

BVMS

Spis treści

1	Korzystanie z Pomocy	14
1.1	Wyszukiwanie informacji	14
1.2	Drukowanie Pomocy	15
2	Użyj najnowszego oprogramowania	16
3	Wstęp	17
3.1	Wersje BVMS	20
3.2	Omówienie aktywacji licencji systemu BVMS	20
4	Ogólne informacje o systemie	22
4.1	Wymagania sprzętowe	23
4.2	Wymagania w zakresie oprogramowania	23
4.3	Wymagania licencyjne	23
5	Pojęcia	24
5.1	Założenia projektowe systemu BVMS	24
5.1.1	Jeden system Management Server	24
5.1.2	Enterprise System.	25
5.1.3	Server Lookup	26
5.1.4	Unmanaged site	28
5.2	Zapis	29
5.2.1	Automatyczne uzupełnianie sieciowe (Automated Network Replenishment, ANR)	29
5.2.2	Zapis podwójny / awaryjny	30
5.2.3	Tryby zapisu VRM	32
5.2.4	Odtwarzanie zapisanych źródeł VRM	34
5.2.5	Przegląd zdarzeń związanych z przechowywaniem danych	38
5.3	Obsługa alarmów	39
5.4	Włączanie/wyłączanie analizy zawartości obrazu (Video Analysis)	41
5.5	Mapowanie zdarzeń ONVIF	42
5.6	Wylogowanie w przypadku braku aktywności	43
5.7	Program Operator Client niezależny od wersji	44
5.7.1	Praca w trybie zgodności	44
5.8	Tryby podglądu kamery panoramicznej	44
5.8.1	Kamera panoramiczna 360° do montażu podłogowego lub sufitowego	45
5.8.2	Kamera panoramiczna 180° do montażu podłogowego lub sufitowego	47
5.8.3	Kamera panoramiczna 360° do montażu ściennego	48
5.8.4	Kamera panoramiczna 180° do montażu ściennego	49
5.8.5	Przycięty widok w kamerze panoramicznej	50
5.9	Tunelowanie SSH	51
5.10	Wieloscieżkowość	51
5.11	Open ID Connect (OIDC) i Identity Provider (IdP)	52
5.12	Rozpoznawanie tablic rejestracyjnych	52
6	Obsługiwany sprzęt	53
6.1	Instalowanie urządzeń	54
6.2	Instalowanie klawiatury KBD Universal XF	54
6.3	Podłączanie klawiatury Bosch IntuiKey do systemu BVMS	54
6.3.1	Możliwe sposoby podłączenia klawiatury Bosch IntuiKey	55
6.3.2	Podłączanie klawiatury Bosch IntuiKey do odbiornika	56
6.3.3	Aktualizacja oprogramowania układowego klawiatury Bosch IntuiKey	57
6.4	Podłączanie krosownicy Bosch Allegiant do systemu BVMS	58
6.4.1	Połączenia krosownicy Bosch Allegiant – informacje ogólne	58

6.4.2	Konfiguracja kanału sterującego	60
6.4.3	Koncepcja systemu satelitarnego Bosch Allegiant	62
6.5	Polecenia CCL systemu Allegiant obsługiwane w systemie BVMS	63
7	Rozpoczęcie pracy	65
7.1	Instalacja modułów oprogramowania	65
7.2	Używanie kreatora Config Wizard	65
7.3	Uruchamianie programu Configuration Client	72
7.4	Wybieranie wersji językowej modułu Configuration Client	73
7.5	Wybieranie wersji językowej modułu Operator Client	73
7.6	Skanowanie w poszukiwaniu urządzeń	74
7.7	Dostęp do systemu	74
7.8	Używanie funkcji Server Lookup	74
7.9	Aktywacja licencji na oprogramowanie	75
7.9.1	Okno dialogowe Manager licencji (menu Narzędzia)	76
7.9.2	Okno dialogowe Dodawanie licencji	77
7.9.3	Okno dialogowe Inspektor licencji (menu Narzędzia)	77
7.10	Utrzymanie systemu BVMS	77
7.11	Wymiana urządzenia	78
7.11.1	Wymiana MS / EMS	78
7.11.2	Wymiana VRM	79
7.11.3	Wymiana nadajnika lub dekodera	80
7.11.4	Wymiana stacji roboczej Operator Client	83
7.11.5	Testy końcowe	83
7.11.6	Odzyskiwanie DIVAR IP	83
7.12	Konfiguracja synchronizacji czasowej	83
7.13	Konfigurowanie nośnika zapisu nadajnika	84
8	Tworzenie Enterprise System	85
8.1	Konfigurowanie funkcji listy serwerów dla systemu Enterprise System	85
8.2	Tworzenie grupy Enterprise User Group	86
8.3	Tworzenie konta Enterprise Account	86
8.4	Uwierzytelnianie za pomocą tokenów	87
9	Konfiguracja skryptów poleceń	89
9.1	Zarządzanie skryptami poleceń	89
9.2	Konfigurowanie opcji automatycznego wykonywania skryptu poleceń	90
9.3	Importowanie skryptu poleceń	90
9.4	Eksportowanie skryptu poleceń	90
9.5	Konfigurowanie startowego skryptu poleceń (strona ustawień)	91
10	Zarządzanie danymi konfiguracyjnymi	92
10.1	Uaktywnienie konfiguracji roboczej	92
10.2	Uaktywnienie konfiguracji	93
10.3	Eksportowanie danych konfiguracyjnych	94
10.4	Importowanie danych konfiguracyjnych	94
10.5	Eksportowanie danych konfiguracyjnych do aplikacji serwera OPC	95
10.6	Sprawdzanie stanu nadajników/dekoderów	95
10.7	Konfigurowanie monitorowania SNMP	95
10.8	Tworzenie raportów	96
11	Przykładowe konfiguracje	97
11.1	Dodawanie interfejsu do ATM/POS-Bridge firmy Bosch	97
11.2	Dodawanie wejścia alarmowego do urządzenia Bosch Allegiant	98

