen

- *Konfigurera automatiskt inspelningsläge för en pool, sidan 172*

13.11.4**Sidan Inspelningshantering**

Aktiva inspelningar indikeras av

Peka på ikonen. Detaljerad information om de aktiva inspelningarna visas.

Inspelningar hanteras manuellt

Inspelningarna hanteras lokalt på kodaren. Alla relevanta inställningar måste utföras manuellt. Kodaren/IP-kameran används endast för direktsändning. Den ska inte tas bort från VRM automatiskt.

Inspelning 1 hanteras av VRM

Inspelningarna i kodaren hanteras av systemet VRM.

Dubbel VRM

Kodarens 2:a inspelning hanteras av en sekundär VRM.

Fliken iSCSI-medium

Klicka här för att visa den tillgängliga iSCSI-lagringen som är ansluten till kodaren.

Fliken Lokalt medium

Klicka här för att visa den tillgängliga lokala lagringen på kodaren.

Lägg till

Klicka här för att lägga till en lagringsenhet i listan över hanterade lagringsmedier.

Ta bort

Klicka här för att ta bort en lagringsenhet från listan över hanterade lagringsmedier.

Se

– *Konfigurera lagringsmediet för en kodare, sidan 214*

13.11.5**Sidan Recording preferences**

Sidan **Inspelningsinställningar** visas för varje kodare. Fliken visas endast om enheten tilldelats till ett VRM-system.

Primärt mål

Visas endast om listan **Inspelningsinställningsläge** på sidan **Pool** är inställd på **Reserv**.

Välj posten för det önskade målet.

Sekundärt mål

Visas endast om listan **Inspelningsinställningsläge** på sidan **Pool** är inställd på **Reserv** och om listan **Användning av sekundärt mål** är inställd på **På**.

Välj posten för det önskade målet för att konfigurera reservläget.

Se

– *Poolsidan, sidan 170*

13.12**Konfigurera multicast**

För varje tilldelad kamera kan du konfigurera en multicast-adress med port.

Konfigurera multicast:

1. Markera önskad kryssruta för att aktivera multicast.
2. Skriv in en giltig multicastadress och ett portnummer.
3. Om det behövs konfigurerar du fortlöpande multicaststreaming.

Fliken Flersändning (multicasting)

Huvudfönster > **Enheter** >  >  eller

Huvudfönster > **Enheter** >  >  eller

Huvudfönster > **Enheter** > utvidga  > utvidga  >  > 

> fliken **Nätverk** > fliken **Flersändning (multicasting)**

Här kan du konfigurera multicast för de tilldelade kamerorna.

Aktivera

Klicka för att aktivera multicast för den här kameran.

Multicast-adress

Infoga en giltig multicast-adress (i intervallet 224.0.0.0 - 239.255.255.255).

Ange 1.0.0.0. En unik multicast-adress infogas automatiskt baserat på enhetens MAC-adress.

Port

När en brandvägg används anger du ett portvärde som är konfigurerat som en oblockerad port i brandväggen.

Strömmande

Klicka för att aktivera kontinuerlig multicast-strömning till växeln. Det innebär att multicast-anslutningen inte föregås av en RCP+-registrering. Kodaren strömmar alltid alla data till växeln. Växeln skickar i sin tur (om ingen IGMP-multicastfiltrering stöds eller är konfigurerad) dessa data till alla portar, med resultatet att växeln svämmar över.

Du behöver strömning när du använder en icke-Bosch-enhet för att ta emot en multicast-ström.

**Obs!**

Fleranvändarströmmar är endast säkra om kodaren har fast programvara version 7.0 eller senare och kryssrutan **Säker anslutning** är markerad.

Se

- *Kryptering av live-video (Redigera kodare), sidan 206*

14 Sidan ONVIF

Huvudfönster > **Enheter** > expandera  > 

eller

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  > expandera  > 

Se

- Sidan Video Streaming Gateway-enhet, sidan 189
- Sidan Endast live, sidan 198

14.1 Lägga till en endast live-ONVIF-enhet genom avsökning

Så här lägger du till endast live-ONVIF-enheter genom avsökning:

1. Högerklicka på  och klicka på **Sök efter endast live-ONVIF-kodare**. Dialogrutan **BVMS Scan Wizard** visas.
2. Markera önskade kryssrutor för de enheter som du vill lägga till.
3. Klicka på **Nästa >>**. Dialogrutan **Autentisera enheter** i guiden visas.
4. Ange lösenordet för varje enhet som skyddas med ett lösenord. Lösenordskontrollen sker automatiskt om du inte skriver något i lösenordsfältet inom ett par sekunder, eller om du klickar utanför lösenordsfältet. Om samtliga enheter har samma lösenord kan du ange det i det första **Lösenord**-fältet. Högerklicka sedan på detta fält och klicka på **Kopiera cell till kolumn**.

I kolumnen **Status** anges lyckade inloggningar med .

Misslyckade inloggningsförsök anges med .

5. Klicka på **Slutför**. Enheten läggs till i enhetsträdet.

14.2 Sidan ONVIF-kodare

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  > expandera  >  > Fliken **ONVIF-kodare**

eller

Huvudfönster > **Enheter** > expandera  >  > Fliken **ONVIF-kodare**

Visar information om en ONVIF-kodare som endast används live och som har lagts till i BVMS.

Namn

Visar namnet på ONVIF-enheten. Du kan byta namn på den direkt i enhetsträdet.

Nätverksadress

Visar enhetens IP-adress.

Tillverkare

Visar tillverkarens namn.

Modell

Visar modellens namn.

Videoingångar

Ange antalet kameror som är anslutna till den här kodaren.

Ljudingångar

Ange antalet ljudingångar som är anslutna till den här kodaren.

Larmingångar

Ange antalet larmingångar som är anslutna till den här kodaren.

Reläer

Ange antalet reläer som är anslutna till den här kodaren.

Se

- *Sidan ONVIF-kodarthändelser, sidan 221*
- *Lägga till en kodare för endast live video, sidan 206*
- *Konfigurera en ONVIF-mappningstabell, sidan 225*

14.3**Sidan ONVIF-kodarthändelser**

Från BVMS 10.0 kan ONVIF-kodarthändelser hämtas från VSG- eller ONVIF-kodaren direkt. Om du lägger till en ny ONVIF-kodare är kryssrutan **hämta ONVIF-händelser från VSG (Profil S, T)** markerad som standard och profil T stöds.

Följande funktioner stöds endast om en ONVIF-kodare läggs till i systemet via en VSG-enhet:

- Om ONVIF-kodarthändelser hämtas från VSG är standard-ONVIF-händelser redan mappade.
- Operatören kan slå på eller av reläer i Operator Client.

**Obs!**

Det går bara att hämta ONVIF-händelser från VSG från VSG version 7.0. Om du migrerar till BVMS version 10.0 hämtas befintliga ONVIF-kodarthändelser från ONVIF-kodaren direkt. Du måste uppdatera VSG till version 7.0.

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  > expandera

 >  > Fliken **ONVIF-kodarthändelser**
eller

Huvudfönster > **Enheter** > expandera  >  > Fliken **ONVIF-kodarthändelser**
Du måste mappa ONVIF-händelser till BVMS-händelser om ONVIF-kodarthändelser hämtas från ONVIF-kodaren direkt. Detta garanterar att du längre fram kan konfigurera ONVIF-händelser som BVMS-larm.

**Obs!**

Om ONVIF-kodarthändelser hämtas från VSG är standard-ONVIF-händelser redan mappade.

Mappningstabell

Du kan skapa eller redigera en mappningstabell.



Klicka på  för att visa dialogrutan **Lägg till mappningstabell**.

Klicka på  för att visa dialogrutan **Byt namn på mappningstabell**.

Klicka på  om du vill ta bort mappningstabellen med alla dess rader.

Klicka på  eller  för att importera eller exportera en ONVIF-mappningstabell.

Händelser och larm

Välj en BVMS-händelse för mappning till en ONVIF-händelse.

Lägg till rad

Klicka här om du vill lägga till en rad i mappningstabellen.

Om det finns flera rader inträffar en händelse så länge en rad är sann.

Ta bort rad

Klicka här om du vill ta bort den valda raden från mappningstabellen.

ONVIF-ämne

Skriv eller välj en sträng, t.ex.

tns1:VideoAnalytics/tnsaxis:MotionDetection

ONVIF-datanamn

Skriv eller välj en sträng.

ONVIF-datatyp

Skriv eller välj en sträng.

ONVIF-datavärde

Skriv eller välj en sträng eller ett tal.

Om ONVIF-händelser hämtas från VSG mappas följande händelser till VSG som standard:

- **Global ändring – upptäckt**
- **Global ändring – hittades inte**
- **Rörelseavkänning - Rörelse upptäckt**
- **Rörelseavkänning - Rörelse stoppad**
- **Referensbildkontroll - Avjusterad**
- **Referensbildkontroll - Justerad**
- **Videoavbrott - Videosignal förlorad**
- **Videoavbrott - Videosignalen är OK**
- **Videoavbrott - Videosignalsstatus okänd**
- **Videosignal för suddig – videosignal OK**
- **Videosignal för suddig – Videosignal inte OK**
- **För ljus videosignal - Videosignalen är OK**
- **För ljus videosignal - Videosignal inte OK**
- **För mörk videosignal - Videosignalen är OK**
- **För mörk videosignal - Videosignal inte OK**
- **För mycket brus i videosignalen - Videosignalen är OK Videosignal inte OK**
- **Relästatus - Relä öppnat**
- **Relästatus - Relä stängt**
- **Relästatus - Relä fel**

- **Ingångstillstånd - Ingång öppnad**
- **Ingångstillstånd - Ingång stängd**
- **Ingångstillstånd - Ingångsfel**

Se

- *Starta ONVIF Camera Event Driver Tool från Configuration Client, sidan 197*
- *ONVIF-händelsemappning, sidan 39*
- *Konfigurera en ONVIF-mappningstabell, sidan 225*

14.3.1

Lägga till och ta bort en ONVIF-profil

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  > expandera

 >  > Fliken **ONVIF-kodarhändelser**
eller

Huvudfönster > **Enheter** > expandera  >  > Fliken **ONVIF-kodarhändelser**
Du kan lägga till, ta bort och ändra ONVIF-profiler för en kodare.

Så här lägger du till:

1. Klicka på **Lägg till....**
2. Ange ett namn på profilen i dialogrutan **Lägg till profil**.
3. Klicka på **Nästa >**.
4. Markera den önskade kameran i nästa dialogruta.
5. Klicka på **Nästa >**.
6. Välj den önskade kodarprofilen i nästa dialogruta.
7. Klicka på **Spara**.

Den nya profilen sparas.

Inställningarna för den här profilen är ifyllda med värden från den valda kodarprofilen. Du kan vid behov ändra dessa värden.

Så här tar du bort:

- Markera en profil i listan och klicka på **Ta bort**.

Så här ändrar du:

1. Markera en profil i listan.
2. Ändra inställningarna.

14.3.2

Exportera en tabell för mappning av ONVIF-fil

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  > expandera

 >  > Fliken **ONVIF-kodarhändelser**
eller

Huvudfönster > **Enheter** > expandera  >  > Fliken **ONVIF-kodarhändelser**

Du kan exportera en ONVIF-mappningstabell som en fil (OMF-fil). Mappningstabellen sparas för den valda kodarmodellen.

Så här exporterar du:

1. Klicka på .
2. Ange ett filnamn och klicka på **Spara**.

ONVIF-mappningstabellen exporteras som en OMF-filen för den valda kodarmodellen.

Se

– *Sidan ONVIF-kodarkodningar, sidan 221*

14.3.3

Importera en tabell för mappning av ONVIF-fil

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  > expandera



> Fliken **ONVIF-kodarkodningar**

eller

Huvudfönster > **Enheter** > expandera  >  > Fliken **ONVIF-kodarkodningar**

Du kan importera en ONVIF-mappningstabell som en fil (OMF-fil).

Utgivna ONVIF-mappningsfiler sparas i följande katalog på Configuration Client:

– `%programdata%\Bosch\VMS\ONVIF`

Om samma mappningstabellnamn redan har importerats visas ett felmeddelande.

Om en nyare version av filen har importerats visas en varning. Klicka på **OK** om du vill importera filen. Annars klickar du på **Avbryt**.

Så här importerar du:

1. Klicka på .
2. Markera filen och klicka på **Öppna**.
Dialogrutan **Importera mappningstabell** visas.
3. Gör lämpliga inställningar.
4. Klicka på **OK**.

Dialogrutan Importera mappningstabell

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  > expandera



> fliken **ONVIF-kodarkodningar** > 

eller

Huvudfönster > **Enheter** > expandera  >  > fliken **ONVIF-kodarkodningar** > 

Tillverkare

Visar vilket tillverkarnamn mappningstabellen gäller.

Modell

Visar vilket modellnamn mappningstabellen gäller.

Beskrivning

Visar ytterligare information, till exempel om testade kameramodeller.

Namn på mappningstabell

Visar namnet på mappningstabellen. Ändra namnet om det redan används i BVMS.

Du kan välja ett av följande alternativ för att bestämma vilka ONVIF-kodare du vill använda mappningstabellen till.

Tillämpa endast på vald ONVIF-kodare

Tillämpa på alla ONVIF-kodare för listade modeller

Tillämpa på alla ONVIF-kodare från tillverkaren

Befintlig ONVIF-händelsemappning har fortsatt. Du kan inte importera OMT-filer från tidigare BVMS-versioner.

14.3.4

Konfigurera en ONVIF-mappningstabell

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  > expandera

 >  > Fliken **ONVIF-kodarehändelser**
eller

Huvudfönster > **Enheter** > expandera  >  > Fliken **ONVIF-kodarehändelser**

Du kan konfigurera mappningstabeller och mappa ONVIF-händelser till BVMS-händelser.

Du konfigurerar en mappningstabell för alla ONVIF-kodare av samma modell eller alla ONVIF-kodare från samma tillverkare.

Klicka på  om du vill uppdatera ONVIF-kodare som har lagts till offline med en händelsemappning som hör till en redan tillagd ONVIF-kodare från samma tillverkare och/eller med samma modellnamn.

För flerkanalskodare kan du konfigurera händelsekällorna, t.ex. en viss kamera eller ett visst relä.

Så här skapar du en mappningstabell:

1. Klicka på .
Dialogrutan **Lägg till mappningstabell** visas.
2. Skriv in ett namn på mappningstabellen.
3. Välj poster i listorna **Tillverkare** och **Modell** om du vill.
Om du väljer **<inget>** i båda listorna gäller händelsemappningen bara för den här enheten.
Om du väljer **<inget>** i listan **Modell** och tillverkarens namn i listan **Tillverkare** gäller händelsemappningen alla enheter från samma tillverkare.
Om du väljer tillgängliga poster i båda listorna gäller händelsemappningen alla enheter från samma tillverkare och den aktuella modellen.
4. Klicka på **OK**.
Du kan nu redigera mappningstabellen, till exempel genom att lägga till en rad i händelsen **Rörelse upptäckt**.

Så här redigerar du en mappningstabell:

1. Klicka på .
Dialogrutan **Byt namn på mappningstabell** visas.
2. Ändra de önskade posterna.

Så här lägger du till eller tar bort händelsemappningar:

1. Välj önskat namn i listan **Mappningstabell**.
2. Lägg till en rad: klicka på **Lägg till rad**.
3. Välj de önskade posterna på raden.
Om det finns flera rader utlöses en händelse om någon av raderna är sann.
4. Ta bort en rad: klicka på **Ta bort rad**.

Så här tar du bort en mappningstabell:

1. Klicka på namnet på de händelsemappningar som du vill ta bort på listan **Mappningstabell**.

2. Klicka på .

Så här konfigurerar du en händelsekälla:

1. Utvidga  och klicka på  eller  eller .
2. Klicka på fliken **ONVIF-händelsekälla**.
3. Aktivera den händelse som är konfigurerad på den här raden i kolumnen **Utlös händelse**.
4. Välj de önskade händelsedefinitionerna.

Dialogrutan Lägg till/byt namn på ONVIF-mappningstabell

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  > expandera 
 >  > Fliken **ONVIF-kodarrhändelser** >  eller 
 eller

Huvudfönster > **Enheter** > expandera  >  >  > Fliken **ONVIF-kodarrhändelser** > 
 eller 

Gör att du kan lägga till en mappningstabell. Om den här mappningstabellen ska fungera som mall för kommande ONVIF-kodare för samma tillverkare och modell måste du välja de korrekta posterna.

Namn på mappningstabell

Skriv ett namn som förenklar identifieringen.

Tillverkare

Välj en post i aktuella fall.

Modell

Välj en post i aktuella fall.

Se

- Aktivera loggning för ONVIF-händelser, sidan 349
- ONVIF-händelsemappning, sidan 39
- Sidan ONVIF-kodarrhändelser, sidan 221
- Sidan ONVIF-händelsekälla, sidan 239

14.4

Sidan ONVIF-konfiguration

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  > expandera 
 >  > fliken **ONVIF-konfiguration**
 eller

Huvudfönster > **Enheter** > expandera  >  > fliken **ONVIF-konfiguration**

Du kan markera flera ONVIF-kodare och ändra inställningar på sidan **Videokodarprofil**. De ändrade inställningarna gäller för alla valda enheter.

Sidan är bara tillgänglig för ONVIF-kodare.

**Obs!**

Begränsningar för ONVIF-konfiguration

Inställningar som du utför på de här sidorna kanske inte utförs korrekt eftersom de inte stöds av kameran. ONVIF-kameror som stöds testades endast med standardinställningarna.

14.4.1**Enhetsåtkomst**

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  > expandera  >  > fliken **ONVIF-konfiguration** > fliken **Huvudinställningar** > fliken **Enhetsåtkomst** eller

Huvudfönster > **Enheter** > expandera  > expandera  > fliken **ONVIF-konfiguration** > fliken **Huvudinställningar** > fliken **Enhetsåtkomst**

Tillverkare

Visar den valda kodarens tillverkare.

Modell

Visar den valda kodarens modell.

Obs! Om du vill exportera alla händelsemappningar i en ONVIF-mappingsfil väljer du det här modellnamnet som filnamn.

Maskinvaru-ID

Visar den valda kodarens maskinvaru-id.

Version av fast programvara

Visar versionen på den valda kodarens fasta programvara.

Obs! Kontrollera med kompatibilitetslistan för BVMS om versionen för den fasta programvaran är korrekt.

Serienummer

Visar den valda kodarens serienummer.

MAC-adress

Visar den valda kodarens MAC-adress.

ONVIF-version

Visar den valda kodarens ONVIF-version.

För BVMS krävs ONVIF version 2.0.

14.4.2**Datum/tid**

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  > expandera  >  > fliken **ONVIF-konfiguration** > fliken **Huvudinställningar** > fliken **Datum/tid** eller

Huvudfönster > **Enheter** > expandera  > expandera  > fliken **ONVIF-konfiguration** > fliken **Huvudinställningar** > fliken **Datum/tid**

Tidzon

Välj den tidszon där systemet befinner sig.

Om det är flera enheter som används i systemet eller nätverket är det viktigt att synkronisera deras interna klockor. Det går t.ex. bara att identifiera och korrekt utvärdera samtidiga inspelningar om alla enheter körs tidsmässigt synkroniserade.

1. Ange aktuellt datum. Eftersom enhetens tid kontrolleras av den interna klockan är det inte nödvändigt att ange veckodag. Den läggs till automatiskt.
2. Skriv in aktuell tid eller klicka på **Synkr. Dator** för att överföra datorns tid till enheten.

Obs!

Det är viktigt att datumet och tiden stämmer för inspelningen. Felaktig datum- och tidsinställning skulle kunna förhindra korrekt inspelning.

14.4.3

Användarhantering

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  > expandera



> > fliken **ONVIF-konfiguration** > fliken **Huvudinställningar** > fliken

Användarhantering

eller

Huvudfönster > **Enheter** > expandera  > expandera  > fliken **ONVIF-konfiguration** > fliken **Huvudinställningar** > fliken **Användarhantering**

De här användarinställningarna används för tredjepartsprogram för exempelvis direkt webbklientsåtkomst till kodare.

Följande användarroller för åtkomst till tredjepartsprogram kan användas:

- **Anonym:** Rollen har endast obegränsad åtkomst till de enheter där inga användare från andra roller (**Användare**, **Operatör**, **Administratör**) har registrerats. För enheter med minst en ovannämnd användare har den anonyma användaren endast rätt att visa tidsinställningarna.
- **Administratör** (stöds inte av Configuration Client): Den här rollen har åtkomst till alla programsektioner och -funktioner, behörighet att starta om enheten, återställa inställningar och uppdatera den fasta programvaran samt att skapa andra användare med olika åtkomstbehörigheter.

Den första användaren som skapats på enheten måste vara **Administratör**.

Du kan se skillnader i operatörens och användarens standardåtkomstbehörigheter för

Operatör-rollen och **Användare**-rollen i följande tabell.

ONVIF-konfigurationsavsnitt eller -funktion	Operatör	Användare
Identifiering	VISA	DOLD
Tidsinställningar	VISA	VISA
Nätverksinställningar	VISA	VISA
Användare	DOLD	DOLD
Reläinställningar	ÄNDRA	VISA
Livevideo (inklusive rtsp-länk)	ÄNDRA	ÄNDRA
Videoströmning	ÄNDRA	VISA
Profiler	ÄNDRA	VISA

ÄNDRA – ändra aktuella och skapa nya inställningar.

VISA – inställningar är inte dolda, men det är inte tillåtet att ändra och skapa dem.

DOLDA – vissa inställningar, eller till och med hela avsnitt, döljs.

Användare

Visar en lista över tillgängliga användare av enheten.

Lösenord

Skriv ett lösenord.

Bekräfta lösenord

Bekräfta det angivna lösenordet.

Roll

Välj önskad roll för den valda användaren. Rollen bestämmer åtkomsträttigheterna.

14.4.4

Sidan Videokodarprofil

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  > expandera

 >  > fliken **ONVIF-konfiguration** > fliken **Kamera** > fliken **Videokodarprofil**
eller

Huvudfönster > **Enheter** > expandera  >  > fliken **ONVIF-konfiguration** > fliken **Kamera** > fliken **Videokodarprofil**

Profiler är ganska avancerade och innefattar ett antal parametrar som är beroende av varandra. Generellt är det därför bäst att använda de fördefinierade profilerna. Ändra bara en profil om du har kunskap om alla konfigurationsalternativ.

Profiler

Klicka på önskat namn.

Obs!

De profiler som konfigurerats här kan väljas i Configuration Client.



Gå till huvudfönstret och klicka på **Kameror och inspelning** och  eller  .
Standardinställningen <Automatisk> kan ändras till en av de angivna och konfigurerade profilerna

Obs! Tänk på att när du aktivt använder mer än en profil för en enda enhet gäller vissa prestandabegränsningar och kameran kan begränsa kvaliteten på en ström automatiskt i överbelastningssituationer.

Namn

Du kan ange ett nytt namn på profilen här. Namnet visas sedan i listan med tillgängliga profiler i fältet Aktiv profil.

Kodning

Välj önskad codec.

Upplösning

Välj önskad upplösning för videobilden.

Kvalitet

Med den här parametern kan du minska belastningen på kanalen genom att minska bilddefinitionen. Parametern anges med hjälp av skjutreglaget: Positionen längst till vänster motsvarar den högsta bilddefinitionen, positionen längst åt höger – den lägsta belastningen på videokanalen.

Gräns för bildfrekvens

Bildrutehastighet (bilder per sekund) anger hur många bildrutor per sekund som registreras av videokameran som är ansluten till enheten. Den här parametern visas bara i informativt syfte. Om ett kodningsintervall finns minskar den slutliga kodade bildrutehastigheten med den angivna faktorn.

Gräns för bithastighet

Ju mindre bithastigheten är, desto mindre är filstorleken på den slutliga videon. Men när bithastigheten minskas betydligt måste programmet använda kraftfullare komprimeringsalgoritmer, vilket också minskar videokvaliteten.

Välj den maximala utgående bithastigheten i kbit/s. Den högsta datahastigheten överskrider inte under några omständigheter. Beroende på inställningarna för videokvaliteten för I- och P-frames kan enstaka bilder hoppas över.

Värdet som anges här ska vara minst 10 % högre än den typiska måldatabithastigheten.

Kodningsintervall

Kodningsintervallet (antal bildrutor) anger i vilken takt bildrutorna från kameran kodas. När intervallkodningen till exempel komprimerar 25, betyder det att 1 av 25 inspelade bildrutor per sekund kodas och överförs till användaren. Det största värdet minskar belastning på kanalen, men kan orsaka att information hoppas över från de bildrutor som inte har kodats. När kodningsintervallet minskar ökar frekvensen för bilduppdateringen samt belastningen på kanalen.

GOP-längd

GOP-längd kan endast redigeras om kodaren är H.264 eller H.265. Den här parametern anger längden på bildgruppen mellan de två nyckelramarna. Ju högre värdet är, desto mindre är belastningen på nätverket, men videokvaliteten påverkas.

En post med 1 betyder att I-frames skapas kontinuerligt. En post med 2 betyder att varannan bild är en I-frame, 3 betyder att bara var tredje bildruta är en sådan och så vidare. Bildrutorna däremellan kodas som P-frames eller B-frames.

Sessiontimeout

Timeoutgränsen för RTSP-sessionen nås för den relaterade videoströmmen.

Sessiontimeouten är ett sätt att hålla igång RTSP-sessionen med en enhet.

Flersändning (multicasting) - IP-adress

Ange en giltig multicastadress som ska användas i multicastläge (kopiering av dataströmmen i nätverket).

Med inställningen 0.0.0.0 körs kodaren för strömmen i multiunicastläge (kopiering av dataströmmen i enheten). Kameran stöder multiunicastanslutningar för upp till fem samtidigt anslutna mottagare.

Kopiering av data innebär en tung belastning på processorn och kan leda till försämring av bildkvaliteten under vissa omständigheter.

Flersändning (multicasting) - Port

Välj destinationsport för RTP-fleranvändarläget (multicast). En enhet kan hantera RTCP. I det här fallet ska portvärdet vara jämnt för att låta den motsvarande RTCP-strömmen mappas till nästa högre (udda) destinationsportnummer enligt definitionen i RTSP-specifikationen.

Flersändning (multicasting) - TTL

Ett värde för hur länge multicast-datapaketen är aktiva på nätverket kan anges. Värdet måste vara större än 1 om multicast ska köras via en router.



Obs!

Fleranvändardrift (multicast) är bara möjlig med UDP-protokollet. TCP-protokollet kan inte hantera fleranvändaranslutningar (multicast).

Om enheten används bakom en brandvägg väljer du TCP (HTTP-port) som överföringsprotokoll. Välj UDP för användning i ett lokalt nätverk.

14.4.5

Ljudkodarprofil

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  > expandera



> fliken **ONVIF-konfiguration** > fliken **Kamera** > fliken **Ljudkodarprofil**

eller

Huvudfönster > **Enheter** > expandera  >  > fliken **ONVIF-konfiguration** > fliken **Kamera** > fliken **Ljudkodarprofil**

Profiler är ganska avancerade och innefattar ett antal parametrar som är beroende av varandra. Generellt är det därför bäst att använda de fördefinierade profilerna. Ändra bara en profil om du har kunskap om alla konfigurationsalternativ.

Kodning

Välj önskad kodning för ljudkällan om det är möjligt:

- **G.711 [ITU-T G.711]**
- **G.726 [ITU-T G.726]**
- **AAC [ISO 14493-3]**

Bithastighet

Välj önskad bithastighet, till exempel 64 kbit/s, för överföring av ljudsignalen.

Samplingsfrekvens

Ange utgångshastighet för samplingen i kHz, till exempel 8 kbit/s.

Sessiontimeout

Timeoutgränsen för RTSP-sessionen nås för den relaterade ljudströmmen. Sessionstimeouten är ett sätt att hålla igång RTSP-sessionen med en enhet.

14.4.6

Bildvisning, allmänt

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  > expandera



> fliken **ONVIF-konfiguration** > fliken **Kamera** > fliken **Bildvisning, allmänt**

eller

Huvudfönster > **Enheter** > expandera  > expandera  > fliken **ONVIF-konfiguration** > fliken **Kamera** > fliken **Bildvisning, allmänt**

Ljusstyrka

Justera ljusstyrkan efter arbetsmiljön.

Färgmättnad

Justera färgmättnaden i bilden så att färgåtergivningen på bildskärmen blir så realistisk som möjligt.

Kontrast

Du kan anpassa kontrasten i videobilden efter din arbetsmiljö.

Skärpa

Ändrar bildens skärpa.

Ett lågt värde minskar bildens skärpa. Ökad skärpa ger större detaljrikedom. Extra skärpa kan ge större detaljrikedom på bilder av registreringsskyltar, ansiktsdrag och kanterna på vissa ytor, men kan samtidigt öka kraven på bandbredden.

IR-filter

Välj läge för IR-filtret.

Med AUTO-läget hanterar exponeringsalgoritmen när IR-filtret aktiveras.

14.4.7**Motljuskompensation**

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  > expandera



> fliken **ONVIF-konfiguration** > fliken **Huvudinställningar** > fliken

Bakbelysningskompensation

eller

Huvudfönster > **Enheter** > expandera  > expandera  > fliken **ONVIF-konfiguration** > fliken **Huvudinställningar** > fliken **Bakbelysningskompensation**

Beroende på enhetsmodell, kan du konfigurera parametrar för motljuskompensation här.

Läge

Välj **Av** för att stänga av motljuskompensationen.

Välj **På** för att fånga detaljer vid hög kontrast och extrema ljusförhållanden.

Nivå

Ange eller välj önskat värde.

14.4.8**Exponering**

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  > expandera



> fliken **ONVIF-konfiguration** > fliken **Huvudinställningar** > fliken **Exponering**

eller

Huvudfönster > **Enheter** > expandera  > expandera  > fliken **ONVIF-konfiguration** > fliken **Huvudinställningar** > fliken **Exponering**

Beroende på enhetsmodell kan du konfigurera parametrar för exponering här.

Läge

Välj **Auto** att aktivera exponeringsalgoritmen på enheten. Värdena i följande fält används av algoritmen:

- **Prioritet**
- **Fönster**

- **Min. exponeringstid**
- **Max. exponeringstid**
- **Min. förstärkning**
- **Maximal förstärkning**
- **Min. bländare**

Välj **Manuellt** för att inaktivera exponeringsalgoritmen på enheten. Värdena i följande fält används av algoritmen:

- **Exponeringstid**
- **Gain (förstärkn.)**
- **Bländare**

Prioritet

Konfigurera läget för exponeringsprioritet (långt brus/bildrutehastighet).

Fönster

Definiera en rektangulär exponeringmask.

Min. exponeringstid

Konfigurera den minsta exponeringstiden [μ s].

Max. exponeringstid

Konfigurera den längsta exponeringstiden [μ s].

Min. förstärkning

Konfigurera intervallet för den minsta sensorförstärkningen [dB].

Maximal förstärkning

Konfigurera intervallet för den största sensorförstärkningen [dB].

Min. bländare

Konfigurera den minsta dämpningen av inkommande ljus som påverkas av bländaren [dB]. 0 dB mappar till en helt öppen bländare.

Max. bländare

Konfigurera den största dämpningen av inkommande ljus som påverkas av bländaren [dB]. 0 dB mappar till en helt öppen bländare.

Exponeringstid

Konfigurera den fasta exponeringstiden [μ s].

Gain (förstärkn.)

Konfigurera den fasta förstärkningen [dB].

Bländare

Konfigurera den fasta dämpningen av inkommande ljus som påverkas av bländaren [dB]. 0 dB mappar till en helt öppen bländare.

14.4.9

Fokus

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  > expandera  >  > fliken **ONVIF-konfiguration** > fliken **Huvudinställningar** > fliken **Fokus**
eller

Huvudfönster > **Enheter** > expandera  > expandera  > fliken **ONVIF-konfiguration** > fliken **Huvudinställningar** > fliken **Fokus**

Beroende på enhetsmodell kan du konfigurera parametrar för fokus här.

På den här sidan kan objektivet flyttas absolut, relativt eller kontinuerligt. Fokusjusteringen med den här åtgärden inaktiverar autofokusfunktionen. En enhet med stöd för fjärrstyrd fokuskontroll stöder vanligtvis kontroll via den här flyttåtgärden. Fokuspositionen representeras av ett visst numeriskt värde. Status för fokuseringen kan vara något av följande:

FLYTTAR

OK

OKÄNT

Dessutom kan felinformation visas, ett placeringsfel indikeras till exempel av maskinvaran.

Läge

Välj **Auto** för att aktivera automatisk fokusering av objektivet när som helst efter föremålet i bilden. Värdena i följande fält används av algoritmen:

- **Närgräns**
- **Bortre gräns**

Välj **Manuellt** att justera fokus manuellt. Värdena i följande fält används av algoritmen:

- **Standardhastighet**

Standardhastighet

Konfigurera standardhastigheten för fokusflyttningar (när hastighetsparametern inte finns).

Bortre gräns

Konfigurera den närgränsen för fokusobjektivet [m].

Bortre gräns

Konfigurera den bortre gränsen för fokusobjektivet [m].

14.4.10

Brett dynamiskt intervall

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  > expandera

 >  > fliken **ONVIF-konfiguration** > fliken **Huvudinställningar** > fliken **Brett dynamiskt intervall**

eller

Huvudfönster > **Enheter** > expandera  > expandera  > fliken **ONVIF-konfiguration** > fliken **Huvudinställningar** > fliken **Brett dynamiskt intervall**

Beroende på enhetsmodell, kan du konfigurera parametrar för bredd dynamiskt intervall här.

Läge

Ange eller välj önskat värde.

Nivå

Ange eller välj önskat värde.

14.4.11

Vitbalans

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  > expandera

 >  > fliken **ONVIF-konfiguration** > fliken **Huvudinställningar** > fliken **Vitbalans**

eller

Huvudfönster > **Enheter** > expandera  > expandera  > fliken **ONVIF-konfiguration** > fliken **Huvudinställningar** > fliken **Vitbalans**

Beroende på enhetsmodell kan du konfigurera parametrar för vitbalans här.

Läge

Autoläge gör att kameran kontinuerligt kan justera för optimal färgåtergivning med en metod som utnyttjar den genomsnittliga reflektansen eller i en miljö med naturliga ljuskällor. I det manuella läget kan förstärkningen för rött, grönt och blått ställas in manuellt i önskat läge. Vitpunktsförskjutningen behöver bara ändras för särskilda scenförhållanden:

- ljuskällor inomhus och för belysning med färgade lysdioder
- natriumånglampor (gatubelysning)
- för alla dominanta färger i bilden, till exempel det gröna på en fotbollsplan eller på ett spelbord

R-förstärkning

I det manuella vitbalanseringsläget kan du justera det röda förstärkningsreglaget för att förskjuta den fabriksinställda vitpunktsinställningen (mindre rött ger mer cyanfärg).

B-förstärkning

I det manuella vitbalanseringsläget kan du justera det blå förstärkningsreglaget för att förskjuta den fabriksinställda vitpunktsinställningen (mindre blått ger mer gult).

14.4.12

Nätverksåtkomst

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  > expandera

 >  > fliken **ONVIF-konfiguration** > fliken **Nätverk** > fliken **Nätverksåtkomst**
eller

Huvudfönster > **Enheter** > expandera  > expandera  > fliken **ONVIF-konfiguration** > fliken **Nätverk** > fliken **Nätverksåtkomst**

Här kan du konfigurera olika inställningar för nätverk.

Ethernet IPv4

DHCP

Om en DHCP-server används i nätverket för dynamisk tilldelning av IP-adresser kan du aktivera godkännande av IP-adresser som tilldelas automatiskt till kodaren.

BVMS använder IP-adressen för den unika tilldelningen av kodare. DHCP-servern måste ha stöd för den fasta tilldelningen mellan IP-adress och MAC-adress och måste ställas in korrekt så att en IP-adress, när den tilldelats, behålls varje gång datorn startas om.

Nätmask

Ange lämplig delnätmask för den inställda IP-adressen.

Om DHCP-servern har aktiverats tilldelas nätmasken automatiskt.

Standard-gateway

Om du vill att modulen ska upprätta en anslutning till en fjärrplats i ett annat subnät, anger du IP-adressen till gatewayen här. I annat fall låter du fältet vara tomt (0.0.0.0).

Ethernet IPv6

DHCP

Ange eller välj önskat värde.

IP-adress

Visar IPv6-adressen för enheten, som tillhandahålls av DHCP-servern.

Prefixlängd

Visar prefixlängden för enheten, som tillhandahålls av DHCP-servern.

Standard-gateway

Visar standardgatewayen för enheten, som tillhandahålls av DHCP-servern.

Värddatorns namn

Ange eller välj önskat värde.

DNS

Med en DNS-server kan enheten lösa en adress som indikeras som ett namn. Ange IP-adressen till DNS-servern här.

NTP-servrar

Ange IP-adressen till den önskade tidsservern eller låt DHCP-servern göra det åt dig. Kodaren kan ta emot tidssignalen från en tidsserver med hjälp av olika tidsserverprotokoll och sedan använda den för att ställa in den interna klockan. Modulen hämtar tidssignalen automatiskt en gång i minuten. Ange IP-adressen till en tidsserver här. Det här alternativet ger en hög noggrannhet och krävs för särskilda tillämpningar.

HTTP-portar

Välj en annan HTTP-webbläsarport om det behövs. HTTP-standardporten är 80. Om du endast vill tillåta säkra anslutningar via HTTPS är du tvungen att avaktivera HTTP-porten.

Obs! Stöds inte av BVMS.

HTTPS-portar

Obs! Stöds inte av BVMS.

Om du vill bevilja åtkomst till nätverket via en säker anslutning väljer du en HTTPS-port om det behövs. HTTPS-standardporten är 443. Välj alternativet **Av** om du vill inaktivera HTTPS-portarna. Nu är endast osäkra anslutningar möjliga.

Standard-gateway

Ange eller välj önskat värde.

RTSP-portar

Välj vid behov en annan port för utbytet av RTSP-data. RTSP-standardporten är 554. Välj **Av** om du vill inaktivera RTSP-funktionen.

Zero konfiguration address

Aktivera eller inaktivera upptäckt av nollkonfiguration för den valda kameran.

Nollkonfiguration är en alternativ metod för DHCP och DNS för att tilldela IP-adresser till kameror. Det skapar automatiskt en användbar IP-nätverksadress utan konfiguration eller särskilda servrar.

Obs! I ONVIF-standardens används endast tjänstupptäckten av nollkonfigurationen.

Alternativt, utan nollkonfiguration, måste nätverket tillhandahålla tjänster, som DHCP eller DNS.

I annat fall konfigureras nätverksinställningarna för varje IP-kamera manuellt.

ONVIF upptäcktsläge

Om det aktiverats kan kameran sökas igenom i nätverket. Detta inkluderar dess funktioner.

Om det avaktiverats skickar inte kameran några upptäcktsmeddelanden för att undvika DOS-attacker.

Vi rekommenderar att upptäckt inaktiveras när kameran lagts till i konfigurationen.

Ange eller välj önskat värde.

Aktivera DynDNS

Tillåt för att aktivera DynDNS.

Med dynamisk DNS (Domain Name Service) kan du välja enhet via internet med ett värddamn, utan att behöva känna till den aktuella IP-adressen för enheten. För att göra det måste du ha ett konto hos en dynamisk DNS-leverantör och du måste registrera det önskade värddamnet för enheten på den webbplatsen.

Obs!

Information om tjänsten, registreringsprocessen och tillgängliga värddamn får du från DynDNS-leverantören på dyndns.org.

Typ

Ange eller välj önskat värde.

Namn

Ange namnet på ditt DynDNS-användarkonto.

TTL

Ange eller välj önskat värde.

14.4.13

Områden

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  > expandera  >  > fliken **ONVIF-konfiguration** > fliken **Nätverk** > fliken **Områden**
eller

Huvudfönster > **Enheter** > expandera  >  > fliken **ONVIF-konfiguration** > fliken **Nätverk** > fliken **Områden**

Du kan lägga till eller ta bort områden för ONVIF-enheten med URI:er som har följande format:

```
onvif://www.onvif.org/<path>
```

Följande exempel illustrerar användningen av områdesvärdet. Det här är bara ett exempel, och inte alls en indikation av vilken typ av områdesparameter som ska ingå i en kodarkonfiguration. I det här exemplet förutsätter vi att kodaren har konfigurerats med följande områden:

```
onvif://www.onvif.org/location/country/china
onvif://www.onvif.org/location/city/beijing
onvif://www.onvif.org/location/building/headquarter
onvif://www.onvif.org/location/floor/R5
onvif://www.onvif.org/name/ARV-453
```

Du kan ge enheten en detaljerad plats och ett enhetsnamn för att identifiera den i enhetslistan.