11.3	Dodanie i konfiguracja 2 kamer sieciowych Dinion z zapisem VRM	98
12	Globalne okna systemu Configuration Client	100
12.1	Okno konfiguracji	100
12.2	Polecenia menu	101
12.3	Okno dialogowe Manager uaktywnienia (menu System)	103
12.4	Okno dialogowe Uaktywnij konfigurację (menu System)	104
12.5	Okno dialogowe Inicjujące skanowanie urządzeń (menu Sprzęt)	104
12.6	Ochrona urządzenia za pomocą okna dialogowego Globalne hasło domyślne (menu Sprzęt)	105
12.7	Chroń magazyny iSCSI za pomocą okna dialogowego Hasło CHAP (menu Sprzęt)	105
12.8	Okno dialogowe zmiany hasła urządzenia (menu Urządzenie)	106
12.9	Okno dialogowe aktualizacji oprogramowania układowego urządzenia (menu Urządzenie)	107
12.10	Okno dialogowe zmieniania ustawień sieciowych urządzenia i sieci (menu Urządzenie)	108
12.11	Okno dialogowe Monitor urządzeń (menu Sprzęt)	110
12.12	Okno dialogowe Edytor skryptu poleceń (menu Narzędzia)	110
12.13	Okno dialogowe Manager zasobów (menu Narzędzia)	111
12.14	Okno dialogowe Budowa sekwencji (menu Narzędzia)	111
12.15	Okno dialogowe Manager licencji (menu Narzędzia)	111
12.15.1	Okno dialogowe Dodawanie licencji	112
12.16	Okno dialogowe Inspektor licencji (menu Narzędzia)	112
12.17	Okno dialogowe Monitorowanie stacji roboczej (menu Narzędzia)	112
12.18	Okna dialogowe raportów (menu Raporty)	113
12.18.1	Okno dialogowe Harmonogramy zapisu	113
12.18.2	Okno dialogowe Ustawienia zaplanowanego zapisu	113
12.18.3	Okno dialogowe Harmonogramy zadań	113
12.18.4	Okno dialogowe Parametry kamer i zapisu	113
12.18.5	Okno dialogowe Ustawienia jakości strumienia	113
12.18.6	Okno dialogowe Ustawienia zdarzeń	113
12.18.7	Okno dialogowe Ustawienia zdarzeń złożonych	113
12.18.8	Okno dialogowe Ustawienia alarmowe	113
12.18.9	Okno dialogowe Skonfigurowani użytkownicy	114
12.18.10	Okno dialogowe Grupy i konta użytkowników	114
12.18.11	Okno dialogowe Uprawnienia urządzenia	114
12.18.12	Okno dialogowe Uprawnienia do obsługi	114
12.18.13	Konfigurowanie okna dialogowego Uprawnienia	114
12.18.14	Okno dialogowe Uprawnienia grupy użytkowników	114
12.18.15	Okno dialogowe Ustawienia zabezpieczeń	114
12.18.16	Okno dialogowe Uprawnienia aplikacji	114
12.18.17	Okno dialogowe Wyłączone urządzenia	114
12.19	Okno dialogowe Ustawienia alarmów (menu Ustawienia)	115
12.20	Okno dialogowe Ustawienia SNMP (menu Ustawienia)	115
12.21	Okno dialogowe Ustawienia serwera LDAP (menu Ustawienia)	116
12.21.1	Przypisywanie grupy LDAP	117
12.22	Okno dialogowe Definiowanie kolejności grup użytkowników LDAP (menu Ustawienia)	118
12.23	Okno dialogowe Ustawienia tokena dostępu (menu Ustawienia)	118
12.24	Okno dialogowe Ustawienia zaufanych certyfikatów (menu Ustawienia)	120
12.25	Okno dialogowe Opcje (menu Ustawienia)	120
13	strona Urządzenia	124
13.1	Aktualizowanie stanów i informacji o wydajności urządzeń	124
13.2	Zmienianie hasła urządzeń sieciowych	125

13.3	Dodawanie urządzenia	125
13.4	Strona listy serwerów/książki adresowej	128
13.4.1	Okno dialogowe Dodaj serwer	129
13.4.2	Konfigurowanie funkcji Server Lookup	129
13.4.3	Konfigurowanie listy serwerów	129
13.4.4	Eksportowanie listy serwerów	130
13.4.5	Importowanie listy serwerów	130
13.5	Strona DVR (cyfrowego rejestratora wizyjnego)	130
13.5.1	urządzenia DVR	131
13.5.2	Dodawanie urządzenia DVR poprzez skanowanie	132
13.5.3	Dodanie okna dialogowego DVR	132
13.5.4	Karta Ustawienia	133
13.5.5	Karta Kamery	133
13.5.6	Karta wejść	133
13.5.7	Karta Przekazniki	133
13.5.8	Konfiguracja zintegrowanego rejestratora DVR	133
13.6	strona Krosownice wizyjne	134
13.6.1	Dodawanie urządzenia Bosch Allegiant	134
13.6.2	Konfigurowanie urządzenia Bosch Allegiant	134
13.6.3	strona Wyjścia	135
13.6.4	strona Wejścia	136
13.6.5	strona Połączenie	136
13.6.6	strona Kamery	136
13.7	strona Stacja robocza	136
13.7.1	Ręczne dodawanie stacji roboczej	137
13.7.2	Konfigurowanie klawiatury Bosch IntuiKey (strona Ustawienia) (stacja robocza)	137
13.7.3	Konfigurowanie startowego skryptu poleceń (strona ustawień)	138
13.7.4	strona Ustawienia	138
13.7.5	Zmiana adresu sieciowego stacji roboczej	140
13.8	Strona Odbiorniki	140
13.8.1	Ręczne dodawanie nadajnika	140
13.8.2	Okno dialogowe Edytuj nadajnik/odbiornik	142
13.8.3	Zmiana hasła nadajnika/dekodera (Zmień hasło / Wprowadź hasło)	143
13.8.4	Profil odbiornika	144
13.8.5	Wyświetl. na monitorze	145
13.8.6	Konfigurowanie klawiatury Bosch IntuiKey (odbiornik)	145
13.8.7	Konfigurowanie odbiornika podłączonego do klawiatury Bosch IntuiKey	145
13.8.8	Usuń logo dekodera	146
13.9	Strona Grupy monitorów	146
13.9.1	Ręczne dodawanie grupy monitorów	146
13.9.2	Konfigurowanie grupy monitorów	146
13.10	strona Urządzenia komunikacyjne	147
13.10.1	Dodawanie serwera poczty elektronicznej/SMTP	148
13.10.2	strona Serwer SMTP	148
13.10.3	Konfiguracja urządzenia komunikacyjnego	149
13.10.4	Okno dialogowe Wyślij testową wiadomość e-mail	149
13.11	Strona ATM/POS-Bridge	149
13.11.1	Ręczne dodawanie interfejsu do ATM/POS-Bridge firmy Bosch	150
13.11.2	strona Interfejs do ATM/POS Bridge firmy Bosch	150

13.11.3	Konfiguracja urządzenia peryferyjnego	151
13.11.4	Strona ustawień urządzenia DTP	151
13.11.5	Strona ustawień ATM	151
13.11.6	strona Wejścia	152
13.12	Czytniki kart	152
13.12.1	Okno dialogowe Dodaj czytnik kart	152
13.12.2	Strona ustawień czytnika kart	153
13.13	strona Wirtualne wejścia	153
13.13.1	Ręczne dodawanie wirtualnych wejść	153
13.14	strona SNMP	154
13.14.1	Ręczne dodawanie SNMP	154
13.14.2	Konfigurowanie odbiornika komunikatów trap SNMP (strona odbiornika komunikatów trap SNMP)	154
13.14.3	Okno dialogowe Narzędzie do rejestrowania komunikatów Trap SNMP	155
13.15	Strona Przypisz klawiaturę	156
13.16	strona Moduły wejścia / wyjścia	157
13.16.1	Ręczne dodawanie modułu wejścia-wyjścia	157
13.16.2	Konfiguracja modułu wejścia / wyjścia	158
13.16.3	strona ADAM	158
13.16.4	strona Wejścia	158
13.16.5	strona Przekazniki	159
13.17	Strona Emulacja komend CCL krosownicy Allegiant	159
13.17.1	Ręczne dodawanie emulacji poleceń CCL krosownicy Allegiant	160
13.17.2	Polecenia CCL krosownicy Allegiant	160
13.17.3	Konfigurowanie usługi emulacji poleceń CCL urządzenia Allegiant	160
13.18	Strona Centrale alarmowe	160
13.18.1	Ręczne dodawanie centrali alarmowej	161
13.18.2	Strona Ustawienia	161
13.19	Strona systemów kontroli dostępu	161
13.19.1	Dodawanie systemu kontroli dostępu	162
13.19.2	Edycja systemu kontroli dostępu	162
13.19.3	Strona Ustawienia	163
13.20	Strona analizy obrazu	163
13.20.1	Strona ustawień Video Analytics	163
13.20.2	Dodawanie urządzenia analizy sygnału wizyjnego	163
13.20.3	Strona urządzeń Person Identification Device	164
13.20.4	Dodawanie urządzenia PID (Person Identification Device)	164
13.20.5	Strona PID	165
13.20.6	Przywracanie dostępu do PID po awarii serwera BVMS Management Server.	165
13.20.7	Dodawanie kamer do urządzenia PID (Person Identification Device)	166
13.20.8	Konfigurowanie parametrów kamery do obsługi alarmów Person Identification.	166
13.20.9	Konfigurowanie grup osób	167
13.20.10	Dodawanie urządzenia Tattile LPR	168
13.21	strona Urządzenia VRM	168
13.21.1	Dodawanie urządzeń VRM poprzez skanowanie:	169
13.21.2	Ręczne dodawanie podstawowego lub pomocniczego urządzenia VRM	170
13.21.3	Edytowanie urządzenia VRM	172
13.21.4	strona Ustawienia VRM	172
13.21.5	strona SNMP	172
13.21.6	Strona Konta	172