I tabellen visas de grundläggande funktionerna och andra standardiserade egenskaper för enheten:

Kategori	Definierade värden	Beskrivning
type	video_encoder	Enheten är en nätverksenhet för videokodning.
	Ptz	Enheten är en PTZ-enhet.
	audio_encoder	Enheten har stöd för ljudkodare.
	video_analytics	Enheten har stöd för videoanalyser.
	Network_Video_Transmitter	Enheten är en nätverksvideosändare.
	Network_Video_Decoder	Enheten är en nätverksvideokodare.

Kategori	Definierade värden	Beskrivning
	Network_Video_Storage	Enheten är en nätverksenhet för videolagring.
	Network_Video_Analytic	Enheten är en nätverksenhet för videoanalyser.
plats	Alla teckensträngar eller sökvägsvärden.	Stöds ej av BVMS.
maskinvar a	Alla teckensträngar eller sökvägsvärden.	En sträng eller ett sökvägsvärde som beskriver maskinvaran för enheten. En enhet ska innehålla minst en maskinvarupost i områdeslistan.
namn	Alla teckensträngar eller sökvägsvärden.	Enhetens sökbara namn. Det här namnet visas i enheten och det logiska trädet.

Områdesnamn, modell och tillverkaren påverkar hur enheten visas i enhetsträdet och ONVIF-kodarens identifierings- och huvudinställningar.

14.4.14

Reläer

Huvudfönster > **Enheter** > expandera  > expandera  > expandera  > expandera



> > fliken **ONVIF-konfiguration** > fliken **Gränssnitt** > fliken **Relä**



Huvudfönster > **Enheter** > expandera  > expandera  > fliken **ONVIF-konfiguration** > fliken **Gränssnitt** > fliken **Relä**

Fysisk inaktiv status för en reläutgång kan konfigureras genom att viloläget ställs in på **öppen** eller **stängd** (inversion av reläbeteendet).

Enhetens digitala utgångar som är tillgängliga visas med respektive namn, t.ex.:

- **AlarmOut_0**
- **AlarmOut_1**

För eventuell händelsemappning för reläer i BVMS, använd de namn som anges här.

Läge

Reläet kan fungera i två lägen:

- **Dubbelstabil**: När du ställt in läget ändras det inte.
- **Enkelstabil**: När du ställt in läget återgår reläet till inaktiv status efter den angivna fördröjningstiden.

Viloläge

Välj **Öppen** om du vill att reläet ska fungera som en normalt öppen kontakt, eller välj **Stängd** om reläet ska fungera som en normalt stängd kontakt.

Fördröjningstid

Ställ in fördröjningstiden. Efter den här tidsperioden växlar reläet tillbaka till viloläget om det har konfigurerats i det **enkelstabila** läget.

Om du som vill testa alla konfigurationer som hör till en relälägesförändring klickar du på **Aktivera** eller **Avaktivera** för att växla reläet. Du kan kontrollera så att relähändelserna fungerar korrekt för den konfigurerade kameran: statusdisplayen för reläikonen i det logiska trädet, händelser i larmlistan eller händelseloggen.

Aktivera

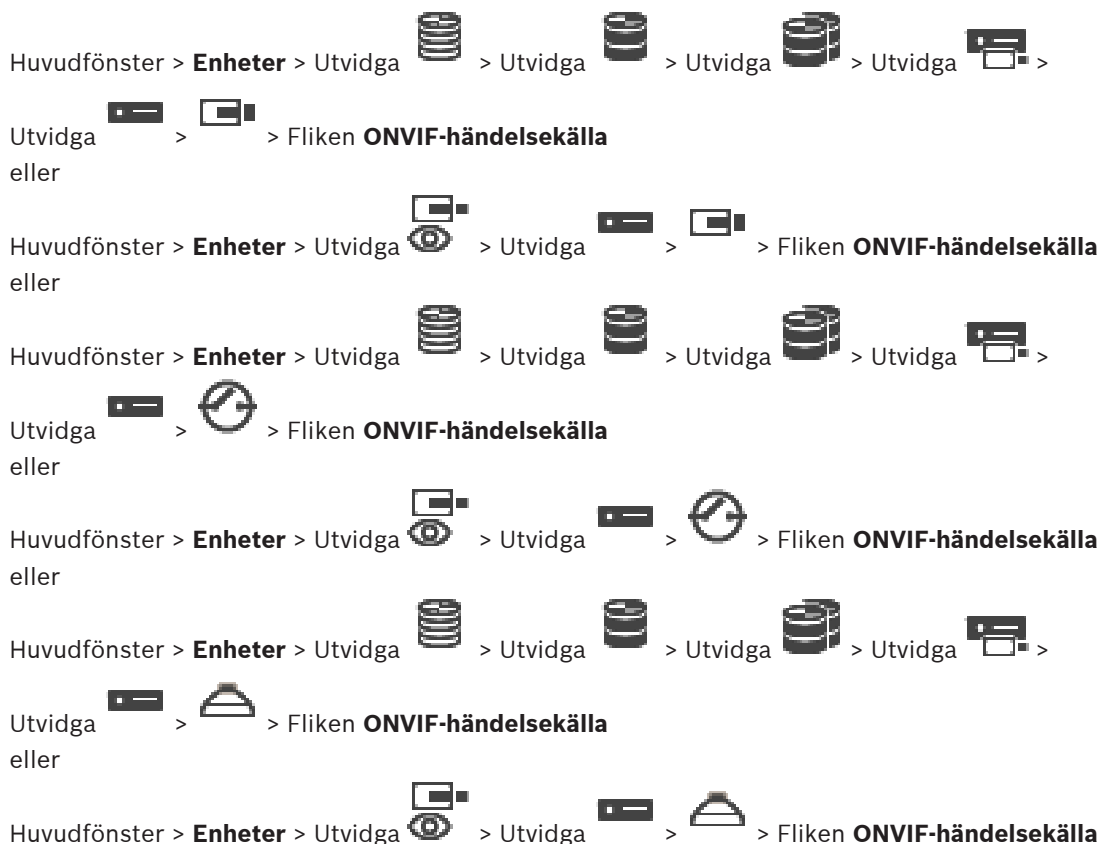
Klicka för att byta relä till det konfigurerade inaktiva viloläget.

Avaktivera

Klicka för att växla reläet till det konfigurerade icke-viloläget.

14.5

Sidan ONVIF-händelsekälla



Du kan konfigurera en källas (videokanal, ingång eller relä) ONVIF-händelser. En definition för en aktiverad händelse läggs till i kodarens mappningstabell.

För en flerkanalskodare kan du t.ex. ange för vilken kamera en **Rörelse upptäckt**-händelse utlöses.

Utlös händelse

Aktivera den här händelsen.

ONVIF-ämne

Skriv eller välj en sträng.

ONVIF-källnamn

Skriv eller välj en sträng.

ONVIF-källtyp

Skriv eller välj en sträng.

ONVIF-källvärde

Skriv eller välj en sträng.

Se

- *ONVIF-händelsemappning, sidan 39*
- *Konfigurera en ONVIF-mappningstabell, sidan 225*

14.6

Tilldela en ONVIF-profil



Du kan tilldela en ONVIF-kamera en kodbricka för ONVIF Media Profile.

Du kan tilldela antingen för live-video eller för inspelning.

Tilldela en kodbricka för live-video:

- ▶ I kolumnen **Live-video – Profil** väljer du önskad post.

Tilldela en kodbricka för inspelning:

- ▶ I kolumnen **Inspelning – Profil** väljer du önskad post.

Se

- *Sidan Kameror, sidan 266*

15

Sidan Kartor och struktur

**Obs!**

BVMS Viewer har bara grundläggande funktioner. Avancerade funktioner ingår i BVMS Professional. Detaljerad information om de olika BVMS utgåvorna finns på www.boschsecurity.com och BVMS Snabbvalsguiden: [BVMS snabbvalsguide](#).

Antalet objekt nedanför en post visas inom hakparenteser.

Huvudfönster > **Kartor och struktur**

Behörigheter kan gå förlorade. Om du flyttar en grupp med enheter förlorar dessa enheter sina behörighetsinställningar. Du måste ställa in behörigheterna på sidan **Användargrupper** igen.

Visar enhetsträdet, det logiska trädet, och **globala kart** fönstret.

Gör att du kan införa en struktur för alla enheter i BVMS. Din struktur visas i det logiska trädet.

Gör att du kan utföra följande uppgifter:

- Konfigurera hela det logiska trädet
- Hantera resurser
- Skapa kommandoskript
- Skapa sekvenser
- Skapa kartvyportar
- Skapar felövervakningsreläer
- Lägga till webbplatskartor och skapa hotspots

Hotspots på kartor kan vara:

- Kameror
- Ingångar
- Reläer
- Kommandoskript
- Sekvenser
- Dokument
- Länkar till andra webbplatskartor
- VRM
- iSCSI
- Läsare av ett passersystem
- Inbrottspaneler
- Management Server för Enterprise Systems

Resursfiler kan vara:

- Mappa filer
- Dokumentfiler
- Länkar till externa webbadresser
- Ljudfiler
- Länkar till externa applikationer

Ikoner

	Visar en dialogruta för hantering av resursfiler.
	Visar en dialogruta för att lägga till och hantera kommandoskript i det logiska trädet.
	Visar en dialogruta för att lägga till och redigera en kamerasekvensfil.

	Skapar en mapp i det logiskt träd.
	Visar en dialogruta för att lägga till kartresursfiler.
	Skapar en kartvyport i det logiskt träd.
	Visar en dialogruta för att lägga till en fil med ett dokument.
	Visar en dialogruta för att lägga till en länk i en extern applikation.
	Visar en dialogruta för att lägga till ett felövervakningsrelä.

Symboler

	Enhet har lagts till i det logiska träd.
---	--

Skriv in en sträng och tryck på ENTER-tangenten för att filtrera de visade objekten. Endast objekt som innehåller strängen och deras motsvarande föräldraobjekt (endast i träd) visas. Antalet filtrerade objekt och det totala antalet objekt visas. Ett aktivt filter indikeras med . Skriv in strängar inom dubbla citattecken för att hitta dem exakt, till exempel filtrerar "Camera 1" kamerorna med exakt detta namn, inte camera 201. Avbryt filtreringen genom att klicka på .

16 Konfigurera kartor och det logiska trädet

I det här kapitlet ges information om hur du konfigurerar det logiska trädet och hur du hanterar resursfiler såsom kartor.



Obs!

Om du flyttar en grupp av enheter i det logiska trädet, så kommer de enheterna att förlora sina behörighetsinställningar. Du måste ställa in behörigheterna på sidan **Användargrupper** igen.

- Klicka på för att spara inställningarna.
- Klicka på om du vill ångra den senaste inställningen.
- Klicka på för att aktivera konfigurationen.

Se

- *Resurshanteraren-dialogrutan, sidan 246*
- *Välj resurs-dialogrutan, sidan 246*
- *Sekvensbyggare-dialogrutan, sidan 249*
- *Lägg till sekvens-dialogrutan, sidan 251*
- *Lägg till sekvenssteg-dialogrutan, sidan 251*
- *Lägg till URL-dialogrutan, sidan 247*
- *Välj karta för länk-dialogrutan, sidan 252*
- *Dialogrutan för felövervakningsrelä, sidan 258*
- *Dialogrutan Länk till extern applikation, sidan 248*

16.1 Konfigurera det logiska trädet

Huvudfönster > **Kartor och struktur** > **Logiskt träd** flik

Du kan lägga till enheter, resursfiler, kartvyportar, sekvenser, klientkommandoskript och mappar i det logiska trädet. Enheter är listade i enhetsträdets och du kan dra alla nivåer i enhetsträdets till det logiska trädets.

En resursfil kan till exempel vara en anläggningskarta, ett dokument, en webbfil, ljudfil, ett kommandoskript eller en kamerasekvensfil.

- En anläggningskarta är en fil som du kan lägga till i det logiska trädets. Om du lägger till en karta i det logiska trädets skapas en kartmapp där du kan sortera de logiska enheterna som är specifika för den mappen.
- En kartvyport är ett område på en global karta med en specifik mitt- och zoomnivå.
- En mapp hjälper dig att ytterligare organisera enheter i det logiska trädets.

När du startar Configuration Client för första gången, är det logiska trädets tomt.

Om en användargrupp saknar behörighet för en enhet (t.ex. en kamera), så visas inte enheten på anläggningskartan, på kartvyn eller i det logiska trädets.

Du kan lägga till följande poster från enhetsträdets eller det logiska trädets som anläggningspunkt på en anläggningskarta:

- Kameror
- Ingångar
- Reläer
- Kommandoskript
- Sekvenser

- Dokument
- Länkar till andra webbplatskartor
- VRM
- iSCSI
- Läsare av ett passersystem
- Inbrottspaneler
- Management Server för Enterprise Systems

Tillägget av en post på en anläggningskarta skapar en aktiveringspunkt på kartan.

När du lägger till en post i en kartmapp i det logiska trädet, så visas det också i det övre vänstra hörnet på kartan. När du lägger till en post i en kartmapp, läggs den också till i motsvarande kartnod i det logiska trädet för Operator Client.

Du kan lägga till följande poster från enhetsträdet på en global karta:

- Kameror

För konfigurering av det logiska trädet utför du en del eller alla följande steg flera gånger.

Se

- *Sidan Kartor och struktur, sidan 241*

16.2

Lägga till en enhet till det logiska trädet

Huvudfönster > **Kartor och struktur Logiskt träd > fliken**

Så här kan du lägga till en enhet:

- ▶ Dra ett objekt från enhetsträdet till platsen där det behövs i det logiska trädet. Du kan dra en hel nod med alla underobjekt från enhetsträdet till det logiska trädet. Du kan markera flera enheter samtidigt genom att hålla CTRL- eller SKIFT-tangenten nedtryckt.

Se

- *Sidan Kartor och struktur, sidan 241*

16.3

Ta bort ett trädobjekt

Huvudfönster > **Kartor och struktur Logiskt träd > fliken**

Så här tar du bort ett trädobjekt från det logiska trädet:

- ▶ Högerklicka på ett objekt i det logiska trädet och välj **Ta bort**. Om det valda objektet innehåller underobjekt visas en meddelanderuta. Bekräfta genom att klicka på **OK**. Objektet tas bort. När du tar bort ett objekt från en kartmapp i det logiska trädet tas det även bort från kartan.

Se

- *Sidan Kartor och struktur, sidan 241*

16.4

Hantera resursfiler

Huvudfönster **Kartor och struktur > > fliken Logiskt träd >**  eller

Huvudfönster > **Larm >** 

Du kan importera resursfiler i följande format:

- DWF-filer (2 D, kartresursfiler)

- PDF
- JPG
- PNG
- HTML-filer
- MP3 (ljudfil)
- TXT-filer (kommandoskript eller kamerasekvenser)
- MHT-filer (webbarkiv)
- URL-filer (länkar till webbsidor)
- HTTPS URL-filer (länkar till Intelligent Insights-widgetar)
- WAV (ljudfil)

De importerade resursfilerna läggs till i en databas. De är inte länkade till originalfilerna.

**Obs!**

Efter var och en av följande uppgifter:

Klicka på  för att spara inställningarna.

Importera en resursfil:

1. Klicka på  .
Dialogrutan **Importera resurs** visas.
2. Välj en eller flera filer.
3. Klicka på **Öppna**.
De valda filerna läggs till i listan.
Om en fil redan har importerats visas en meddelanderuta.
Om du väljer att importera en fil som redan importerats läggs en ny uppgift till i listan.

Importera en resursfil:

1. Välj en resursfil.
2. Klicka på  .
Den valda resursfilen tas bort från listan.

Ändra namn på en resursfil:

1. Välj en resursfil.
2. Klicka på  .
3. Skriv in det nya namnet.
Originalfilens namn och datum för skapande kvarstår.

Ersätta innehållet i en resursfil:

1. Välj en resursfil.
2. Klicka på  .
Dialogrutan **Ersätt resurs** visas.
3. Välj en fil med lämpligt innehåll och klicka på **Öppna**.
Resursnamnet kvarstår, originalfilens namn byts ut mot det nya filnamnet.

Exportera en resursfil:

1. Välj en resursfil.
2. Klicka på  .
En dialogruta där du kan välja en katalog visas.

3. Välj lämplig katalog och klicka på **OK**.
Originalfilen exporteras.

Se

- *Välj resurs-dialogrutan, sidan 246*

16.4.1**Resurshanteraren-dialogrutan**

Huvudfönster > **Kartor och struktur** >  > dialogrutan **Resurshanteraren**

Gör att du kan hantera resursfiler.

Du kan hantera följande filformat:

- DWF-filer (kartresursfiler)
När filerna ska användas i Operator Client konverteras de till ett bitmapsformat.
- PDF
- JPG
- PNG
- HTML-filer (HTML-dokument, t.ex. åtgärdsplaner)
- MP3 (ljudfil)
- TXT-filer (textfiler)
- URL-filer (innehåller länkar till webbsidor eller Intelligent Insights-widgetar)
- MHT-filer (webbarkiv)
- WAV (ljudfil)
- EXE



Klicka för att visa en dialogruta för import av en resursfil.

Klicka för att visa dialogrutan



Lägg till URL.

Klicka för att visa dialogrutan



Länk till extern applikation.



Klicka för att ta bort den valda resursfilen.



Klicka för att ändra namn på den valda resursfilen.



Klicka för att visa en dialogruta där du kan byta ut den valda resursfilen mot en annan.



Klicka för att visa en dialogruta för export av den valda resursfilen.

16.4.2**Välj resurs-dialogrutan**

Huvudfönster > **Kartor och struktur** >



Gör det möjligt att lägga till en kartfil i DWF-, PDF-, JPG- eller PNG-format till det logiska trädet.

Välj en resursfil:

Klicka på ett filnamn för att välja en kartfil. Innehållet i vald fil visas i förhandsvisningsdelen.

Hantera...

Klicka för att visa dialogrutan **Resurshanteraren**.

Se

- *Lägga till en karta, sidan 251*
- *Tilldela en karta till en mapp, sidan 252*
- *Lägga till ett dokument, sidan 247*

16.5

Lägga till ett dokument

Huvudfönster > **Kartor och struktur Logiskt träd > fliken**

Du kan lägga till textfiler, HTML-filer (inklusive MHT-filer), URL-filer (med en internetadress) eller HTTPS URL-filer (som till exempel innehåller en Intelligent Insights-widget) som dokument. Och du kan lägga till en länk till ett annat program.

Innan du kan lägga till ett dokument måste du importera dokumentfiler.

Se *Hantera resursfiler, sidan 244* för ytterligare information om att importera dokumentfiler.

Så här lägger du till en kartdokumentfil/en Intelligent Insights-widget:

1. Se till att den dokumentfil du vill lägga till redan har importerats.
2. Välj en mapp där du vill lägga till det nya dokumentet.
3. Klicka på . Dialogrutan **Välj resurs** visas.
4. Markera en fil i listan. Om de filer som krävs inte är tillgängliga i listan klickar du på **Hantera...** för att visa dialogrutan **Resurshanteraren** för import av filer.
5. Klicka på **OK**. Ett nytt dokument läggs till under vald mapp.

Se

- *Välj resurs-dialogrutan, sidan 246*
- *Hantera resursfiler, sidan 244*

16.5.1

Lägg till URL-dialogrutan

Huvudfönster > **Kartor och struktur** >  > 

Gör att du kan lägga till en HTTP-internetadress (URL) eller en HTTPS-internetadress såsom Intelligent Insights-widgetar i systemet. Du kan lägga till denna URL i det logiska trädets som ett dokument. Användaren kan visa en internetsida eller en Intelligent Insights-widget i sin Operator Client.

Namn

Ange ett displaynamn för URL-adressen.

URL

Ange URL-adressen.

Endast för säker anslutning**Användare**

Ange användarnamnet för HTTPS URL.

Lösenord:

Ange lösenordet för HTTPS URL.

Visa lösenord

Klicka här om du vill att det angivna lösenordet ska visas. Var försiktig så att ingen obehörig kan se lösenordet.

Se

- *Lägga till ett dokument, sidan 247*

16.6 Dialogrutan Länk till extern applikation

Huvudfönster > **Kartor och struktur** > **Logiskt träd** flik >  > **Resurshanteraren**

dialogrutan >  > **Länk till extern applikation** dialogrutan

Gör att du kan lägga till en länk till ett externt program. Länken måste vara giltig på den arbetsstation där den används.



Obs!

Ett externt program som börjar med en välkomstskärm fungerar inte som förväntat.

Ett externt program som delar funktioner med Operator Client fungerar inte som tänkt och kan, i sällsynta fall, leda till att Operator Client kraschar.

Namn

Skriv in ett namn för den länk som visas i det logiska trädet.

Sökväg

Skriv in eller bläddra till sökvägen för det externa programmet. Den här sökvägen måste vara giltig på arbetsstationen där användaren av Operator Client använder länken.

Argument

Ange om nödvändigt argument för kommandot som kör det externa programmet.

16.7 Lägga till ett kommandoskript

Huvudfönster > **Kartor och struktur** **Logiskt träd** > **fliken**

Innan du kan lägga till Kommandoskript, måste du ha skapat eller importerat kommandoskriptfiler.

Se *Konfiguration av kommandoskript, sidan 85* för detaljer vid behov.

Lägga till en kommandoskriptfil:

1. Välj en mapp där du vill lägga till det nya kommandoskriptet.

2. Klicka på . Dialogrutan **Välj klientskript** visas.

3. Markera en fil i listan.

4. Klicka på **OK**.

Ett nytt kommandoskript läggs till i vald mapp.

Se

– *Välj resurs-dialogrutan, sidan 246*

16.8 Lägga till en kamerasekvens

Huvudfönster > **Kartor och struktur** **Logiskt träd** > **fliken**

Du kan lägga till en kamerasekvens i rotkatalogen eller i en mapp i det logiska trädet.

Så här lägger du till en kamerasekvens:

1. Välj en mapp i det logiska trädet där du vill lägga till en ny kamerasekvens.

2. Klicka på . Dialogrutan **Sekvensbyggare** visas.

3. Välj en kamerasekvens i listan.

4. Klicka på **Lägg till i logiskt träd**. En ny  läggs till under vald mapp.

Se

– *Sekvensbyggare-dialogrutan, sidan 249*

16.8.1

Sekvensbyggare-dialogrutan

Huvudfönster > **Kartor och struktur** > 

Låter dig hantera kamerasekvenser.

Ikoner

	Klicka för att visa dialogrutan Lägg till sekvens .
	Klicka för att ändra namn på en kamerasekvens.
	Klicka för att ta bort vald kamerasekvens.

Lägg till steg

Klicka för att visa dialogrutan **Lägg till sekvenssteg**.

Ta bort steg

Klicka för att ta bort valda steg.

Steg

Visar stegets nummer. Alla kameror från ett specifikt steg har samma fördröjningstid.

Fördröjning

Gör att du kan ändra fördröjningstiden (sekunder).

Kameranummer

Klicka på en cell för att välja en kamera via dess logiska nummer.

Kamera

Klicka på en cell för att välja en kamera via dess namn.

Kamerafunktion

Klicka på en cell för att ändra kamerans funktion i denna rad.

Data

Ange hur länge den valda kamerafunktionen ska vara aktiv. För att göra den här konfigurationen måste du ha valt en post i kolumnen **Kamera** och en post i kolumnen

Kamerafunktion.

Dataenhet

Välj enheten för vald tid, till exempel sekunder. För att göra den här konfigurationen måste du ha valt en post i kolumnen **Kamera** och en post i kolumnen **Kamerafunktion**.

Lägg till i logiskt träd

Klicka för att lägga till vald kamerasekvens till det logiska trädet och stänga dialogrutan.

Se

– *Hantera förkonfigurerade kamerasekvenser, sidan 249*

16.9

Hantera förkonfigurerade kamerasekvenser

Huvudfönster > **Kartor och struktur** **Logiskt träd** > **fliken**

Du kan utföra följande uppgifter för att hantera kamerasekvenser:

– Skapa en kamerasekvens

- Lägga till ett steg med ny fördröjningstid till en befintlig kamerasekvens
- Ta bort ett steg från en kamerasekvens
- Ta bort kamerasekvens

**Obs!**

Om konfigurationen ändras och aktiveras fortsätter en kamerasekvens (förkonfigurerad eller automatisk) vanligtvis när Operator Client har startats om.

I följande fall fortsätter dock inte sekvensen:

En monitor som sekvensen har konfigurerats att visas på har tagits bort.

Läget för en monitor (enkel/fyrbildsvy) som sekvensen har konfigurerats att visas på har ändrats.

Det logiska numret för en monitor som sekvensen har konfigurerats att visas på har ändrats.

**Obs!**

Efter var och en av följande uppgifter:

Klicka på  för att spara inställningarna.

Så här skapar du en kamerasekvens:

1. Välj en mapp i det logiska trädet där du vill skapa en kamerasekvens.

2. Klicka på .
Dialogrutan **Sekvensbyggare** visas.

3. I dialogrutan **Sekvensbyggare** klickar du på .
Dialogrutan **Lägg till sekvens** visas.

4. Ange passande värden.

5. Klicka på **OK**.

En ny kamerasekvens  läggs till.

För detaljerad information om olika fält, se onlinehjälpfen för lämpligt programfönster.

Lägga till ett steg med ny fördröjningstid till en kamerasekvens:

1. Välj önskad kamerasekvens.
2. Klicka på **Lägg till steg**.
Dialogrutan **Lägg till sekvenssteg** visas.
3. Gör lämpliga inställningar.
4. Klicka på **OK**.
Ett nytt steg läggs till i kamerasekvensen.

Ta bort ett steg från en kamerasekvens:

- ▶ Högerklicka på önskad kamerasekvens och klicka på **Ta bort steg**.
Steget med det högsta numret tas bort.

Ta bort en kamerasekvens:

1. Välj önskad kamerasekvens.
2. Klicka på . Den valda kamerasekvensen tas bort.

Se

- *Sekvensbyggare-dialogrutan, sidan 249*

16.9.1 Lägg till sekvens-dialogrutan

Huvudfönster > **Kartor och struktur** >  > dialogrutan **Sekvensbyggare** > 
Låter dig konfigurera egenskaperna för en kamerasekvens.

Sekvensnamn:

Ange ett lämpligt namn för den nya kamerasekvensen.

Logiskt nummer.

För användning med ett Bosch IntuiKey-tangentbord ange ett logiskt nummer för sekvensen.

Fördröjning:

Ange lämplig fördröjningstid.

Kameror per steg:

Ange antalet kameror för varje steg.

Steg:

Ange lämpligt antal steg.

16.9.2 Lägg till sekvenssteg-dialogrutan

Huvudfönster > **Kartor och struktur** >  > knappen **Lägg till steg**
Låter dig lägga till ett steg med ny fördröjningstid till en befintlig kamerasekvens.

Fördröjning:

Ange lämplig fördröjningstid.

16.10 Lägga till en mapp

Huvudfönster > **Kartor och struktur** **Logiskt träd > fliken**

Så här lägger du till en mapp:

1. Välj en mapp där du vill lägga till den nya mappen.
2. Klicka på . En ny mapp läggs till under vald mapp.
3. Klicka på  för att ändra namn på mappen.
4. Ange det nya namnet och tryck på ENTER.

Se

– *Sidan Kartor och struktur, sidan 241*

16.11 Lägga till en karta

Huvudfönster > **Kartor och struktur** **Logiskt träd > fliken**

Innan du kan lägga till en karta måste du importera kartresursfiler.

Se *Hantera resursfiler, sidan 244* för mer information om att importera en kartresursfil.

Lägga till en karta:

1. Se till att den kartresursfil du vill lägga till redan har importerats.
2. Välj en mapp där du vill lägga till den nya kartan.

3. Klicka på . Dialogrutan **Välj resurs** visas.
4. Välj en fil i listan.

Om de filer som krävs inte är tillgängliga i listan, klicka på **Hantera...** för att visa dialogrutan för **Resurshanteraren** för import av filer.

5. Klicka på **OK**.

En ny karta  läggs till under vald mapp.
Kartan visas.

Alla enheter inom denna mapp visas i det övre vänstra hörnet på kartan.

Se

– *Välj resurs-dialogrutan, sidan 246*

16.12

Lägga till en länk till en annan karta

Huvudfönster > **Kartor och struktur Logiskt träd > fliken**

När du har lagt till minst två kartor kan du lägga till en länk från en karta till den andra så att användaren kan klicka från den ena kartan till en som den är länkad till.

Lägga till en länk:

1. Klicka på en kartmapp  i det logiska trädet.
2. Högerklicka på kartan och klicka **Skapa länk**.
Då **Välj karta till länk** visas dialogrutan.
3. Klicka på en karta  i dialogrutan.
4. Klicka på **Välj**.
5. Dra objektet till lämplig plats på kartan.

16.12.1

Välj karta för länk-dialogrutan

Huvudfönster > **Kartor och struktur** > Välj en kartmapp  i det logiska trädet > Högerklicka på kartan och klicka på **Skapa länk**

Låter dig välja en karta för att skapa en länk till en annan karta.



Klicka på en annan karta för att välja denna.

Välj

Klicka för att infoga länken i den valda kartan.

16.13

Tilldela en karta till en mapp

Huvudfönster > **Kartor och struktur Logiskt träd > fliken**

Innan du kan tilldela kartor måste du importera kartresursfiler.

Se *Hantera resursfiler, sidan 244* för detaljer vid behov.

Tilldela en kartresursfil:

1. Högerklicka på en mapp och klicka på **Tilldela karta**.
Dialogrutan **Välj resurs** visas.
2. Välj en kartresursfil i listan.
3. Klicka på **OK**. Den valda mappen visas som .
Kartan visas i kartfönstret.
Alla objekt inom denna mapp visas i det övre vänstra hörnet på kartan.

Se

– *Sidan Kartor och struktur, sidan 241*
– *Välj resurs-dialogrutan, sidan 246*

16.14 Hantera enheter på en anläggningskarta

Huvudfönster > **Kartor och struktur** Logiskt träd > **fliken**

Innan du kan hantera enheter på en anläggningskarta måste du lägga till en karta eller tilldela en karta till en mapp och lägga till enheter i mappen.



Obs!

Efter var och en av följande uppgifter:

Klicka på  för att spara inställningarna.

Så här placerar du objekt på en anläggningskarta:

1. Välj en kartmapp.
2. Dra enheter från enhetsträdet till kartmappen.
Enheter i en kartmapp finns längst upp till vänster på anläggningskartan.
3. Dra objekten till lämpliga platser på anläggningskartan.

Så här tar du bort ett objekt i det logiska trädet endast från anläggningskartan:

1. Högerklicka på objektet på kartan och klicka **Osynlig**.
Objektet tas bort från anläggningskartan.
Objektet finns kvar i det logiska trädet.
2. För att göra det synligt igen högerklickar du på enheten i det logiska trädet och klickar **Synlig på kartan**.

Så här tar du bort ett objekt från anläggningskartan och från hela det logiska trädet:

- Högerklicka på objektet i det logiska trädet och klicka på **Ta bort**.
Objektet tas bort från anläggningskartan och från det logiska trädet.

Så här ändrar du ikonerna för en kameras riktning:

- Högerklicka på objektet, peka på **Byt bild** och välj önskad ikon.
Ikonen ändras.

Så här ändrar du ett objekts färg:

- Högerklicka på objektet och klicka på **Byt färg**. Välj önskad färg.
Ikonen ändras.

Så här kringgår du eller slutar att kringgå en enhet på en anläggningskarta:

1. Högerklicka på den specifika enheten på anläggningskartan.
2. Klicka på **Kringgå / Sluta kringgå**.



Obs!

Du kan filtrera enheter som har kringgåts i textfältet för sökning.

Se

- *Kringgå enheter, sidan 259*
- *Sidan Kartor och struktur, sidan 241*

16.15 Konfigurera globala kartor och kartvyportar

Huvudfönster > **Kartor och struktur** > **Global karta** fliken

För att kunna använda onlinekartor eller Map-based tracking assistant i Operator Client måste du lägga till och konfigurera kameror på den globala kartan.

Du kan konfigurera kartvyportar från en global karta. En kartvyport är ett område på den globala kartan med ett specifikt mitt- och zoomnivå. En kartvyport kan visas i en bildruta i Operator Client.

Om du vill skapa en kartvyport eller använda Map-based tracking assistant i Operator Client gör du följande först:

1. Välj bakgrundskarttyp för den globala kartan.
2. Dra kamerorna till den globala kartan.
3. Konfigurera kamerornas riktning och visningskon på den globala kartan.

Om du vill skapa en kartvyport eller använda Map-based tracking assistant i Operator Client **på flera olika våningar** gör du först följande:

1. Välj bakgrundskarttyp för den globala kartan.
2. Lägg till en karta på den globala kartan.
Obs! Den första kartan som du lägger till kommer att vara bottenvåningen. Om du väljer offline-bakgrundsmappningstypen **Inga** blir den första karta som du lägger till bakgrundskartan.
3. Lägg till våningar på bottenvåningen eller på bakgrundskartan.
4. Välj önskad våning.
5. Dra kamerorna till våningskartan.
6. Konfigurera riktning och visningskon för dina kameror.

16.15.1

Konfigurera den globala kartan

Du kan definiera bakgrundsmappningstyper för den globala kartan och söka efter kameror, platser och adresser.

Så här ändrar du bakgrundskarttyp för den globala kartan:

1. Gå till huvudfönstret och välj menyn **Inställningar** > kommandot **Alternativ....**
2. Välj lämpligt alternativ.
Obs! Om du har tillgång till Internet kan du välja en bakgrundskarttyp online (Here kartor). Om du inte har tillgång till Internet väljer du offline-bakgrundskarttypen **Inga**.
Du måste köpa en licens för att använda onlinekartor.
3. Om du har valt en bakgrundskarttyp online anger du din kunds specifika API-nyckel.
4. Klicka på **Test** för att kontrollera API-anslutningen.
5. Klicka på **OK**.



Obs!

Om du byter typ av bakgrundskarta från online (kartor Here) till offline (**Inga**) eller tvärtom förlorar du alla placerade kamerahotspots och kartvyportar.

Du kan bara definiera en bakgrund för den globala kartan. Den här bakgrunden gäller för alla kartvyportar.

Så här söker du efter kameror eller platser på den globala kartan:

1. Skriv namnet på en kamera, plats eller adress i sökfältet.
Så snart du börjar skriva en rullgardinsmeny med en lista med relevanta alternativ visas.
2. Välj respektive alternativ i listan

Kameran, platsen eller adressen visas och indikeras med en flagga  i några sekunder.

Se

- *Dialogrutan Alternativ (menyn Inställningar), sidan 114*

16.15.2

Konfigurera kameror på den globala kartan

Så här konfigurerar du en kamera på den globala kartan:

Obs! Om du har konfigurerat flera våningar på kartor kontrollerar du att du väljer rätt våning där du vill konfigurera kamerorna.

1. Välj **Global karta** -fliken.
2. Om du vill gå till den plats där du vill placera kameran skriver du en adress eller en plats i sökfältet.

Du kan också zooma in och ut med knapparna  och  eller musrullningshjulet.

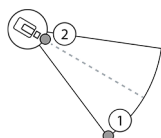
3. Dra en kamera från enhetsträdet till respektive område på den globala kartan.
4. Klicka på kameran för att välja den.
5. Konfigurera kamerans riktning och vinkel.

Obs! När du väljer en kupolkamera ser du den nåbara vykonen och den faktiska vinkeln. En varningssymbol anger att kupolkameran behöver en horisontell och vertikal kalibrering. Om du vill kalibrera kupolkameran öppnar du förhandsgranskningen av livevideon.

6. Klicka på  om du vill visa en livevideoförhandsvisning av den valda kameran. Förhandsgranskningen av videon kan hjälpa dig att konfigurera riktningen och vinkeln.
7. Klicka på  om du vill dölja videoförhandsgranskningen av den markerade kameran.

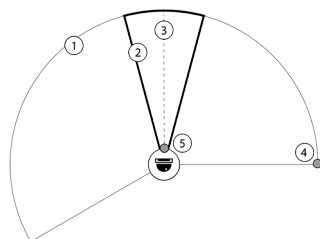
Obs! Om du lägger till en kamera på den globala kartan och inte redan har lagt till den här kameran i det logiska trädet läggs den automatiskt till i slutet av det logiska trädet.

Så här konfigurerar du kamerans riktning och vinkel:



1. Dra för att konfigurera vinkeln.
2. Dra för att rotera och konfigurera riktningen.

Så här konfigurerar du den vågräta riktningen och vinkeln för en PTZ-kamera (plattform CPP4 eller högre):



1. Den nåbara visningskonen anger det teoretiskt nåbara visningsområdet.
2. Den faktiska vinkeln anger PTZ-kamerans faktiska PTZ-position
3. Panoreringsvinkel 0.
4. Dra för att konfigurera vinkeln.
5. Dra för att rotera och konfigurera riktningen.



Obs!

För att säkerställa optimal användning av Map-based tracking assistant, måste du också justera PTZ-kamerans vertikala position. Vi rekommenderar att du justerar den vertikala positionen i livevideoförhandsvisningen baserat på en välkänd position i området, till exempel baserat på ett distinkt monument. Sedan används alltid denna konfigurerade vertikala position i Map-based tracking assistant.

Så här visar eller döljer du kameraförhandsvisningar:

1. Klicka på  om du vill visa en livevideoförhandsvisning av den valda kameran.
Alternativt
Högerklicka på kameran och välj **Visa förhandsgranskningar**.
Videoförhandsvisningen kan hjälpa dig att konfigurera riktungs- och visningskonen.
2. Klicka på  om du vill dölja videoförhandsvisningen för den valda kameran.
Alternativt
Högerklicka på kameran och välj **Dölj förhandsgranskningar**.

Så här tar du bort en kamera från den globala kartan:

- Högerklicka på kameran och välj **Ta bort**.

Så här gör du en kamera synlig på alla våningar:

- Högerklicka på kamerans aktiveringspunkt och välj **Synlig på alla våningar**.
Kameran är nu alltid synlig när du väljer en annan våning.

Gruppering av kamera aktiveringspunkter

Om du redan har flera kameror konfigurerade på den globala kartan och zoomar ut, grupperas kamerans aktiveringspunkter till aktiveringspunktgrupper. Antalet enskilda aktiveringspunkter i en aktiveringspunktsgrupp visas. En markerad kamera visas inte som en del av ett kluster.

16.15.3**Lägga till kartor på den globala kartan**

Du kan lägga till dina egna bygg kartfiler ovanpå den globala kartan.

Våra BVMS operatörer kan då få en mer detaljerad bild av vissa kameraplatser.

Så här lägger du till en karta på den globala kartan:

1. Välj **Global karta** -fliken.
2. Om du vill gå till den plats där du vill placera karta skriver du en adress eller en plats i sökfältet.

Du kan också zooma in och ut med knapparna  och  eller musrullningshjulet.

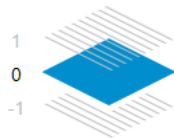
3. Klicka på .
4. Fönstret **Välj resurs** öppnas.
5. Välj en karta och klicka på **OK**.
6. Klicka på och dra  för att rotera kartan.
7. Klicka på och dra  för att flytta kartan.
8. Använd dragpunkterna för att justera kartans storlek.
9. Klicka på  för att ta bort kartan.

Obs! Om du vill lägga till flera våningar kommer den första kartan som du lägger till att vara

bottenvåningen. Bottenvåningen indikeras av siffran 0 i fältet .

Så här lägger du till fler våningar på bottenvåningen:

1. Klicka på siffran 0 i fältet .



Fältet öppnas.

2. Välj den våning där du vill lägga till en karta.
3. **Obs!** Du kan bara välja nästa högre eller nedre våning för att lägga till en karta.
4. Klicka på .
- Fönstret **Välj resurs** öppnas.
5. Välj en karta och klicka på **OK**.
6. Ändra den tillagda våningskartan så att dess position matchar bottenvåningskartans position.

Så här gör du en våning synlig på alla våningar:

1. Högerklicka på någon av justeringsikonerna på respektive våningskarta, ☺, + eller ×.
2. Välj **Synlig på alla våningar**.

Denna våning är nu alltid synlig när du väljer en annan våning.