13.21.7	strona Zaawansowane	173
13.21.8	Zapis szyfrowany na urządzeniach VRM	173
13.21.9	Zmiana hasła urządzenia VRM	175
13.21.10	Dodawanie puli VRM	175
13.21.11	Ręczne dodawanie awaryjnego VRM	175
13.21.12	Dodawanie nadmiarowego urządzenia VRM	176
13.21.13	Dodawanie nadajników poprzez skanowanie	177
13.21.14	Dodawanie urządzeń VSG poprzez skanowanie	178
13.21.15	Synchronizowanie konfiguracji systemu BVMS	178
13.21.16	Importowanie konfiguracji z VRM	178
13.22	Strona puli	179
13.22.1	Konfigurowanie automatycznego trybu zapisu dla puli	180
13.22.2	Ręczne dodawanie nadajnika	181
13.22.3	Ręczne dodawanie urządzenia iSCSI	182
13.22.4	Ręczne dodawanie urządzenia Video Streaming Gateway	183
13.22.5	Ręczne dodawanie urządzenia iSCSI DSA E-Series	184
13.22.6	Dodawanie nadajników poprzez skanowanie	186
13.22.7	Dodawanie urządzeń VSG poprzez skanowanie	187
13.22.8	Konfigurowanie podwójnego zapisu w drzewie urządzeń	187
13.23	Strona Bosch Encoder / Decoder (Nadajnik/odbiornik firmy Bosch)	188
13.24	Strona urządzenia iSCSI	188
13.24.1	Pula pamięci iSCSI	188
13.24.2	Ręczne dodawanie urządzenia iSCSI	189
13.24.3	Ręczne dodawanie urządzenia iSCSI DSA E-Series	190
13.24.4	Konfiguracja urządzenia iSCSI	192
13.24.5	Strona Konfiguracja podstawowa	194
13.24.6	Okno dialogowe Balans obciążenia	195
13.24.7	Przenoszenie systemu iSCSI do innej puli (Zmień pulę...)	195
13.24.8	Strona Jednostki LUN	196
13.24.9	Dodawanie jednostki LUN	196
13.24.10	Formatowanie urządzenia o określonym numerze LUN	198
13.24.11	Okno dialogowe iqn-Mapper	198
13.25	Strona Urządzenie Video Streaming Gateway	198
13.25.1	Ręczne dodawanie urządzenia Video Streaming Gateway	199
13.25.2	Edytowanie komponentu Video Streaming Gateway	200
13.25.3	Dodawanie kamery do urządzenia VSG	201
13.25.4	Okno dialogowe Dodaj / Edytuj nadajnik Bosch	202
13.25.5	Okno dialogowe Dodaj / Edytuj nadajnik ONVIF	203
13.25.6	Okno dialogowe Dodaj / Edytuj kamerę JPEG	205
13.25.7	Okno dialogowe Dodaj / Edytuj nadajnik RTSP	206
13.25.8	Przenoszenie bramy VSG do innej puli (Zmień pulę)	207
13.25.9	Konfigurowanie multicastingu (karta trybu Multicast)	207
13.25.10	Konfigurowanie rejestrowania (karta Zaawansowane)	208
13.25.11	Uruchamianie narzędzia ONVIF Camera Event Driver Tool za pomocą Configuration Client	208
13.26	strona Tylko podgląd bieżący i lokalna pamięć masowa	209
13.26.1	Dodawanie urządzeń podglądu bieżącego poprzez skanowanie	209
13.26.2	Ręczne dodawanie nadajnika	210
13.26.3	Dostarczanie hasła docelowego dla dekodera (Uwierzytelnij...)	211
13.27	strona Lokalne urządzenia pamięci masowej	211

13.28	Strona Unmanaged Site	212
13.28.1	Ręczne dodawanie lokalizacji unmanaged site	212
13.28.2	Importowanie niezarządzanych lokalizacji	213
13.28.3	Strona Unmanaged Site	213
13.28.4	Dodawanie niezarządzanego urządzenia sieciowego	213
13.28.5	Konfigurowanie strefy czasowej	214
14	Strona Bosch Encoder / Decoder / Camera (Nadajnik/odbiornik/kamera firmy Bosch)	215
14.1	Ręczne dodawanie nadajnika	217
14.2	Dodawanie nadajnika do puli VRM	218
14.3	Dodawanie nadajnika udostępniającego tylko podgląd bieżący	218
14.4	Dodawanie nadajnika z pamięcią lokalną	218
14.5	Dodawanie pojedynczej kamery zastępczej	218
14.6	Importowanie kamer z pliku CSV	219
14.7	Dodawanie nadajnika Bosch ze wstępnie skonfigurowaną geolokalizacją	221
14.8	Edytowanie nadajnika	221
14.8.1	Szyfrowanie obrazu wizyjnego na żywo (Edytuj nadajnik)	221
14.8.2	Aktualizacja informacji o funkcjach urządzenia (Edytuj nadajnik)	222
14.8.3	Okno dialogowe Edytuj nadajnik/odbiornik	222
14.9	Zarządzanie sprawdzaniem autentyczności	224
14.9.1	Sprawdzanie autentyczności	224
14.9.2	Konfigurowanie uwierzytelniania	225
14.9.3	Przesyłanie certyfikatu	226
14.9.4	Pobieranie certyfikatu	226
14.9.5	Instalowanie certyfikatu na stacji roboczej	226
14.10	Dostarczanie hasła docelowego dla dekodera (Uwierzytelnij...)	227
14.11	Zmiana hasła nadajnika/dekodera (Zmień hasło / Wprowadź hasło)	227
14.12	Przenoszenie nadajnika do innej puli (Zmień pulę)	228
14.13	Odzyskiwanie zapisów z wymienianego nadajnika (Tworzenie powiązań z zapisami poprzednika)	229
14.14	Konfigurowanie nadajników/odbiorników	230
14.14.1	Konfigurowanie nośnika zapisu nadajnika	230
14.14.2	Konfiguracja wielu nadajników / odbiorników	230
14.14.3	Konfigurowanie trybu zapisu awaryjnego w nadajniku	232
14.14.4	Strona Zarządzanie zapisem	233
14.14.5	Strona Preferencje zapisu	233
14.14.6	Konfiguracja dekoderek do wyświetlania OSD	233
14.15	Konfigurowanie trybu Multicast	234
15	Strona ONVIF	236
15.1	Dodawanie urządzenia ONVIF tylko do podglądu bieżącego za pomocą skanowania	236
15.2	Strona Nadajnik zgodny ze standardem ONVIF	236
15.3	Strona ONVIF Encoder Events (Zdarzenia nadajników ONVIF)	237
15.3.1	Dodawanie i usuwanie profilu ONVIF	239
15.3.2	Eksportowanie pliku tablicy odwzorowań ONVIF	240
15.3.3	Importowanie pliku tablicy odwzorowań ONVIF	240
15.3.4	Konfigurowanie tabeli odwzorowań ONVIF	241
15.4	Strona Konfiguracja ONVIF	243
15.4.1	Dostęp do urządzenia	243
15.4.2	Data/godzina	244
15.4.3	Zarządzanie użytkownikami	244
15.4.4	Strona Profil nadajnika wizyjnego	245

15.4.5	Profil nadajnika fonicznego	247
15.4.6	Przetw. obrazów - ogólne	248
15.4.7	Kompensacja tła	248
15.4.8	Ekspozycja	249
15.4.9	Ogniskowanie	250
15.4.10	Szeroki zakres dynamiki	250
15.4.11	Balans bieli	251
15.4.12	Dostęp do sieci	251
15.4.13	Zakresy	253
15.4.14	Przełączniki	254
15.5	Strona ONVIF Event Source (Źródło zdarzeń ONVIF)	255
15.6	Przypisywanie profilu ONVIF	256
16	Strona rozpoznawania tablic rejestracyjnych	257
17	Karta Mapy i struktura	258
18	Konfiguracja map i drzewa logicznego	260
18.1	Konfigurowanie okna Drzewo logiczne	260
18.2	Dodawanie urządzenia do okna Drzewo logiczne	261
18.3	Usuwanie elementu drzewa	261
18.4	Zarządzanie plikami zasobów	262
18.4.1	Okno dialogowe Manager zasobów	263
18.4.2	Okno dialogowe Wybierz zasób	264
18.5	Dodawanie dokumentu	264
18.5.1	Okno dialogowe Dodaj adres URL	264
18.6	Okno dialogowe Łącze do aplikacji zewnętrznej	265
18.7	Dodawanie skryptu poleceń	265
18.8	Dodawanie sekwencji kamer	266
18.8.1	Okno dialogowe Budowa sekwencji	266
18.9	Zarządzanie wstępnie zaprogramowanymi sekwencjami kamer	267
18.9.1	Okno dialogowe Dodaj sekwencję	268
18.9.2	Okno dialogowe Dodaj krok sekwencji	268
18.10	Dodawanie folderu	268
18.11	Dodawanie mapy	269
18.12	Dodawanie łącza do innej mapy	269
18.12.1	Okno dialogowe Wybierz mapę dla łącza	269
18.13	Przypisywanie mapy do folderu	270
18.14	Zarządzanie urządzeniami na mapie obszaru	270
18.15	Konfiguracja mapy globalnej i okna roboczego mapy	271
18.15.1	Konfigurowanie mapy globalnej	271
18.15.2	Konfigurowanie kamer na mapie globalnej	272
18.15.3	Dodawanie map na mapie globalnej	274
18.16	Dodawanie okna roboczego mapy	275
18.17	Włączanie Map-based tracking assistant	275
18.18	Dodawanie przełącznika awaryjnego	276
18.18.1	Okno dialogowe Przełącznik awaryjny	276
18.19	Konfigurowanie pomijania urządzeń	277
19	strona Harmonogramy	278
19.1	strona Harmonogramy zapisu	278
19.2	strona Harmonogramy zadań	278
20	Konfigurowanie harmonogramów	280