Obs! Om du inte har tillgång till Internet och du har valt offline-bakgrundskartatypen **Inga** kan du lägga till en karta som bakgrundskarta. Vi rekommenderar att du gör denna bakgrundskarta synlig på alla våningar. Bakgrundskartan kommer då alltid att vara synlig om du väljer en annan våning.

16.16

Lägga till en kartvyport

Huvudfönster > **Kartor och struktur** Logiskt träd > **fliken**

Lägga till en kartvyport:

1. Klicka på  om du vill lägga till en kartvyport.
2. Skriv namnet på kartvyporten.
3. Om du vill gå till den plats där du vill skapa kartvyporten skriver du en adress eller plats i sökfältet på den globala kartan.

Om du inte känner till adressen eller platsen kan du zooma in och ut med knapparna



och



eller musrullningshjulet.

4. Klicka på  för att spara din konfiguration.



Obs!

Om en kartvyport innehåller olika våningar är det våningen som väljs när konfigurationen sparas som visas i Operator Client när operatören öppnar kartvisningsområdet. Operatören kan ändra våningen i kartvisningsområdet i bildrutan efteråt.

16.17

Aktivera Map-based tracking assistant för kartbaserad spårning

Map-based tracking assistant hjälper dig att spåra rörliga objekt över flera kameror.

Respektive kameror måste konfigureras på den globala kartan. Om ett intressant rörligt objekt visas i live-, uppspelnings- eller larmbildsfönstret kan användaren starta Map-based tracking assistant som visar alla kameror i närheten automatiskt.

Så här aktiverar du Map-based tracking assistant:

1. Gå till huvudfönstret och välj menyn **Inställningar** > kommandot **Alternativ....**
2. Markera kryssrutan **Aktivera systemfunktion.**
3. Klicka på **OK.**

16.18**Lägga till ett felövervakningsrelä**

Huvudfönster > **Kartor och struktur** > **Logiskt träd** fliken > **Felövervakningsrelä** dialogrutan

Avsedd användning

Ett felövervakningsrelä aktiveras vid ett allvarligt systemfel så att ett externt larm går (varningsljus, siren osv.).

Användaren måste återställa reläet manuellt.

Felövervakningsreläet kan vara något av följande:

- BVIP-kodarrelä eller avkodarrelä
- ADAM-relä
- Inbrottspanelsutdata

Exempel

Om något händer som allvarligt påverkar systemets funktion (till exempel ett fel på en hårddisk) eller en incident inträffar som utgör en säkerhetsrisk (till exempel att en referensbild inte kan kontrolleras) aktiveras felövervakningsreläet. Det kan till exempel göra att ett ljudlarm går eller att dörrar stängs automatiskt.

Funktionsbeskrivning

Du kan konfigurera ett enskilt relä som ett felövervakningsrelä. Felövervakningsreläet aktiveras automatiskt när någon av flera användardefinierade händelser inträffar. Aktiveringen av ett relä betyder att ett kommando skickas till reläet om att det ska stängas. Den efterföljande händelsen "Relä stängt" kopplas bort från kommandot och genereras och tas emot endast om reläet ändras fysiskt. Till exempel skickar ett relä som redan är stängt inte denna händelse. Bortsett från att felövervakningsreläet aktiveras automatiskt av användardefinierade händelser fungerar det som vilket annat relä som helst. Felövervakningsreläet kan alltså avaktiveras av användare i Operator Client. Webbklienten kan också medge avaktivering av felövervakningsreläet. Eftersom vanliga åtkomstbehörigheter även gäller för felövervakningsreläet är det viktigt att beakta de inloggade användarnas rättigheter.

Så här lägger du till:

1. Välj önskat relä i listan **Felövervakningsrelä.**
2. Klicka på **Händelser ...**
Dialogrutan **Val av händelse för felövervakningsrelä** visas.
3. Klicka för att välja önskade händelser som kan utlösa felövervakningsreläet.
4. Klicka på **OK.**
Felövervakningsreläet läggs till i systemet.

16.18.1**Dialogrutan för felövervakningsrelä**

Huvudfönster > **Kartor och struktur** > **Logiskt träd** fliken > **Felövervakningsrelä** dialogrutan

Du kan lägga till ett felövervakningsrelä i systemet. Du definierar reläet som ska användas som felövervakningsrelä och du konfigurerar de händelser som ska utlösa felövervakningsreläet.

Reläet måste redan vara konfigurerat i det logiska trädet.

Felövervakningsrelä

Välj önskat relä i listan.

Händelser ...

Klicka för att visa dialogrutan **Val av händelse för felövervakningsrelä**.

16.19**Kringgå enheter**

Huvudfönster > **Kartor och struktur Logiskt träd > fliken**

Du kan kringgå vissa kodare, kameror, ingångar och reläer, till exempel vid konstruktionsarbete. Om en kodare, kamera, ingång eller ett relä kringgås stoppas inspelningen, BVMS Operator Client visar inga händelser eller larm och larm registreras inte i loggboken.

Kamerorna som kringgås visar fortfarande direktsänd video i Operator Client och operatören har fortfarande åtkomst till gamla inspelningar.

**Obs!**

Om kodaren kringgås genereras inga larm eller händelser för någon kamera eller ingång eller för något relä för kodaren i fråga. Om en kamera, en ingång eller ett relä kringgås separat och den aktuella enheten kopplas bort från kodaren genereras fortfarande larm.

Så här kringgår du eller slutar att kringgå i det logiska trädet eller i enhetsträdet:

1. Högerklicka på enheten i det logiska trädet eller i enhetsträdet.
2. Klicka på **Kringgå** / **Sluta kringgå**.

Så här kringgår du eller slutar att kringgå en enhet på en karta:

Se *Hantera enheter på en anläggningskarta, sidan 253*

**Obs!**

Du kan filtrera enheter som har kringgåtts i textfältet för sökning.

Se

- *Hantera enheter på en anläggningskarta, sidan 253*

17

Sidan Scheman

Huvudfönster >

Gör att du kan konfigurera inspelningsscheman och uppgiftsscheman.



Klicka här för att ändra namn på valt inspelnings- eller uppgiftsschema.

Inspelningsscheman

Visar trädet för inspelningsscheman. Välj en post för att konfigurera.

Uppgiftsscheman

Visar trädet för uppgiftsscheman. Välj en post för att konfigurera.

Lägg till

Klicka för att lägga till ett nytt uppgiftsschema.

Ta bort

Klicka för att ta bort valt uppgiftsschema.

Se

– *Konfigurera scheman, sidan 262*

17.1

Sidan Inspelningsscheman

Huvudfönster > > Välj ett objekt i trädet för inspelningsscheman

Låter dig konfigurera inspelningsscheman.

Veckodagar

Klicka för att visa schematabellen för veckodagar. Tidsperioderna för alla konfigurerade inspelningsscheman visas.

Dra muspekaren för att välja tidsperioderna för valt schema. Alla valda celler får färgen som finns i det valda schemat.

Dygnets 24 timmar visas horisontellt. Varje timme delas in i 4 celler. En cell motsvarar 15 minuter.

Helgdagar

Klicka för att visa schematabellen för helgdagar.

Undantagsdagar

Klicka för att visa schematabellen för undantagsdagar.

Lägg till

Klicka för att visa dialogrutan där du lägger till nödvändiga helgdagar eller undantagsdagar.

Ta bort

Klicka för att visa dialogrutan där du tar bort nödvändiga helgdagar eller undantagsdagar.

Se

- *Konfigurera ett inspelningsschema, sidan 262*
- *Lägga till helgdagar och undantagsdagar, sidan 264*
- *Ta bort helgdagar och undantagsdagar, sidan 265*
- *Ändra namn på ett schema, sidan 265*

17.2

Sidan Uppgiftsscheman

Huvudfönster > > Välj ett objekt i trädet för uppgiftsscheman

Låter dig konfigurera tillgängliga uppgiftsscheman. Du kan konfigurera en standard eller ett återkommande mönster.

Standard

Klicka för att visa schematabellen där du konfigurerar standarduppgiftsscheman. Om du konfigurerar ett standardmönster gäller inget återkommande mönster för det valda schemat.

Återkommande

Klicka för att visa schematabellen där du konfigurerar ett återkommande mönster för det valda uppgiftsschemat. Till exempel, du konfigurerar ett schema för andra tisdagen i varje månad eller före den 4:e juli varje år. Om du konfigurerar ett återkommande mönster gäller inget standardmönster för det valda uppgiftsschemat.

Veckodagar

Klicka för att visa schematabellen för veckodagar.

Dra muspekaren för att välja tidsperioderna för valt schema. De valda cellerna visas i det valda schemats färg.

Dygnets 24 timmar visas horisontellt. Varje timme delas in i 4 celler. En cell motsvarar 15 minuter.

Helgdagar

Klicka för att visa schematabellen för helgdagar.

Undantagsdagar

Klicka för att visa schematabellen för undantagsdagar.

Ta bort allt

Klicka för att rensa tidsperioderna för alla tillgängliga dagar (veckodagar, helgdagar, undantagsdagar).

Välj alla

Klicka för att välja tidsperioderna för alla tillgängliga dagar (veckodagar, helgdagar, undantagsdagar).

Lägg till...

Klicka för att visa dialogrutan där du lägger till nödvändiga helgdagar eller undantagsdagar.

Ta bort...

Klicka för att visa dialogrutan där du tar bort helgdagar eller undantagsdagar.

Upprepningsmönster

Klicka på hur ofta du vill att uppgiftsschemat ska återkomma (dagligen, veckovis, månadsvis, årligen) och välj sedan motsvarande alternativ.

Dagsmönster

Dra muspekaren för att välja tidsperiod/en/erna för det återkommande mönstret.

Se

- *Lägga till ett uppgiftsschema, sidan 263*
- *Konfigurera ett standarduppgiftsschema, sidan 263*
- *Konfigurera ett återkommande uppgiftsschema, sidan 263*
- *Ta bort ett uppgiftsschema, sidan 264*
- *Lägga till helgdagar och undantagsdagar, sidan 264*
- *Ta bort helgdagar och undantagsdagar, sidan 265*
- *Ändra namn på ett schema, sidan 265*

18 Konfigurera scheman

Huvudfönster > **Scheman**

Det finns två tillgängliga schematyper:

- Inspelningsscheman
- Uppgiftsscheman

Du kan maximalt konfigurera 10 olika inspelningsscheman i Tabell för inspelningsscheman. I de här segmenten kan kamerorna uppföra sig olika. T.ex. kan de ha olika bildhastighet och upplösningsinställningar (kan konfigureras på sidan **Kameror och inspelning**). Vid varje tidpunkt är exakt ett inspelningsschema giltigt. Det finns inga luckor och inga överlappningar. Du konfigurerar uppgiftsscheman för schemaläggning av olika händelser som kan uppstå i ditt system (kan konfigureras på sidan **Händelser**).

Se ordlistan för definitioner av inspelningsscheman och uppgiftsscheman.

Scheman används på andra sidor i Configuration Client:

- Sidan **Kameror och inspelning**
Används för att konfigurera inspelning.
- Sidan **Händelser**
Används för att avgöra när händelser utlöser loggning, larm eller utförande av kommandoskript.
- Sidan **Användargrupper**
Används för att avgöra när medlemmarna av en användargrupp kan logga in.
- Klicka på  för att spara inställningarna.
- Klicka på  om du vill ångra den senaste inställningen.
- Klicka på  för att aktivera konfigurationen.

Se

- Sidan *Inspelningsscheman*, sidan 260
- Sidan *Uppgiftsscheman*, sidan 260

18.1 Konfigurera ett inspelningsschema

Huvudfönster > **Scheman**

Du kan lägga till undantagsdagar och helgdagar till alla inspelningsscheman. De här inställningar åsidosätter de normala veckoinställningarna.

Ordningsföljden för nedåttstigande prioritet är: undantagsdagar, helgdagar, veckodagar.

Det maximala antalet inspelningsscheman är 10. De första tre uppgifterna konfigureras

standardmässigt. Du kan ändra dessa inställningar. Uppgifter med en grå ikon  har inte en konfigurerad tidsperiod.

Inspelningsscheman delar samma veckodagar.

Varje standarduppgiftsschema har sina egna veckodagsmönster.

Konfigurera ett inspelningsschema:

1. Välj ett schema i trädet **Inspelningsscheman**.
2. Klicka på fliken **Veckodagar**.
3. Dra muspekaren i fältet **Schematabell** för att välja tidsperioder för valt schema. De valda cellerna visas i det valda schemats färg.

Anteckningar:

- Du kan markera en tidsperiod på en veckodag för ett inspelningsschema med färgen för ett annat inspelningsschema.

Se

- *Sidan Inspelningsscheman, sidan 260*

18.2**Lägga till ett uppgiftsschema**

Huvudfönster > **Scheman**

Lägga till ett uppgiftsschema:

1. Klicka på **Lägg till**.
En ny uppgift läggs till.
2. Lägg till lämpligt namn.
3. Klicka på **Standard** för ett vanligt uppgiftsschema eller **Återkommande** för ett återkommande uppgiftsschema.
Om du ändrar inställning visas en meddelanderuta. Klicka på **OK** om du vill ändra schematyp.

Ett vanligt uppgiftsschema visas som , ett återkommande uppgiftsschema som .

4. Gör lämpliga inställningar för det valda schemat.

Se

- *Sidan Uppgiftsscheman, sidan 260*

18.3**Konfigurera ett standarduppgiftsschema**

Huvudfönster > **Scheman**

Varje standarduppgiftsschema har sina egna veckodagsmönster.

Konfigurera ett standarduppgiftsschema så här:

1. Gå till trädet **Uppgiftsscheman** och välj ett standarduppgiftsschema.
2. Klicka på fliken **Veckodagar**.
3. Dra muspekaren i fältet **Schematabell** för att välja tidsperioder för valt schema.

Se

- *Sidan Uppgiftsscheman, sidan 260*

18.4**Konfigurera ett återkommande uppgiftsschema**

Huvudfönster > **Scheman**

Varje återkommande uppgiftsschema har sitt eget dagsschema.

Konfigurera ett återkommande uppgiftsschema:

1. I trädet **Uppgiftsscheman**, välj ett återkommande uppgiftsschema .
2. I fältet **Upprepningsmönster** klickar du på hur ofta du vill att uppgiftsschemat ska återkomma (**Dagligen**, **Per vecka**, **Per månad**, **Per år**) och gör sedan motsvarande inställningar.
3. Välj lämpligt startdatum i listan **Startdatum**.
4. I fältet **Dagsmönster**, dra muspekaren för att välja passande tidsperiod.

Se

- *Sidan Uppgiftsscheman, sidan 260*

18.5 Ta bort ett uppgiftsschema

Huvudfönster > > Välj ett objekt i trädet **Uppgiftsscheman**

Ta bort ett uppgiftsschema:

1. Välj ett objekt i trädet **Uppgiftsscheman**.
2. Klicka på **Ta bort**.

Uppgiftsschemat tas bort. Alla objekt som tilldelas till detta schema är inte schemalagda.

Se

- *Sidan Uppgiftsscheman, sidan 260*

18.6 Lägga till helgdagar och undantagsdagar

Huvudfönster > **Scheman**



Obs!

Du kan konfigurera tomma undantagsdagar och helgdagar. Undantagsdagar och helgdagar ersätter schemat för motsvarande veckodag.

Exempel:

Den gamla konfigurationen:

Veckodagsschemat har konfigurerats till att vara aktivt från 9:00 till 10:00

Undantagsdagsschemat har konfigurerats till att vara aktivt från 10:00 till 11:00

Resultatet: aktivitet från 10:00 till 11:00

Samma beteende gäller för helgdagar.

Du kan lägga till helgdagar och undantagsdagar till ett inspelningsschema eller till ett uppgiftsschema.

Inspelningsscheman har samma helgdagar och undantagsdagar.

Varje standarduppgiftsschema har sina egna helgdags- eller undantagsdagsmönster.

Lägga till helgdagar och undantagsdagar i ett schema:

1. Välj ett schema i trädet **Inspelningsscheman** eller i trädet **Uppgiftsscheman**.
2. Klicka på fliken **Helgdagar**.
3. Klicka på **Lägg till**.
Dialogrutan **Lägg till helgdag(ar)** visas.
4. Välj en eller flera helgdagar och klicka på **OK**.
De valda helgdagarna läggs till i schematabellen.
5. Dra pekaren för att välja lämplig tidsperiod (det går inte för inspelningsscheman).
Valda celler rensas och tvärtom.
6. Klicka på fliken **Undantagsdagar**.
7. Klicka på **Lägg till**.
Dialogrutan **Lägg till undantagsdag(ar)** visas.
8. Välj en eller flera specialdagar och klicka på **OK**.
De valda specialdagarna läggs till i schematabellen.
9. Dra pekaren för att välja lämplig tidsperiod (det går inte för inspelningsscheman).
Valda celler rensas och tvärtom.
Sorteringsordningen för tillagda helgdagar och undantagsdagar är kronologisk.

Anteckningar:

- Du kan markera en tidsperiod på en helgdag eller undantagsdag för ett inspelningsschema med färgen för ett annat inspelningsschema.

Se

- *Sidan Inspelningsscheman, sidan 260*
- *Sidan Uppgiftsscheman, sidan 260*

18.7**Ta bort helgdagar och undantagsdagar**

Huvudfönster > **Scheman**

Du kan ta bort helgdagar och undantagsdagar från ett inspelningsschema eller från ett uppgiftsschema.

Ta bort heldagar och undantagsdagar från ett uppgiftsschema:

1. Välj ett schema i trädet **Inspelningsscheman** eller i trädet **Uppgiftsscheman**.
2. Klicka på fliken **Helgdagar**.
3. Klicka på **Ta bort**.
Dialogrutan **Markera de helgdagar som ska tas bort** visas.
4. Välj en eller flera helgdagar och klicka på **OK**.
De valda helgdagarna tas bort från schematabellen.
5. Klicka på fliken **Undantagsdagar**.
6. Klicka på **Ta bort**.
Dialogrutan **Markera undantagsdagarna som ska tas bort** visas.
7. Välj en eller flera undantagsdagar och klicka på **OK**.
De valda undantagsdagarna tas bort från schematabellen.

Se

- *Sidan Inspelningsscheman, sidan 260*
- *Sidan Uppgiftsscheman, sidan 260*

18.8**Ändra namn på ett schema**

Huvudfönster >

Ändra namn på ett schema:

1. Välj ett objekt i trädet **Inspelningsscheman** eller i trädet **Uppgiftsscheman**.
2. Klicka på  .
3. Ange det nya namnet och tryck på ENTER. Uppgiften namnändras.

Se

- *Sidan Inspelningsscheman, sidan 260*
- *Sidan Uppgiftsscheman, sidan 260*

19 Sidan Kameror och inspelning



Obs!

BVMS Viewer har bara grundläggande funktioner. Avancerade funktioner ingår i BVMS Professional. Detaljerad information om de olika BVMS utgåvorna finns på www.boschsecurity.com och BVMS Snabbvalsguiden: [BVMS snabbvalsguide](#).

Huvudfönster > **Kameror och inspelning**

Visar kameratabellens sida eller en sida med en inspelningstabell.

Gör att du kan konfigurera kameraegenskaper och inspelningsinställningar.

Gör att du kan filtrera kamerorna som visas efter typ.

Ikoner

	Klicka för att kopiera inspelningsinställningar från ett inspelningsschema till ett annat.
	Klicka för att visa dialogrutan Kvalitetsinställningar för ström .
	Klicka för att visa dialogrutan Schemalagda inspelningsinställningar .
	Klicka för att visa dialogrutan för konfiguration av en vald PTZ-kamera.
	Visar alla tillgängliga kameror oavsett deras lagringsenhet.
	Klicka här för att ändra kameratabellen enligt vald lagringsenhet.
	Visar motsvarande kameratabell. Inga inspelningsinställningar finns tillgängliga eftersom de här kamerorna inte spelas in i BVMS.
	Klicka här för att välja vilka kolumner som ska visas i tabellen Kameror .

Filter...

Skriv in en sträng och tryck på ENTER-tangenten för att filtrera de visade objekten. Endast objekt som innehåller strängen och deras motsvarande föräldraobjekt (endast i träd) visas. Antalet filtrerade objekt och det totala antalet objekt visas. Ett aktivt filter indikeras med . Skriv in strängar inom dubbla citattecken för att hitta dem exakt, till exempel filtrerar "Camera 1" kamerorna med exakt detta namn, inte camera 201.

Avbryt filtreringen genom att klicka på .

19.1 Sidan Kameror

Huvudfönster > **Kameror och inspelning** > Klicka på en ikon för att ändra sidan för kameror



enligt önskad lagringsenhet, till exempel

Visar diverse information om kameror som är tillgängliga i BVMS.

Gör att du kan ändra följande kameraegenskaper:

- Kameranamn
- Tilldelning av en ljudkälla
- Logiskt nummer
- PTZ-styrning, om sådan är tillgänglig
- Livekvalitet (VRM och live/lokal lagring)
- Profil för inspelningsinställningar
- Minsta och längsta lagringstid
- Avkänningsområde (ROI)
- ANR (Automated Network Replenishment)
- Dubbel strömning

Så här anpassar du tabellen Kameror:

1. Klicka på  för att välja vilka kolumner som ska visas i tabellen **Kameror**.
2. Klicka på en kolumnrubrik för att sortera tabellen efter denna kolumn.

Kamera - Kodare

Visar enhetstypen.

Kamera - Kamera

Visar kamerans namn.

Kamera - Nätverksadress

Visar kamerans IP-adress.

Kamera - Plats

Visar kamerans plats. Om kameran ännu inte är tilldelad ett logiskt träd visas **Inte tilldelad plats**.

Kamera - Enhetsfamilj

Visar namnet på den enhetsfamilj som den valda kameran tillhör.

Kamera - Antal

Klicka på en cell för att redigera det logiska numret som kameran automatiskt fick när den upptäcktes. Om du anger ett nummer som redan använts visas ett motsvarande felmeddelande.

Det logiska numret är åter "ledigt" när kameran tas bort.

Ljud

Klicka på en cell för att tilldela en ljudkälla till kameran.

Om ett larm med låg prioritet uppstår och hos en kamera som har ljudkonfigurerats spelas denna ljudsignal till och med fastän ett larm med högre prioritet visas vid det tillfället. Detta stämmer dock endast om högprioritetslarmet inte har någon ljudkonfiguration.

Strömmar / Strömgränser

Denna kolumn är endast avläst och anger strömningsgränserna för respektive kamera.

Obs! Strömningsgränserna visas bara för CPP13- och CPP14-kameror.

**Obs!**

Du kan inte redigera strömningsgränser i BVMS. Du kan redigera dem på kodarens webbplats eller i Configuration Manager. När du har redigerat strömningsgränserna på webbplatsen eller i Configuration Manager måste du uppdatera enhetens funktioner i BVMS. Om du inte uppdaterar enhetens funktioner skriver BVMS över de uppdaterade strömningsgränserna med de gamla inställningarna som visades när du senast uppdaterade enhetens funktioner.

Ström 1 - Codec / Ström 2 - Codec

Klicka på en cell för att välja önskad codec för kodning av strömmen.

Ström 3 - Codec

Välj önskad videoupplösning genom att klicka på en cell.

Värdena för videoupplösning läses in från kodaren. Det kan ta ett tag att visa dessa värden.

Obs! Endast CPP13- och CPP14-kameror stöder en tredje ström. Denna kolumn visas bara om du har konfigurerat minst en kamera som stöder en tredje ström.

Ström 1 - Kvalitet / Ström 2 - Kvalitet / Ström 3 - Kvalitet

Välj önskad ström kvalitet som ska användas live eller för inspelning. Du konfigurerar kvalitetsinställningarna i dialogrutan **Kvalitetsinställningar för ström**.

Ström 1 - Aktiv plattform / Ström 2 - Aktiv plattform / Ström 3 - Aktiv plattform

Visar namnet på plattformsinställningarna i dialogrutan **Kvalitetsinställningar för ström**. Den här kolumnen är skrivskyddad och anger vilka profilinställningar som kommer att skrivas till kodaren.

**Obs!**

Du kan bara använda ström 3 för livevisning. Inspelning är inte möjlig.

Live-video – Ström (endast VRM och endast live och lokal lagring)

Klicka i en cell för att välja strömmen för en VRM eller en kodare för lokal lagring/enda live.

Live-video – Profil (endast tillgänglig för ONVIF-kameror)

Klicka i en cell för att söka efter de tokens för liveprofiler som finns tillgängliga för den här ONVIF-kameran.

Om du väljer posten **<Automatisk>** används automatiskt strömmen med högst kvalitet.

Obs! Om du väljer en Video Streaming Gateway-enhet för att hämta livevideon i en arbetsstation blir **Live-video** är inställningen – **Profil**-inställningen inaktuell. Istället används inställningen **Inspelning – Profil** även för livevideo.

Live-video - ROI

Klicka om du vill aktivera Region of Interest (ROI). Detta är bara möjligt om följande post i kolumnen **Kvalitet** har valts för ström 2 och ström är kopplad till livevideo: H.264 MP SD ROI eller H.265 MP SD ROI.

Obs! Om ström 1 används live för en specifik arbetsstation kan operatörsklienten som körs på arbetsstationen inte aktivera ROI för kameran.



aktiveras automatiskt i tabellen .

Inspelning - Inställning

Klicka i en cell för att välja önskad inspelningsinställning. Du konfigurerar de tillgängliga inspelningsinställningarna i dialogrutan **Schemalagda inspelningsinställningar**.

Inspelning – Profil (endast tillgänglig för ONVIF-kameror)

Klicka i en cell för att söka efter de kodbrickor för inspelningsprofiler som finns tillgängliga för den här ONVIF-kameran. Välj önskad post.

Inspelning - ANR

Markera en kryssruta för att aktivera ANR-funktionen. Du kan bara aktivera funktionen om kodaren har rätt version av den fasta programvaran och rätt enhetstyp.

Inspelning - Max längd före larm

Visar den beräknade längden på förlarm för kameran. Det här värdet kan hjälpa dig att beräkna nödvändig lagringskapacitet på det lokala lagringsmediet.

**Obs!**

Om en speglad VRM redan har konfigurerats för en kodare kan du inte ändra några inställningar för denna kodare i kolumnerna **Sekundär inspelning**.

Sekundär inspelning – Inställning (endast tillgänglig om en sekundär VRM-enhet har konfigurerats)

Klicka i en cell för att ställa in en schemalagd inspelning för dubbel strömning för kodaren. Det kan hända att konfigurationen inte medger den konfigurerade ström kvaliteten för sekundär inspelning. Den ström kvalitet som har konfigurerats för primär inspelning används då i stället.

Sekundär inspelning – Profil (endast tillgänglig för ONVIF-kameror)

Klicka i en cell för att söka efter kodbrickor för inspelningsprofiler som finns tillgängliga för den här ONVIF-kameran.



(Endast synlig när du klickar på  **Alla**)

Markera en kryssruta för att aktivera PTZ-styrning.

Obs!

För portinställningar, se COM1.

Port (Endast synlig när du klickar på  **Alla**)

Klicka på en cell för att specificera vilken av kodarens serieportar används för PTZ-styrning.

För en PTZ-kamera ansluten till ett Bosch Allegiant-system kan du välja **Allegiant**. För en sådan kamera måste du använda en stamlinje.

Protokoll (Endast synlig när du klickar på  **Alla**)

Klicka på en cell för att välja lämpligt protokoll för PTZ-styrningen.

PTZ-adress (Endast synlig när du klickar på  **Alla**)

Ange adressnumret för PTZ-styrningen.

Inspelning – Minsta lagringstid [dagar]**Sekundär inspelning - Minsta lagringstid [dagar] (endast VRM och lokal lagring)**

Klicka på en cell för att ändra minsta antalet dagar som videomaterialet från den här kameran ska lagras. Videoinspelningar som är nyare än detta antal dagar tas inte bort automatiskt.

Inspelning – Längsta lagringstid [dagar]**Sekundär inspelning - Längsta lagringstid [dagar] (endast VRM och lokal lagring)**

Klicka på en cell för att ändra högsta antalet dagar som videomaterialet från den här kameran ska lagras. Videoinspelningar som är äldre än detta antal dagar tas bort automatiskt. 0 = obegränsat.

Se

- Konfigurera dubbel strömning i kameratabellen, sidan 282
- Konfigurera fördefinierade positioner och extra kommandon, sidan 279
- Konfigurera PTZ-portinställningar, sidan 279
- Konfigurera inställningarna för ström kvalitet, sidan 272
- Kopiera och klistra in i tabeller, sidan 271
- Konfigurera ANR-funktionen, sidan 282
- Exportera kameratabellen, sidan 272
- Tilldela en ONVIF-profil, sidan 283

- Konfigurera ROI-funktionen, sidan 281

19.2

Sidor för inspelningsinställningar

Huvudfönster > **Kameror och inspelning** >  > Klicka på fliken Inspelningsschema (till

exempel )

Gör att du kan konfigurera inspelningsinställningarna.

Inspelningsschemana som visas konfigureras i **Scheman**.

Endast de kolumner som är beskrivna inte ingår i en kameratabell.

- Klicka på en kolumnrubrik för att sortera tabellen efter denna kolumn.

Kontinuerlig inspelning

I kolumnen **Kvalitet** kan du klicka på en cell för att avaktivera inspelningen eller för att välja ström kvalitet för ström 1.

I kolumnen  markerar du en kryssruta för aktivering av ljud.

Inspelning live-/före-händelse

I kolumnen **Kvalitet** klickar du på en cell för att välja ström kvalitet på live-visningen (krävs för direktuppspelning) och inspelningsläget före händelse (krävs för rörelse- och larminspelning) för ström 2. Om dubbelströmmande är aktivt i den här kodaren kan du välja ström 1 att använda liveinspelning eller inspelning före händelse.

I kolumnen  markerar du en kryssruta för aktivering av ljud.

Rörelseinspelning

I kolumnen **Kvalitet** klickar du på en cell för att avaktivera inspelningen eller för att välja ström kvalitet för ström 1.

I kolumnen  markerar du en cell för aktivering av ljud.

I kolumnen **Före-händelse[r]** klickar du på en cell och väljer inspelningstid före rörelsehändelsen i sekunder.

I kolumnen **Efter-händelse[r]** klickar du på en cell och väljer inspelningstid efter rörelsehändelsen i sekunder.

Larminspelning

I kolumnen **Kvalitet** klickar du på en cell för att välja ström kvalitet för ström 1.

Konfigurera motsvarande larm för att aktivera larminspelning.

I kolumnen  markerar du en kryssruta för aktivering av ljud.

I kolumnen **Före-händelse[r]** klickar du på en cell och väljer tid före larmet i sekunder.

I kolumnen **Efter-händelse[r]** klickar du på en cell och väljer tid efter larmet i sekunder.

Se

- Kopiera och klistra in i tabeller, sidan 271

20

Konfigurera kameror och inspelningsinställningar

**Obs!**

Det här dokumentet beskriver vissa funktioner som inte är tillgängliga för BVMS Viewer. Detaljerad information om de olika BVMS utgåvorna finns i www.boschsecurity.com och BVMS snabbvalsguiden: [BVMS snabbvalsguide](#).

Huvudfönster > Kameror och inspelning

Detta kapitel tillhandahåller information om hur du konfigurerar kamerorna i ditt systemBVMS. Du konfigurerar diverse kameraegenskaper och inspelningsinställningar.

- Klicka på  för att spara inställningarna.
- Klicka på  om du vill ångra den senaste inställningen.
- Klicka på  för att aktivera konfigurationen.

Se

- *Sidan Kameror, sidan 266*
- *Dialogrutan Schemalagda inspelningsinställningar (endast VRM och Lokal lagring), sidan 276*
- *Kvalitetsinställningar för ström-dialogrutan, sidan 273*
- *Dialogrutan med fördefinierade positioner och extra kommandon, sidan 280*
- *Dialogrutan Kopiera inspelningsinställningar, sidan 282*

20.1

Kopiera och klistra in i tabeller

Du kan konfigurera många objekt samtidigt inom en kameratabell, en händelsekonfigurationstabell eller en larmkonfigurationstabell.

Du kan kopiera de konfigureringsbara värdena från en tabellrad till andra rader:

- Kopiera alla värden från en rad till andra rader.
- Kopiera endast ett värde från en rad till en annan rad.
- Kopiera värdet från en cell till en hel kolumn.

Du kan kopiera värdena på två olika sätt:

- Kopiera till Urklipp och klistra sedan in.
- Kopiera och klistra in direkt .

Du kan avgöra vilka rader du klistrar in till:

- Kopiera till alla rader.
- Kopiera till markerade rader.

Kopiera och klistra in alla konfigureringsbara värden från en rad till en annan rad:

1. Högerklicka på raden som innehåller önskat värde och klicka på **Kopiera rad**.
2. Klicka på den radrubrik vars rads innehåll du vill ändra.
För att markera fler än en rad, tryck på CTRL-tangenten och peka med musen på de andra radrubrikerna.
3. Högerklicka på tabellen och klicka på **Klistra in**.
Värdena kopieras.

Kopiera och klistra in ett värde från en rad till en annan rad:

1. Högerklicka på raden som innehåller önskat värde och klicka på **Kopiera rad**.
2. Högerklicka på cellen som du vill ändra, peka på **Klistra in cell i** och klicka på **Aktuell cell**.
Värdet kopieras.

Kopiera alla konfigureringsbara värden direkt:

1. Klicka på den radrubrik vars rads innehåll du vill ändra.
För att markera fler än en rad, tryck på CTRL-tangenten och peka med musen på de andra radrubrikerna.
2. Högerklicka på raden som innehåller de önskade värdena, peka på **Kopiera rad till** och klicka på **Valda rader**.
Värdena kopieras.

Kopiera ett värde direkt:

1. Klicka på den radrubrik vars rads innehåll du vill ändra.
För att markera fler än en rad, tryck på CTRL-tangenten och peka med musen på de andra radrubrikerna.
2. Högerklicka på cellen som innehåller det önskade värdet, peka på **Kopiera cell till** och klicka på **Urval i kolumn**.
Värdet kopieras.

Kopiera en cells värde till alla andra celler i denna kolumn:

- ▶ Högerklicka på cellen som innehåller det önskade värdet, peka på **Kopiera cell till** och klicka på **Fullständig kolumn**.
Värdet kopieras.

Duplicera en rad:

- ▶ Högerklicka på raden och klicka på **Lägg till kopierad rad**.
Raden läggs till nedanför med ett nytt namn.

Se

- *Sidan Kameror, sidan 266*
- *Dialogrutan Schemalagda inspelningsinställningar (endast VRM och Lokal lagring), sidan 276*
- *Sidan Händelser, sidan 284*
- *Sidan Larm, sidan 289*

20.2

Exportera kameratabellen

Huvudfönster > **Kameror och inspelning**

Eller

Huvudfönster > **Kameror och inspelning** > Klicka på en ikon för att ändra sidan för kameror



enligt önskad lagringsenhet, till exempel .

Visar diverse information om kameror som är tillgängliga i BVMS.

Du kan exportera kameratabellen till en CSV-fil.

Så här exporterar du:

1. Högerklicka någonstans i kameratabellen och klicka på **Exportera tabell...**
2. I dialogrutan skriver du ett lämpligt filnamn.
3. Klicka på **Spara**.
Den valda kameratabellen exporteras till en CSV-fil.

20.3

Konfigurera inställningarna för ström kvalitet

Lägga till en inställningspost för ström kvalitet:

1. Klicka på  för att lägga till en ny post i listan.
2. Skriv in ett namn.

Ta bort en inställningspost för ström kvalitet:

- Markera en post i listan och klicka på  för att ta bort posten.
Du kan inte ta bort standardposter.

Ändra namn på en inställningspost för ström kvalitet:

1. Markera en post i listan.
2. Ange det nya namnet i fältet **Namn**.
Det går inte att byta namn på standardposterna.
3. Klicka på **OK**.

Konfigurera inställningarna för ström kvalitet:

1. Markera en post i listan.
2. Gör lämpliga inställningar.

20.3.1**Kvalitetsinställningar för ström-dialogrutan**

Huvudfönster > **Kameror och inspelning** > 

Gör att du kan konfigurera profiler för ström kvalitet som du senare kan tilldela på sidan

Kameror och inspelning för kameror eller i dialogrutan **Schemalagda inspelningsinställningar**.

Ström kvalitet är en kombination av videoupplösning, bildhastighet, maximal bandbredd och videokomprimering.

Ström kvaliteter

 Välj en fördefinierad ström kvalitet och klicka på  för att lägga till en ny ström kvalitet baserad på den fördefinierade ström kvaliteten. När du väljer en enkel ström och klickar på  kopieras ström kvalitetsinställningen som en fristående nod på högsta nivå.

 Klicka om du vill ta bort en vald ström kvalitet. Du kan inte ta bort ström kvalitetsinställningarna.

I listan visas alla tillgängliga fördefinierade ström kvalitetsinställningar. Vi rekommenderar att en ström kvalitet tilldelas med samma namn som kamerans plattform.

Följande profiler för ström kvalitet är tillgängliga:

Image optimized: Inställningarna är optimerade för bildkvalitet. De här inställningarna kan belasta nätverket.

Bit rate optimized: Inställningarna är optimerade för låg bandbredd. De här inställningarna kan minska bildkvaliteten.

Balanced: Inställningarna är en kompromiss mellan optimal bildkvalitet och optimal bandbreddsanvändning.

Följande profiler för ström kvalitet är tillgängliga sedan BVMS 9.0 för att ge stöd för funktionen Intelligent Streaming på Bosch-kameror:

Cloud optimized 1/8 FR: Inställningarna är optimerade för låg bandbredd och är identiska för alla kameratyper.

PTZ optimized: Inställningarna är optimerade för PTZ-kameror.

Image optimized quiet / standard / busy

Bit rate optimized quiet / standard / busy

Balanced quiet / standard / busy

Kategorier för motivtyp:

quiet: Inställningarna är optimerade för bilder med låg aktivitet. 89 % statiskt motiv, 10 % normalt motiv, 1 % hektiskt motiv.

standard: Inställningarna är optimerade för bilder med medelhög aktivitet. 54 % statiskt motiv, 35 % normalt motiv, 11 % hektiskt motiv.

busy: Inställningarna är optimerade för bilder med hög aktivitet. 30 % statiskt motiv, 55 % hektiskt motiv, 15 % välfyllt motiv.

Procentvärdena representerar fördelningen under en dag.

Som standard används profilen Balanced standard.

**Obs!**

För varje kombination av kameraplattform (CPP3-CPP7.3) och för varje tillgänglig upplösning finns det en specifik inställning så att du kan ange rätt bithastigheter för kamerorna. Profilen måste väljas manuellt med motsvarande typ av motiv för varje kamera.

**Obs!**

Vid installation av uppdateringar måste de nya profilerna väljas manuellt för att aktiveras. De gamla profilerna finns kvar.

Namn

Visa namnet på strömkvaliteten. Du kan byta namn när du lägger till en ny ström kvalitet.

SD-videoupplösning

Välj önskad videoupplösning. För HD-kvalitet kan du konfigurera SD-kvalitetet på ström 2.

Bildkodningsintervall

Flytta skjutreglaget eller ange lämpligt värde.

Systemet hjälper dig att beräkna det motsvarande värdet för IPS.

Med bildkodningsintervallet konfigurerar du med vilket intervall som bilder kodas och överförs.

Om 1 anges kodas alla bilder. Om 4 anges betyder det att endast var fjärde bild kodas, de följande tre bilderna hoppas över. Det här kan vara särskilt fördelaktigt när bandbredden är låg. Ju lägre bandbredden är, desto högre bör detta värde vara för att uppnå video av bästa kvalitet.

GOP-struktur

Välj den struktur som du behöver för GOP (Group-of-Pictures). Beroende på om du prioriterar minsta möjliga fördröjning (endast IP-bilder) eller minsta möjliga bandbreddsanvändning, väljer du IP, IBP eller IBBP. (GOP är inte tillgängligt på alla kameror.)

Obs!

B-bilder stöds endast av kameror upp till en upplösning på 1 080 p och från version 6.40 av den fasta programvaran.

Målbithastighet [Kbps]

Flytta skjutreglaget eller ange lämpligt värde.

Datahastigheten kan begränsas för encodern så att bandbredden utnyttjas optimalt i nätverket. Måldatahastigheten ska anges i enlighet med den önskade bildkvaliteten för typiska scener utan allt för mycket rörelser.

För komplexa bilder eller frekventa ändringar av bilden med många rörelser kan den här gränsen temporärt överskridas upp till det värde som du anger i fältet **Maximal bithastighet [kbit/s]**.

Maximal bithastighet [kbit/s]

Flytta skjutreglaget eller ange lämpligt värde.

Med den maximala bithastigheten konfigurerar du den maximala överföringshastigheten vilken inte får överskridas.

Du ställer in en gräns för bithastigheten för att på ett säkert sätt kunna bestämma lämpligt diskutrymme för lagring av videodata.

Beroende på videokvalitetsinställningarna för I- och P-bildrutor kan enstaka bilder hoppas över.

Värdet som anges här ska vara minst 10 % högre än värdet som anges i fältet **Målbithastighet [Kbps]**. Om det angivna värdet är för lågt justeras det automatiskt.

I-frame-avstånd

Med den här parametern ställer du in de intervaller i vilka I-bildrutor kodas. Klicka på **Automatiskt** för att infoga I-bildrutor efter behov. Posten 1 indikerar att I-bildrutor skapas kontinuerligt. Posten 2 indikerar att bara varannan bild är en I-bildruta och 3 att bara var tredje bild är det osv. I-bildrutor däremellan kodas som P-bildrutor.

Kvalitetsnivå på bildruta

Här kan du ange ett värde mellan 0 och 100 för både I-bildrutor och P-bildrutor. Det lägsta värdet resulterar i högsta kvalitet och lägsta bilduppdateringstakt. Det högsta värdet resulterar i högsta bilduppdateringstakt och lägsta bildkvalitet.

Ju lägre den tillgängliga överföringsbandbredden är, desto högre blir justeringen av kvalitetsnivån för att bibehålla hög kvalitet på videon.

Obs!

Du justerar videokvaliteten beroende på rörelsen och detaljnivån i videon. Om du markerar kryssrutorna **Automatiskt** justeras det optimala förhållandet mellan rörelse och bildupplösning automatiskt.

VIP X1600 XFM4-inställningar

Här kan du konfigurera följande H.264-inställningar för kodarmodulen VIP X 1600 XFM4.

H.264-avblockeringsfilter: Välj det här alternativet för att förbättra den visuella kvaliteten och förutsägelseprestanda genom att jämna ut vassa kanter.

CABAC: Välj det här alternativet för att aktivera högeffektiv komprimering. Använder mycket processorkraft.

Se

– *Konfigurera inställningarna för ström kvalitet, sidan 272*

20.4

Konfigurera kameraegenskaper

Huvudfönster > **Kameror och inspelning** > 

Så här ändrar du kameraegenskaper:

1. Klicka på en cell i kolumnen **Kamera** och ange ett nytt namn på kameran.
Det här namnet visas på alla andra ställen där kameror listas.
 2. Gör lämpliga inställningar i övriga kolumner.
- För detaljerad information om olika fält, följ länken till lämpligt programfönster.

Se

– *Sidan Kameror, sidan 266*

20.5

Konfigurera inspelningsinställningar (endast VRMoch Lokal lagring)

Huvudfönster > > **Kameror och inspelning** 

Du kan konfigurera inspelningsinställningarna för alla enheter som är tillagda i VRM-enhetsobjektet i enhetsträdet.

Obs! För inspelning, se till att motsvarande VRM eller lokal lagring är korrekt konfigurerad.

VRM: **Enheter** > Utvidga  > 

Lokal lagring: **Enheter** > Utvidga  > 

Lägga till en post i inspelningsinställningarna:

1. Klicka på  när du vill lägga till en ny post i listan.
2. Skriv in ett namn.

Ta bort en post i inspelningsinställningarna:

- Markera en post i listan och klicka på  när du vill ta bort registreringen.
Du kan inte ta bort standardposter.

Byta namn på en post i inspelningsinställningarna:

1. Markera en post i listan.
2. Ange det nya namnet i fältet **Namn:**.
Det går inte att byta namn på standardposterna.
3. Klicka på **OK**.

Konfigurera inspelningsinställningar:

1. Markera en post i listan.
 2. Gör lämpliga inställningar och klicka på **OK**.
 3. Klicka på  eller på .
 4. I kolumnen **Inspelning** väljer du det önskade inspelningsläget för varje kodare.
- För detaljerad information om olika fält, se onlinehjälpens för lämpligt programfönster.

Se

- *Dialogrutan Schemalagda inspelningsinställningar (endast VRM och Lokal lagring), sidan 276*

20.6

Dialogrutan Schemalagda inspelningsinställningar (endast VRM och Lokal lagring)

Huvudfönster > **Kameror och inspelning** > 

Låter dig utforma schemaberoende inspelningsinställningar för varje tillgänglig enhetsfamilj. En enhetsfamilj är tillgänglig när åtminstone en kodare i denna enhetsfamilj har lagts till enhetsträdet. I tabellen **Kameror** tilldelar du varje kamera en sådan inspelningsinställning. Du använder schemalagd inspelning som utformats på **Scheman**-sidan.

Obs! Om du slår av eller på normal inspelning gäller detta alla enhetsfamiljer.

Scheduled Recording Settings

Available Recording Settings

+

×

Alarm Recording

Alarm Recording Night and Weekend

Continuous, Alarm Recording

No Recording

Recording

Recording Night and Weekend

Lila, Orange Alarm Motion recording , P...

RecordingSchedule

Red, V1

Edit Recording Settings

Name:

Alarm Recording

Device Family 1

Device Family 2

Device Family 3

VSG

Day

Night

Weekend

Recording 4

Recording 5

R

◀

▶

Recording Settings

Recording

☒ On

☐ Off

☒ Audio recording

☒ Meta data recording

Continuous or Pre-alarm Recording

Recording Mode

Continuous

Stream

Stream 1

Quality

No modification

Duration (Pre-alarm)

00:00:10

Alarm Recording Settings

Alarm Recording

☒ On

☐ Off

Motion Alarm

☐ On

☒ Off

Stream

Stream 1

Quality

Good

Duration (Post-alarm)

00:00:10

OK

Cancel

Tillgängliga inspelningsinställningar

Välj en fördefinierad inspelningsinställning för att ändra egenskaperna för den. Du kan lägga till eller ta bort en användardefinierad inställning.

Namn:

Skriv in ett namn på den nya inspelningsinställningen.

Flik för enhetsfamilj

Välj en enhetsfamilj som du vill konfigurera inspelningsinställningarna för.

Flik för inspelningsschema

Välj ett inspelningsschema för att konfigurera inspelningsinställningarna för den valda enhetsfamiljen.

Inspelning

Slå på eller av den normala inspelningen (kontinuerlig och förlarm).

Ljudinspelning

Välj om du vill spela in ljud.

Metadatainspelning

Välj om du vill spela in metadata.

Inspelningsläge

Välj önskat inspelningsläge.

Följande objekt finns:

- **Kontinuerlig**
- **Före larm**

Ström

Välj önskad ström som ska användas för normal inspelning.

Obs! Det beror på enhetsfamiljen vilka strömmar som finns.

Kvalitet

Välj önskad ström kvalitet som ska användas för normal inspelning. De tillgängliga kvalitetsinställningarna konfigureras i dialogrutan **Kvalitetsinställningar för ström**.

Varaktighet (före larm)

Ange den önskade inspelningstiden före ett larm. Du anger tiden i formatet tt.mm.ss.

Obs! Endast aktiverad när **Före larm** har valts.

**Obs!**

För förlarmsinställningar mellan 1 och 10 lagras förlarmen automatiskt i kodarens RAM-minne om det finns tillräckligt utrymme, annars i lagringsutrymmet.

Förlarmsinställningar som är längre än 10 s lagras i lagringsutrymmet.

Lagring av förlarm i kodarens RAM-minne är bara möjligt från och med version 5.0 av den fasta programvaran.

Inställningar för larminspelning

Gör att du kan slå på och av larminspelningen för kameran.

Rörelselarm

Gör att du kan slå på och av larminspelning som utlöses av rörelse.

Ström

Välj den ström som ska användas för larminspelningar.

Obs! Det beror på enhetsfamiljen vilka strömmar som finns.

Kvalitet

Välj önskad ström kvalitet som ska användas för larminspelning. De tillgängliga kvalitetsinställningarna konfigureras i dialogrutan **Kvalitetsinställningar för ström**.

Endast enheter som tillhör enhetsfamilj 2 eller 3: När du väljer posten **Ingen modifiering** använder larminspelningen samma ljudkvalitet som kontinuerlig inspelning/förlarmsinspelning.

Vi rekommenderar att du använder posten **Ingen modifiering**. När du väljer en strömningskvalitet för larminspelning ändras bara värdena för bildkodningsintervall och målbithastighet enligt inställningarna i denna strömningskvalitet. Övriga kvalitetsinställningar som används konfigureras i kvalitetsinställningen som tilldelats den kontinuerliga inspelningen/förlarmsinspelningen.

Varaktighet (efter larm)

Ange önskad larminspelningstid. Du anger tiden i formatet tt.mm.ss.

Se

- *Kopiera och klistra in i tabeller, sidan 271*
- *Konfigurera inspelningsinställningar (endast VRMoch Lokal lagring), sidan 275*

20.7

Konfigurera PTZ-portinställningar

Huvudfönster > **Enheter** > Utvidga  > Utvidga  >  > fliken **Gränssnitt** > fliken **Kringutrustning**

Huvudfönster > **Enheter** >  >  > fliken **Gränssnitt** > fliken **Kringutrustning**

Du kan endast konfigurera portinställningar för en kodare där kamerans styrning är tillgänglig och aktiverad.

När kodaren eller PTZ-kameran byts ut bibehålls inte portinställningarna. Dessa måste konfigureras igen.

Kontrollera portinställningarna efter uppgradering av den fasta programvaran.

Konfigurera portinställningar för en kodare:

- ▶ Gör de inställningar som krävs.
Inställningarna börjar gälla omedelbart efter det att de har sparats. Konfigurationen behöver inte aktiveras.

För detaljerad information om olika fält, se onlinehjälp för lämpligt programfönster.

20.8

Konfigurera fördefinierade positioner och extra kommandon

Huvudfönster > **Kameror och inspelning** > 

Du kan fördefiniera och spara kamerapositioner för PTZ-, ROI- och panoramakameror. För PTZ-kameror kan du också definiera extrakommandon.

Obs! Ställ först in portinställningarna för PTZ-kameran innan du ställer in PTZ-kamerainställningarna. Annars fungerar inte PTZ-styrningen i dialogrutan.

Så här konfigurerar du en fördefinierad position:

1. Välj nödvändig kodare i **Kameror**-tabellen.
2. Endast för PTZ-kameror: Aktivera en PTZ-kameras styrning genom att markera kryssrutan i

kolumnen .

3. Klicka på -knapp.
Dialogrutan **Fördefinierade positioner och AUX-kommandon** visas.
4. Du kan definiera antalet fördefinierade positioner som du vill använda.
5. Välj den position som du vill definiera.
6. I förhandsgranskningsfönstret använder du muskontrollen för att navigera till den position du vill konfigurera.
Bläddra för att zooma in och ut och dra för att flytta bildsektionen.
7. Om det behövs skriver du ett namn på den konfigurerade positionen.

8. Klicka på  om du vill spara den fördefinierade positionen.

Obs! Klicka på  för varje definierad position. Annars sparas inte positionen.

9. Klicka på **OK**.

Så här visar du redan konfigurerade fördefinierade positioner:

1. Välj nödvändig kodare i **Kameror**-tabellen.
2. Klicka på -knapp.
Dialogrutan **Fördefinierade positioner och AUX-kommandon** visas.
3. Välj lämplig position.

4. Klicka på .

Den fördefinierade kamerapositionen visas i förhandsgranskningsfönstret.

Obs!

Fördefinierade positioner för PTZ- och ROI-kameror lagras direkt i kameran. Fördefinierade positioner för panoramakameror lagras i BVMS.

PTZ-kameror rör sig fysiskt till den fördefinierade positionen. Panorama- och ROI-kameror visar bara en bildsektion av hela kameravyn.

Så här konfigurerar du hjälpkommandon för PTZ-kameror:

1. Välj nödvändig kodare i **Kameror**-tabellen.

2. Klicka på -knapp.

Dialogrutan **Fördefinierade positioner och AUX-kommandon** visas.

3. Välj **AUX-kommandon**-fliken.

4. Gör lämpliga inställningar.

5. Klicka på  om du vill spara de fördefinierade kommandona.

För detaljerad information om olika fält, se onlinehjälp för lämpligt programfönster.

Se

- *Dialogrutan med fördefinierade positioner och extra kommandon, sidan 280*
- *Konfigurera PTZ-portinställningar, sidan 279*
- *Konfigurera ett larm, sidan 301*
- *Välj bildruteinnehåll-dialogrutan, sidan 290*
- *Larmalternativ-dialogrutan, sidan 292*
- *Dialogrutan Välj bildruteinnehåll (MG), sidan 291*

20.9

Dialogrutan med fördefinierade positioner och extra kommandon

Huvudfönster > **Kameror och inspelning** >  > Välj en PTZ-, ROI- eller panoramakamera >



Gör att du kan konfigurera en PTZ-, ROI- eller panoramakamera.

För ROI- och panoramakameror finns inga hjälpkommandon tillgängliga.

Obs! Ställ först in portinställningarna för PTZ-kameran innan du ställer in PTZ-kamerainställningarna. Annars fungerar inte PTZ-styrningen i dialogrutan.

Ikoner

	Klicka för att flytta kameran till en fördefinierad position eller för att utföra kommandot.
	Klicka för att spara den fördefinierade positionen eller kommandot.

Fliken Fördefinierade positioner

Klicka för att visa tabellen med fördefinierade positioner.

Nr

Visar den fördefinierade positionens nummer.

Namn

Klicka på en cell för att redigera namnet på den fördefinierade positionen.

Fliken AUX-kommandon (endast för PTZ-kameror)

Klicka för att visa tabellen med extrakommandon.

Obs! Om en ONVIF-kodare har stöd för hjälpkommandon tillhandahålls extrakommandona från ONVIF-kodaren direkt.

Nr

Visar extrakommandots nummer.

Namn

Klicka på en cell för att redigera namnet på extrakommandot.

Kod

Klicka på en cell för att redigera kommandots kod.

Se

- *Konfigurera PTZ-portinställningar, sidan 279*
- *Konfigurera fördefinierade positioner och extra kommandon, sidan 279*

20.10**Konfigurera ROI-funktionen**

Huvudfönster > **Kameror och inspelning** > 

Du kan aktivera ROI-funktionen för en fast HD-kamera.

Du måste konfigurera ström 2 för live-video och du måste konfigurera codecen H.264 MP SD ROI eller H.265 MP SD ROI för ström 2.

Kontrollera att ström 2 används för live-video på varje arbetsstation där ROI ska användas.

Aktivera ROI:

1. Gå till kolumnen **Ström 2 – Codec** och välj codecen H.264 MP SD ROI eller H.265 MP SD ROI.
2. Gå till kolumnen **Live-video – Ström** och välj **Ström 2**.
3. Gå till kolumnen **Live-video – ROI** och markera kryssrutan.

Avaktivera ROI:

1. I kolumnen **Live-video – ROI** klickar du för att avmarkera kryssrutan.
2. I kolumnen **Ström 2 – Codec** väljer du önskad codec.

Se

- *Sidan Kameror, sidan 266*

20.11**Kopiera inspelningsinställningar**

Huvudfönster > **Kameror och inspelning** > Klicka på en ikon för inspelningsenheten (till

exempel ) > Klicka på en flik för inspelningsschema (till exempel **Dag**)

Du kan kopiera inspelningsinställningar från ett inspelningsschema till ett annat.

Kopiera inspelningsinställningarna i en vald tabellrad:

1. Välj en tabellrad som innehåller önskade inspelningsinställningar.
2. Klicka på . Dialogrutan **Kopiera inspelningsinställningar** visas.

3. Välj ett inspelningsschema i listan dit du vill kopiera inställningarna.
4. Klicka på **Kopiera nuvarande val**.
5. Klicka på **OK**. Inspelningsinställningarna för den valda tabellraden kopieras.

Kopiera alla inspelningsinställningar för ett inspelningsschema:

1. Klicka på . Dialogrutan **Kopiera inspelningsinställningar** visas.
2. Välj ett inspelningsschema i listan dit du vill kopiera inställningarna.
3. Klicka på **Kopiera alla**.
4. Klicka på **OK**. Inspelningsinställningarna för alla tabellrader kopieras.

20.11.1

Dialogrutan Kopiera inspelningsinställningar

Huvudfönster > **Kameror och inspelning** > Klicka på en ikon för inspelningsenheten, till

exempel  > Klicka på en flik för inspelningsschema (till exempel **Dag**) > 
Låter dig kopiera inspelningsinställningar från ett Inspelningsschema till ett annat.

Kopiera alla

Klicka för att kopiera alla inspelningsinställningar i det valda schemat till ett annat schema.

Kopiera nuvarande val

Klicka för att endast kopiera inspelningsinställningarna i de markerade tabellraderna till ett annat schema.

20.12

Konfigurera ANR-funktionen

Huvudfönster > **Kameror och inspelning** > 
Innan du kan aktivera ANR-funktionen måste du lägga till och konfigurera lagringsmediet för önskad kodare.
För att kunna konfigurera ANR-funktionen måste du avaktivera dubbel strömning för kodaren. ANR-funktionen fungerar bara på kodare med fast programvara av version 5.90 eller senare. Alla kodartyper har inte stöd för ANR även om rätt version är installerad.

Så här aktiverar du:

- ▶ I kolumnen **ANR** markerar du kryssrutan på raden för önskad kamera.

Se

- *Konfigurera dubbel strömning i kameratabellen, sidan 282*
- *Sidan Kameror, sidan 266*
- *Konfigurera lagringsmediet för en kodare, sidan 214*

20.13

Konfigurera dubbel strömning i kameratabellen

Huvudfönster > **Kameror och inspelning** > 
Du måste avaktivera ANR-funktionen för att kunna konfigurera dubbel strömning. Om du konfigurerar dubbel strömning för en kamera i en flerkanalskodare kontrollerar systemet att samma inspelningsmål konfigureras för kodarens samtliga kameror.

Så här konfigurerar du:

1. I kolumnen **Sekundär inspelning – Mål** klickar du i cellen för önskad kodare och därefter på önskad pool för en sekundär VRM-enhet.
Den berörda kodarens samtliga kameror konfigureras automatiskt att spelas in på den valda sekundära VRM-enheten.
2. I kolumnen **Inställning** väljer du en inställning för schemalagd inspelning.

Se

- *Konfigurera dubbel strömning i enhetsträdet, sidan 178*
- *Konfigurera ANR-funktionen, sidan 282*
- *Dubbel strömning/reservinspelning, sidan 28*
- *Sidan Kameror, sidan 266*

20.14**Hantera Video Streaming Gateway****Se**

- *Sidan Video Streaming Gateway-enhet, sidan 189*
- *Dialogrutan Lägg till kodare från Bosch, sidan 192*
- *Dialogrutan Lägg till ONVIF-kodare, sidan 193*
- *Dialogrutan Lägg till JPEG-kameror, sidan 194*
- *Dialogrutan Lägg till RTSP-kodare, sidan 195*

20.14.1**Tilldela en ONVIF-profil**

Huvudfönster > **Kameror och inspelning** >

Du kan tilldela en ONVIF-kamera en kodbricka för ONVIF Media Profile.

Du kan tilldela antingen för live-video eller för inspelning.

Tilldela en kodbricka för live-video:

- I kolumnen **Live-video** – **Profil** väljer du önskad post.

Tilldela en kodbricka för inspelning:

- I kolumnen **Inspelning** – **Profil** väljer du önskad post.

Se

- *Sidan Kameror, sidan 266*

21 Sidan Händelser

Huvudfönster > **Händelser**

Visar händelseträdet med alla tillgängliga händelser och en tabell för händelsekonfiguration av varje händelse. Händelserna är gruppindelade efter typ, till exempel är alla kamerainspelningshändelser som kontinuerlig inspelning eller larminspelning grupperade under Inspelningsläge.

Tillgängliga händelser grupperas bakom motsvarande enheter. En statusändring hos en enhet

visas bakom  som . Alla andra händelser visas under enhetsavhängiga grupper som



För varje händelse kan du konfigurera:

- Utlösa ett larm enligt ett schema (inte tillgängligt för alla händelser).
- Logga händelsen i enlighet med ett schema. En händelse visas i händelselistan för Operator Client om den loggas.
- Utför ett kommandoskript enligt ett schema (inte tillgängligt för alla händelser).

- För händelser av typen : Lägga till textdata i inspelningar.

Om händelsen inträffar tillämpas dina inställningar.

Du kan skapa en sammansatt händelse som kombinerar flera händelser med booleska uttryck.

- Klicka på ett trädojekt för att visa motsvarande tabell för händelsekonfiguration.



Klicka för att duplicera en händelse. Använd detta för att generera flera larm för en särskild händelse.



Klicka för att ta bort en duplicerad eller en sammansatt händelse.



Klicka för att ändra namn på den valda sammansatta händelsen.



Klicka för att visa en dialogruta där du kan skapa sammansatta händelser genom att använda booleska uttryck från andra händelser (maximalt 10).

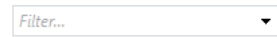
Sammansatta händelser läggs till i tabellen för händelsekonfiguration.



Klicka för att redigera den valda sammansatta händelsen.



Klicka för att visa en dialogruta där du kan skapa och redigera kommandoskript.



Skriv in en sträng och tryck på ENTER-tangenten för att filtrera de visade objekten. Endast objekt som innehåller strängen och deras motsvarande föräldraobjekt (endast i träd) visas. Antalet filtrerade objekt och det totala antalet objekt visas. Ett aktivt filter indikeras med . Skriv in strängar inom dubbla citattecken för att hitta dem exakt, till exempel filtrerar "Camera 1" kamerorna med exakt detta namn, inte camera 201.

Avbryt filtreringen genom att klicka på .

Se

- *Konfigurera händelser och larm, sidan 297*
- *Konfiguration av kommandoskript, sidan 85*
- *Dialogrutan Alternativ (menyn Inställningar), sidan 114*
- *Konfigurera blinkande aktiveringspunkter, sidan 303*

21.1

Fliken Avstudsningstillningar

Obs! För en del händelser är fliken Avstudsningstillningar inte tillgänglig på grund av tekniska begränsningar.

Låter dig konfigurera avstudsningstillningarna för vald händelse.

Avstudsningstid

Under angiven tidsperiod ignoreras alla ytterligare händelser.

Prioritet för händelsestatus

För en händelsestatus kan du tilldela en prioritetsinställning.

Redigera prioriteringar

Klicka här för att visa dialogrutan för att konfigurera en prioritetsinställning.

Lägg till inställning

Klicka här för att lägga till en rad för att konfigurera en återstudsinställning som avviker från återstudsinställningarna för alla enheter.

Ta bort inställning

Klicka här för att ta bort en vald rad. Markera en rad genom att klicka på den vänstra radrubriken.

21.2

Fliken Inställningar för avancerad kartvisning

Du kan bara konfigurera färglägena på kartor om du markerar alternativet **Aktivera avancerad statusvisning (färgning av aktiva punkter på kartor beroende på status)** eller alternativet **Aktivera avancerad statusvisning (färgning av aktiva punkter på kartor beroende på larm)** i dialogrutan **Alternativ**.

För varje  -händelse eller -larm kan du konfigurera bakgrundsfärgen och beteendet (blinkande eller fast) för aktiveringspunkter. Du kan till exempel konfigurera inställningarna så

att  -händelse eller -larm på en enhet gör att enhetsikonen på kartan börjar blinka när enhetens status ändras.

Du kan också konfigurera visningsprioriteten för alla aktiveringspunkter. Detta är obligatoriskt när olika händelser inträffar för samma enhet. (1 = högsta prioritet)

Den konfigurerade färgen gäller för alla aktiveringspunkter med samma visningsprioritet. Du

kan ändra färg, beteende och prioritet för alla  -händelser eller -larm: den ändrade färgen

och det ändrade beteendet används för alla aktiveringspunkter för alla andra  -händelser eller -larm som har samma prioritet.

Aktivera färglägen på kartor

Klicka om du vill ange att aktiveringspunkterna för enheterna som tillhör händelsen ska visas med färgad bakgrund och eventuell blinkning på kartor.

Visningsprioritet på karta:

Klicka på pilarna om du vill ändra prioriteten för aktiveringspunkterna för enheterna som tillhör händelsen.

Bakgrundsfärg på karta:

Klicka på färgfältet och välj bakgrundsfärg för aktiveringspunkterna för enheterna som tillhör händelsen.

Obs! Alla tillståndshändelser för enheter med samma prioritet har samma färg.

Blinkar

Klicka om du vill aktivera blinkning för aktiveringspunkterna för enheterna som tillhör händelsen.

21.3**Fliken Inställningar för händelsekonfiguration****Enhet**

Visar namnet på enheten eller schemat.

Nätverk

Visar IP-adressen för motsvarande IP-enhet.

Utlöser larm

Klicka på en cell för att välja Inspelning eller Uppgiftsschema för larmutlösning.

Välj **Alltid** om du vill att larmet ska utlösas oberoende av tidpunkten.

Välj **Aldrig** om du inte vill att larmet ska utlösas.

Logga

I kolumnen **Schema** klickar du på en cell för att välja Inspelning eller Uppgiftsschema för loggning.

Välj **Alltid** om du vill att händelsen ska utlösas oberoende av tidpunkten.

Välj **Aldrig** om du inte vill att händelsen ska utlösas.

Skript

I kolumnen **Skript** klickar du på en cell för att välja ett kommandoskript.

I kolumnen **Schema** klickar du på en cell för att välja Inspelning eller Uppgiftsschema för körning av ett kommandoskript.

Välj **Alltid** om du vill att kommandoskriptet ska utföras oberoende av tidpunkten.

Välj **Aldrig** om du inte vill att kommandoskriptet ska utföras.

Inspelning av textdata

Du kan se till att textdata läggs till i den kontinuerliga inspelningen från en kamera.

Obs! Den här kolumnen är bara tillgänglig för händelser som innehåller textdata, till exempel

ATM/POS-enheter > ATM-ingång > Dataingång

21.4**Redigerare för kommandoskript-dialogrutan**

Huvudfönster > **Händelser** > 

Låter dig skapa och redigera kommandoskript.



Klicka för att spara de ändrade inställningarna.



Klicka för att återställa de sparade inställningarna.



Klicka för att kontrollera koden i ett skript.



Klicka för att skapa en skriptdelsfil.



Klicka för att ta bort en skriptdelsfil.



Klicka för att visa en dialogruta för import av skriptfil.



Klicka för att visa en dialogruta för export av skriptfil.



Klicka för att konvertera ett befintligt skript till det andra tillgängliga skriptspråket. All befintlig skripttext tas bort.

SDK

? Klicka för att visa onlinehjälp för BVMS-skript-API.



? Klicka för att visa onlinehjälp för BVMS.



Klicka för att stänga dialogrutan **Redigera för kommandoskript**.

Se

– *Konfiguration av kommandoskript, sidan 85*

21.5

Skapa sammansatt händelse / dialogrutan Redigera sammansatt händelse



Huvudfönster > **Händelser** >

Låter dig skapa eller ändra en sammansatt händelse.

Filter...

Skriv in en sträng och tryck på ENTER-tangenten för att filtrera de visade objekten. Endast objekt som innehåller strängen och deras motsvarande föräldraobjekt (endast i träd) visas. Antalet filtrerade objekt och det totala antalet objekt visas. Ett aktivt filter indikeras med . Skriv in strängar inom dubbla citattecken för att hitta dem exakt, till exempel filtrerar "Camera 1" kamerorna med exakt detta namn, inte camera 201.

Avbryt filtreringen genom att klicka på .

Händelsenamn:

Ange namnet som krävs för den sammansatta händelsen.

Händelselägen:

Välj statusändringen som ska vara del av en sammansatt händelse.

Objekt:

Välj ett eller flera av de tillgängliga objekten för det valda händelseläget. Det här läget och det valda objektet visas i det sammansatta händelsesträdet som direkt underordnat rotoperatör.

Sammansatt händelse:

Gör att du kan skapa sammansatta händelser i det sammansatta händelsesträdet. Alla omedelbart underordnade objekt under en boolesk operator (AND, OR) kombineras med den här operatör.

Se

- *Skapa en sammansatt händelse, sidan 300*
- *Redigera en sammansatt händelse, sidan 301*

21.6

Välj skriptspråk-dialogrutan



Huvudfönster > **Händelser** >

Låter dig ställa in skriptspråket för dina kommandoskript.

Du kan inte ändra skriptspråket för existerande kommandoskript.

Skriptspråk:

Välj det skriptspråk som krävs.

Se

- *Konfiguration av kommandoskript, sidan 85*

21.7 Dialogrutan Redigera prioriteter för händelsetyp

Huvudfönster > **Händelser** > fliken **Avstudsningstillställningar** > knappen **Redigera prioriteringar**

Du kan konfigurera lämpliga prioriteringar för olika tillståndsförändringar för en händelsetyp, t.ex. Virtuellt ingång stängd och Virtuellt ingång öppet. En tillståndsförändring med högre prioritet åsidosätter avstudsningstiden för en annan tillståndsförändring med lägre prioritet.

Namn på prioritering:

Skriv in ett namn för prioritetstillställningen.

Tillståndsvärde

Visar namnen på händelsestatusar för vald händelse.

Tillståndsprioritet

Ange önskad prioritet. 1=högst prioritet, 10=lägst prioritet.

21.8 Välj enheter-dialogrutan

Huvudfönster > **Händelser** >  eller  > fliken **Avstudsningstillställningar** > knappen **Lägg till inställning**

Välj

Markera kryssrutan för önskad post och klicka på **OK** för att lägga till en rad i tabellen **Enheter med avvikande avstudsningstillställningar**.

21.9 Dialogrutan Inspelning av textdata

Huvudfönster > **Händelser** > Välj  **Dataingång** i händelseträdet (textdata måste finnas tillgängliga, till exempel **Läsarenheter för nyckelkort** > **Nyckelkortsläsare** > **Avvisat kort**) > kolumnen **Inspelning av textdata** > ...

Du kan konfigurera för vilka kameror textdata ska läggas till i den kontinuerliga inspelningen.

Se

- *Utlösa larminspelning med textdata, sidan 302*

22

Sidan Larm

Huvudfönster > **Larm**

Visar händelseträdet och en tabell för larmkonfiguration för varje händelse. Endast händelserna som konfigurerades på sidan **Händelser** visas.

I tabellerna konfigurerar du för varje händelse hur ett larm som utlösts av denna händelse visas och vilka kameror som spelar in och visas när detta larm inträffar.

Vissa händelser konfigureras som larm som standard, till exempel ett systemfel.

För följande händelser kan du inte konfigurera ett larm:

- Ändring av inspelningsläge
- Ändring av larmstatus
- De flesta användaråtgärder, t.ex. PTZ-åtgärd

Klicka för att visa dialogrutan  **Resurshanteraren**.



Visar en dialogruta för att ställa in larm som är giltiga för denna Management Server.

Skriv in en sträng och tryck på ENTER-tangenten för att filtrera de visade objekten. Endast objekt som innehåller strängen och deras motsvarande föräldraobjekt (endast i träd) visas. Antalet filtrerade objekt och det totala antalet objekt visas. Ett aktivt filter indikeras med . Skriv in strängar inom dubbla citattecken för att hitta dem exakt, till exempel filtrerar "Camera 1" kamerorna med exakt detta namn, inte camera 201.

Avbryt filtreringen genom att klicka på .

- ▶ Klicka på ett trädobjekt för att visa motsvarande tabell för larmkonfiguration.

Enhet

Visar enheten för det händelsevillkor som valts i händelseträdet.

Nätverksadress

Visar IP-adressen för motsvarande IP-enhet.

Larmidentitet

I kolumnen **Prioritet** klickar du i en cell för att ange larmprioriteten för valt larm (**100** är låg prioritet, **1** är hög prioritet). I kolumnen **Titel** klickar du i en cell för att ange larmrubriken som ska visas i BVMS, till exempel i larm listan. I kolumnen **Färg** klickar du i en cell för att visa en dialogruta där du kan välja en larmfärg som ska visas i Operator Client, t.ex. i larmlistan.

Larmbildrutor

I kolumnerna **1-5**, klicka på ... i en cell för att visa en dialogruta där du kan välja en kamera.

Du kan endast välja en kamera som har lagts till i det logiska trädet i **Kartor och struktur**.

Du kan konfigurera antalet tillgängliga larmbildrutor i dialogrutan **Larminställningar**.

I kolumnen **Ljudfil** klickar du på ... i en cell för att visa en dialogruta där du kan välja en ljudfil som spelas upp i händelse av ett larm.

Larmalternativ

Klicka på ... i en cell för att visa dialogrutan **Larmalternativ**.

Se

- *Larmhantering, sidan 38*

22.1

Dialogrutan Larminställningar

Huvudfönster > **Larm** > 

Fliken Larminställningar**Högsta antal bildrutor per larm:**

Ange det maximala antalet bilder på larmpaneler som ska visas i händelse av ett larm.

Auto-rensningstid:

Ange antalet sekunder som går innan larmet automatiskt inaktiveras.

Detta gäller endast för larm som är inställda på **Radera larmet automatiskt efter konfigurerad tid (dialogrutan "Larminställningar")** på sidan **Larm**.

Larmvisning på flera rader i larmbildfönstret

Markera kryssrutan om du vill aktivera visning av larmläge med flera rader i larmbildsfönstret.

**Obs!**

För befintliga larmkonfigurationer är larmvisning med flera rader aktiverat. För nya larmkonfigurationer är standardvärdet inaktiverat och läget enbildsvy är aktiverat.

Ange längden på tillståndsutlösta larminspelningar:

Markera kryssrutan för att aktivera en tidsgräns för statusutlösta larminspelningar. Ange antal minuter för larminspelningens varaktighet. larminspelningen stoppas automatiskt efter den angivna tiden.

Användaren kan ange en varaktighet mellan 1 och 1 440 minuter.

När ett larm utlöser en inspelning med en konfigurerad tidsgräns:

- Om larmet utlöses igen innan tidsgränsen har uppnåtts fortsätter inspelningen och timeouten startar om från noll.
- Om larmet avbryts innan tidsgränsen uppnås fortsätter inspelningen till den inställda tidsgränsen efter larmet.

Fliken Monitorgrupper**Visningsföljd vid samma larmprioritet**

Välj den önskade posten för att sortera larm med samma prioritet i enlighet med tidsstämplarna.

Visa tom skärm

Klicka för att konfigurera att ingenting visas på en monitor som inte används för larmvisning.

Fortsätt livevisning

Klicka för att konfigurera att livevisning visas på en monitor som inte används för larmvisning.

Se

- *Konfigurera inställningar för alla larm, sidan 301*

22.2**Välj bildruteinnehåll-dialogrutan**

Huvudfönster > **Larm** >  eller  > kolumnen **Larmbildrutor** > Klicka på ... i en av kolumnerna **1-5**

Medger val av det logiska trädobjekt som visas och spelas in (om objektet är en kamera) för valt larm.

**Obs!**

En anläggningskarta som visas i en larmbildruta är optimerad för visning och innehåller bara den initiala visningen av den ursprungliga kartfilen.

Sök objekt

Ange text för att kunna hitta ett objekt i det logiska trädet.

Sök

Klicka om du vill söka efter kameran med angiven söktext i beskrivningen.

Live

Klicka för att bestämma att kamerans livebild visas i händelse av larm.

Direktuppspelning

Klicka för att bestämma att kamerans direktuppspelning visas.

Återspolningstiden för larmdirektuppspelning konfigureras på sidan **Operatörsfunktioner**, se *Sidan Användarfunktioner, sidan 314*.

Pausa uppspelningen

Markera kryssrutan så visas kamerans larmdirektuppspelning med direktuppspelning pausad. Användaren kan starta direktuppspelning om det behövs.

Loopa uppspelningen

Markera kryssrutan så visas kamerans larmdirektuppspelning med seriekopplad direktuppspelning.

Den seriekopplade direktuppspelningen i larmbildsrutan är återspolningstiden plus varaktigheten för larmläget plus för- och efterspolningstid.

Spela in denna kamera

Markera kryssrutan för att aktivera larminspelning för den här kameran i händelse av larm. Om ett larm utlöses spelar den här kameran in med larminspelningens kvalitet. Inspelningen varar så länge som larmläget pågår, plus förlarmstid och tid efter larm. Den här inställningen ändrar direkt inställningen för larminspelning i dialogrutan **Larmalternativ** och vice versa.

Obs! Om en fördefinierad position är vald för en panoramakamera lagras inte bara den här bildsektionen utan hela cirkelvyn.

Fördefinierad panoramaposition

Om du har valt en panoramakamera kan du välja en fördefinierad kameraposition. När en användare av Operator Client accepterar larmet visas larmbilden i den fördefinierade positionen i beskuren vy.

Om **<inget>** är markerat visas larmbilden i panoramavyn.

Se

- *Sidan Användarfunktioner, sidan 314*
- *Konfigurera ett larm, sidan 301*

22.3

Dialogrutan Välj bildruteinnehåll (MG)

Huvudfönster >



Larm > eller  > kolumnen **Larmalternativ** > Klicka på ... > dialogrutan

Larmalternativ > **Monitorgrupp**-fliken > Klicka på ... i någon av de 1–10 kolumnerna

Gör att du kan välja en kamera från det logiska trädet. Den här kameran kommer att visas på den tilldelade monitorn i händelse av valt larm.

Sök objekt

Ange text för att kunna hitta ett objekt i det logiska trädet.

Sök

Klicka om du vill söka efter kameran med angiven söktext i beskrivningen.

Fördefinierad panoramaposition

Om du har valt en panoramakamera kan du välja en fördefinierad kameraposition. När en användare av Operator Client accepterar larmet visas larmbilden i den fördefinierade positionen i beskuren vy.

Om du väljer **<inget>** visar avkodaren larmbilden i cirkelvyn.

Ingen kamera

Klicka om du vill ta bort en kamera från kolumnen med monitorgrupp.

Obs!

Vyfältet för en fördefinierad panoramakameraposition skiljer sig mellan Operator Client och Configuration Client och avkodaren.



Obs!

Om du vill använda konfigurerade fördefinierade positioner för panoramakameror måste för panoramakameran vara eller .

22.4

Larmalternativ-dialogrutan

Huvudfönster > **Larm** >  eller  > kolumnen **Larmalternativ** > ...

Gör att du kan konfigurera följande inställningar för larm:

- Kameror som startar inspelning i händelse av larm.
- Aktivera skydd för dessa larminspelningar.
- Aktivera och konfigurera inställningar för avvikande larmlängd.
- Utlösa PTZ-kommandon i händelse av larm.
- Meddelanden som skickas i händelse av larm.
- Arbetsflöde som måste följas i händelse av larm.
- Tilldela kameror som visas i monitorgrupper i händelse av larm.

Fliken Kameror

Nr	Visar kameranumret så som det är konfigurerat på sidan Kameror och inspelning .
Namn	Visar kameranamnet så som det är konfigurerat på sidan Kameror och inspelning .
Plats	Visar placeringen så som den är konfigurerad på sidan Kartor och struktur .
Inspelning	Markera en kryssruta om du vill aktivera larminspelning för den här kameran i händelse av larm. Om ett larm utlöses spelar den här kameran in med larminspelningskvalitet. Inspelningen varar så länge som larmläget pågår, plus förlarmstid och tid efter larm. Den här inställningen ändrar direkt inställningen för larminspelning i dialogrutan Välj innehåll i bildrutan och vice versa.
Skydda inspelning	Markera en kryssruta om du vill skydda larminspelningen på den här kameran. Obs! Skyddade videodata kommer aldrig att raderas

	automatiskt av VRM. Var medveten om att för många skyddade block kan fylla upp lagringen och kameran kan sluta spela in.
Avvikande längdinställningar för larm	Kryssrutan markeras automatiskt när du markerar kryssrutan Inspelning och kameran har stöd för ANR.
Extrakommando	Klicka på en cell om du vill välja ett extrakommando som ska utföras i händelse av larm. Posterna i den här listan är endast tillgängliga för en PTZ-kamera.
Fördefinierad position	Klicka på en cell om du vill välja en fördefinierad position som ska ställas in i händelse av larm. Posterna i den här listan är endast tillgängliga för en PTZ-kamera.

Fliken Meddelanden

E-post	Markera kryssrutan om du vill skicka ett e-postmeddelande i händelse av larm.
Server	Välj en e-postserver.
Mottagare:	Ange e-postadresserna för mottagarna avgränsade med kommatecken (exempel: name@provider.com).
Text	Skriv meddelandetexten.
Information	Markera kryssrutan om du vill lägga till den tillhörande informationen i meddelandetexten. Obs! För e-postmeddelanden används tidszonen för Management Server.