20.1	Konfigurowanie harmonogramu zapisu	280
20.2	Dodawanie harmonogramu zadań	281
20.3	Konfigurowanie standardowego harmonogramu zadań	281
20.4	Konfigurowanie powtarzającego się harmonogramu zadań	281
20.5	Usuwanie harmonogramu zadań	282
20.6	Dodawanie świąt i dni wolnych od pracy	282
20.7	Usuwanie świąt i dni wolnych od pracy	283
20.8	Zmiana nazwy harmonogramu	283
21	strona Kamery i zapis	284
21.1	strona Kamery	285
21.2	Strony ustawień zapisu	289
22	Konfiguracja kamer i ustawień zapisu	291
22.1	Kopiowanie i wklejanie w tabelach	291
22.2	Eksportowanie tabeli kamery	292
22.3	Konfigurowanie ustawień jakości strumienia	292
22.3.1	Okno dialogowe Ustawienia jakości strumienia	293
22.4	Konfiguracja właściwości kamery	296
22.5	Konfigurowanie ustawień zapisu (tylko dla VRM i lokalnych urządzeniach pamięci masowej)	296
22.6	Okno Ustawienia zaplanowanego zapisu (tylko VRM i lokalna pamięć masowa)	297
22.7	Konfiguracja ustawień portu PTZ	300
22.8	Konfigurowanie predefiniowanych położeń i funkcji dodatkowych	300
22.9	Okno dialogowe predefiniowanych położeń i poleceń pomocniczych	301
22.10	Konfigurowanie funkcji ROI	302
22.11	Konfigurowanie funkcji ANR	302
22.12	Konfigurowanie podwójnego zapisu w tabeli kamery	303
22.13	Zarządzanie bramą Video Streaming Gateway	303
22.13.1	Przypisywanie profilu ONVIF	303
23	strona Zdarzenia	305
23.1	Karta Ustawienia eliminacji odbicia	306
23.2	Karta ustawień zaawansowanego wyświetlania mapy	306
23.3	Karta ustawień konfiguracji zdarzeń	307
23.4	Okno dialogowe Edytor skryptu poleceń	307
23.5	Utwórz Zdarzenie złożone / okno dialogowe Edytuj Zdarzenie złożone	308
23.6	Okno dialogowe Wybierz język skryptu	308
23.7	Okno dialogowe Edytuj priorytety typu zdarzenia	309
23.8	Okno dialogowe Wybierz urządzenia	309
23.9	Okno dialogowe Zapis danych tekstowych	309
24	strona Alarmy	310
24.1	Okno dialogowe Ustawienia alarmowe	311
24.2	Okno dialogowe Wybierz zawartość Okienka obrazu	312
24.3	Okno wyboru Wybierz zawartość okienka obrazu (MG)	313
24.4	Okno dialogowe Opcje alarmu	313
24.5	Okno dialogowe Wybierz zasób	317
25	Konfiguracja zdarzeń i alarmów	318
25.1	Kopiowanie i wklejanie w tabelach	319
25.2	Usuwanie wiersza tabeli	319
25.3	Zarządzanie plikami zasobów	319
25.4	Konfigurowanie zdarzenia	319
25.5	Tworzenie duplikatu zdarzenia	319

25.6	Rejestracja zdarzeń użytkownika	320
25.7	Konfiguracja przycisków zdarzeń użytkownika	320
25.8	Tworzenie zdarzenia złożonego	321
25.9	Edycja zdarzenia złożonego	322
25.10	Konfigurowanie alarmu	322
25.11	Konfiguracja ustawień dla wszystkich alarmów	323
25.12	Konfigurowanie dla alarmu czasów trwania okresu przed i po wystąpieniu alarmu	323
25.13	Wyzwalanie zapisu alarmowego za pomocą danych tekstowych	324
25.14	Dodawanie danych tekstowych do zapisu ciągłego	324
25.15	Ochrona zapisu alarmowego	324
25.16	Konfigurowanie migających miejsc aktywnych	325
25.17	Zdarzenia i alarmy w systemach kontroli dostępu	326
25.18	Zdarzenia i alarmy dla programu Person Identification	326
26	strona Grupy użytkowników	328
26.1	strona Właściwości grupy użytkowników	330
26.2	strona Właściwości użytkowników	331
26.3	strona Właściwości pary logowania	332
26.4	strona Uprawnienia kamery	333
26.5	Strona Priorytety sterowania	334
26.6	Okno dialogowe Kopiuj uprawnienia grupy użytkowników	335
26.7	strona Uprawnienia odbiornika	335
26.8	strona Zdarzenia i alarmy	336
26.9	Strona Dane uwierzytelniające	336
26.10	strona Drzewo logiczne	337
26.11	Strona funkcji operatora	337
26.12	strona Priorytety	341
26.13	strona Interfejs użytkownika	341
26.14	Strona Dostęp do serwera	342
26.15	Strona Konfigurowanie uprawnień	343
26.16	Strona Uprawnienia grup użytkowników	345
26.17	Strona zasad kont	345
26.17.1	Tryb offline programu Operator Client	347
26.18	Uprawnienia do logowania na stronie typu aplikacji	349
26.19	Strona ustawień zarządzania zagrożeniami	350
27	Konfigurowanie użytkowników, uprawnień i dostępu Enterprise	351
27.1	Tworzenie grupy lub konta	352
27.1.1	Tworzenie grupy użytkowników standardowych	352
27.1.2	Tworzenie grupy Enterprise User Group	352
27.1.3	Tworzenie konta Enterprise Account	353
27.2	Tworzenie użytkownika	354
27.3	Tworzenie grupy użytkowników podwójnej autoryzacji	355
27.4	Dodawanie pary logowania do grupy podwójnej autoryzacji	355
27.5	Konfigurowanie grupy administratorów	356
27.6	Wybieranie skojarzonej grupy LDAP	357
27.7	Konfiguracja uprawnień logowania użytkownika	357
27.8	Konfigurowanie uprawnień dotyczących obsługi	358
27.9	Konfigurowanie uprawnień dla urządzenia	358
27.10	Konfigurowanie różnych priorytetów	359
27.11	Kopiowanie uprawnień grupy użytkowników	361