Fliken Arbetsflöde

Spela bara in larm	Markera kryssrutan om du vill ange att kameran endast ska spela in men inte visas om det här larmet utlöses. Den här kryssrutan är endast aktiv om kryssrutan Inspelning under fliken Kameror är markerad.
Radera larmet automatiskt efter konfigurerad tid (dialogrutan "Larminställningar")	Markera kryssrutan om du vill att det här larmet ska rensas automatiskt.
Radera larmet automatiskt när händelsestatus ändras tillbaka till normal	Markera kryssrutan om du vill att det här larmet ska rensas automatiskt när händelsen som utlöser larmet ändrar status. Larmet rensas inte automatiskt om det är accepterat och oaccepterat.
Förhindra larm från att tas bort medan utlösningsvillkoret gäller	Markera kryssrutan om du vill förhindra att det här larmet tas bort så länge som orsaken till larmet finns kvar.

Avvisa dubletter av larm i larmlistan	Markera kryssrutan om du vill undvika larm för samma typ av händelse och enhet som dupliceras i larmlistan för BVMS Operator Client. Så länge ett larm är aktivt (larmstatusen Aktiv eller Godkänd) visas inga ytterligare larm för samma typ av händelse och enhet i larmlistan. Obs! – Händelser loggas fortfarande i loggboken. – Tänk på att alla larmåtgärder som det här larmet utlöser (till exempel att ett SMS skickas, att en larminspelning startar osv.) inte löser ut igen. När larmet har inaktiverats och ett nytt larm har utlöstes för samma enhet och av samma typ av händelse, visas det nya larmet igen i larmlistan och alla larmåtgärder som angetts för larmet utlöses igen. – Den här kryssrutan är förvald för Person Identification-larm.
Visa åtgärdsplan	Markera kryssrutan om du vill aktivera arbetsflödet som måste följas i händelse av larm.
Resurser...	Klicka för att visa dialogrutan Resurshanteraren . Välj ett dokument med en beskrivning av motsvarande arbetsflöde.
Visa en kommentarsruta	Markera kryssrutan om du vill att en kommentarruta ska visas i händelse av larm. I den här kommentarrutan kan användaren lägga till kommentarer om larmet.
Tvinga operatören att behandla arbetsflödet	Markera kryssrutan om du vill tvinga användaren att följa arbetsflödet. Om den här kryssrutan har markerats måste användaren lägga till en kommentar om larmet för att kunna rensa det.
Utför följande klientskript när larm har godkänts:	Välj ett klientkommandoskript som ska köras automatiskt när en användare accepterar ett larm.

Fliken Monitorgrupp

1...10	Klicka på en cell i en numrerad kolumn. Dialogrutan Välj innehåll i bildrutan visas. Välj en kamera från det logiska trädet. Denna kamera kommer att visas på den tilldelade monitorn i händelse av larm. Välj fördefinierade kamerapositioner om det är konfigurerat. Mer information finns i onlinehjälpfen för Välj innehåll i bildrutan -dialogrutan (MG).
Ta bort tabell	Klicka här om du vill ta bort alla kameratilldelningar till monitorgrupper.
Larmnamn	Markera kryssrutan om du vill att larmets titel ska visas som en skärmmeny på monitorerna.

Larmtid	Markera kryssrutan om du vill att larmets tid ska visas som en skärmmeny på monitorerna.
Larmdatum	Markera kryssrutan om du vill att datumet för larmet ska visas som en skärmmeny på monitorerna.
Namn på larmkamera	Markera kryssrutan om du vill att namnet på larmkameran ska visas som en skärmmeny på monitorerna
Larmkameranummer	Markera kryssrutan om du vill att numret på larmkameran ska visas som en skärmmeny på monitorerna.
Endast på den första monitorn	Markera kryssrutan om du vill att larmets titel och tid endast ska visas som en skärmmeny på den första monitorn i monitorgruppen.

Fliken Avvikande längdinställningar för larm

Inställningarna på den här fliken är endast tillgängliga om ANR har aktiverats för kameran.

Använd profilinställningar	Klicka här om du vill aktivera den här inställningen. För den här kameran används inställningarna för längden på förlarm och efterlarm som har konfigurerats i dialogrutan Schemalagda inspelningsinställningar .
Åsidosätt inställningar	Klicka här om du vill aktivera följande inställningar för förlarmets och efterlarmets längd.
Varaktighet (före larm)	Tillgängligt för alla händelser.
Varaktighet (efter larm)	Endast tillgängligt för  -händelser.

Se

- *Dialogrutan Välj bildruteinnehåll (MG), sidan 291*
- *Utlösa larminspelning med textdata, sidan 302*
- *Konfigurera ett larm, sidan 301*
- *Konfigurera längden på förlarm och efterlarm, sidan 302*

22.5

Välj resurs-dialogrutan

Huvudfönster > **Larm** >  eller  > kolumnen **Larmidentitet** > kolumnen **Ljudfil** > Klicka på ...

Låter dig välja en ljudfil som spelas upp vid larm.

Spela upp

Klicka för att spela upp ljudfilen.

Paus

Klicka för att pausa den valda ljudfilen.

Stopp

Klicka för att stoppa den valda ljudfilen

Hantera...

Klicka för att visa dialogrutan **Resurshanteraren**.

Se

- *Konfigurera ett larm, sidan 301*
- *Hantera resursfiler, sidan 298*

23

Konfigurera händelser och larm

Huvudfönster > **Händelser**

eller

Huvudfönster > **Larm**

Detta kapitel tillhandahåller information om hur du konfigurerar händelser och larm i ditt system.

Tillgängliga händelser grupperas bakom motsvarande enheter.

På sidan **Händelser** konfigurerar du när en händelse i BVMS utlöser ett larm, utför ett kommandoskript och loggas.

Exempel (del av en händelsekonfigureringsstabell):

Device	Network	Trigger Alarm	Log	Script
Name	Address	Schedule	Schedule	Script
Camera 1 (172.31.21.20)	172.31.21.20	Never	Always	<none>
Camera 2 (172.31.21.20)	172.31.21.20	Never	Always	<none>
Camera 3 (172.31.21.20)	172.31.21.20	Never	Always	<none>
Camera 3 (172.31.21.21)	172.31.21.21	Never	Always	<none>
Camera 4 (172.31.21.20)	172.31.21.20	Never	Always	<none>
Camera 4 (172.31.21.21)	172.31.21.21	Never	Always	<none>
Main	172.30.11.237	Never	Always	<none>
Main Hall	172.31.21.21	Never	Always	<none>
Main Hall Grd. Floor	172.31.21.21	Never	Always	<none>
Parking Lot	172.30.11.39	Never	Always	<none>

Detta exempel innebär:

Om videosignalen för den valda kameran försvinner utlöses ett larm, händelsen loggas och inget skript utförs.

Under **Larm** definierar du hur ett larm ska visas samt vilka kameror som visas och spelas in i händelse av ett larm.

Vissa systemhändelser konfigureras standardmässigt som larm.

- Klicka på  för att spara inställningarna.
- Klicka på  om du vill ångra den senaste inställningen.
- Klicka på  för att aktivera konfigurationen.

Se

- *Fliken Avstudsningstillningar, sidan 285*
- *Fliken Inställningar för avancerad kartvisning, sidan 285*
- *Fliken Inställningar för händelsekonfiguration, sidan 286*
- *Redigerare för kommandoskript-dialogrutan, sidan 286*
- *Skapa sammansatt händelse / dialogrutan Redigera sammansatt händelse, sidan 287*
- *Välj skriptspråk-dialogrutan, sidan 287*
- *Dialogrutan Redigera prioriteter för händelsetyp, sidan 288*
- *Välj enheter-dialogrutan, sidan 288*
- *Dialogrutan Inspelning av textdata, sidan 288*
- *Dialogrutan Larminställningar, sidan 289*
- *Välj bildruteinnehåll-dialogrutan, sidan 290*
- *Larmalternativ-dialogrutan, sidan 292*

23.1 Kopiera och klistra in i tabeller

Du kan konfigurera många objekt samtidigt inom en kameratabell, en händelsekonfigurationstabell eller en larmkonfigurationstabell med några få klick.

Se *Kopiera och klistra in i tabeller*, sidan 271 för detaljerad information.

23.2 Ta bort en tabellrad

Huvudfönster > **Larm**

Du kan endast ta bort en tabellrad som du eller en annan användare har lagt till, dvs. du kan ta bort duplicerade händelser eller sammansatta händelser.

Sammansatta händelser finns i händelseträdet under **Systemenheter** > **Sammansatta händelser**.

Ta bort en tabellrad:

1. Välj raden.

2. Klicka på .

Se

– *Sidan Händelser*, sidan 284

23.3 Hantera resursfiler

För detaljerad information, se:

– *Hantera resursfiler*, sidan 244.

23.4 Konfigurera en händelse

Huvudfönster > **Händelser**

Konfigurerar en händelse:

1. Välj en händelse eller ett händelseläge i trädet, till exempel **Systemenheter** > **Behörighetskontroll** > **Operatörsautentisering nekad**.

Motsvarande händelsekonfigureringsstabell visas.

2. Klicka i en cell i kolumnen **Utlöser larm** – **Schema** och välj ett schema.

Schemat bestämmer när larmet ska utlösas.

Välj ett inspelningsschema eller uppgiftsschema som du har konfigurerat på sidan **Scheman**.

3. I kolumnen **Logga** - **Schema** klickar du på en cell och markerar lämpligt schema.

Schemat avgör när händelsen loggas.

4. I kolumnen **Skript** - **Skript** klickar du på en cell och markerar ett lämpligt kommandoskript.

5. Klicka i en cell i kolumnen **Skript** – **Schema** och välj ett schema.

Schemat bestämmer när händelsen ska utlösa kommandoskriptet.

Se

– *Sidan Händelser*, sidan 284

23.5 Duplicera en händelse

Huvudfönster > **Händelser**

Du kan duplicera en händelse för att utlösa olika larm för en särskild händelse.

Duplicera en händelse:

1. Välj ett händelsevillkor i trädet. Motsvarande händelsekonfigurationstabell visas.

2. Välj en tabellrad.

3. Klicka på . En ny tabellrad läggs till under. Den har standardinställningen.

Se

– *Sidan Händelser, sidan 284*

23.6

Logga användarhändelse

Huvudfönster > **Händelser** > expandera **Systemenheter** > **Användaråtgärder**

Du kan konfigurera loggningsbeteendet för flera användaråtgärder för varje tillgänglig användargrupp separat.

Exempel:

Logga användarhändelser:

- Välj en användarhändelse för att konfigurera dess loggningsbeteende, t.ex.
Operatörsinloggning.
 Motsvarande händelsekonfigurationstabell visas.
 Varje användargrupp visas i kolumnen **Enhet**.
- Om tillgänglig: I kolumnen **Utlöser larm - Schema** klickar du på en cell och väljer lämpligt schema.
 Schemat avgör när larmet som ska meddela användaren triggas.
 Du kan välja ett inspelnings- eller uppgiftsschema som du konfigurerade under **Scheman**.
- I kolumnen **Logga - Schema** klickar du på en cell och markerar lämpligt schema.
 Schemat avgör när händelsen loggas.
 I exemplet loggas inte operatörsinloggningen för den administrativa gruppen och för den avancerade användargruppen medan däremot operatörsinloggningen för liveanvändargruppen loggas under schemat **Dag**.

Se

– *Sidan Händelser, sidan 284*

23.7

Konfigurera knapp för användarhändelse

Huvudfönster > **Händelser**

Du kan konfigurera knapparna för användarhändelser som finns tillgängliga i Operator Client.

Du kan konfigurera att en eller flera knappar för användarhändelser inte ska visas i Operator Client.

På sidan **Användargrupper** konfigurerar du att knapparna för användarhändelser endast ska finnas tillgängliga i Operator Client för motsvarande användargrupp.

Konfigurera knappar för användarhändelser:

- Välj i trädet **Systemenheter** > **Händelseknappar för Operator Client** > **Händelseknapp har tryckts in.**
 Motsvarande händelskonfigurationstabell visas.
- Välj en knapp för användarhändelse för att konfigurera dess beteende.
- I kolumnen **Utlöser larm - Schema** klickar du på en cell och väljer lämpligt schema.
 Schemat avgör när larmet som ska meddela användaren triggas.
- I kolumnen **Logga - Schema**, klicka på en cell och markera det lämpliga schemat.
 Schemat avgör när händelsen loggas.
 Om du väljer **Aldrig** görs knappen för användarhändelse otillgänglig i Operator Client för alla användargrupper som har behörighet till knappen för användarhändelse.
- I kolumnen **Skript - Skript** klicka på en cell och markera ett lämpligt kommandoskript.
- I kolumnen **Skript - Schema** klickar du på en cell och väljer lämpligt schema.
 Schemat avgör när kommandoskriptet utförs.

Se

– Sidan Händelser, sidan 284

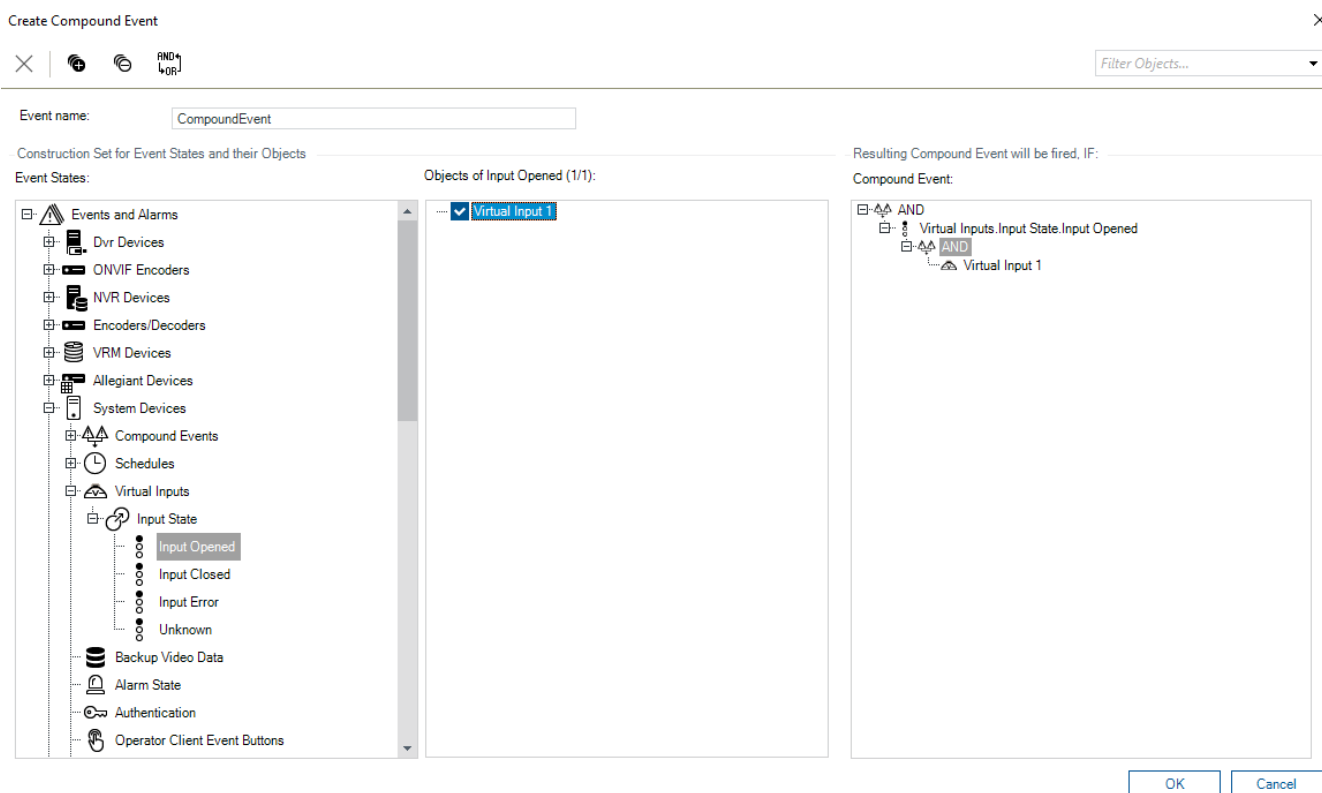
23.8

Skapa en sammansatt händelse

Huvudfönster > **Händelser** >

Du skapar en sammansatt händelse. Du kan endast kombinera statusändringar och deras objekt. Objekt kan till exempel vara scheman och enheter. Du kan kombinera både statusändringar och deras objekt med de booleska uttrycken AND och OR.

Exempel: du kombinerar anslutningsstatusarna för en IP-kamera och en avkodare. Den sammansatta händelsen ska endast inträffa när båda enheterna förlorar anslutningen. I sådant fall använder du operationen AND för de två objekten (IP-kameran och avkodaren) samt för de två anslutningsstatusarna **Videosignal förlorad** och **Frånkopplad**.

**Skapa en sammansatt händelse:**

1. Ange namnet på den sammansatta händelsen i fältet **Händelsenamn:**.
2. Välj en händelsestatus i fältet **Händelselägen:**.
Tillgängliga objekt visas i fältet **Objekt:**.
3. Välj enhet i fältet **Objekt:** efter behov.
Motsvarande händelse och de valda enheterna läggs till i fönstret för sammansatta händelser.
4. Högerklicka på en boolesk operation och ändra den vid behov i fältet **Sammansatt händelse:**.
En boolesk operation definierar kombinationen av dess direkt underordnade element.
5. Klicka på **OK**.
Den nya sammansatta händelsen läggs till i händelsekonfigureringsstabellen. Du hittar den i händelseträdet under **Systemenheter**.

Se

– *Sidan Händelser, sidan 284*

23.9

Redigera en sammansatt händelse

Huvudfönster > **Händelser**

Du kan ändra en sammansatt händelse som du skapat tidigare.

Redigera en sammansatt händelse:

1. Utvidga i händelseträdet **Systemenheter** > **Tillstånd för sammansatt händelse** > **Sammansatt händelse är sann**.
2. Gå till kolumnen **Enhet** i händelsekonfigurationstabellen, högerklicka på den sammansatta händelsen och klicka på **Redigera**.
Dialogrutan **Redigera sammansatt händelse** visas.
3. Gör de nödvändiga inställningarna.
4. Klicka på **OK**.
Den sammansatta händelsen ändras.

Se

– *Sidan Händelser, sidan 284*

23.10

Konfigurera ett larm

Huvudfönster > **Larm**

Innan ett larm konfigureras ska du konfigurera utlösaren i **Händelser**.

Konfigurera ett larm:

1. Välj ett larm i trädet, till exempel **Systemenheter** > **Behörighetskontroll** > **Operatörsautentisering nekad**.
Motsvarande larmkonfigurationstabell visas.
2. I kolumnen **Prioritet** klickar du på ... i en cell för att ange larmprioriteten för valt larm (100 är låg prioritet, 1 är hög prioritet).
I kolumnen **Titel** klickar du på ... i en cell och anger larmrubriken som ska visas i BVMS, t.ex. i larmlistan.
I kolumnen **Färg**, klicka på ... i en cell för att visa en dialogruta där du kan välja en larmfärg som ska visas i Operator Client, t.ex. i larmlistan.
3. I 1-5-kolumnerna klickar du på ... i en cell för att visa dialogrutan **Välj innehåll i bildrutan**.
Gör de nödvändiga inställningarna.
4. I kolumnen **Ljudfil** klickar du på ... i en cell för att visa en dialogruta där du kan välja en ljudfil som spelas upp i händelse av ett larm.
5. I kolumnen **Larmalternativ** klickar du på ... i en cell för att visa dialogrutan **Larmalternativ**.
6. Gör de nödvändiga inställningarna.

För detaljerad information om olika fält, se onlinehjälpn för lämpligt programfönster.

Se

- *Konfigurera en händelse, sidan 298*
- *Sidan Larm, sidan 289*
- *Välj bildruteinnehåll-dialogrutan, sidan 290*
- *Larmalternativ-dialogrutan, sidan 292*

23.11

Konfigurera inställningar för alla larm

Huvudfönster > **Larm**

Du kan ställa in följande larminställningar som är giltiga för denna Management Server:

- Antal bildrutor per larm

- Auto-rensningstid
- Manuell larminspelningstid
- Larmvisning i flera rader i larmbildsfönstret
- Tidsgräns för statusutlösta larminspelningar
- Konfigurera beteendet för alla monitorgrupper

Konfigurera alla larm:

1. Klicka på .
Dialogrutan **Larminställningar** visas.
2. Gör lämpliga inställningar.
 - ▶ Klicka på **OK**.

För detaljerad information om olika fält, se onlinehjälpens för lämpligt programfönster.

Se

- *Dialogrutan Larminställningar, sidan 289*

23.12

Konfigurera längden på förlarm och efterlarm

För att inställningarna för längden på förlarm och efterlarm ska kunna konfigureras måste kameran ha stöd för ANR och fast programvara av version 5.90 eller senare vara installerad.

Huvudfönster > **Kameror och inspelning** > 

- ▶ Klicka för att aktivera **ANR** för önskad kamera.

Huvudfönster > **Händelser**

- ▶ Konfigurera önskad händelse för den ANR-aktiverade kameran.

Huvudfönster > **Larm**

1. Konfigurera ett larm för den här händelsen.
2. Välj  eller .
3. I kolumnen **Larmalternativ** klickar du på ...
Dialogrutan **Larmalternativ** visas.
4. I kolumnen **Inspelning** markerar du kryssrutan för den ANR-aktiverade kameran för att aktivera larminspelning.
Kryssrutan i kolumnen **Avvikande längdinställningar för larm** markeras automatiskt.
5. Klicka på fliken **Avvikande längdinställningar för larm**.
6. Konfigurera inställningarna för larmlängd efter behov.

Se

- *Larmalternativ-dialogrutan, sidan 292*

23.13

Utlösa larminspelning med textdata

Huvudfönster > **Larm**

Du kan utlösa larminspelning med textdata.

Innan du konfigurerar ett larm måste du konfigurera en händelse som innehåller textdata.

Exempel: **Händelser** > Välj  i händelseträdet (textdata måste finnas tillgängliga, till exempel **Läsarenheter för nyckelkort** > **Nyckelkortsläsare** > **Avvisat kort**)

**Obs!**

Välj 0 som återstudstid för den valda händelsen.
Detta garanterar att inga textdata går förlorade.

Så här konfigurerar du larminspelning:

1. Välj ett larm i trädet, till exempel **ATM/POS-enheter > ATM-ingång > Dataingång**. Motsvarande larmkonfigurationstabell visas.
2. Gör de nödvändiga inställningarna.
3. I kolumnen **Larmalternativ** klickar du på ... i en cell för att visa dialogrutan **Larmalternativ**.
4. Klicka på fliken **Kameror** och markera kryssrutan **Inspelning**.

Se

- *Larmalternativ-dialogrutan, sidan 292*
- *Dialogrutan Inspelning av textdata, sidan 288*

23.14**Lägga till textdata för kontinuerlig inspelning**

Huvudfönster > **Händelser** > Välj  **Dataingång** i händelseträdet (textdata måste finnas tillgängliga, till exempel **Läsarenheter för nyckelkort > Nyckelkortsläsare > Avvisat kort**) > kolumnen **Inspelning av textdata** > ...

Du kan infoga textdata i kontinuerliga inspelningar.

23.15**Skydda larminspelning**

Huvudfönster > **Larm**

Innan du kan konfigurera ett larm måste du konfigurera en händelse i **Händelser**.

**Obs!**

Om du skyddar larminspelningen av en kamera raderas aldrig de skyddade videodata VRM automatiskt. Var medveten om att för många skyddade block kan fylla upp lagringen och kameran kan sluta spela in. Du måste ta bort videodata manuellt i Operator Client.

Så här konfigurerar du larminspelning:

1. Välj ett larm i trädet, till exempel **ATM/POS-enheter > ATM-ingång > Dataingång**. Motsvarande larmkonfigurationstabell visas.
2. Gör de nödvändiga inställningarna.
3. I kolumnen **Larmalternativ** klickar du på ... i en cell för att visa dialogrutan **Larmalternativ**.
4. Klicka på fliken **Kameror** och markera kryssrutan **Inspelning**.
1. Markera kryssrutan **Skydda inspelning**.

Se

- *Larmalternativ-dialogrutan, sidan 292*

23.16**Konfigurera blinkande aktiveringspunkter****Obs!**

En blinkande aktiveringspunkt kan endast konfigureras för en händelse ELLER för ett larm.

Huvudfönster > **Händelser**

eller

Huvudfönster > **Larm**

För varje  -händelse eller -larm kan du konfigurera bakgrundsfärgen och beteendet (blinkande eller fast) för aktiveringspunkter. Du kan till exempel konfigurera inställningarna så

att  -händelse eller -larm på en enhet gör att enhetsikonen på kartan börjar blinka när enhetens status ändras.

Du kan också konfigurera visningsprioriteten för alla aktiveringspunkter. Detta är obligatoriskt när olika händelser inträffar för samma enhet. (1 = högsta prioritet)

Den konfigurerade färgen gäller för alla aktiveringspunkter med samma visningsprioritet. Du

kan ändra färg, beteende och prioritet för alla  -händelser eller -larm: den ändrade färgen

och det ändrade beteendet används för alla aktiveringspunkter för alla andra  -händelser eller -larm som har samma prioritet.

Du kan bara konfigurera färglägena på kartor om du markerar alternativet **Aktivera avancerad statusvisning (färgning av aktiva punkter på kartor beroende på status)** eller alternativet **Aktivera avancerad statusvisning (färgning av aktiva punkter på kartor beroende på larm)** i dialogrutan **Alternativ**.

Så här konfigurerar du en blinkande aktiveringspunkt för en händelse:

1. Välj ett händelsetillstånd i trädet (), till exempel **Kodare/avkodare > Kodarrelä > Relästatus > Relä öppnat**.
Motsvarande händelsekonfigureringstabell visas.
2. Klicka på **Aktivera färglägen på kartor**.
3. Ange önskad prioritet i fältet **Visningsprioritet på karta:**.
4. Klicka i fältet **Bakgrundsfärg på karta:** och välj färg.
5. Om du vill klickar du för att aktivera **Blinkar**.

Så här konfigurerar du en blinkande aktiveringspunkt för ett larm:

Se kapitel *Larmidentitet*, sidan 289 på *Sidan Larm*, sidan 289.



Obs!

Aktiveringspunkten blinkar endast om larmet finns med i larmlistan.

Enhetsikonererna på en karta blinkar med samma färg som konfigurerats för larmet eller händelsen.

Se

- *Sidan Händelser*, sidan 284
- *Dialogrutan Alternativ (menyn Inställningar)*, sidan 114

23.17

Händelser och larm för passersystem

Ytterligare information om händelser och larm för passersystem.

Åtkomst begärd-händelse

Händelsen gör det möjligt för en BVMS-operatör att manuellt bevilja eller neka en person åtkomst via ett passersystem. Du kan konfigurera en larminspelning, inspelning av textdata eller ytterligare information till denna händelse.

Åtkomst begärd-händelser skickas endast till BVMS om alternativet **Ytterligare verifiering** har ställts in på varje läsare i passersystemet. I händelsekonfigurationen för BVMS utlöser de **Åtkomst begärd**-händelser som skickas av läsarna alltid ett larm i BVMS.

**Obs!**

Vi rekommenderar att du anger den högsta prioriteten (1) för **Åtkomst begärd**-larm. Detta säkerställer att larmen visas automatiskt och får den nödvändiga uppmärksamheten från operatören.

23.18**Händelser och larm för Person Identification**

Huvudfönster > **Händelser**

Ytterligare information om händelser och larm för Person Identification.

Obehörig person identifierad

För varje kamera kan du konfigurera vilken persongrupp som är behörig eller obehörig att komma åt ett visst område.

Obs! Konfigurationen av obehöriga och auktoriserade persongrupper är endast möjlig om du har behörigheten **Ändra händelseinställningar**.

Så här konfigurerar du Obehörig person identifierad

1. Välj respektive kamera under **Video Analytics**.
2. Välj händelsen **Obehörig person identifierad**.
3. Välj **Obehörig person identifierad**-fliken.
4. Klicka på ... i cellen **Obehörig** eller **Behörig**.
Dialogrutan **Kameraauktorisering** visas.
5. Genom att dra och släppa tilldelar du de konfigurerade persongrupperna till respektive fält.
6. Klicka på **OK**.
För respektive kamera är de konfigurerade persongrupperna nu inställda som auktoriserade eller obehöriga.

24

Sidan Användargrupper

**Obs!**

BVMS Viewer har bara grundläggande funktioner. Avancerade funktioner ingår i BVMS Professional. Detaljerad information om de olika BVMS utgåvorna finns på www.boschsecurity.com och BVMS Snabbvalsguiden: [BVMS snabbvalsguide](#).

Huvudfönster > Användargrupper

Gör det möjligt för dig att konfigurera användargrupper, Enterprise User Groups och Enterprise-åtkomst.

Följande användargrupp är tillgänglig som standard:

- Administrativ grupp (med en administratörsanvändare).

Fliken Användargrupper

Klicka om du vill visa tillgängliga sidor för konfiguration av rättigheter för standardanvändargruppen.

Fliken Enterprise User Groups

Klicka om du vill visa tillgängliga sidor för konfiguration av behörigheter för en Enterprise User Group.

Fliken Enterprise-åtkomst

Klicka om du vill visa tillgängliga sidor för tillägg och konfiguration av Enterprise Access.

Alternativ för användare/användargrupp

Ikon	Beskrivning
	Klicka om du vill ta bort en vald post.
	Klicka om du vill lägga till en ny grupp eller ett nytt konto.
	Klicka om du vill lägga till en ny användare i den valda användargruppen. Ändra standardanvändarnamnet om så önskas.
	Klicka för att lägga till en ny grupp för dubbel behörighet.
	Klicka om du vill lägga till ett nytt inloggningspar för dubbel behörighet.
	Visar en dialogruta där du kan kopiera behörigheter från en vald användargrupp till en annan användargrupp.
	Klicka om du vill visa tillgängliga sidor för konfiguration av behörigheterna för den här gruppen.
	Klicka om du vill visa tillgänglig sida för konfiguration av den här användarens egenskaper.
	Klicka om du vill visa den tillgängliga sidan för konfiguration av den här användarens inloggningspar.
	Klicka om du vill visa tillgängliga sidor för konfiguration av behörigheter för denna dubbelbehörighetsgrupp.

Aktivera ändringar av användarnamn och lösenord



Klicka om du vill aktivera ändringar av lösenord.



Klicka om du vill aktivera ändringar av användarnamn.



Obs!

Användarnamn och lösenord som har ändrats, återställs efter en återställning av konfigurationen.

Behörigheter på ett Enterprise System

För ett Enterprise System kan du konfigurera följande behörigheter:

- Funktionsbehörigheter som Operator Client som definierar det användargränssnitt som används för drift i Enterprise System, t.ex. användargränssnittet för larmmonitorn. Använd en Enterprise User Group. Konfigurera på Enterprise Management Server.
- Enhetsbehörigheter som behöver finnas på plats för drift i en Enterprise Management Server definieras för varje Management Server. Använd Enterprise Accounts. Konfigurera på varje Management Server.

Behörigheter på en fristående Management Server

För att hantera åtkomst till en enskild Management Servers använder du standardanvändargruppen. Du konfigurerar alla behörigheter för denna Management Server i den här användargruppen.

Du kan konfigurera dubbel behörighet för användargrupper för standardanvändargrupper och för Enterprise User Groups.

Typ	Innehåller	Tillgängliga konfigurationsinställningar	Var konfigurerar du?
Användargrupp	Användare	– Funktions- och enhetsbehörigheter	– Management Server
Enterprise User Group	Användare	– Funktionsbehörigheter – Per Management Server: Namn på motsvarande Enterprise Access Account-konton med inloggningsuppgifter	– Enterprise Management Server
Enterprise Account	-	– Enhetsbehörigheter – Kontonyckel	– Management Server
Användargrupp med dubbel behörighet	Användargrupper	– Visa användargrupper	– Visa användargrupper
Dubbel behörighet för Enterprise	Enterprise User Groups	– Se Enterprise User Groups	– Se Enterprise User Groups

Filter...

Skriv in en sträng och tryck på ENTER-tangenten för att filtrera de visade objekten. Endast objekt som innehåller strängen och deras motsvarande föräldraobjekt (endast i träd) visas. Antalet filtrerade objekt och det totala antalet objekt visas. Ett aktivt filter indikeras med . Skriv in strängar inom dubbla citattecken för att hitta dem exakt, till exempel filtrerar "Camera 1" kamerorna med exakt detta namn, inte camera 201.

Avbryt filtreringen genom att klicka på .

24.1

Sidan Egenskaper för användargrupper

Huvudfönster > **Användargrupper** > fliken **Användargrupper** >  > fliken **Operatörsbehörigheter** > fliken **Egenskaper för användargrupper** eller

Huvudfönster > **Användargrupper** > fliken **Enterprise User Groups** >  > fliken **Operatörsbehörigheter** > fliken **Egenskaper för användargrupper**

Möjliggör konfigurerings av följande inställningar för den valda användargruppen:

- Inloggningsschema
- Val av associerad LDAP-användargrupp

Egenskaper för användargrupper

Beskrivning:

Skriv in en informativ beskrivning av användargruppen.

Språk

Välj språk för Operator Client.

Inloggningsschema

Välj en uppgift eller ett inspelningsschema. Användarna i den valda gruppen kan endast logga in i systemet under de tider som finns definierade i detta schema.

LDAP-egenskaper

Sök efter grupper

Klicka för att visa tillgängliga tillhörande LDAP-grupper i **Tillhörande LDAP-grupp** listan. Om du vill välja en associerad LDAP-grupp måste du ange lämpliga inställningar i **Inställningar för LDAP-server** dialogrutan.

Tillhörande LDAP-grupp

Välj en LDAP-grupp i **Tillhörande LDAP-grupp** listan som du vill använda för systemet.

Se

- *Välja en associerad LDAP-grupp, sidan 333*
- *Associera en LDAP-grupp, sidan 111*
- *Schemalägga en användares inloggningsbehörighet, sidan 333*

24.2

Sidan Användaregenskaper

Huvudfönster > **Användargrupper** > fliken **Användargrupper** >  >  eller

Huvudfönster > **Användargrupper** > fliken **Enterprise User Groups** >  > 

Här kan du konfigurera en ny användare i en standardanvändargrupp eller i en Enterprise User Group.

Om du ändrar lösenordet för en användare eller tar bort en användare medan användaren i fråga är inloggad, så kan användaren ändå fortsätta arbeta med Operator Client efter ändringen av lösenordet eller borttagningen. Om anslutningen till Management Server avbryts efter ändringen av lösenordet eller borttagningen (t.ex. efter aktivering av konfigurationen), så kan inte användaren automatiskt återansluta till Management Server utan att logga ut/logga in på Operator Client.

Kontot är aktiverat

Markera kryssrutan om du vill aktivera ett användarkonto.

Fullständigt namn

Ange användarens fullständiga namn.

Beskrivning

Skriv in en informativ beskrivning av användaren.

Användaren måste ändra sitt lösenord vid nästa inloggning

Markera kryssrutan om du vill tvinga användaren att ställa in ett nytt lösenord vid nästa inloggning.

Ange det nya lösenordet

Ange lösenordet för den nya användaren.

Bekräfta lösenordet

Ange det nya lösenordet igen.

**Obs!**

Vi rekommenderar starkt att du tilldelar ett specifikt lösenord till alla nya användare och att du kräver att användaren ändrar det vid inloggning.

**Obs!**

Mobile Video Service-, Web Client-, Bosch iOS App- och SDK-klienter kan inte ändra lösenordet vid inloggning.

Verkställ

Klicka för att verkställa inställningarna.

Klicka på  för att aktivera lösenordet.

Ytterligare information

Efter uppgraderingen till BVMS 9.0.0.x är **Användaregenskaper**-inställningarna följande:

- **Kontot är aktiverat** är inställt.
- **Användaren måste ändra sitt lösenord vid nästa inloggning** är inte inställt.

24.3

Sidan Logga in paregenskaper

Huvudfönster > **Användargrupper** Användargrupper > fliken  > **Ny dubbel**

auktoriseringsgrupp > 
eller

Huvudfönster > **Användargrupper** > fliken **Enterprise User Groups** >  **Ny dubbel**

Enterprise-auktoriseringsgrupp > 

Låter dig ändra ett användargrupspar till en dubbel behörighetsgrupp. Användarna i den första användargruppen är de användare som måste logga in via den första dialogrutan för inloggning. Användarna i den andra användargruppen kan endast bekräfta inloggningen.

Välj inloggningspar

Välj en användargrupp i varje lista.

Tvingande dubbel behörighet

Markera kryssrutan för varje användare som bara ska logga in tillsammans med en användare från den andra användargruppen.

Se

- *Lägga till ett inloggningspar till en grupp med dubbel behörighet, sidan 331*

24.4

Sidan Kamerabehörigheter

Huvudfönster > **Användargrupper** > fliken **Användargrupper** >  > fliken **Enhetsbehörigheter** > fliken **Kamerabehörigheter**
eller

Huvudfönster > **Användargrupper** > fliken **Enterprise-åtkomst** >  > fliken **Enhetsbehörigheter** > fliken **Kamerabehörigheter**

Låter dig konfigurera åtkomstbehörigheterna för funktioner hos en vald kamera eller kameragrupp för den valda användargruppen.

Om nya komponenter läggs till måste kamerabehörigheterna konfigureras i efterhand.

Du kan återkalla åtkomsten till en kamera på sidan **Kamera**.

Kamera

Visar kameranamnet som det är konfigurerat på sidan **Kameror och inspelning**.

Plats

Visar placering av kameran som den är konfigurerad på sidan **Kartor och struktur**.

Åtkomst

Markera en kryssruta för att aktivera åtkomst till den här kameran.

Live-video

Markera en kryssruta för att aktivera användning av live-video.

Live-ljud

Markera en kryssruta för att aktivera användning av live-ljud.

Manuell inspelning

Markera en kryssruta för att aktivera manuell inspelning (larminspelning).

Du kan endast markera eller avmarkera den här kryssrutan när manuell larminspelning är aktiverad på sidan **Operatörsfunktioner**.

Spela upp video

Markera en kryssruta för att möjliggöra användning av videouppspelning.

Du kan endast markera eller avmarkera den här kryssrutan när uppspelning är aktiverad på sidan **Operatörsfunktioner**.

Spela upp ljud

Markera en kryssruta för att aktivera användning av ljuduppspelning.

Du kan endast markera eller avmarkera den här kryssrutan när uppspelning är aktiverad på sidan **Operatörsfunktioner**.

Textdata

Markera en kryssruta för att aktivera visning av metadata.

Du kan endast markera eller avmarkera den här kryssrutan när visning av metadata är aktiverad på sidan **Operatörsfunktioner**.

Exportera

Markera en kryssruta för att möjliggöra export av videodata.

Du kan endast markera eller avmarkera den här kryssrutan när export av videodata är aktiverad på sidan **Operatörsfunktioner**.

PTZ/ROI

Markera en kryssruta för att medge användning av PTZ-kontrollen eller ROI för kameran.

Du kan endast markera eller avmarkera den här kryssrutan när PTZ-styrningen eller ROI för kameran har aktiverats på sidan **Operatörsfunktioner**. Du måste dessutom konfigurera PTZ eller ROI i kameratabellen.

Aux

Markera en kryssruta för att aktivera utförande av extrakommandon.

Du kan endast markera eller avmarkera den här kryssrutan när PTZ-styrningen av en kamera är aktiverad på sidan **Operatörsfunktioner**.

Ange fördefinierad position

Markera en kryssruta för att låta användaren ställa in förpositioner för den här PTZ-kameran.

Du kan också ställa in förpositioner för avkänningsområde (ROI), om denna funktion har aktiverats och tillåts.

Du kan endast markera eller avmarkera den här kryssrutan när PTZ-styrningen av en kamera är aktiverad på sidan **Operatörsfunktioner**.

Referensbild

Markera en kryssruta för att medge uppdatering av referensbilden för den här kameran.

24.5

Sidan Kontrollprioriteter

Huvudfönster > **Användargrupper** > fliken **Användargrupper** >  > fliken **Enhetsbehörigheter** > fliken **Kontrollprioriteter**
eller

Huvudfönster > **Användargrupper** > fliken **Enterprise-åtkomst** >  > fliken **Enhetsbehörigheter** > fliken **Kontrollprioriteter**

Kontrollprioriteter

Flytta skjutreglaget till höger för att minska prioriteten för att erhålla PTZ-kontroller och Allegiant-stamlinjer. En användare med hög prioritet kan låsa PTZ-styrningen och kontrollen över en trunkledning för användare med lägre prioritet. Du ställer in tidsgränsen för låsning av PTZ-styrning i fältet **Tidsgräns i minuter**. Standardinställningen är 1 minut.

Tidsgräns i minuter

Ange tidsperioden i minuter.

Se

– *Konfigurera flera prioriteringar, sidan 334*

24.6 Kopiera behörigheter för användargrupp-dialogrutan

Huvudfönster > **Användargrupper** > fliken **Användargrupper** >  > 
eller

Huvudfönster > **Användargrupper** > fliken **Enterprise User Groups** >  > 
Låter dig välja behörigheter för användargrupper som ska kopieras till utvalda användargrupper.

Kopiera från:

Visar den valda användargruppen. Dess behörigheter ska kopieras till en annan användargrupp.

Inställningar att kopiera

Markera en kryssruta för att välja vilka användargruppbehörigheter du önskar kopiera.

Kopiera till:

Markera kryssrutan för att specificera den användargrupp till vilken de valda behörigheterna för användargruppen ska kopieras.

Se

– *Kopiera behörigheter för användargrupper, sidan 335*

24.7 Sidan Avkodarbehörigheter

Huvudfönster > **Användargrupper** > fliken **Användargrupper** >  > fliken **Enhetsbehörigheter** > fliken **Avkodarbehörigheter**
eller

Huvudfönster > **Användargrupper** > fliken **Enterprise-åtkomst** >  > fliken **Enhetsbehörigheter** > fliken **Avkodarbehörigheter**
Låter dig konfigurera avkodarna som användarna i den här gruppen har åtkomst till.

Avkodare

Visar tillgängliga avkodare.

Klicka på kryssrutan för att ge användargruppen åtkomst till den här avkodaren.

Monitorgrupp

Markera kryssrutan om du vill ge användarna i den valda användargruppen åtkomst till den här monitorgruppen.

24.8 Sidan Händelser och larm

Huvudfönster > **Användargrupper** > fliken **Användargrupper** >  > fliken **Enhetsbehörigheter** > fliken **Händelser och larm**
eller

Huvudfönster > **Användargrupper** > fliken **Enterprise-åtkomst** >  > fliken **Enhetsbehörigheter** > fliken **Händelser och larm**

Låter dig konfigurera behörigheterna för händelseträdet. Du kan till exempel ställa in de händelser som användargruppen har eller inte har behörighet att använda.

Du kan inte ändra dessa inställningar för en standardanvändargrupp.

För varje händelse finns det minst en enhet. Exempelvis är enheterna för händelsen **Videoavbrott** de tillgängliga kamerorna. För en händelse som **Säkerhetskopiering avslutad** är motsvarande enhet **Tidskontrollerad säkerhetskopiering**. Det betyder att en enhet kan vara en programvaruprocess.

1. Expandera ett trädobjekt och markera lämpliga kryssrutor för att aktivera händelserna. I kolumnen **Åtkomst** markerar du kryssrutan för en enhet för att aktivera händelserna för enheten. Åtkomsten till enheterna konfigureras på sidan **Kamera** och på sidan **Kamerabehörigheter**.
2. Om du vill aktivera eller inaktivera alla händelser samtidigt markerar eller avmarkerar du kryssrutan **Händelser och larm**.

24.9

Sidan Inloggningsuppgifter

Huvudfönster > **Användargrupper** > fliken **Enterprise-åtkomst** >  > fliken **Enhetsbehörigheter** > fliken **Inloggningsuppgifter**

Konfigurera inloggningsuppgifterna för ett Enterprise Account på en Management Server. Du kan konfigurera Enterprise Access på varje Management Server som ingår i ditt Enterprise System. Enterprise Management Server använder den här uppgiften för att tillåta åtkomst till enheterna på denna Management Server för den Operator Client som loggar in som en användare i en Enterprise User Group.

Beskrivning:

Skriv en beskrivning för önskat Enterprise Account.

Stark nyckelprincip

Kryssrutan **Stark nyckelprincip** är förvald för alla nya användargrupper.

Vi rekommenderar starkt att du behåller den här inställningen för bättre skydd mot obehörig åtkomst.

Följande regler gäller:

- Minsta nyckellängd enligt inställningen på **Kontopolicyer** sidan för önskad användargrupp.
- Använd inte någon av de tidigare nyckel.
- Använd minst en versal (A–Z).
- Använd minst en siffra (0–9).
- Använd minst ett specialtecken (till exempel: ! \$ # %).

Ange ny nyckel: / Bekräfta nyckel:

Skriv in och bekräfta nyckeln för denna Management Server.

Se

- *Skapa ett Enterprise Account, sidan 329*

24.10

Sidan Logiskt träd

Huvudfönster > **Användargrupper** > fliken **Användargrupper** >  > fliken **Enhetsbehörigheter** > fliken **Logiskt träd**
eller

Huvudfönster > **Användargrupper** > fliken **Enterprise-åtkomst** >  > fliken **Enhetsbehörigheter** > fliken **Logiskt träd**

Låter dig konfigurera det logiska trädet för varje användargrupp.

Så här konfigurerar du behörigheter:

- ▶ Markera eller avmarkera kryssrutorna efter behov.
Om du väljer ett objekt nedanför en nod markeras noden automatiskt.
Om du väljer en nod markeras alla objekt nedanför automatiskt.

Kamera

Markera en kryssruta för att ge användarna i den valda användargruppen åtkomst till motsvarande enheter.

Du kan återkalla åtkomsten till en kamera på sidan **Kamerabehörigheter**.

Monitorgrupp

Markera kryssrutan om du vill ge användarna i den valda användargruppen åtkomst till den här monitorgruppen.

Se

- *Konfigurera enhetsbehörigheter, sidan 334*

24.11**Sidan Användarfunktioner**

Huvudfönster > **Användargrupper** > fliken **Användargrupper** >  > fliken **Operatörsbehörigheter** > fliken **Operatörsfunktioner**
eller

Huvudfönster > **Användargrupper** > fliken **Enterprise User Groups** >  > fliken **Operatörsbehörigheter** > fliken **Operatörsfunktioner**

Låter dig konfigurera diverse behörigheter för den valda användargruppen.

PTZ-styrning av domekameror

Markera kryssrutan för att aktivera styrning av en kamera.

Sidan **Kontrollprioriteter**: I fältet **Kontrollprioriteter** kan du ställa in prioriteten för att överta styrningen för en kamera.

Allegiant-trunkledning

Markera kryssrutan för att aktivera åtkomst till Bosch Allegiant-trunkledningar.

Sidan **Kontrollprioriteter**: I fältet **Kontrollprioriteter** kan du ställa in prioriteten för att erhålla Bosch Allegiant-trunkledningar.

Skriv ut och spara

Markera kryssrutan om du vill tillåta utskrift och lagring av video, kartor och dokument.

Bearbetar larm

Markera kryssrutan för att aktivera bearbetning av larm.

Stäng av Windows skärmläckare vid inkommande larm

Markera kryssrutan om du vill säkerställa att inkommande larm visas även om skärmläckaren är aktiv. Den här inställningen har ingen effekt om skärmläckaren kräver ett användarnamn och lösenord för att avbrytas.

Larmvisning

Markera kryssrutan för att aktivera visning av larm. Om du väljer det här alternativet avaktiveras **Bearbetar larm** samtidigt.

Uppspelning

Markera kryssrutan för att tillåta olika uppspelningsfunktioner.

Exportera video

Markera kryssrutan för att aktivera export av videodata.

Exportera till externa format

markera kryssrutan för att tillåta export av videodata till icke-nativt format.

Skydda video

Markera kryssrutan för att aktivera skydd av videodata.

Sluta skydda video

Markera kryssrutan för att aktivera både skyddade och oskyddade videodata.

Begränsa video (endast användare med den här behörigheten får visa begränsad video)

Markera kryssrutan för att aktivera begränsning av videodata.

Sluta begränsa video

Markera kryssrutan för att aktivera båda, begränsning och borttagning av begränsning av videodata.

**Obs!**

VRM

Konfigurera användarbehörigheterna för att begränsa och begränsa videodata efter BVMS behov.

Endast en användare, som har **Begränsa video (endast användare med den här behörigheten får visa begränsad video)** behörighet, kan se begränsad video på tidslinjen för Operator Client. Det begränsade tidsintervallet visas annars som **Ingen inspelning**.

**Obs!**

DIVAR AN

Konfigurera användarbehörigheter för att begränsa och ta bort begränsningar för videodata på din DIVAR AN enhet efter behov. Skapa en användare i BVMS med samma inloggningsuppgifter och konfigurera behörigheterna för begränsning och borttagning av begränsning av videodata.

Visningen av begränsad video påverkas inte och måste konfigureras separat på DIVAR AN-enheten.

Ta bort video

Markera kryssrutan för att aktivera borttagande av videodata.

Åtkomst till video som har spelats in under perioder då användargruppen inte har haft behörighet att logga in

Markera kryssrutan för att aktivera åtkomst till beskrivna videodata.

Loggboksåtkomst

Markera kryssrutan för att aktivera åtkomst till loggboken.

Radera textdata från loggboksposter (för radering av personrelaterade data)

Markera kryssrutan för att tillåta radering av textdata från loggboksposter.

Händelseknappar för operatör

Markera kryssrutan för att aktivera knapparna för användarhändelser i Operator Client.

Stäng Operator Client

Markera kryssrutan för att aktivera stängning av Operator Client.

Minimera Operator Client

Markera kryssrutan om du vill kunna minimera Operator Client.

Porttelefon med ljud

Markera i kryssrutan för att låta användaren tala i högtalarna på en kodare med funktioner för in- och utgående ljud.

Manuell larminspelning

Markera kryssrutan för att aktivera manuell bearbetning av larm.

Åtkomst till VRM-monitor

Markera kryssrutan om du vill tillåta åtkomst till programvaran VRM Monitor.

Ange referensbild

Markera kryssrutan för att tillåta uppdatering av referensbilden i Operator Client.

Ange områdesurval för referensbild

Markera kryssrutan för att göra det möjligt att välja området i kamerabilden för uppdatering av referensbilden i Operator Client.

Byt lösenord

Markera kryssrutan om du vill att en Operator Client-användare ska kunna ändra lösenordet för inloggning.

Armera inbrottspanelsområden

Markera kryssrutan om du vill tillåta en användare med Operator Client att aktivera områden som har konfigurerats i en inbrottspanel som ingår i din BVMS-konfiguration.

Framtvinga armering av inbrottspanelsområden

Markera kryssrutan för att tillåta en användare av Operator Client att framtvinga aktivering av områden som har konfigurerats i en inbrottspanel som ingår i BVMS-konfigurationen.

Desarmera inbrottspanelsområden

Markera kryssrutan för att tillåta en användare med Operator Client att inaktivera områden som har konfigurerats i en inbrottspanel som ingår i BVMS-konfigurationen.

Stäng av signaler för inbrottspanelsområden

Markera kryssrutan för att tillåta en användare med Operator Client att stänga av larmsirenerna för områden som har konfigurerats i en inbrottspanel som ingår i BVMS-konfigurationen.

Kringgå inbrottspanelspunkter

Markera kryssrutan för att tillåta en användare med Operator Client att ändra läget på punkt som har konfigurerats i en inbrottspanel till läget **Punkt kringgås**. En punkt som har kringgåtts kan inte skicka ett larm. När tillståndet ändras tillbaka till **Punkt kringgås ej**, skickas eventuella väntande larm

Lås upp inbrottspanelsdörrar

Markera kryssrutan om du vill tillåta en användare med Operator Client att låsa upp en dörr som har konfigurerats i en inbrottspanel.

Säkra och osäkra inbrottspanelsdörrar

Markera kryssrutan om du vill tillåta en användare med Operator Client att låsa och låsa upp en dörr som har konfigurerats i en inbrottspanel.

Växla inbrottspanelsdörrar

Markera kryssrutan när en användare med Operator Client ska kunna växla läget på en dörr som har konfigurerats i inbrottspanelen.

Styra åtkomst dörrar

Markera kryssrutan om du vill tillåta att användare av Operator Client byter dörrläge (säker, låst, upplåst).

Personhantering

Markera kryssrutan om du vill att en användare av Operator Client ska kunna hantera personer för Person Identification-larm.

Visningsföljd vid samma larmprioritet

Välj lämpligt värde för att konfigurera ordningsföljden för larmbildrutor i larmvisningen för Operator Client.

Återspolningstid vid direktuppspelning:

Ange antalet sekunder som direktuppspelningen av larm tar.

Upprepa ljudlarm:

Markera kryssrutan och ange antalet sekunder efter vilket ett larmljud upprepas.

Begränsa åtkomsten till inspelad video till de senaste n minuterna:

Markera kryssrutan för att begränsa åtkomsten till inspelade videor.

Ange antal minuter i listan.

Tvinga fram automatisk utloggning av operatören efter så här lång inaktivitet:

Markera kryssrutan för att aktivera automatisk utloggning för Operator Client efter den konfigurerade tidsperioden.

Se

– *Utloggning vid inaktivitet, sidan 40*

24.12

Sidan Prioriteringar

Huvudfönster > **Användargrupper** > fliken **Användargrupper** >  > fliken **Operatörsbehörigheter** > fliken **Prioriteringar**
eller

Huvudfönster > **Användargrupper** > fliken **Enterprise User Groups** >  > fliken **Operatörsbehörigheter** > fliken **Prioriteringar**

Gör att du kan konfigurera timeout för explicit PTZ-låsning. Du kan ställa in prioriteringar för PTZ-styrning och visning av inkommande larm.

Automatisk snabbvisning

Flytta skjutreglaget för att justera prioritetsvärdet för live-bildfönstret eller uppspelningsbildfönstret. Detta värde krävs för att inkommande larm ska kunna avgöra huruvida detta larm ska visas automatiskt i larmbildfönstret.

Till exempel: Om du flyttar skjutreglaget för live-bildfönstret till 50 och för uppspelningsvisningen till 70 och ett larm inträffar med en prioritet på 60, visas larmet endast automatiskt om användaren har aktiverat uppspelningsvisning. Larmet visas inte automatiskt när användaren har aktiverat live-visning.

Se

– *Konfigurera flera prioriteringar, sidan 334*

24.13

Sidan Användargränssnitt

Huvudfönster > **Användargrupper** > fliken **Användargrupper** >  > fliken **Operatörsbehörigheter** > fliken **Användargränssnitt**
eller

Huvudfönster > **Användargrupper** > fliken **Enterprise User Groups** >  > fliken **Operatörsbehörigheter** > fliken **Användargränssnitt**

Här kan du konfigurera användargränssnittet för fyra monitorer som används av Operator Client.

Du kan konfigurera ett flermonitorläge med upp till fyra monitorer. För varje monitor ställer du in vad som ska visas på den, till exempel att monitor 2 bara visar livebildrutor eller att monitor 1 och monitor 2 har bildförhållandet 16:9 för HD-kameror.

Kontrollmonitor

Välj den monitor som ska användas som kontrollmonitor.

Högsta antal rader för bildrutor vid uppspelning

Välj det högsta antalet bildruterader som ska visas i uppspelningsbildfönstret på kontrollmonitorn.

Larmmonitor

Välj den larmmonitor som kan visa antingen live- och larminnehåll eller enbart larminnehåll.

Monitor 1–4

Välj en post i motsvarande lista för varje monitor.

- För kontrollmonitorn är posten **Styrning** förvald och kan inte ändras.
- För larmmonitorn kan du välja någon av följande poster:
 - **Livevideo och larminnehåll**
 - **Endast larminnehåll**
- För de återstående monitorerna kan du välja någon av följande poster:
 - **Endast livevideo**
 - **Karta och dokument**
 - **Två kartor och dokument**
 - **Livevideo på helskärm**
 - **Livebild med fyra bilder**

Högsta antal rader för bildrutor

Välj det högsta antalet bildruterader som ska visas i bildfönstret på en monitor.

Obs! Det här alternativet är endast tillgängligt för följande vyer:

- **Styrning**
- **Endast larminnehåll**
- **Livevideo och larminnehåll**
- **Endast livevideo**

De återstående vyerna har en fast layout med ett fast antal bildruterader och kan inte ändras.

Bildrutors bildförhållande

Välj bildförhållandet för varje monitor för den första starten av Operator Client. Använd 16:9 för HD-kameror.

Spara inställningarna vid avstängning

Markera kryssrutan för att aktivera att systemet kommer ihåg användargränssnittets senaste status när användaren loggar ut från Operator Client. Om kryssrutan inte är markerad startar Operator Client alltid med konfigurerat användargränssnitt.

Återställ standard

Klicka här om du vill återställa standardinställningarna på den här sida. Alla listposter återställs till standardinställningarna.

24.14 Sidan Serveråtkomst

Huvudfönster > **Användargrupper** > fliken **Enterprise User Groups** >  > fliken

Serveråtkomst

Du konfigurerar serveråtkomsten på en Enterprise Management Server.

Du anger namnet på Enterprise Account-kontot och kontots lösenord för varje Management Server i Enterprise System. Kontot konfigureras på varje Management Server.

Management Server

Visar namnet på den Management Server som du konfigurerade på denna Enterprise Management Server.

Nätverksadress

Visar den privata IP-adressen eller DNS-namnet för Management Server.

Servernummer

Visar numret för Management Server. Numret används av ett Bosch IntuiKey-tangentbord för att välja önskad Management Server.

Åtkomst

Välj kryssrutan när du vill tillåta åtkomst till Management Server. Nu är denna Management Server en Enterprise Management Server.

Enterprise Account

Ange namnet på det Enterprise Account-konto som har konfigurerats på Management Server.

Behörighetskontroll

Välj respektive autentiseringsalternativ i dialogrutan **Autentiseringsinställningar**.

Konfigurera API

Markera kryssrutan om åtkomsttoken ska tillåta åtkomst till tjänsten Konfigurera API för Management Server.

Serverbeskrivning

Visar beskrivningstexten för den här servern.

Fler kolumner visas om de har lagts till i serverlistan.

Se

- Skapa en grupp eller ett konto, sidan 328
- Skapa ett Enterprise System, sidan 81
- Konfigurera serverlistan för Enterprise System, sidan 81
- Tokenbaserad autentisering, sidan 83

24.15 Sidan Konfigurationsbehörigheter

Huvudfönster > **Användargrupper** > fliken **Användargrupper** > fliken  > **Operatörsbehörigheter** > fliken **Konfigurationsbehörigheter**
eller

Huvudfönster > **Användargrupper** > fliken **Enterprise User Groups** >  > fliken **Operatörsbehörigheter** > fliken **Konfigurationsbehörigheter**

Låter dig konfigurera olika användarbehörigheter för Configuration Client.

Behörighet att starta Configuration Client innebär skrivskyddad åtkomst.

Inloggningsbehörighet

Markera kryssrutan om du vill tillåta inloggning till Configuration Client-programmet.

Enhetsträd

I det här avsnittet kan du ange behörigheterna på sidan **Enheter**. Markera kryssrutan för respektive behörighet.

Kartor och struktur

I det här avsnittet kan du ange behörigheterna på sidan **Kartor och struktur**. Markera kryssrutan för respektive behörighet.

Scheman

I det här avsnittet kan du ange behörigheterna på sidan **Scheman**. Markera kryssrutan för respektive behörighet.

Kameror och inspelning

I det här avsnittet kan du ange behörigheterna på sidan **Kameror och inspelning**. Markera kryssrutan för respektive behörighet.

Händelser

I det här avsnittet kan du ange behörigheterna på sidan **Händelser**. Markera kryssrutan för respektive behörighet.

Larm

I det här avsnittet kan du ange behörigheterna på sidan **Larm**. Markera kryssrutan för respektive behörighet.

Användargrupper

I det här avsnittet kan du ange behörigheterna för att konfigurera användargrupper. Markera kryssrutan för respektive behörighet.

**Obs!**

Av säkerhetsskäl utesluter kryssrutan **Konfigurera användargrupper/Enterprise Accounts/LDAP-serverinställningar/Inställningar för åtkomsttoken/Inställningar för betrott certifikat** och kryssrutan **Konfigurera användare** varandra.

Menykommandon

I det här avsnittet kan du ange behörigheterna för att konfigurera menykommandon. Markera kryssrutan för respektive behörighet.

Rapporter

I det här avsnittet kan du ange behörigheterna för att konfigurera rapporter. Markera kryssrutan för respektive behörighet.

**Obs!**

Om du vill använda Config API-tjänsten för Management Server, måste du välja följande

Konfigurationsbehörigheter:

- Tillåt inloggning till konfigurationsklienten
- Ändra enhetsegenskaper
- Anropa Aktiveringshanteraren

**Obs!**

Om du vill konfigurera **Inställningar för betrott certifikat** måste du välja behörigheten **Konfigurera användargrupper/Enterprise Accounts/LDAP-serverinställningar och åtkomsttoken**.

24.16 Sidan Användargruppbehörigheter

Huvudfönster > **Användargrupper** > fliken **Användargrupper** >  > fliken **Operatörsbehörigheter** > fliken **Behörigheter för användargrupp** eller

Huvudfönster > **Användargrupper** > fliken **Enterprise User Groups** >  > fliken **Operatörsbehörigheter** > fliken **Behörigheter för användargrupp**

Låter dig ange i vilka användargrupper som användarna i en viss användargrupp kan lägga till nya användare.



Obs!

Du kan bara tilldela användargrupsbehörigheter till en användargrupp som du tidigare har tilldelat behörighet att konfigurera användare. Du tilldelar den här behörigheten på sidan **Konfigurationsbehörigheter**.



Obs!

Användarna i en standardanvändargrupp har inte behörighet att lägga till nya användare i den administrativa gruppen. Den här kryssrutan är inte aktiverad.

Se

– *Sidan Konfigurationsbehörigheter, sidan 319*

24.17 Sidan Kontoprinciper

Huvudfönster > **Användargrupper** > fliken **Användargrupper** >  > fliken **Säkerhet** > fliken **Kontopolicyer** eller

Huvudfönster > **Användargrupper** > fliken **Enterprise User Groups** >  > fliken **Säkerhet** > fliken **Kontopolicyer**

Låter dig konfigurera inställningar för användare och lösenord.

Policy om starka lösenord

Markera kryssrutan om du vill aktivera lösenordsprincipen.

Mer information finns i *Konfigurerar användare, behörigheter och Enterprise Access, sidan 327*.



Obs!

Inställningen **Policy om starka lösenord** gäller bara för användarna om kryssrutan är markerad i motsvarande användargrupp.

Vi rekommenderar starkt att du behåller den här inställningen för bättre skydd mot obehörig åtkomst.

Kortast tillåtna lösenord

Den här inställningen anger det minsta antal tecken som ett lösenord för ett användarkonto måste innehålla.

Markera kryssrutan om du vill aktivera inställningen och ange det minsta antalet tecken.

Högsta ålder för lösenord i dagar

Den här inställningen anger hur länge (i antal dagar) som ett lösenord kan användas innan systemet kräver att användaren ändrar det.

Markera kryssrutan om du vill aktivera inställningen och ange det högsta antalet dagar.

Antalet använda lösenord i historiken

Den här inställningen anger hur många unika nya lösenord som måste associeras med ett användarkonto innan ett gammalt lösenord kan återanvändas.

Markera kryssrutan om du vill aktivera inställningen och ange det minsta antalet lösenord.

Högsta antal ogiltiga inloggningsförsök

Den här inställningen avgör inaktivering av ett konto efter ett visst antal ogiltiga inloggningsförsök.

Markera kryssrutan om du vill aktivera inställningen och ange det högsta antalet försök.

Om kryssrutan **Högsta antal ogiltiga inloggningsförsök** är markerad kan du ange följande två inställningar:

Varaktighet för kontoutelåsning

Den här inställningen avgör hur många minuter ett inaktiverat konto förblir inaktiverat innan det aktiveras automatiskt.

Markera kryssrutan om du vill aktivera inställningen och ange antalet minuter.

Återställ kontoutelåsningsräknaren efter

Den här inställningen avgör hur många minuter som måste förflyta från den tidpunkt då en användare inte kan logga in innan räknaren för misslyckade inloggningsförsök återställs till noll.

Markera kryssrutan om du vill aktivera inställningen och ange antalet minuter.

**Obs!**

Om det maximala antalet ogiltiga inloggningsförsök överskrider inaktiveras kontot.

Om kryssrutan **Varaktighet för kontoutelåsning** inte är markerad måste kontot aktiveras manuellt.

Om kryssrutan **Varaktighet för kontoutelåsning** är markerad aktiveras kontot automatiskt efter den definierade tidsperioden.

**Obs!**

Räknaren av ogiltiga inloggningsförsök återställs till noll:

Efter en lyckad inloggning.

Eller efter den angivna tidsperioden om kryssrutan **Återställ kontoutelåsningsräknaren efter** är markerad.

Inaktivera offline-klient

Markera kryssrutan om du vill inaktivera inloggning till en offlineklient.

Ytterligare information

Från och med BVMS 9.0 gäller följande inställningar för **Kontopolicyer** som standard:

- Kryssrutan **Policy om starka lösenord** är markerad som standard.
- Kryssrutan **Kortast tillåtna lösenord** är markerad som standard. Standardvärdet är 10.
- Kryssrutan **Högsta ålder för lösenord i dagar** är inte markerad som standard. Standardvärdet är 90.
- Kryssrutan **Antalet använda lösenord i historiken** är inte markerad som standard. Standardvärdet är 10.

- Kryssrutan **Högsta antal ogiltiga inloggningsförsök** är inte markerad som standard. Standardvärdet är 1.
- Kryssrutan **Inaktivera offline-klient** är inte markerad som standard.

Från BVMS 10.0.1 väljs följande **Kontopolicyer**-inställningar som standard för alla användargrupper:

- **Högsta antal ogiltiga inloggningsförsök**
- **Varaktighet för kontoutelåsning**
- **Återställ kontoutelåsningsräknaren efter**

24.17.1

Operator Client offline

Genom offlinefunktionen hos Operator Client blir följande användarfall möjliga:

- Operator Client fortsätter fungera live, för uppspelning och export utan någon anslutning till Management Server-datorn.
- Om en arbetsstation har anslutits en gång till Management Server-datorn kan den logga in offline när som helst med vilken användare som helst.

Offlineläget för BVMS kräver version 3.0 eller senare.

Om en Operator Client-arbetsstation tappar anslutningen till Management Server-datorn går det att arbeta vidare. Vissa viktiga funktioner är ändå tillgängliga, t.ex. livevideo och uppspelning av video.

Från och med BVMS V5.5 kan en Operator Client-arbetsstation användas offline med en konfiguration av BVMS V5.0.5.



Obs!

När lösenordet ändras på Management Server under perioden då Operator Client är offline registreras inte lösenordsändringen automatiskt i Operator Client.

Användaren måste logga in med det nya lösenordet när Operator Client är online.

Användaren måste logga in med det gamla lösenordet när Operator Client är offline. Det här ändras inte förrän en ny konfiguration har aktiverats och överförs till Operator Client-arbetsstationen.



Obs!

När en kamera anropas för visning i en monitorgrupp med ett Bosch Intuikey-tangentbord anslutet till arbetsstationen, och arbetsstationen är offline, skickas inte en felton via tangentbordet.

24.17.1.1

Arbeta i offlineläget

När Operator Client kopplas bort från en hanteringsserver visas en motsvarande överlagringsikon i det logiska trädet på den fränkopplade Management Server. Du kan fortsätta arbeta med Operator Client även om fränkopplingen varar längre, men vissa funktioner är inte tillgängliga.

Om anslutningen till Management Server återupprättas visas en motsvarande överlagringsikon. Om en ny konfiguration på en Management Server har aktiverats visas en motsvarande ikon i det logiska trädet på ikonen för den Management Server som påverkas och en dialogruta visas under några sekunder. Godkänn eller avvisa den nya konfigurationen.

Om din Operator Client-instans är schemalagd för att logga ut vid en specifik tidpunkt, inträffar denna utloggning även om anslutningen till Management Server inte återupprättas vid den här tidpunkten.

När en användare av Operator Client loggar in med Serversökning i offline-läget visas serverlistan från den senaste framgångsrika inloggningen. Offlineläget betyder här att Operator Client-arbetsstationen inte har någon nätverksanslutning till servern som innehåller serverlistan.

Funktioner som inte är tillgängliga i fränkopplat läge

Följande funktioner är inte tillgängliga i Operator Client om det inte finns någon uppkoppling till Management Server:

- **Larmlista:**
Detta omfattar även hantering av larm. Larmlistan är tom men fylls automatiskt när anslutningen fungerar igen.
- **Allegiant:**
Det går inte att hantera stamlinjen. I tidigare versioner stängdes Allegiant-kameror automatiskt med ett meddelande när hanteringen av en stamlinje inte fungerade. Från och med BVMS V3.0 visar vi en mer användarvänlig bildruta där användaren informeras om att det inte går att visa den här kameran för tillfället.
- **MG:**
Det går inte att dra kameror till MG-kontrollen. Kontrollen är inaktiverad men aktiveras automatiskt när anslutningen fungerar igen.
- **PTZ-prioriteringar:**
Utan en anslutning till Management Server kan en Operator Client som är offline ansluta en PTZ-kamera förutsatt att PTZ-kameran inte är låst. Dome-prioriteringarna uppdateras automatiskt när anslutningen fungerar igen.
- **Matning:**
Ingångarna kan inte växlas.
- **Loggbok:**
Loggboken är inte tillgänglig och går inte att öppna. Ett öppet fönster för sökning i Loggboken stängs inte automatiskt. Befintliga sökresultat går att använda och exportera.
- **Operator Client SDK:**
Operator Client SDK-funktioner med IServerApi kan inte behandlas.
Det går inte att skapa ett RemoteClientApi.
Vissa metoder som bara är tillgängliga i klient-API:t fungerar inte, t.ex. ApplicationManager (pröva GetUserName()).
- **Ändring av lösenord:**
Operatören kan inte ändra sitt lösenord.
- **Relä:**
Reläer går inte att växla.
- **Serverskript:**
Servermetoderna i IServerApi behandlas, men de kan inte skickas till klienten. De är:
 - AlarmManager
 - AnalogMonitorManager
 - CameraManager
 - CompoundEventManager
 - DecoderManager
 - DeviceManager
 - DomeCameraManager
 - EventManager
 - InputManager
 - LicenseManager
 - Loggbok

- MatrixManager
- RecorderManager
- RelayManager
- ScheduleManager
- SendManager
- SequenceManager
- VirtualInputManager
- Tillståndsoverlagringar:
Inga kamerors, ingångars eller reläers tillståndsoverlagringar är tillgängliga.

Operator Clients tillstånd

En BVMS Operator Client ger feedback om sitt tillstånd i bild och ord.

Följande Operator Client-tillstånd är möjliga:

- : Operator Client är ansluten till Management Server.
- : Operator Client är inte ansluten till Management Server. En anledning kan vara att Management Server har kopplats bort fysiskt från nätverket.
- : Detta tillstånd visas bara efter en återupprättad anslutning till Management Server. Alla berörda funktioner fungerar igen, men konfigurationen av Operator Client är föråldrad eftersom det finns en nyare konfiguration i systemet. Uppdatera konfigurationen genom att logga in igen.
- : Denna tillståndssikonen visas när Management Server har en tidigare version eller vissa Management Server-server inte körs.
- : Denna ikon visas när Management Server har anslutningsproblem. Detaljerad information om servertillståndet finns i verktygstipset.
- : Denna ikon visas när flera inloggningar i Management Server med samma användarnamn nekas.
- : Denna ikon visas när tillståndet är okänt
- : Den här ikonen visas när licensen inte är tillgänglig
- : Den här ikonen visas när Management Server finns i en annan tidszon.

Enhetstillståndsoverlagring

Enhetstillstånden (inspelningspunkt, för mycket brus, för mörkt, ...) bearbetas av Management Server. När klienten och servern kopplas från varandra kan tillståndet inte uppdateras på klienten. En ny tillståndsoverlagring ger en visuell indikation på att inga enhetstillstånd är tillgängliga för tillfället. Om klienten har upprättat en anslutning till servern igen uppdateras tillståndsoverlagringarna automatiskt.

-  Tillstånd okänt
Tillståndsoverlagringen för en enhet i det logiska trädet eller på en karta när klienten är fränkopplad från Management Server-datorn.

Anledningar till fränkoppling

Anledningarna till fränkopplingen mellan Operator Client och Management Server kan vara:

- Den fysiska anslutningen är bruten.
- Den inloggade användarens lösenord har ändrats under den tid han eller hon var offline.
- Management Server har gett bort den flytande arbetsstationslicensen till en annan Operator Client som var online medan den nu frångopplade Operator Client var offline.
- Operator Client och Management Server har olika versioner (Management Server tidigare än version 5.5).

25

Konfigurerar användare, behörigheter och Enterprise Access

**Obs!**

BVMS Viewer har bara grundläggande funktioner. Avancerade funktioner ingår i BVMS Professional. Detaljerad information om de olika BVMS utgåvorna finns på www.boschsecurity.com och BVMS Snabbvalsguiden: [BVMS snabbvalsguide](#).

Huvudfönster > Användargrupper

Det här kapitlet innehåller information om hur du konfigurerar användargrupper, Enterprise User Groups och Enterprise Access.

Du konfigurerar alla enhetsbehörigheter och funktionsbehörigheter per användargrupp, inte per användare.

Följande regler gäller:

- En BVMS-användare kan endast vara medlem i en BVMS-användargrupp eller Enterprise User Group. En LDAP-användare kan vara medlem i flera LDAP-användargrupper.
- Du kan inte ändra inställningarna för en standardanvändargrupp.
- Den här användargruppen har tillgång till alla enheter i hela det logiska trädets och tilldelas schemat **Alltid**.
- För att komma åt Windows-användargruppen för en domän används LDAP-användargrupper.
- Klicka på  för att spara inställningarna.
- Klicka på  om du vill ångra den senaste inställningen.
- Klicka på  för att aktivera konfigurationen.

Policy om starka lösenord

För bättre skydd mot obehörig åtkomst rekommenderar vi att du använder starka lösenord för användarkonton.

Av den anledningen aktiveras en stark lösenordsprincip som standard för alla nya användargrupper. Detta gäller administratörsanvändargruppen samt standardanvändargrupper, Enterprise User Group-grupper och Enterprise-åtkomst.

Följande regler gäller:

- Minsta lösenordslängd enligt inställningen på sidan **Kontopolicyer** för önskad användargrupp.
- Använd inte någon av de tidigare lösenorden.
- Använd minst en versal (A–Z).
- Använd minst en siffra (0–9).
- Använd minst ett specialtecken (till exempel ! \$ # %).

När administratörsanvändaren startar Configuration Client för första gången visas dialogrutan **Ett brott mot lösenordspolicyn har skett** och användaren uppmanas att ställa in ett lösenord för administratörsanvändarkontot. Vi rekommenderar starkt att du använder den här inställningen och att du anger ett starkt lösenord för administratörsanvändarkontot baserat på principreglerna för lösenord.

När du skapar nya användargrupper i Configuration Client är principinställningen för starka lösenord aktiverad som standard. Om du inte anger lösenord för de nya användarkontona för relevant användargrupp kan du inte aktivera konfigurationen. Dialogrutan **Ett brott mot lösenordspolicyn har skett** visas med en lista över alla användare som saknar lösenord. Ange lösenorden som saknas för att aktivera konfigurationen.

Se

- Sidan Kontoprinciper, sidan 321
- Sidan Egenskaper för användargrupper, sidan 308
- Sidan Användaregenskaper, sidan 308
- Sidan Logga in paregenskaper, sidan 309
- Sidan Kamerabehörigheter, sidan 310
- Sidan Kontrollprioriteter, sidan 311
- Kopiera behörigheter för användargrupp-dialogrutan, sidan 312
- Sidan Avkodarbehörigheter, sidan 312
- Sidan Händelser och larm, sidan 312
- Dialogrutan LDAP-inställningar (menyn Inställningar), sidan 109
- Sidan Inloggningsuppgifter, sidan 313
- Sidan Logiskt träd, sidan 313
- Sidan Användarfunktioner, sidan 314
- Sidan Prioriteringar, sidan 317
- Sidan Användargränssnitt, sidan 317
- Sidan Serveråtkomst, sidan 319

25.1

Skapa en grupp eller ett konto

Huvudfönster > **Användargrupper**

Du kan skapa en standardanvändargrupp, en Enterprise User Group eller en Enterprise Account.

För att anpassa användargruppens behörigheter efter dina behov skapar du en ny användargrupp och ändrar dess inställningar.

25.1.1

Skapa en standardanvändargrupp

Huvudfönster > **Användargrupper**

Så här skapar du en standardanvändargrupp:

1. Klicka på fliken **Användargrupper**.
2. Klicka på .
Dialogrutan **Ny användargrupp** visas.
3. Ange namnet och en beskrivning.
4. Klicka på **OK**.
En ny grupp läggs till i motsvarande träd.
5. Högerklicka på den nya användargruppen och klicka på **Ändra namn**.
6. Ange önskat namn och tryck på Enter.

Se

- Sidan Egenskaper för användargrupper, sidan 308
- Sidan Användarfunktioner, sidan 314
- Sidan Prioriteringar, sidan 317
- Sidan Användargränssnitt, sidan 317

25.1.2

Skapa en Enterprise User Group

Huvudfönster > **Användargrupper**

Du skapar en Enterprise User Group för ett Enterprise System på Enterprise Management Server.

Du skapar en Enterprise User Group med användare för att konfigurera deras funktionsbehörigheter. Dessa funktionsbehörigheter finns på en Operator Client som är ansluten till Enterprise Management Server. Ett exempel på en funktionsbehörighet är användargränssnittet till larmmonitorn.

Så här skapar du en Enterprise User Group:

1. Klicka på fliken **Enterprise User Groups**.
Obs! Fliken **Enterprise User Groups** är bara tillgänglig om rätt licens är tillgänglig och om en eller flera Management Server-datorer har konfigurerats i **Enheter > Enterprise System > Serverlista/adressbok**.
2. Klicka på .
Dialogrutan **Ny Enterprise-användargrupp** visas.
3. Ange namnet och en beskrivning.
4. Klicka på **OK**.
Enterprise User Group läggs till i motsvarande träd.
5. Högerklicka på den nya Enterprise-gruppen och klicka på **Ändra namn**.
6. Ange önskat namn och tryck på Enter.
7. På sidan **Operatörsbehörigheter** konfigurerar du funktionsbehörigheter och serveråtkomst för de konfigurerade Management Server-datorerna efter behov.

Se

- *Sidan Egenskaper för användargrupper, sidan 308*
- *Sidan Användarfunktioner, sidan 314*
- *Sidan Prioriteringar, sidan 317*
- *Sidan Användargränssnitt, sidan 317*
- *Sidan Serveråtkomst, sidan 319*

25.1.3

Skapa ett Enterprise Account

Huvudfönster > **Användargrupper**



Obs!

Minst en enhet måste konfigureras i enhetsträdet innan du kan lägga till ett Enterprise Account.

Du skapar ett Enterprise Account på en Management Server. Upprepa åtgärden på varje Management Server som ingår i ditt Enterprise System.

Du skapar ett Enterprise Account för att konfigurera enhetsbehörigheterna för en Operator Client som använder ett Enterprise System.

Så här skapar du ett Enterprise Account:

1. Klicka på fliken **Enterprise-åtkomst**.
2. Klicka på .
Dialogrutan **Nytt Enterprise Account** visas.
3. Ange namnet och en beskrivning.

4. Den **Användaren måste ändra sitt lösenord vid nästa inloggning** kryssrutan är förvald för alla nya användarkonton.
Ange nyckeln i enlighet med principreglerna för nycklar och bekräfta nyckeln.
5. Klicka på **OK**.
Ett nytt Enterprise Account läggs till i motsvarande träd.
6. Högerklicka på det nya Enterprise Account-kontot och klicka på **Ändra namn**.
7. Ange önskat namn och tryck på Enter.
8. Konfigurera inloggningsuppgifterna och enhetsbehörigheterna efter behov på sidan **Enhetsbehörigheter**.