28	Strona Audit Trail	362
28.1	Protokołowanie szczegółów w funkcji Audit Trail	363
28.2	Okno dialogowe filtrów w funkcji Audit Trail	363
29	Konfigurowanie wizyjnego systemu wykrywania pożaru	365
29.1	Konfigurowanie kamery wykrywania pożaru	365
29.2	Dodawanie nadajnika do puli VRM	366
29.3	Dodawanie nadajników poprzez skanowanie	366
29.4	Dodawanie urządzeń podglądu bieżącego poprzez skanowanie	366
29.5	Dodawanie nadajników z obsługą lokalnego urządzenia pamięci masowej poprzez skanowanie	367
29.6	Konfiguracja zdarzenia alarmu pożarowego	367
29.7	Konfigurowanie alarmu pożarowego	368
30	Konfigurowanie MIC IP 7000 podłączonego do zasilacza VIDEOJET connect 7000	369
31	Rozwiązywanie problemów	370
31.1	Ustawienie żadanego języka w systemie Windows	372
31.2	Przywracanie połączenia z klawiaturą Bosch IntuiKey	372
31.3	Zmniejszenie liczby kamer systemu Allegiant	372
31.4	Używane porty	373
31.5	Włączanie rejestrowania zdarzeń ONVIF	379
	Słowniczek	381

1 Korzystanie z Pomocy



Uwaga!

W niniejszym dokumencie opisano niektóre funkcje, które nie są dostępne w programie BVMS Viewer.

Szczegółowe informacje na temat poszczególnych wersji systemu BVMS znajdują się na stronie www.boschsecurity.com oraz w Skróconym poradniku wyboru systemu BVMS: [Skrócony poradnik wyboru systemu BVMS](#).

Aby uzyskać dodatkowe informacje o wykonywaniu różnych czynności w systemie BVMS, należy skorzystać z pomocy online w jeden z poniższych sposobów.

Aby użyć polecenia Spis treści, Indeks lub Szukaj:

- ▶ W menu **Pomoc** kliknij pozycję **Wyświetl pomoc**. Użyć przycisków i łączy do nawigacji.

Aby uzyskać pomoc na temat okna:

- ▶ Na pasku narzędzi kliknąć  .
LUB
- ▶ Nacisnąć klawisz F1, aby uzyskać pomoc na temat każdego okna programu.

1.1 Wyszukiwanie informacji

Informacje w pomocy można wyszukiwać na kilka sposobów.

Aby odszukać informacje w Pomocy online, należy:

1. W menu **Pomoc** kliknąć pozycję **Pomoc**.
2. Jeśli lewe okno nie jest widoczne, kliknąć przycisk **Pokaż**.
3. W oknie Pomoc wykonać następujące czynności:

Kliknij:	Aby:
Spis treści	Wyświetlić spis treści Pomocy online. Kliknąć poszczególne książki, aby wyświetlić strony odpowiadające tematom, oraz poszczególne strony, aby wyświetlić odpowiadający im temat w prawym oknie.
Indeks	Wyszukać określone słowa lub frazy albo wybrać z listy słów kluczowych. Kliknąć dwukrotnie słowo kluczowe, aby wyświetlić powiązany z nim temat w prawym oknie.
Wyszukaj	Zlokalizować słowa lub frazy w spisie tematów. Wprowadzić w polu tekstowym słowo lub frazę, nacisnąć klawisz ENTER i wybrać żądany temat z listy tematów.

Teksty dotyczące interfejsu użytkownika są zaznaczone czcionką **pogrubioną**.

- ▶ Strzałka informuje, iż można kliknąć podkreślony tekst lub kliknąć element w aplikacji.

Tematy pokrewne

- ▶ Kliknij, aby wyświetlić temat z informacją o aktualnie używanym oknie programu. Ten temat zawiera informacje o elementach sterujących okna aplikacji.

Pojęcia, Strona 24 zawiera podstawowe informacje na temat wybranych zagadnień.



Uwaga!