Se

- *Policy om starka lösenord*, sidan 327
- *Sidan Inloggningsuppgifter*, sidan 313
- *Sidan Logiskt träd*, sidan 313
- *Sidan Händelser och larm*, sidan 312
- *Sidan Kontrollprioriteter*, sidan 311
- *Sidan Kamerabehörigheter*, sidan 310
- *Sidan Avkodarbehörigheter*, sidan 312

25.2

Skapa en användare

Huvudfönster > **Användargrupper** > fliken **Användargrupper**
eller

Huvudfönster > **Användargrupper** > fliken **Enterprise User Groups**

Du skapar en användare som en ny medlem i en befintlig standardanvändargrupp eller Enterprise User Group.

**Obs!**

En användare som vill använda ett Bosch IntuiKey-tangentbord som är anslutet till en avkodare måste ha ett användarnamn och lösenord som endast består av siffror. Användarnamnet får ha max 3 siffror. Lösenordet får ha max 6 siffror.

Så här skapar du en användare:

1. Välj en grupp och klicka på  eller högerklicka på önskad grupp och klicka på **Ny användare**.
En ny användare läggs till i trädet **Användargrupper**.
2. Högerklicka på den nya användaren och klicka på **Ändra namn**.
3. Ange önskat namn och tryck på Enter.
4. Ange användarnamnet och en beskrivning på sidan **Användaregenskaper**.
5. Kryssrutan **Användaren måste ändra sitt lösenord vid nästa inloggning** är markerad som standard för alla nya användarkonton.
Ange lösenordet i enlighet med principreglerna för lösenord och bekräfta lösenordet.
6. Klicka på **Verkställ** för att tillämpa inställningarna.
7. Klicka på  för att aktivera lösenordet.

Se

- *Sidan Användaregenskaper*, sidan 308
- *Policy om starka lösenord*, sidan 327
- *Sidan Användargrupper*, sidan 306

25.3

Skapa en grupp med dubbla behörigheter

Huvudfönster > **Användargrupper** > fliken **Användargrupper**
eller

Huvudfönster > **Användargrupper** > fliken **Enterprise User Groups**

Du kan skapa en dubbel behörighet för en standardanvändargrupp eller för en Enterprise User Group.

Dubbel behörighet finns inte för Enterprise-åtkomst.

Du väljer två användargrupper. Medlemmarna i de användargrupperna är medlemmar i den nya gruppen med dubbel behörighet.

Så här skapar du en grupp med dubbel behörighet:

1. Klicka på .
Dialogrutan **Ny dubbel auktoriseringsgrupp** eller dialogrutan **Ny dubbel Enterprise-auktoriseringssgrupp** visas.
2. Ange ett namn och en beskrivning.
3. Klicka på **OK**.
En ny grupp med dubbel behörighet läggs till i motsvarande träd.
4. Högerklicka på den nya gruppen med dubbel behörighet och klicka på **Ändra namn**.
5. Ange önskat namn och tryck på Enter.

Se

- *Lägga till ett inloggningspar till en grupp med dubbel behörighet, sidan 331*
- *Sidan Egenskaper för användargrupper, sidan 308*
- *Sidan Användarfunktioner, sidan 314*
- *Sidan Prioriteringar, sidan 317*
- *Sidan Användargränssnitt, sidan 317*

25.4

Lägga till ett inloggningspar till en grupp med dubbel behörighet

Huvudfönster > **Användargrupper** > fliken **Användargrupper** >  **Ny dubbel auktoriseringsgrupp**

Huvudfönster > **Användargrupper** > fliken **Enterprise User Groups** >  **Ny dubbel Enterprise-auktoriseringssgrupp**

Så här lägger du till ett inloggningspar till en grupp med dubbel behörighet:

1. Välj önskad grupp med dubbel behörighet och klicka på  eller högerklicka på gruppen och klicka på **Nytt inloggningspar**.
En dialogruta visas.
2. Välj en användargrupp i varje lista.
Användarna i den första användargruppen är de användare som måste logga in i den första inloggningsdialogrutan, och användarna i den andra användargruppen bekräftar inlogningen.
Du kan välja samma grupp i båda listorna.

3. Välj **Tvingande dubbel behörighet** för varje grupp, om det behövs.
När den här kryssrutan är markerad kan en användare i den första gruppen endast logga in tillsammans med en användare i den andra gruppen.
När den här kryssrutan är avmarkerad kan en användare i den första gruppen logga in på egen hand, men endast med åtkomstbehörighet till den egna gruppen.
4. Klicka på **OK**.
Ett nytt inloggningspar läggs till i lämplig grupp med dubbel behörighet.
5. Högerklicka på det nya inloggningsparet och klicka på **Ändra namn**.
6. Ange önskat namn och tryck på Enter.

Se

- *Skapa en grupp med dubbla behörigheter, sidan 331*
- *Sidan Logga in paregenskaper, sidan 309*

25.5**Konfigurerar den administrativa gruppen**

Huvudfönster > **Användargrupper** > fliken **Användargrupper**  Administrativ grupp
Gör att du kan lägga till nya administratörsanvändare i den administrativa gruppen, ändra namn på administratörsanvändare och ta bort dem från den administrativa gruppen.

Så här lägger du till en ny administratörsanvändare i den administrativa gruppen:

1. Klicka på  eller högerklicka på den administrativa gruppen och klicka på **Lägg till ny användare**.
En ny administratörsanvändare läggs till i den administrativa gruppen.
2. Ange användarnamnet och en beskrivning på sidan **Användaregenskaper**.
3. Kryssrutan **Användaren måste ändra sitt lösenord vid nästa inloggning** är förvald för alla nya användarkonton.
Ange lösenordet i enlighet med principreglerna för lösenord och bekräfta lösenordet.
4. Klicka på **Verkställ** för att tillämpa inställningarna.

5. Klicka på  för att aktivera lösenordet.

Ändra namn på en administratörsanvändare:

1. Högerklicka på administratörsanvändaren och klicka på **Ändra namn**.
2. Ange önskat namn och tryck på ENTER.

3. Klicka på  om du vill aktivera ändringen av användarnamnet.

Ta bort en användare som administratör från Administrativ grupp:

- ▶ Högerklicka på administratörsanvändaren och klicka på **Ta bort**.
Administratörsanvändaren tas bort från Administrativ grupp.

Obs!

Du kan bara ta bort en administratörsanvändare från den administrativa gruppen om det finns andra administratörsanvändare.

Om det bara finns en administratörsanvändare kan du inte ta bort användaren.

Se

- *Sidan Användargrupper, sidan 306*
- *Sidan Användaregenskaper, sidan 308*

- *Policy om starka lösenord , sidan 327*

25.6 Välja en associerad LDAP-grupp

Huvudfönster > **Användargrupper** > fliken **Användargrupper** >  > fliken **Operatörsbehörigheter** > fliken **Egenskaper för användargrupper** eller

Huvudfönster > **Användargrupper** > fliken **Enterprise User Groups** >  > fliken **Operatörsbehörigheter** > fliken **Egenskaper för Enterprise-användargrupp**

Du kan konfigurera LDAP-grupper i standardanvändargrupper eller Enterprise User Groups.

Så här väljer du en associerad LDAP-grupp:

1. Klicka på knappen **Sök efter grupper**.
 2. I listan **Tillhörande LDAP-grupp** väljer du respektive LDAP-grupp.
- För detaljerad information om olika fält, följ länken till lämpligt programfönster.

Se

- *Dialogrutan LDAP-inställningar (menyn Inställningar), sidan 109*
- *Sidan Egenskaper för användargrupper, sidan 308*

25.7 Schemalägga en användares inloggningsbehörighet

Huvudfönster > **Användargrupper** > fliken **Användargrupper** >  > fliken **Operatörsbehörigheter** > fliken **Egenskaper för användargrupper** eller

Huvudfönster > **Användargrupper** > fliken **Enterprise User Groups** >  > fliken **Operatörsbehörigheter** > fliken **Egenskaper för Enterprise-användargrupp**

Du kan begränsa medlemmarna i en användargrupp eller Enterprise User Group så att de bara kan logga in på sina datorer under bestämda tidsperioder.

Du kan inte ändra dessa inställningar för en standardanvändargrupp.

Schemalägga inloggning:

1. Klicka på fliken **Egenskaper för användargrupper**.
2. Välj ett schema i listan **Inloggningsschema**.

25.8 Konfigurera funktionsbehörigheter

Huvudfönster > **Användargrupper** > fliken **Användargrupper** >  > fliken **Operatörsbehörigheter** > fliken **Egenskaper för användargrupper** eller

Huvudfönster > **Användargrupper** > fliken **Enterprise User Groups** >  > fliken **Operatörsbehörigheter** > fliken **Egenskaper för Enterprise-användargrupp**

- Du kan konfigurera funktionsbehörigheter som åtkomst till loggboken eller inställningar för användargränssnittet.
- Du kan inte ändra dessa inställningar för en standardanvändargrupp.
- Du konfigurerar funktionsbehörigheter i vanliga användargrupper eller Enterprise User Groups.

För detaljerad information om olika fält, se onlinehjälp för lämpligt programfönster.

För detaljerad information om olika fält, följ länken till lämpligt programfönster.

Se

- *Sidan Egenskaper för användargrupper, sidan 308*
- *Sidan Användarfunktioner, sidan 314*
- *Sidan Prioriteringar, sidan 317*
- *Sidan Användargränssnitt, sidan 317*
- *Sidan Serveråtkomst, sidan 319*

25.9

Konfigurerar enhetsbehörigheter

Huvudfönster > **Användargrupper** > fliken **Användargrupper** > fliken **Enhetsbehörigheter** eller

Huvudfönster > **Användargrupper** > fliken **Enterprise-åtkomst** > fliken **Enhetsbehörigheter**

Du kan ställa in behörigheterna separat för alla enheter i det logiska trädet.

När du har flyttat behöriga enheter till en mapp som inte är tillåten för denna användargrupp måste du ställa in behörigheterna för mappen för att bevilja åtkomst till dess enheter.

- Du kan inte ändra dessa inställningar för en standardanvändargrupp.
- Du konfigurerar enhetsbehörigheter i standardanvändargrupper eller Enterprise Accounts.

För detaljerad information om olika fält, se onlinehjälp för lämpligt programfönster.

För detaljerad information om olika fält, följ länken till lämpligt programfönster.

Se

- *Sidan Logiskt träd, sidan 313*
- *Sidan Händelser och larm, sidan 312*
- *Sidan Kontrollprioriteter, sidan 311*
- *Sidan Kamerabehörigheter, sidan 310*
- *Sidan Avkodarbehörigheter, sidan 312*

25.10

Konfigurerar flera prioriteringar

Huvudfönster > **Användargrupper** > fliken **Användargrupper** eller

Huvudfönster > **Användargrupper** > fliken **Enterprise User Groups** eller

Huvudfönster > **Användargrupper** > fliken **Enterprise-åtkomst**

Du kan konfigurera följande prioriteringar:

- För standardanvändargrupper och **Enterprise User Groups**: Du kan konfigurera larmprioriteringar för live-läge och uppspelningsläge.
- För standardanvändargrupper och **Enterprise-åtkomst**: Du kan konfigurera prioriteringar för att hämta PTZ-kontroller och Bosch Allegiant -trunkeringsrader.
Du kan konfigurera en tidsperiod för PTZ-låsning, dvs. en användare med högre prioritet kan ta över kamerakontrollen från en användare med en lägre prioritet och låsa den under den här tidsperioden.

Så här konfigurerar du live- och uppspelningsprioriteringar:

1. Välj en standardanvändargrupp eller en Enterprise User Group.
2. Klicka på **Operatörsbehörigheter**.
3. Klicka på fliken **Prioriteringar**.
4. Flytta skjutreglagen efter behov i fältet **Automatisk snabbvisning**.

Så här konfigurerar du prioriteringar för PTZ- och Bosch Allegiant-trunkeringsrader:

1. Välj en standardanvändargrupp eller en Enterprise Account.
2. Klicka på fliken **Enhetsbehörigheter**.

3. Klicka på fliken **Kontrollprioriteter**.
4. Flytta skjutreglagen efter behov i fältet **Kontrollprioriteter**.
5. I listan **Tidsgräns i minuter**, välj angivelsen som behövs.

Se

- *Sidan Kontrollprioriteter, sidan 311*
- *Sidan Prioriteringar, sidan 317*

25.11

Kopiera behörigheter för användargrupper

Huvudfönster > **Användargrupper** > fliken **Användargrupper**
eller

Huvudfönster > **Användargrupper** > fliken **Enterprise User Groups**
eller

Huvudfönster > **Användargrupper** > fliken **Enterprise-åtkomst**

Du kan kopiera behörigheter från en grupp eller ett konto till en annan. Du måste ha konfigurerat minst 2 grupper eller konton.

Så här konfigurerar du behörigheter:

1. I trädet för användargrupper väljer du en grupp eller ett konto.



2. Klicka på .

Dialogrutan **Kopiera användargruppbehörigheter** visas.

3. Välj lämpliga behörigheter och passande målgrupp eller konto.
4. Klicka på **OK**. Gruppbehörigheterna för den här gruppen kopieras till den andra gruppen eller kontot. Dialogrutan stängs.

26 Konfigurera videobaserat system för brandlarm

För konfigurering av ett videobaserat brandlarmssystem måste du göra följande:

1. Konfigurera branddetektering i branddetekteringskameran.
Du kan använda kamerans webbsida för den här configurationen.
För detaljerad information om hur du konfigurerar en branddetekteringskamera kan du se
– *Konfigurera en branddetekteringskamera, sidan 336*
2. Lägg till den här branddetekteringskameran i systemet. Du kan lägga till branddetekteringskameran till en VRM-pool, som en livekodare eller som en kodare för lokal lagring.
För detaljerad information om hur du lägger till en kamera kan du se
– *Lägga till en kodare till en VRM-pool, sidan 205*
– *Lägga till en kodare för endast live video, sidan 206*
– *Lägga till en kodare för lokal lagring, sidan 206*
3. Konfigurera en brandhändelse för den här kameran.
– *Konfigurera en brandhändelse, sidan 338*
4. Konfigurera larm för brandhändelsen.
– *Konfigurera ett brandlarm, sidan 339*

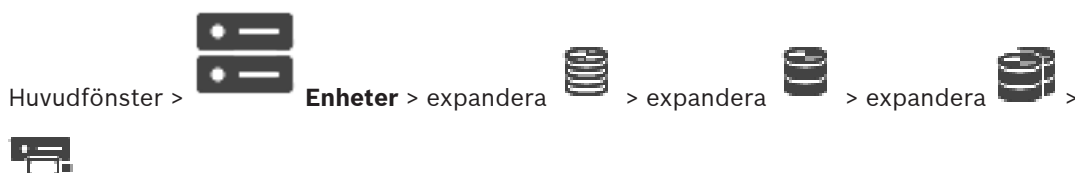
Se

- *Lägga till en kodare till en VRM-pool, sidan 337*
- *Lägga till en kodare för endast live video, sidan 206*
- *Lägga till en kodare för lokal lagring, sidan 206*
- *Konfigurera en brandhändelse, sidan 338*
- *Konfigurera ett brandlarm, sidan 339*

26.1 Konfigurera en branddetekteringskamera



eller



eller



eller



För att kunna konfigurera ett videobaserat brandlarm måste du konfigurera branddetektering på branddetekteringskameran.

Mer information finns i instruktionshandboken för branddetekteringskameran.

Så här konfigurerar du:

1. Högerklicka på enhetsikonen och klicka på **Visa webbsidan i webbläsaren**.
2. Klicka på **INSTÄLLNINGAR**.
3. I navigeringsrutan expanderar du **Larm** och klickar på .
4. Gör önskade inställningar.

26.2**Lägga till en kodare till en VRM-pool**

Läs mer om att lägga till kodare i en VRM-pool här: *Lägga till kodare genom avsökning, sidan 169*.

Se

- *Lägga till en enhet, sidan 118*

26.3**Lägga till kodare genom avsökning****Så här lägger du till kodare genom avsökning:**

1. Högerklicka på  och klicka på **Sök efter kodare**. Dialogrutan **BVMS Scan Wizard** visas.
2. Välj de kodare som krävs, välj önskad VRM-pool och klicka på **Tilldela** för att tilldela dem till poolen.
3. Klicka på **Nästa >>**. Dialogrutan **Autentisera enheter** i guiden visas.
4. Ange lösenordet för varje enhet som skyddas med ett lösenord. Lösenordskontrollen sker automatiskt om du inte skriver något i lösenordsfältet inom ett par sekunder, eller om du klickar utanför lösenordsfältet. Om samtliga enheter har samma lösenord kan du ange det i det första **Lösenord**-fältet. Högerklicka sedan på detta fält och välj **Kopiera cell till kolumn**.

I kolumnen **Status** indikeras lyckade inloggningsförsök med .

Misslyckade inloggningsförsök indikeras med .

5. Klicka på **Slutför**. Enheten läggs till i enhetsträdet.

-ikonen anger ett fel som du måste åtgärda. Mer information om det specifika felet finns i knappbeskrivningen.

26.4**Lägga till live-enheter från Bosch genom avsökning****Så här lägger du till live-enheter från Bosch genom avsökning:**

1. Högerklicka på  och klicka på **Sök efter endast live-kodare**. Dialogrutan **BVMS Scan Wizard** visas.
2. Markera önskade kryssrutor för de enheter som du vill lägga till.
3. Klicka på **Nästa >>**. Dialogrutan **Autentisera enheter** i guiden visas.
4. Ange lösenordet för varje enhet som skyddas med ett lösenord. Lösenordskontrollen sker automatiskt om du inte skriver något i lösenordsfältet inom ett par sekunder, eller om du klickar utanför lösenordsfältet. Om samtliga enheter har samma lösenord kan du ange det i det första **Lösenord**-fältet.

Högerklicka sedan på detta fält och välj **Kopiera cell till kolumn**.



I kolumnen **Status** indikeras lyckade inloggningsförsök med .



Misslyckade inloggningsförsök indikeras med .

5. Klicka på **Slutför**.

Enheten läggs till i enhetsträdet.

-ikonen anger ett fel som du måste åtgärda. Mer information om det specifika felet finns i knappbeskrivningen.

26.5

Lägga till kodare för lokal lagring genom avsökning

Huvudfönster > **Enheter** > utvidga >

Medger tillägg och konfigurering av kodare med lokal lagring.

Så här lägger du till kodare för lokal lagring genom avsökning:



1. Högerklicka på i enhetsträdet och klicka på **Sök efter kodare med lokal lagring**. Dialogrutan **BVMS Scan Wizard** visas.

2. Markera önskade kryssrutor för de enheter som du vill lägga till.

3. Klicka på **Nästa >>**.

Dialogrutan **Autentisera enheter** i guiden visas.

4. Ange lösenordet för varje enhet som skyddas med ett lösenord.

Lösenordskontrollen sker automatiskt om du inte skriver något i lösenordsfältet inom ett par sekunder, eller om du klickar utanför lösenordsfältet.

Om samtliga enheter har samma lösenord kan du ange det i det första **Lösenord**-fältet.

Högerklicka sedan på detta fält och välj **Kopiera cell till kolumn**.



I kolumnen **Status** indikeras lyckade inloggningsförsök med .



Misslyckade inloggningsförsök indikeras med .

5. Klicka på **Slutför**.

Enheten läggs till i enhetsträdet.

26.6

Konfigurera en brandhändelse



Huvudfönster > **Händelser**

Så här konfigurerar du:

1. I trädet väljer du **Kodare/avkodare > Kamera > Brand- eller röktillstånd > Brand eller rök har identifierats**.

Motsvarande händelsekonfigurationstabell visas.

2. Klicka i en cell i kolumnen **Utlöser larm – Schema** och välj ett schema.

Schemat bestämmer när larmet ska utlösas.

Välj ett inspelningsschema eller uppgiftsschema som du har konfigurerat på sidan **Scheman**.

3. Gör nödvändiga inställningar.

Obs! Du kan använda samma procedur för de andra tillgängliga brandhändelserna.

26.7 Konfigurera ett brandlarm

Huvudfönster > **Larm**

Så här konfigurerar du:

1. I trädet väljer du **Kodare/avkodare > Kamera > Brand- eller röktilstånd > Brand eller rök har identifierats**.
Motsvarande larmkonfigurationstabell visas.
2. Gör nödvändiga inställningar.

27

Konfigurera en MIC IP 7000 som är ansluten till en VIDEOJET 7000 connect

För att styra en MIC IP 7000-kamera som är ansluten till en VIDEOJET 7000 connect måste du göra följande konfiguration för att det ska fungera.

Innan du lägger till MIC IP-kameran i BVMS utför du följande uppgifter:

1. Återställ både MIC IP 7000-kameran och VIDEOJET 7000 connect-enheten till fabriksinställningarna på webbsidan för varje enhet.
2. Ställ in MIC IP 7000-kameran på **MIC IP Starlight 7000 HD-VJC-7000**-varianten.
3. Konfigurera MIC IP 7000-kameran och VIDEOJET 7000 connect-enheten enligt dokumentationen som levererades med enheterna.
4. Om du vill använda ANR kör du verktyget ANR Setup Utility för VIDEOJET 7000 connect-enheten.

Utför den här uppgiften på en dator som ingår i samma nätverk som VIDEOJET 7000 connect-enheten.

Du hittar verktyget ANR Setup Utility på produktkatalogsidan för VIDEOJET 7000 connect-enheten.

Utför den här proceduren om du vill lägga till och konfigurera MIC IP 7000-kameran i BVMS:

1. I enhetsträdet lägger du endast till MIC IP 7000-kameran.
Du kan inte lägga till VIDEOJET 7000 connect-enheten i BVMS.
2. Högerklicka på den kamera som nyss lagts till och klicka på **Redigera kodare**.
Dialogrutan **Redigera kodare** visas.
Enhetsfunktionerna hämtas automatiskt enligt varianten som konfigurerats ovan.
3. Om det behövs kan du konfigurera ANR på sidan **Kameror och inspelning**.

28

Felsökning

Detta kapitel innehåller information om hur du hanterar kända problem genom att använda BVMS Configuration Client.

Problem under installationen

Problem	Orsak	Lösning
Installationen visar fel tecken.	Windows-språkinställningarna är fel.	<i>Konfigurera önskat språk i Windows, sidan 343</i>
Installationen stoppas med ett meddelande som anger att OPC Server inte kan installeras.	OPC Server-filer kan inte skrivas över.	Avinstallera OPC Core Components Redistributable och starta om installationsprogrammet för BVMS.
Programvaran kan inte avinstalleras via installationsprogrammet.		Starta Control Panel > Add/Remove Programs och avinstallera BVMS.

Problem omedelbart efter att programmet startas

Problem	Orsak	Lösning
BVMS visar fel språk.	Windows är inte inställt på önskat språk.	<i>Konfigurera språket för Configuration Client, sidan 69</i> eller <i>Konfigurera språket för Operator Client, sidan 69</i>
Dialogrutan för inloggning för Operator Client visar fel språk.	Trots att du har ändrat språk för Operator Client i Configuration Client är språket i dialogrutan för inloggning för Operator Client beroende av Windows-språket.	<i>Konfigurera önskat språk i Windows, sidan 343</i>

Problem med visningsspråk

Problem	Orsak	Lösning
Vissa displaytexter i Configuration Client eller Operator Client är på ett annat språk, oftast engelska.	Operativsystemets språk på datorn där Management Server är installerat är ofta engelska. När BVMS-databasen skapas på datorn skapas därför många displaytexter på engelska. De ändras inte oavsett Windows-språket på en Operator Client-dator. För att undvika sådana språkskillnader kan du installera Management	Ändra inte detta.

Problem	Orsak	Lösning
	Server-programvaran på en dator med rätt gränssnittsspråk i Windows.	

Problem med Bosch IntuiKey-tangentbord

Problem	Orsak	Lösning
Bosch IntuiKey-tangentbordet utlöser ett larm och displayen med skärmknappar visar Off Line.	Anslutningen till arbetsstationen slutar fungera. Antingen är kabeln skadad eller ej i kontakten eller så har arbetsstationen återställts.	Återupprätta anslutningen till ett Bosch IntuiKey-tangentbord, sidan 343

Problem med inställningarna på ljudkortets kontrollpanel för inspelning

Problem	Orsak	Lösning
Rundgång förekommer vid användning av Intercom-funktioner.	På ljudkortets kontrollpanel för inspelning måste mikrofonen vara markerad, inte stereo mix (eller något annat). Operator Client kontrollerar konfigurationsfilen under starten och ändrar inställningar i inspelningsstyrningen därefter. Den här konfigurationsfilen innehåller en standardpost som kanske inte överensstämmer med systemkonfigurationen. Inställningen återställs varje gång Operator Client startas.	Ändra inställningen i konfigurationsfilen för Operator Client till mikrofon.

Krascha Configuration Client

Problem	Orsak	Lösning
Configuration Client kraschar.	Om för många kameror som inte anslutits till Bosch Video Management System konfigurerats i en Allegiant-fil så kan du minska antalet. På så sätt undviks onödig systembelastning.	Se <i>Minska antalet Allegiant-kameror</i> , sidan 343.



-support

Få tillgång till våra **supporttjänster** på www.boschsecurity.com/xc/en/support/.

Bosch Security and Safety Systems tillhandahåller support inom följande områden:

- [Appar och verktyg](#)

- [Byggnadsinformationsmodellering](#)
- [Garanti](#)
- [Felsökning](#)
- [Reparation och byte](#)
- [Produktsäkerhet](#)



Bosch Building Technologies-akademien

Besök Bosch Building Technologies-akademiens webbplats och få åtkomst till **kurser**, **videogenomgångar** och **dokument**: www.boschsecurity.com/xc/en/support/training/

28.1 Konfigurera önskat språk i Windows

Om du vill ändra displayspråket för inställningarna för BVMS måste du byta språk i Windows. För att aktivera språkeställningarna startas datorn om efter att följande steg har utförts.

Konfigurera önskat språk:

1. Klicka på **Start**, klicka på **Kontrollpanelen** och dubbelklicka sedan på **Nationella inställningar och språkeställningar**.
2. Klicka på fliken **Avancerat** under **Språk för program som inte stöder Unicode**, välj önskat språk.
3. Klicka på **OK**.
4. I alla de kommande meddelanderutorna klickar du på **Ja**.
Datorn startas om.

28.2 Återupprätta anslutningen till ett Bosch IntuiKey-tangentbord

1. Stick in kabeln igen eller vänta tills arbetsstationen är online.
Meddelandet Off Line försvinner.
2. Tryck på snabbtangenter Terminal för att ange BVMS.

28.3 Minska antalet Allegiant-kameror

Du behöver Allegiant Master Control Software för att redigera Allegiant-filen.

Så här minskar du antalet Allegiant-kameror:

1. Starta Master Control Software.
2. Öppna Allegiant-filen.
3. Klicka på fliken Camera.
4. Markera de kameror som inte behövs.
5. På Edit-menyn klickar du på Delete.
6. Spara filen. Filstorleken förblir oförändrad.
7. Upprepa det sista steget för de skärmar du inte behöver. Klicka på fliken Monitors.
8. Importera den här filen i Bosch Video Management System (se *Lägga till en enhet, sidan 118*).

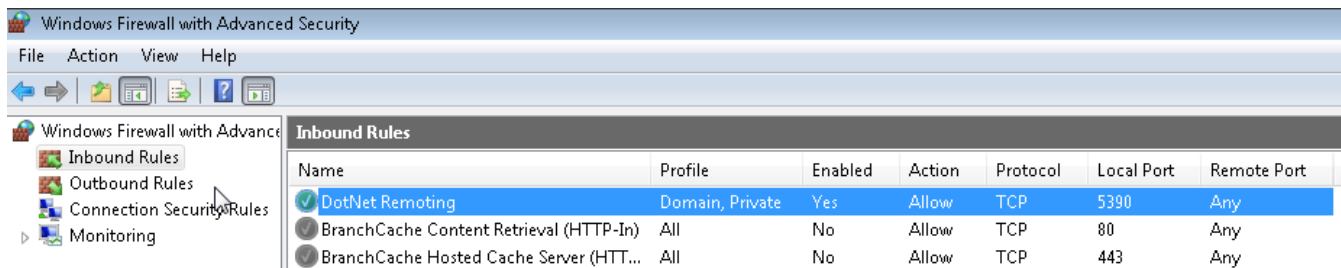
28.4 Använda portar

I det här avsnittet hittar du listor över de portar som måste vara öppna inom ett LAN-nätverk för alla BVMS-komponenter. Dessa portar får inte vara öppna mot Internet. För drift via Internet måste säkra anslutningar som VPN användas.

I varje tabell anges de lokala portarna som måste vara öppna på den dator som servern är installerad på eller på den router/nivå 3-switch som är ansluten till maskinvaran.

I en Windows-brandvägg konfigurerar du en regel för inkommande trafik för varje öppen port. Tillåt alla utgående anslutningar för alla BVMS-programtillämpningar.

Exempel på en enkel regel för inkommande trafik i brandväggen i Windows 7



Management Server-/Enterprise Management Server-portar

Server (lyssnare)	Protokoll	Inkommande portar	Klient (frågande)	Anmärkning
Management Server	UDP	123	Kodare	TimeServer NTP
Management Server	TCP	5322	Operator Client,	SSH-anslutning
Management Server	TCP	5389	ONVIF-enhet	ONVIF-proxy, händelseavisering
Management Server	TCP	5390	Operator Client, Configuration Client,	.NET-fjärranrop
Management Server	TCP	5392	Operator Client, Configuration Client, Mobile Video Service, BVMS SDK Program	WCF, gateway.push.apple.com
Management Server	TCP	5393	Operator Client, VRM, MVS	Data-Access-Service
Management Server	TCP	5395	Configuration Client, Operator Client	Användarinställningar, filöverföring
Management Server	UDP	12544	SNMP-klient	BVMS SNMP hämta port
Management Server	TCP	5399	REST API-klient	API-konfiguration
Management Server	TCP	5443	PID	PID-anslutning

Video Recording Manager-portar

Server (lyssnare)	Protokoll	Inkommande portar	Klient (frågande)	Anmärkning
VRM	TCP	554	RTSP-klient	Hämta primär RTSP-ström
VRM	TCP	1756	Management Server, Configuration Client	via RCP+
VRM	UDP	1757	Management Server, Operator Client	Avsök målsändning

Server (lyssnare)	Protokoll	Inkommande portar	Klient (frågande)	Anmärkning
VRM	UDP	1758	Management Server, Configuration Client	Svarstid för avsökning
VRM	UDP	1800. 1900	Management Server, Operator Client	Avsök målflersändning
VRM	TCP	80	Operator Client	Primär VRM-uppspelning via http
VRM	TCP	443	Operator Client	Primär VRM-uppspelning via https
VRM	TCP	555	RTSP-klient	Hämta sekundär RTSP-ström
VRM	TCP	81	Operator Client	Sekundär VRM-uppspelning via http
VRM	TCP	444	Operator Client	Sekundär VRM-uppspelning via https

Mobile Video Service-portar

Server (lyssnare)	Protokoll	Inkommande portar	Klient (frågande)	Anmärkning
Mobile Video Service	TCP	80	Management Server, Operator Client, Configuration Client, HTML-klient, mobilappar	Åtkomst via http
Mobile Video Service	TCP	443	Management Server, Operator Client, Configuration Client, HTML-klient, mobilappar	Åtkomst via https
Mobile Video Service	TCP	2195	Apple Push-avisering	Mac iOS
Mobile Video Service	UDP	1064-65535	Kodare, VRM	Liveströmning
Mobile Video Service-kodkonverterare	TCP	5382	Mobile Video Service-mobiloperatör	Medieström
Mobile Video Service-kodkonverterare	TCP	5385	Mobile Video Service-mobiloperatör	Medieström
Mobile Video Service BVMS-operatör	TCP	5383	Operator Client	Medieström
Mobile Video Service-mobiloperatör	TCP	5384	HTML-klient, mobilappar	Medieström

Server (lyssnare)	Protokoll	Inkommande portar	Klient (frågande)	Anmärkning
Mobile Video Service-kodkonverterare	TCP	5385	Mobile Video Service-mobiloperatör	Medieström

iSCSI-lagringssystemportar

Konfigurera vidarekoppling av portar vid den anslutna routern för enheten.

Server (lyssnare)	Protokoll	Inkommande portar	Klient (förfrågare)	Anmärkning
iSCSI-lagringssystem	TCP	3260	Kodare, VRM, Configuration Client	

Bosch Video Streaming Gateway-portar

Server (lyssnare)	Protokoll	Inkommande portar	Klient (frågande)	Anmärkning
Bosch Video Streaming Gateway	TCP	8756-8762	VRM, Management Server, Configuration Client	RCP +
Bosch Video Streaming Gateway	TCP	8080-8086	VRM, Management Server, Configuration Client, Operator Client	HTTP
Bosch Video Streaming Gateway	TCP	8443-8449	VRM, Management Server, Configuration Client, Operator Client	HTTPS
Bosch Video Streaming Gateway	TCP	1757	VRM Configuration Client	Avsök målsändning
Bosch Video Streaming Gateway	TCP	1758	VRM Configuration Client	Svarstid för avsökning
Bosch Video Streaming Gateway	TCP	1800, 1900	VRM Configuration Client	Avsök målförsändning
Bosch Video Streaming Gateway	UDP	1064-65535	Kodare, VRM	

ONVIF-kameraportar

Konfigurera vidarekoppling av portar vid den anslutna routern för enheten.

Server (lyssnare)	Protokoll	Inkommande portar	Klient (förfrågare)	Anmärkning
ONVIF-kamera	TCP	80	Management Server, VSG, Configuration Client, Operator Client	Åtkomst via http
ONVIF-kamera	TCP	443	Management Server, VSG, Configuration Client, Operator Client	Åtkomst via https
ONVIF-kamera	RTSP	554	Management Server, VSG, Configuration Client, Operator Client	

BVMS Operator Client-/Cameo SDK-portar

Server (lyssnare)	Protokoll	Inkommande portar	Klient (förfrågare)	Anmärkning
Operator Client	TCP	5394	BVMS SDK-tillämpning, BIS	WCF
Operator Client	UDP	1024-65535	Kodare, VRM	Liveströmning
Operator Client	TCP	443	Kodare	Fjärråtkomst, krypterad direktvisning

BVMS Configuration Client

Server (lyssnare)	Protokoll	Inkommande portar	Klient (frågande)	Anmärkning
Configuration Client	UDP	1024-65535	Kodare	Videoströmning

Kodarportar

Konfigurera vidarekoppling av portar vid den anslutna routern för enheten.

Server (lyssnare)	Protokoll	Inkommande portar	Klient (frågande)	Anmärkning
Kodare	TCP	1756	Avkodare, Management Server, VRM, Operator Client, Configuration Client, BVMS SDK-tillämpning	Via RCP+, om säker anslutning inte är aktiverad
Kodare	UDP	1757	Avkodare, Management Server, Operator Client	Sök efter mål
Kodare	UDP	1758	Avkodare, Management Server, Operator Client	Svarstid för avsökning
Kodare	UDP	1800, 1900	Avkodare, Management Server, Operator Client	Avsök målflersändning
Kodare	TCP	80	Operator Client, BVMS SDK-tillämpning, VSG	Åtkomst via http
Kodare	TCP	443	Operator Client, BVMS SDK Tillämpning, VSG, VRM	Åtkomst via https, om säker anslutning är aktiverad

Server (lyssnare)	Protokoll	Inkommande portar	Klient (frågande)	Anmärkning
Kodare	UDP	123	Management Server, VRM	SNTP
Kodare	UDP	161	Management Server, VRM	SNMP
Kodare	TCP	554	Operator Client, BVMS SDK-tillämpning, VSG	RTSP-strömning
Kodare	TCP	3260	Kodare (utgående)	iSCSI-inspelning

Valfria kodarportar

Server (lyssnare)	Protokoll	Inkommande portar	Klient (förfrågare)	Anmärkning
FTP	TCP	21		
SSDP	UDP	1900		
UPNP	UDP	3702		
SRTSP	UDP	9554		
RTSP skicka	UDP	15344, 15345		

BVMS-avkodarportar

Konfigurera vidarekoppling av portar vid den anslutna routern för enheten.

Server (lyssnare)	Protokoll	Inkommande portar	Klient (frågande)	Anmärkning
Avkodare	TCP	1756	Management Server, Operator Client, Configuration Client, BVMS SDK-tillämpning	via RCP+
Avkodare	UDP	1757	Management Server, Operator Client	Sök efter mål
Avkodare	UDP	1758	Management Server, Operator Client	Svarstid för avsökning
Avkodare	UDP	1800, 1900	Management Server, Operator Client	Sök efter mål i multicast-aktiverat nätverk
Avkodare	TCP	80	Operator Client	Åtkomst via http
Avkodare	TCP	443	Operator Client	Åtkomst via https
Avkodare	UDP	1024-65535	Kodare	Strömningsportar
Avkodare	UDP	123	Management Server, VRM	SNTP
Avkodare	UDP	161	Management Server, VRM	SNMP

DVR-portar

Konfigurera vidarekoppling av portar vid den anslutna routern för enheten.

Server (lyssnare)	Protokoll	Inkommande portar	Klient (förfrågare)	Anmärkning
DVR-styrning	TCP	80	Management Server, Configuration Client, Operator Client	Åtkomst via http

PID, Person Identification-portar

Server (lyssnare)	Protokoll	Inkommande portar	Klient (förfrågare)	Anmärkning
PID	TCP	8443	Management Server	Åtkomst via https

LPR, portar på adaptern till BVMS-enheten

Server (lyssnare)	Protokoll	Inkommande portar	Klient (frågånde)	Anmärkning
Adapter till BVMS-enhet	TCP	31000	Tattile-kamera	VRC

AMS, Access Management System-portar

Server (lyssnare)	Protokoll	Inkommande portar	Klient (förfrågare)	Anmärkning
AMS	TCP	62904	Management Server	Åtkomst via https

28.5 Aktivera loggning för ONVIF-händelser



Obs!

Observera att den här funktionen snart upphör.

Använd ONVIF Camera Event Driver Tool för enkel ONVIF-händelsemappning.

Se *Starta ONVIF Camera Event Driver Tool från Configuration Client*, sidan 197.

Du kan aktivera loggning av ONVIF-händelser om du t.ex. får problem med att ta emot BVMS-händelser. Loggning hjälper dig att hitta orsaken.

Så här aktiverar du loggning:

- Öppna filen `%programfiles%\Bosch\VMS\AppData\Server\CentralServer\BVMSLogCfg.xml` i ett lämpligt redigeringsprogram, till exempel Notepad. Kör programmet Notepad som administratör.
- Leta dig fram till raden med följande sträng:
`Add logging for onvif events of a device by network address`
De kommenterade raderna innehåller en kort förklaring.
- Ange `OnvifEvents.<Networkaddress>` som loggningsnamn.
Skriv bara `OnvifEvents` om du vill logga händelserna för samtliga ONVIF-enheter.
- Ange `DEBUG` som nivåvärde för alla inkommande och utgående händelser.
Ange `INFO` för alla utgående händelser.
Ange `WARN` eller `ERROR` om du vill inaktivera funktionen.

Obs! Aktiveringen kan kräva en omstart av den centrala servern.

Följande rader visar ett exempel på hur man loggar händelser från enheten 172.11.122.22 med alla utgående och inkommande händelser:

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

Se

- *Starta ONVIF Camera Event Driver Tool från Configuration Client, sidan 197*
- *Konfigurera en ONVIF-mappningstabell, sidan 225*
- *ONVIF-händelsemappning, sidan 39*

Ordlista

Aktiveringspunkt

Muskänslig ikon på en karta. Aktiveringspunkter konfigureras i Configuration Client. Aktiveringspunkter kan till exempel vara kameror, reläer och ingångar. Operatören kan använda aktiveringspunkter för att söka efter och välja en enhet i en byggnad. Aktiveringspunkter kan visas med blinkande bakgrundsfärg när en specifik händelse inträffar eller när ett larm utlöses.

Allegiant

Bosch-serien med analoga matrisväxlarsystem.

Anläggningskartfiler

BVMS stöder följande plats kartfiler: PNG, JPG, PDF och DWF.

ANR

Automated Network Replenishment. Integrerad process som kopierar data som saknas från en videomottagare till nätverksvideoinspelare efter ett nätverksfel. Kopierade videodata fyller ut det tomrum som bildas efter nätverksfelet. Därför behöver mottagaren någon typ av lokal lagring. Inspelningsskapaciteten på den här lokala lagringenheten beräknas med följande formel: $(\text{nätverksbandbredd} \times \text{beräknad stilleståndstid} + \text{säkerhetsmarginal}) \times (1 + 1/\text{säkerhetskopieringshastighet})$. Denna inspelningsskapacitet krävs eftersom den kontinuerliga inspelningen måste fortsätta under kopieringsprocessen.

Användargrupp

Användargrupper används till att definiera gemensamma användarattribut såsom behörigheter, privilegier och PTZ-prioritet. Genom att bli medlem av en grupp ärver användaren automatiskt alla attribut för den gruppen.

Arbetsstation

I BVMS-miljön: En dedikerad dator där Operator Client är installerad. Den här datorn är konfigurerad som en arbetsstation i Configuration Client så att specifika funktioner kan användas.

ATM

Automatic Teller Machine (Bankomat)

avkodare

Ändrar en digital ström till en analog ström.

Beröringsfri utplacering

Metod för automatisk nedladdning, installation och körning av .NET-program utan ändring av register eller delade systemkomponenter. Med Bosch Video Management System, används beröringsfri utplacering för uppdatering av operatörsklienter från hanteringsservern. Uppdateringen sker om en ny version lagras på hanteringsservern och när varje användare loggar in på operatörsklienten. Om du arbetar med en operatörsklient mot flera hanteringsserverdatorer använder den beröringsfria distributionen endast den programvaruversion som är lagrad på den hanteringsserver som operatörsklienten senast loggade in på. När du försöker logga in på en annan hanteringsserver med en annan programvaruversion visas hanteringsserver som offline eftersom programvaruversionerna inte överensstämmer.

B-frame

Bidirectional frame. Del av en metod för videokomprimering.

Bildfönster

Utrymme för bildrutor, struktureras med hjälp av ett mönster för bildfönster.

Bildruta

Används för att visa live eller inspelad video av en enda kamera, en webbplatskarta, ett dokument, en sekvens, en övervakningsgrupp, ett externt program eller en kartvyport.

Bildrutelist

Verktygsfält för en bildruta.

BIS

Building Integration System

Bosch ATM/POS-brygga

Mottar strängar via seriell kabel / COM-gränssnitt och vidarebefordrar dessa strängar via ethernet-kabel (TCP/IP). Strängarna är vanligtvis POS-data eller transaktioner vid bankomater.

CCL-emulering

Emulering av kommandokonsolspråket (Command Console Language) som används för att styra en Allegiant-matris. Du kan använda dessa kommandon för att växla en BVMS IP-kamera/-

kodare till en BVMS IP-avkodare. Du kan inte styra analoga kameror eller själva Allegiant-matrisen direkt.

Direktuppspelning

Spelar upp den inspelade bilden för vald kamera i en bildruta eller på liveskärmen. Starttiden (antalet sekunder i förfluten tid eller återspolningstid) kan konfigureras.

Distorsionskorrigering

Användning av programvara för att omvandla en cirkelformad bild från ett fisheye-objektiv med radiell distorsion till en rätlinjig bild för normal visning (distorsionskorrigering).

DNS

Domain Name System. En DNS-server omvandlar en URL (www.myDevice.com, till exempel) till en IP-adress i nätverk som använder TCP/IP-protokoll.

Dokument

De dokumentfiler som stöds av BVMS är HTM, URL, MHT, HTML, TXT.

DTP

En DTP-enhet (Data Transform Processor) transformerar seriella data från uttagsautomater till ett definierat dataformat och skickar dessa data via Ethernet till BVMS. Du måste se till att ett transformeringsfilter är inställt på DTP-enheten. Denna inställning utförs med en separat programvara från DTP-enhetens tillverkare.

dubbel behörighet

Säkerhetsriktlinjer som kräver att två olika användare loggar in på operatörsklienten. Båda användarna måste vara medlemmar av en vanlig Bosch Video Management System-användargrupp. Den här användargruppen (eller de här användargrupperna om användarna är medlemmar av olika användargrupper) måste tillhöra en dubbel behörighetsgrupp. En dubbel behörighetsgrupp har sina egna åtkomstbehörigheter inom Bosch Video Management System. Den här dubbla behörighetsgruppen bör ha fler behörigheter än den normala användargrupp som användaren tillhör. Exempel: Användaren A är medlem av en användargrupp som kallas Grupp A. Användaren B är medlem av Grupp B. Dessutom konfigureras en dubbel behörighetsgrupp med Grupp A och Grupp

B som medlemmar. För användare av Grupp A är dubbel behörighet valfritt, för användare av Grupp B är det obligatoriskt. När användare A loggar på visas en andra dialogruta för att bekräfta inloggningen. I den här dialogrutan kan en andra användare logga in om han finns tillgänglig. Om inte, kan användare A fortsätta och starta operatörsklienten. Han har sedan endast åtkomsträttigheter för Grupp A. När användare B loggar in visas återigen en andra dialogruta för inloggning. I denna dialogruta måste en andra användare logga in. Om inte kan användare B inte starta operatörsklienten.

Dubbla strömmar

Dubbla strömmar gör att en inkommande dataström samtidigt kan koda till två olika, individuellt konfigurerade inställningar. Detta skapar två dataströmmar: en för live-inspelning och inspelning före händelse, den andra för normal inspelning, rörelseinspelning och larminspelning.

duplex

Villkor som används för att definiera riktningen för dataöverföring mellan två parter. Halv-duplex tillåter dataöverföring i båda riktningarna, men inte samtidigt. Full-duplex tillåter samtidig dataöverföring.

DWF

Design Web Format. Används för att visa tekniska ritningar på en datormonitor.

DVR-styrning

Digital videoinspelare

DynDNS

Dynamic Domain Name System. En DS-värdtjänst som lagrar IP-adresser i en databas. Med Dynamic DNS kan du ansluta till enheten via Internet med hjälp av värdnamnet på enheten. Se DNS.

Enhetsfamilj

Kodare/IP-kameror från Bosch kan höra till en av följande enhetsfamiljer: Enhetsfamilj 1, enhetsfamilj 2 eller enhetsfamilj 3. Enheter i enhetsfamilj 1 kan bara spela in ström 1. Enheter i enhetsfamilj 2 kan spela in ström 1 eller ström 2. Enheter i enhetsfamilj 3 kan bara spela in antingen ström 1, ström 2 eller I-bildruta.

Enhetsträd

Hierarkisk lista för alla tillgängliga enheter i systemet.

Enterprise Account

Enterprise Account är en auktorisering som gör det möjligt för en Operator Client-användare att ansluta till enheterna på en Management Server som ingår i ett Enterprise System. I ett Enterprise Account är alla behörigheter konfigurerade för enheterna på denna Management Server. Operator Client kan anslutas samtidigt till alla Management Server-datorer som ingår i Enterprise System. Den här åtkomsten styrs av medlemskapet i en Enterprise User Group, och av enhetsbehörigheterna som konfigurerats i Enterprise Account för den här instansen av Management Server.

Enterprise Management Server

Enterprise Management Server är en BVMS Management Server-värd för konfigurationen av Enterprise User Group-grupper. Du behöver en eller flera Enterprise User Group-grupper som hänvisar till en eller flera serverdatorer. Rollerna för Enterprise Management Server och Management Server kan kombineras i en konfiguration.

Enterprise System

Enterprise System är en funktion i Bosch Video Management System som ger en Operator Client-användare åtkomst till flera Management Server-datorer samtidigt.

Enterprise User Group

Enterprise User Group är en användargrupp som har konfigurerats på en Enterprise Management Server. Enterprise User Group definierar de användare som är behöriga för åtkomst till flera Management Server-datorer samtidigt. Definierar de funktionsbehörigheter som är tillgängliga för dessa användare.

Enterprise-åtkomst

Enterprise-åtkomst är en funktion i BVMS som består av ett eller flera Enterprise Account-konton. Varje Enterprise Account innehåller enhetsbehörigheter för enheter på en viss Management Server.

flera sökvägar

Användning av datorlagringsteknik med flera sökvägar.

flera sökvägar

Datorlagringsteknik som använder flera definierade fysiska sökvägar som ansluter dataservern till ett lagringsmål (med hjälp av olika styrenheter, bussar, växlar eller liknande) som en reserv- eller belastningsutjämningslösning (redundans, effektivitet).

Fördröjning

Förinställd tid som en kamera visas i ett bildfönster tills nästa kamera visas under en kamerasekvens.

GSM

Globalt system för mobil kommunikation. Standard för digitala mobiltelefoner.

H.264

Standard för kodning (komprimering) av digitala ljud- och videoinspelningar för multimediasprogram. Standarden inkluderar olika profiler som kan se olika ut beroende på tillverkare. Följande profiler finns tillgängliga: Baseline, Baseline+, Huvudprofil. Baseline (används inte i Bosch Video Management System) stöder 2 CIF. Baseline+ stöder 4 CIF och har en bättre bildkvalitet än Baseline. Huvudprofilen stöder 4 CIF och har en högeffektiv kompressionsalgoritm kallad CABAC (Context-adaptive binary arithmetic coding). Denna är främst avsedd för högkvalitativ kodning för lagring.

H.265

H.265 är en videokomprimeringsstandard som definieras av ISO2 och ITU3 och ratificerades den 29 oktober, 2014. Standarden betraktas som en efterföljare till MPEG-4 AVC (Advanced Video Codec), som även kallas H.264, för att kunna komprimera upplösningar från 4K och ultra-HD upp till 36 megapixel.

Händelse

En omständighet eller status som är kopplad till ett larm och/eller en åtgärd. Händelser kan uppstå från många olika källor som t.ex. kameror, arkiv, kataloger, digitala ingångar etc. De kan inkludera

start-inspelningslägen, förlust av signallägen, meddelanden att disk är full, användarinloggning, utlösare för digitala ingångar etc.

I-frame

Intra frame. Del av en metod för videokomprimering. Innehåller information för en komplett bild till skillnad från P- eller B-frames som innehåller information om ändringar jämfört med föregående eller nästa bildruta.

Inbrottskontrollpanel

Allmänt namn på kärnenheten i ett inbrotts säkerhetssystem från Bosch. Det går att ansluta knappsatser, moduler, detektorer och andra enheter till kontrollpanelen.

Inspelningsschema

Används för schemaläggning av vissa händelser som t.ex. start av säkerhetskopiering eller begränsning av inloggning. Inspelningsscheman kan inte ha luckor eller överlappningar. Det avgör dessutom videoinspelningskvaliteten.

Intercom-funktioner

Används för att tala via högtalare på en kodare. Den här kodaren måste ha funktioner för in- och utgående ljud. Intercom-funktionerna kan tilldelas per användargrupp.

IPS

Bilder per sekund. Antal videobilder som överförs eller spelas in per sekund.

IQN

iSCSI Qualified Name. Initiatörsnamnet i IQN-format används för att tillhandahålla adresser till både iSCSI-initiatörer och målenheter. Med IQN mapping skapar du en initiatörsgrupp som styr åtkomsten till LUN-enheter på en iSCSI-målenhet och du skriver in initiatörsnamnen i den här initiatörsgruppen för varje kodare och VRM-enhet. Endast enheterna vars initiatörsnamn som läggs till i en initiatörsgrupp har behörighet att få åtkomst till en LUN. Se LUN och se iSCSI.

iSCSI

Internet Small Computer System Interface. Protokoll som hanterar lagring via ett TCP/IP-nätverk. iSCSI medger åtkomst till lagrad data från var som helst i nätverket. Särskilt sedan Gigabit Ethernet kom till har det blivit prisvärt att ansluta iSCSI-lagringsservrar som fjärrhårddiskar i ett

datornätverk. När det gäller iSCSI kallas servern som tillhandahåller lagringsresurser för ett iSCSI-mål medan klienten som ansluter till servern och använder dess resurser kallas för en iSCSI-initiatör.

JPEG

Joint Photographic Expert Group

JPEG

Joint Photographic Experts Group.
Kodningsprocess för stillbilder.

Kartvyport

En kartvyport är en region på skärmen som används för att visa en definierad del av den globala geolokaliseringskartan.

Kodare

Ändrar en analog ström till en digital ström, t.ex. för att integrera analoga kameror i ett digitalt system som t.ex. Bosch Video Management System. Vissa kodare har en lokal lagringsplats, t.ex. ett Flash-kort eller en USB-hårddisk, eller också kan de lagra videodata på iSCSI-enheter. IP-kameror har en inbyggd kodare.

Kommandoskript

Makro som administratören kan programmera så att det bygger en automatiskt åtgärd så som placering av en PTZ-kamera eller skickar e-postmeddelanden. För den funktionen tillhandahåller Bosch Video Management System en specifik grupp av kommandon. Kommandoskript delas in i klientskript och serverskript. Klientskript används hos klientarbetsstationer för att utföra särskilda uppgifter som kan köras på en klientarbetsstation. Serverskript utförs automatiskt genom en händelse som utlöstes i systemet. De får argument från händelsen, t.ex. datum och tid. Ett kommandoskript kan bestå av flera skriptdelar. Du kan skapa ett kommandoskript genom att använda följande skriptspråk: C#, VB.Net. Kommandoskript utförs automatiskt som svar på händelser eller larm i enlighet med ett schema (endast serverskript), manuellt från det logiska trädets eller manuellt från ikoner eller kartor.

Korrigerig av kantdistorsion

Distorsionskorrigering sker i själva kameran.

kringgå/sluta kringgå

När du kringgår en enhet ignoreras alla larm som enheten kan generera, vilket är praktiskt i särskilda situationer, t.ex. vid underhållsarbete. När du slutar att kringgå en enhet ignoreras inte enheten längre.

Larm

Händelse som är konfigurerad för att skapa ett larm. Detta är en särskild situation (rörelse upptäckt, ringklockan ringde, signalen försvann etc.) som kräver omedelbar uppmärksamhet. Ett larm kan visa live-video, uppspelningsvideo, en åtgärdsplan, en webbsida eller en karta.

Larmbildsfönster

Bildfönster för att visa en eller flera larmbildrutor.

Larmlista

Fönster i Bosch Video Management System används för att visa en lista med aktiva larm.

LDAP

Lightweight Directory Access Protocol. Nätverksprotokoll som använder TCP / IP och tillåter åtkomst till kataloger. En katalog kan till exempel vara en lista på användargrupper och deras åtkomstbehörigheter. Bosch Video Management System använder denna för att få åtkomst till samma användargrupper som MS Windows eller något annat användarhanteringssystem för företag.

Live-läge

Funktion i Operator Client. Används för livevisning av video.

Loggbok

Utrymme för loggning av alla händelser i Bosch Video Management System.

Logiskt nummer

Logiska nummer är unika ID:n som tilldelas till varje enhet i systemet som en enkel referens. Logiska nummer är endast unika inom en särskild enhetstyp. En vanlig användning av logiska nummer är kommandoskript.

Logiskt träd

Träd med en anpassad struktur för alla enheter. Det logiska trädet används i Operator Client för att välja kameror och andra enheter. I Configuration Client konfigureras och skräddarsys

det "kompletta logiska trädet" (på sidan Kartor och struktur) för varje användargrupp (på sidan Användargrupper).

LUN

Logical Unit Number (nummer för logisk enhet). Används i iSCSI-miljön för att rikta sig till en individuell diskenhet eller en virtuell partition (volym). Partitionen är en del av RAID-diskenheterna (iSCSI-målet).

Mappa filer

BVMS stöder följande kartfiler: PNG och JPG.

Master Control Software

Programvara som används som gränssnitt mellan Bosch Video Management System och en Allegiant-enhet. Version 2.8 eller senare används.

MHT

Kallas även "webbarkiv". Filformat som kan spara alla HTML- och bildfiler från en internetsajt i en fil. För att undvika problem rekommenderar vi att MHT-filer bara skapas med Internet Explorer 7.0 eller högre.

monitorgrupp

En grupp av monitorer som är anslutna till avkodare. Monitorgruppen kan användas för larmbehandling i ett specifikt fysiskt område. Till exempel kan en installation med tre fysiskt separata kontrollrum ha tre monitorgrupper. Monitorerna i en monitorgrupp är logiskt konfigurerad på rader och kolumner, och kan ställas in på olika layouter, t.ex. helskärm eller fyrbildsvy.

NVR

Bosch Network Video Recorder (nätverksvideoinspelare); dator i Bosch Video Management System som lagrar ljud- och videodata, fungerar som reserv-NVR eller som redundant NVR. Den här NVR-enheten skiljer sig från VIDOS NVR som kan integreras i Bosch Video Management System.

Nätverksövervakning

Måttet för nätverksrelaterade värden och utvärdering av dessa värden gentemot konfigureringsbara trösklar.

OID

Object Identifier. Term i SNMP-miljön. Bestämmer en MIB-variabel.

område

En grupp med identifieringsenheter som är anslutna till säkerhetssystemet.

områden

Område är en term som används i samband med ONVIF-kameror. Det är en parameter som används för avsökning av en ONVIF-enhet. Vanligtvis innehåller parametern en URI som följande: onvif: // www.onvif.org/<sökväg>. Parametern <sökväg> kan till exempel vara video_encoder eller audio_encoder. En ONVIF-enhet kan ha flera områden. Den här URI:en betecknar enhetens uppgiftsområde.

ONVIF

Open Network Video Interface Forum. Global standard för nätverksvideoprodukter. Enheter som uppfyller ONVIF kan utbyta livevideo, ljud, metadata och styrningsinformation, och upptäcks och ansluts till nätverkstillämpningar som videohanteringssystem helt automatiskt.

Operator Client

Komponent i Bosch Video Management System som tillhandahåller användargränssnittet för systemövervakning och drift.

Operatörsklientsarbetsstation

Dator i Bosch Video Management System-miljön för visning av live- och uppspelningsvideo samt för konfigurationsuppgifter. Operatörsklienten är installerad på din dator.

P-frame

Predicted frame. Del av en metod för videokomprimering.

PID

person identification device. Den extraherar egenskaper hos en person från en bild, till exempel ansiktet. Den kör särskilda algoritmer som kan identifiera en person i en videoström.

Port

1) På dator- och telekommunikationsenheter är en port (substantiv) generellt ett specifikt ställe för fysisk anslutning till någon annan enhet, vanligtvis med ett uttag och en kontakt av något slag. Vanligtvis levereras en persondator med en eller flera seriella portar och vanligtvis en parallellport. 2) Inom programmering är en port (substantiv) ett "logiskt anslutningsställe" och specifikt, genom att

använda internetprotokollet TCP/IP, det sätt som ett klientprogram använder för att specificera ett visst serverprogram på en dator i ett nätverk. Avancerade program som använder TCP/IP, som webbprotokollet Hypertext Transfer Protocol, har portar med nummer som tilldelats i förväg. Dessa kallas "välkända portar" och har tilldelats av Internet Assigned Numbers Authority (IANA). Andra programprocesser tilldelas portnummer dynamiskt för varje anslutning. När en tjänst (serverprogram) först startas säger man att det ansluter till dess avsedda portnummer. När något klientprogram vill använda den servern måste det också begära att få ansluta till det avsedda portnumret. Portnumren är från 0 till 65535. Portarna 1 till 1023 är reserverade för användning av specifika privilegierade tjänster. Port 80 är standardmässigt definierad för HTTP-tjänst och behöver inte anges i Uniform Resource Locator (URL).

POS

Point of sale.

Primär VRM

Synonym för VRM.

PTZ-kamera

Kamera med panorerings-, lutnings- och zoomfunktion.

punkt

En identifieringsenhet som är ansluten till säkerhetssystemet. Punkter visas enskilt på knappsatsen och med anpassad text. Texten kan beskriva en viss dörr, rörelsedetektor, rökdetektor eller ett skyddat område såsom ÖVERVÅNING eller GARAGE.

RAID

Redundant uppsättning av oberoende diskar. Används för att organisera två eller flera hårddiskar som om de vore en drivenhet. På en sådan drivenhet delas eller reproduceras data. Detta används för att uppnå högre kapacitet, tillförlitlighet och hastighet.

RCP

Remote Control Protocol

Referensbild

En referensbild jämförs kontinuerligt med den aktuella videobilden. Om den aktuella videobilden i de markerade områdena skiljer sig från referensbilden, så löser ett larm ut. Det möjliggör upptäckt av sabotage som annars inte skulle ha upptäckts, t.ex. om kameran vrids åt sidan.

Reserv-VRM

Programvara i BVMS-miljön. Övertar uppgiften från den tilldelade primära eller sekundära VRM-enheten när ett fel uppstår.

RMon och Snmp

Simple Network Management Protocol. IP-baserat protokoll som låter dig inhämta information från nätverksenheter (GET), ställa in parametrar hos nätverksenheter (SET) och meddelas om vissa händelser (EVENT).

ROI

Avkänningsområde. ROI används för att spara bandbredd när ett avsnitt av kamerabilden zoomas in med en fast HD-kamera. Avsnittet fungerar som en PTZ-kamera.

RTP

Real-Time Transport Protocol: ett överföringsprotokoll för video och ljud i realtid

RTSP

Real Time Streaming Protocol. Ett nätverksprotokoll som möjliggör styrning av kontinuerlig överföring av audiovisuella data eller programvara över IP-baserade nätverk.

Sammansatt händelse

Kombination av olika händelser. Kombinationen använder booleska uttryck, d.v.s. OCH och ELLER. Du kan endast kombinera statusändringar, till exempel en ändring i anslutningsstatus till oansluten eller aktivering av ett schema.

Sekundär VRM

Programvara i BVMS-miljön. Ser till att inspelningen som utförs av en eller flera primära VRM-enheter samtidigt överförs till ytterligare ett iSCSI-mål. Inspelningsinställningarna kan avvika från inställningarna på den primära VRM-enheten.

server

BVMS-server som hanterar enheter.

Serversökning

En åtkomstmetod för en användare av Configuration Client eller Operator Client som vill ansluta till flera av systemets accesspunkter i sekvens. En accesspunkt i systemet kan vara en Management Server eller en Enterprise Management Server.

Skimming

Sabotage på en nyckelkortsläsare. En skimningsenhet läser av kortdata på magnetremsan utan kortinnehavarens vetskap.

Speglad VRM

Programvara i BVMS-miljön. Specialfall för en sekundär VRM-enhet. Ser till att inspelningen som utförs av en primär VRM-enhet samtidigt överförs till ytterligare ett iSCSI-mål med samma inspelningsinställningar.

Stamlinje

Analoga utgångar från en analog matris vilka är anslutna till en kodarenhet. Därmed kan matrisvideokällor användas i Bosch Video Management System.

TCP

Transmission Control Protocol

TCP/IP

Transmission Control Protocol / Internet Protocol. Också känd som Internetprotokollen. En uppsättning kommunikationsprotokoll som används för att överföra data över ett IP-nätverk.

Textdata

Data från en POS eller ATM (bankomat), t. ex. datum och tid eller bankkontonummer som lagras med motsvarande videodata för att tillhandahålla ytterligare information för utvärdering.

Trap

Term i SNMP-miljön för ett oefterfrågat meddelande från en övervakad enhet (agent) till ett nätverksövervakningssystem (överordnad styrenhet) om en händelse i denna enhet.

UDP

User Datagram Protocol. Ett protokoll utan anslutning som används för att utväxla data via ett IP-nätverk. UDP är mer effektivt än TCP för videoöverföring på grund av lägre resursförbrukning.

unmanaged site

Objekt i enhetsträdet i BVMS som kan innehålla videonätverksenheter, t.ex. digitala videoinspelare. De här enheterna hanteras inte av Management Server i ditt system. Operator Client-användaren kan ansluta till enheterna på en unmanaged site-plats efter behov.

Uppgiftsschema

Används för att schemalägga händelser som kan uppstå i Bosch Video Management System, till exempel utförande av ett kommandoskript. Under Händelser tilldelar du uppgiftsscheman till händelser. Du även använda inspelningsscheman till att schemalägga händelser. Du kan konfigurera tidsperioder för varje veckodag, helgdagar samt undantagsdagar med ett standarduppgiftsschema. Med ett återkommande uppgiftsschema konfigurerar du återkommande tidsperioder. De kan återkomma varje dag, varje vecka, varje månad eller varje år.

URI

Uniform Resource Identifier. Sträng för att identifiera en nätverksresurs. Varje URI består av schema, behörighet, sökväg, fråga, fragment. Endast schema och fragment är obligatoriskt för en mobil videotjänst. Exempel: `http:<schema>//example.com<authority>/over/thererepath?name=ferret<query>#nose<fragment>`

URL-adress

Uniform Resource Locator

VCA

Analys av videoinnehåll: datoranalys av videoströmmar för att kunna ta reda på vad som händer på scenen som övervakas. Se även Intelligent Video Analytics

Video Streaming Gateway (VSG)

Virtuell enhet som gör att du kan integrera kameror från Bosch, ONVIF-kameror, JPEG-kameror och RTSP-kodare.

Videoanalys

Videoanalys är en programvaruprocess som jämför en kamerabild med lagrade bilder av specifika personer eller föremål. I händelse av en matchning utlöser programvaran ett larm.

Videoupplösning

Specifikation av vågräta och lodräta pixlar överförs via videosignaler. 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 x 480 QCIF = 176 x 120 HD 720p = kodad 1280 x 720 1080p = kodad 1920 x 1080

Virtuell ingång

Används för att vidarebefordra händelser från tredjepartssystem till Bosch Video Management System.

VRM

Video Recording Manager (videoinspelningshanterare). Programvarupaket i Bosch Video Management System som hanterar lagring av video (MPEG-4 SH++, H.264 och H.265) med ljuddata och metadata på iSCSI-enheter i nätverket. VRM underhåller en databas med information om inspelningsskälla och en lista med tillhörande iSCSI-enheter. VRM fungerar som en tjänst som körs på en dator i Bosch Video Management System-nätverket. VRM lagrar inte videodata utan distribuerar i stället lagringsmöjligheter på iSCSI-enheter till kodarna samtidigt som lastbalansering hanteras mellan flera iSCSI-enheter. VRM strömmar uppspelning från iSCSI till operatörsklienter.

Återspolningstid

Antalet sekunder när en bildruta växlas till direktuppspelning.

Återstudstid

Tidsperiod som börjar med att en händelse inträffar. Under denna tidsperiod godtas oftast ingen annan händelse av samma slag. Detta förhindrar exempelvis att en kontrollsensor skapar ett stort antal händelser. För händelser med flera tillstånd kan du konfigurera en olika prioritetsinställningar för de olika tillstånden. Följande exempel hjälper dig att få en djupare förståelse för begreppet avstudsningstid. Exempel 1 berör händelser som skapar samma tillstånd: händelsen Systeminformation inträffar och den konfigurerade avstudsningstiden börjar. Under denna tid inträffar en annan händelse av typen Systeminformation. Den här händelsen av typen Systeminformation godtas inte som en ny händelse. Exempel 2 berör händelser som skapar

olika tillstånd med samma prioritet: händelsen Rörelse upptäckt inträffar och den konfigurerade avstudsningstiden börjar. Under den här tiden inträffar händelsen Rörelse avbruten med samma prioritet. Händelsen med stoppad rörelse godtas inte som en ny händelse. Exempel 3 berör även händelser som orsakar olika tillstånd med samma prioritet: tillståndet för en virtuell ingång är påslagen. Tillståndsprioriteringarna för båda tillståndsändringar är identiska. Vid en viss tidpunkt stängs den virtuella ingången av, och avstudsningstiden börjar. Under avstudsningstiden är den virtuella ingången påslagen. Den här tillståndsändringen accepteras inte som en ny händelse eftersom den har samma prioritet. När avstudsningstiden har gått ut, så är den virtuella ingången i ett annat tillstånd. Påslagningen får en tidsstämpel från slutet av avstudsningstiden, och ingen ny avstudsningstid börjar. Exempel 4 berör händelser med olika prioritet som skapar samma tillstånd: händelsen Rörelse upptäckt inträffar och den konfigurerade avstudsningstiden börjar. Under denna tid inträffar händelsen med stoppad rörelse med en högre prioritet. Händelsen Rörelse avbruten accepteras som en ny händelse, men avstudsningstiden börjar inte om. Exempel 5 berör även händelser med olika prioritet som orsakar olika tillstånd: tillståndet för en virtuell ingång är avstängd. Tillståndsprioriteten för påslagen är 5, och för avstängd är den 2. Vid en viss tidpunkt slås den virtuella ingången på (prio 5), och avstudsningstiden börjar. Under avstudsningstiden är den virtuella ingången avstängd (prio 2). Den här tillståndsändringen accepteras som en ny händelse eftersom den har högre prioritet. Avstudsningstiden för den första påslagningen fortsätter. Inga ytterligare tillståndsändringar accepteras under avstudsningstiden.

Innehållsförteckning

Symboler

åtkomst nekad

Allegiant-CCL-emulering	150
ändra IP-adress	101, 118, 132, 215
ändra lösenord	136, 166, 205, 212
ändra nätverksadress	132
ändra nätverksadressen	215
ändra pool	213
ändring av lösenord	309

A

aktivera	88
Bosch Video Management System	71
tidigare konfiguration	89
aktivering	91
fördröjd	88, 100
konfiguration	88
aktiveringspunkter	241
Allegiant	
CCL-emulering	119, 151
för många kameror	343
kontrollkanal	57, 58
Network Host-program	57
PTZ-kamera	269
satellitsystem	58
version av fast programvara	49, 50
Allegiant CCL-emulering	151
Allegiant CCL-kommandon	59
Allegiant-CCL-emulering	
åtkomst nekad	150
Allegiant-fil	343
Allegiant-matris	118, 126, 127
allt-i-ett-system	61
analog matris	126
analog monitorgrupp	115, 119
anpassade händelser	284, 300
ANR	79, 215, 268
ansluta	
Allegiant-matris och BVMS	54
Bosch IntuiKey-tangentbord och BVMS	50
anslutningssträng	114
använda hjälpen	14
användare	
delete	309
ta bort	309
användargrupper	306, 308
användarhändelseknapp	299
arbetsstation	115
ATM POS-enhet	118

Audio Intercom-funktioner	316
autentiseringsverifiering	211
automatisk nyinloggning	88
automatisk omstart	88
automatisk utloggning	114
automatisk visning av larm	39
automatiskt	171
automatiskt inspelningsläge	171
avkodare	
Bosch IntuiKey-tangentbord	137
avkodare:mållösenord	200, 212
Avkänningsområde	268, 281, 311

B

behörigheter	241, 243
bildförhållandet 16/9	318
blinkande enhetsikoner	285, 304
Bosch IntuiKey-tangentbord	49, 50, 53, 119, 129, 137, 147
Bosch Video Management System	16
aktivera	71
GUI-språk	341
licensiering	71
onlinehjälp	14
översikt	16
brandlarmskamera	336
brandvägg	192
Brottsutredande sökning	129, 132
BVIP-avkodare	77, 207
BVIP-enhet	
lösenord	136, 205, 212
Webbsida	205
BVIP-kodare	77, 207
lägg till	133, 172, 199
lägga till	133, 172, 199
BVIP-kodare: lägga till	134, 208
byt lösenord	309

C

CABAC	275
CCL-emulering	151
CCTV-tangentbord	147
anslutningsavbrott	342
CLL-kommandon	151
codecar	275
Configuration Wizard	
Mobile Video Service	61

D

datablad	20
----------	----

DCZ-tangentbord	147	för många Allegiant-kameror	343
DiBos-enhet	118	fördrojd aktivering	88, 100
digital videoinspelare	118	G	
digitalt tangentbord	147	globala larminställningar	301
domekamera	279, 280	globalt standardlösenord	68, 88, 100
DSA E-Series	176, 177, 181, 182	grundkonfiguration:	183
DTP3N	143	gränssnittsinställningar	
dubbel behörighet	310	VIP XD	137
dubbel inspelning	28	GUI-språk	341
dubbel strömning	178, 282	H	
dubbla IP-adresser	100	H.264	275
dubbla strömmar	131	H.264-avkodningsfilter	275
duplicera en händelse	298	hanteringsserver	20, 323
DVR-enhet	123	HD-kameror	318
E		helgdagar	264
enheter utan lösenordsskydd	88	hitta	
enhetsbyte	73, 74	enheter	102, 103, 104, 117, 242, 266, 284, 287, 289, 308
enhetsfunktioner		information i hjälpen	14
uppdatering	77, 207	hjälp	14, 15
enhetsruta	241	hjälp om Bosch Script API	85
Enhetsträd	117, 164, 241	HTML-filer	241
enhetsövervakare	91	I	
Enterprise Management Server	319	i offlineläge	309
Enterprise System	23, 81	I/O-moduler	119
Enterprise User Groups	306	importera	
e-postenhet	118	Kommandoskript	86
ersätt innehåll	244	resursfiler	244
exempel	93	inaktivera forcerat lösenordsskydd	100
konfigurera VRM-inspelning	94	inaktivitet	114
lägga till Bosch Allegiant-ingångslarm	94	inbrottspanel	153, 154
lägga till Bosch ATM/POS-brygga	93	inget lösenord	88
export		initial kamera	139
konfigurationsdata till OPC	91	Inspelningsinställningar	218
exportera		inspelningskvalitet	273
Kameratabell	272	inspelningsläge	
Kommandoskript	86	reserv	170
konfigurationsdata	89	inspelningsläge för	170
MOV	315	Inspelningstabell	266
F		Intercom-funktioner	316
felövervakningsrelä	258	IntuiKey-tangentbord	147
filtrering	102, 103, 104, 117, 242, 266, 284, 287, 289, 308	iPad	152
fjärrexport	41	IP-adress	
flermonitorläge	318	dubletter	100
flytta enhet	186, 196, 213	ändra	101, 118, 132, 215
forcerat lösenordsskydd	100	iPhone	152
Forensic Search	95, 130	IP-standardadress	100
frånkopplad	323	IQN mapping	183
fyrbildsvy	139	iSCSI-enhet	183

iSCSI-lagringspool	161	LDAP-användare	308
iSCSI-lagringspoolen	179	LDAP-användargrupper	111, 308, 333
iSCSI-lagringssystemet	179	LDAP-grupp	111, 333
K		licensiering	
kamerarunda	241, 249, 251	Bosch Video Management System	71
kamerasekvens	241, 249, 251	konfigurationsguide	68
karta		Stratus-server	71
blinkande aktiveringspunkter	285, 304	logga	301
kartlänkar	252	logga ONVIF-händelser	349
kartor	241	loggboksdata	114
kartvyport	253	anslutningssträng	114
KBD Universal XF-tangentbord	129	Logging	165
KBD-Universal XF-tangentbord	49, 50, 119	loggning	299
Klientkommandoskript		Logiskt träd	243, 294
utförs vid start	87, 130	LUN-enheter	
accepterat larm	294	större än 2 TB	171
körs vid uppstart	86	lägen	101, 102, 103
knapp för användarhändelse	299	lägg till ohanterad plats	201
kodare		lägg till unmanaged site	201, 203
lägga till	169, 177, 205, 337	lägg till videoanalysenhet	156
Webbsida	205	lägg till VRM	161
kodare: reservinspelningsläge	217	lägga till Bosch Allegiant-ingångslarm	94
kodkonverteringstjänst	152	lägga till Bosch ATM/POS-brygga	93
-kodning på NVRs	117, 164	lägga till BVIP-avkodare	133, 172, 199
Kommandoskript	241, 248	lägga till BVIP-kodare	133, 134, 172, 199, 208
exportera	86	lägga till en kodare	169, 177, 205, 337
hjälp om Bosch Script API	85	lägga till pool	
importera	86	VRM	167
kompatibilitetsläge	41	lägga till textdata i en kontinuerlig inspelning	288
konfigurationsdata		länk till kartan	252
exportera	89	lösenord	136, 205, 212
konfigurationsdata till OPC		lösenord saknas	88
export	91	lösenordsändring	166
konfigurera VRM-inspelning	94	M	
konverteringstjänst	152	Management Server	23
kopiera och klistra in	271	manuell inspelning	41, 289, 302
krascha		Map-based tracking assistant för kartbaserad spårning	
Configuration Client	342	257	
kringgå		menykommandon	97
punkt	316	MIC IP 7000	340
kringutrustning	118	Mobila videotjänster	152
L		Mobile Video Service	61
larm		monitorgrupp	138, 139, 290, 294
sorteringsordning	290	enbildsvy	139
larminspelning	289, 302, 303	fyrbildsvy	139
larminspelningsläge	275, 276	initial kamera	139
larmkarta	290	lägg till	138
larmprioritet	334	OSD	139
larmsekvens	289, 302	startkamera	139

MOV	315	PTZ-kamera	279, 280
multicast	192	Allegiant	269
multival	243, 244	PTZ-kontroll	
Måldatahastighet	274	blockering	317, 334
mållösenord	200, 212	PTZ-styrning	
N		blockering	311
nedkopplad	323	punkt	
NVR	20	kringgå	316
nya DiBos-enheter	125, 126	R	
nätverksadress		radera användare	309
ändra	132, 215	RAM-inspelning	276
nätverksövervakningsenhet	118	redundant inspelning	28
O		redundant VRM	28, 120, 168
Obehörig person		relä	
Obehörig person upptäckt	305	tekniskt fel	258
oberoende Operator Client	323	reservinspelningsläge	
offline	323	kodare	217
offlineläge	323	resursfiler	244
onlinehjälp om programmet	14	importera	244
ONVIF-loggning	349	ripplande sensorer	301
ONVIF-mediaprofil	268	ROI	268, 281, 311
OPC Server	341	S	
Operator Client	16, 243	sammansatta händelser	284, 300
opålitligt nätverk	152	sekundär inspelning	178, 282
P		Sekundär VRM	28, 120, 163
panoreringskamera		Sekundär VRM-reserv	167
visningslägen	42	sekvens	251
Passersystem	154	Server ID	74
Person identification		Serverinitiatörsnamn	164
Lägg till kameror till person identification device		Serverlista	
158		lägga till kolumner	81, 122
Lägga till en person identification device	156	radera kolumner	81, 122
Person identification device	156	Servernätverk	201, 202, 203
pool		Serversökning	122
flytta enhet	186, 196, 213	Sidan Allegiant-CCL-emulering	150
VRM	167, 213	skaffa PTZ-kontroll	334
ändra	213	skapa	
pooling	179	kommandoskript	85
poolning	161	skriva ut hjälpen	15
pop-up vid automatiskt larm	39	skydda larminspelning	303
Primär reserv-VRM	167	SNMP-inställningar	109
Primär VRM	28, 120, 162	SNMP-meddelanden	
profil	273	get	109
PTZ-blockering	311, 317, 334	skicka	109
		sorteringsordning	
		larm	290
		språk	341
		Configuration Client	114
		Operator Client	308

standardkonfiguration	183	utlösa inspelning av textdata	303
standardlösenord	88, 100	W	
standardström	129, 268	Webbklient	152
status	91	versionskommentarer	20
stor LUN-enhet	171, 175, 181, 186, 187	Video Streaming Gateway	118
stora LUN-enheter	171	videoanalys	155
Stratus-server		VIDEOJET 7000 connect	340
licensiering	71	VIP X 1600 XFM4	275
ström	268, 278	VIP XD	49
styra en kamera	275	fyrbildsvy	139
styrning av kamera	95	gränssnittsinställningar	137
stänga av larmsirener	316	halvduplexläge	137
synkronisera		virtuell ingång	118
VRM-konfiguration	170	visningslägen för panoreringskamera	42
synkronisering	79	WLAN	152
systemkrav	20	VRM	
sök		lägg till	161
kodare	120	lägga till pool	167
kodare, endast live	120	pool	167, 213
lokala lagringskodare	120	Primär	28, 120, 162
VRM	120	Primär reserv	167
söka efter IP-adresser i konflikt	100	redundant	28, 120, 168
sökning		Reserv	28, 120, 167
i subnät	114	sekundär	28, 120, 163
T		Sekundär reserv	167
ta bort användare	309	VRM 3.50	170
ta bort förprogrammerade lägen	279	VRM-lagringspool	161, 179
tid efter händelse	275, 276	VRM-reserv	28, 120, 167
tid efter larm	276		
tid före händelse	275, 276		
tiden efter händelsen	270		
tiden före händelsen	270		
tidigare konfiguration	89		
tidsserver	79		
tidssynkronisering	79		
tidszon	201, 202		
tillstånd	97		
tomma lösenord	88		
tryck-för-tal	316		
tysta signaler	316		
U			
UHD kameror	131		
undantagsdagar	264		
uppdatera status	101, 102, 103		
uppdatera tillstånd	97		
uppdatering			
enhetsfunktioner	77, 207		
uppgradering av fast programvara			
Bosch IntuiKey-tangentbord	53		

Bosch Security Systems B.V.

Torenallee 49

5617 BA Eindhoven

Netherlands

www.boschsecurity.com

© Bosch Security Systems B.V., 2022

Building solutions for a better life.

202205091347