Ten symbol oznacza potencjalne ryzyko uszkodzenia mienia lub utraty danych.

1.2

Drukowanie Pomocy

Podczas korzystania z pomocy online tematy i informacje można drukować bezpośrednio z okna przeglądarki.

Aby wydrukować temat Pomocy:

1. Kliknąć prawym przyciskiem myszy w prawym oknie i wybrać polecenie **Drukuj**.
Zostanie otwarte okno **Drukuj**.
2. Kliknąć przycisk **Drukuj**.
⇒ Temat zostanie wydrukowany na wybranej drukarce.

2 Użyj najnowszego oprogramowania

Nowe aktualizacje tworzymy tylko dla wersji oprogramowania w stanie ogólnej lub ograniczonej dostępności. Więcej informacji:

[Usługi i wsparcie oprogramowania Bosch Building Technologies.](#)

Więcej informacji można znaleźć na stronach poniżej:

- Informacje ogólne: <https://www.boschsecurity.com/xc/en/support/product-security/>
- Zalecenia dotyczące bezpieczeństwa, czyli lista zidentyfikowanych luk i proponowanych rozwiązań: <https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html>

Firma Bosch nie ponosi żadnej odpowiedzialności za jakiegokolwiek szkody spowodowane korzystaniem z jej produktów w połączeniu z nieaktualnym oprogramowaniem.

3

Wstęp

Kliknij łącze, aby uzyskać dostęp do licencji składników OSS (ang. Open Source Software) używanych przez system BVMS i aplikację Mobile App:

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



Objęte jednym lub kilkoma zastrzeżeniami patentów wymienionych na patentlist.hevcadvance.com.

BVMS

BVMS łączy cyfrowy obraz, dźwięk i dane w dowolnej sieci IP.

System składa się z następujących modułów oprogramowania:

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

Aby uruchomić system, należy wykonać następujące czynności:

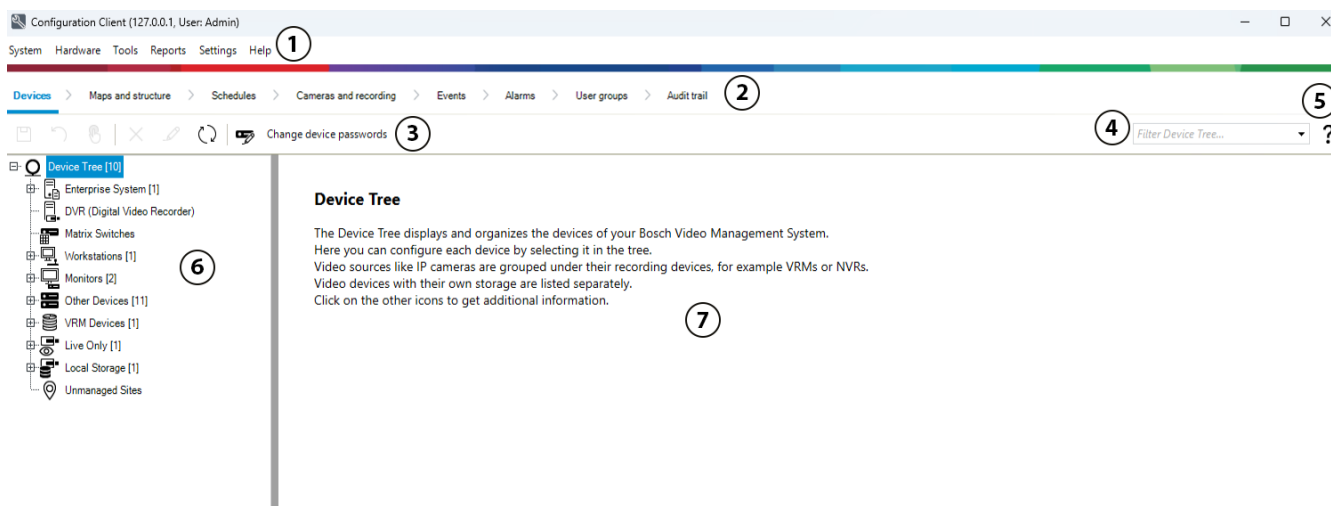
- Zainstalować usługi (Management Server i VRM)
- Zainstalować moduły Operator Client oraz Configuration Client.
- Połączyć się z siecią
- Dołączyć urządzenia do sieci
- Konfiguracja podstawowa:
 - Dodać urządzenia (np. przez polecenie skanowania).
 - Utworzyć strukturę logiczną.
 - Skonfigurować harmonogramy, kamery, zdarzenia i alarmy.
 - Skonfigurować grupy użytkowników

BVMS Configuration Client

Program Configuration Client systemu BVMS pozwala rozpocząć konfigurowanie urządzeń i następnie skonfigurować drzewo logiczne. Po wykonaniu tych dwóch kroków na odpowiednich kartach można skonfigurować harmonogramy, nagrania, zdarzenia i alarmy dla urządzeń. Ostatni krok polega na skonfigurowaniu grup użytkowników na karcie grup użytkowników. Po skonfigurowaniu wszystkich kart od lewej do prawej wszystko jest skonfigurowane i operator może zacząć korzystać z programu Operator Client.

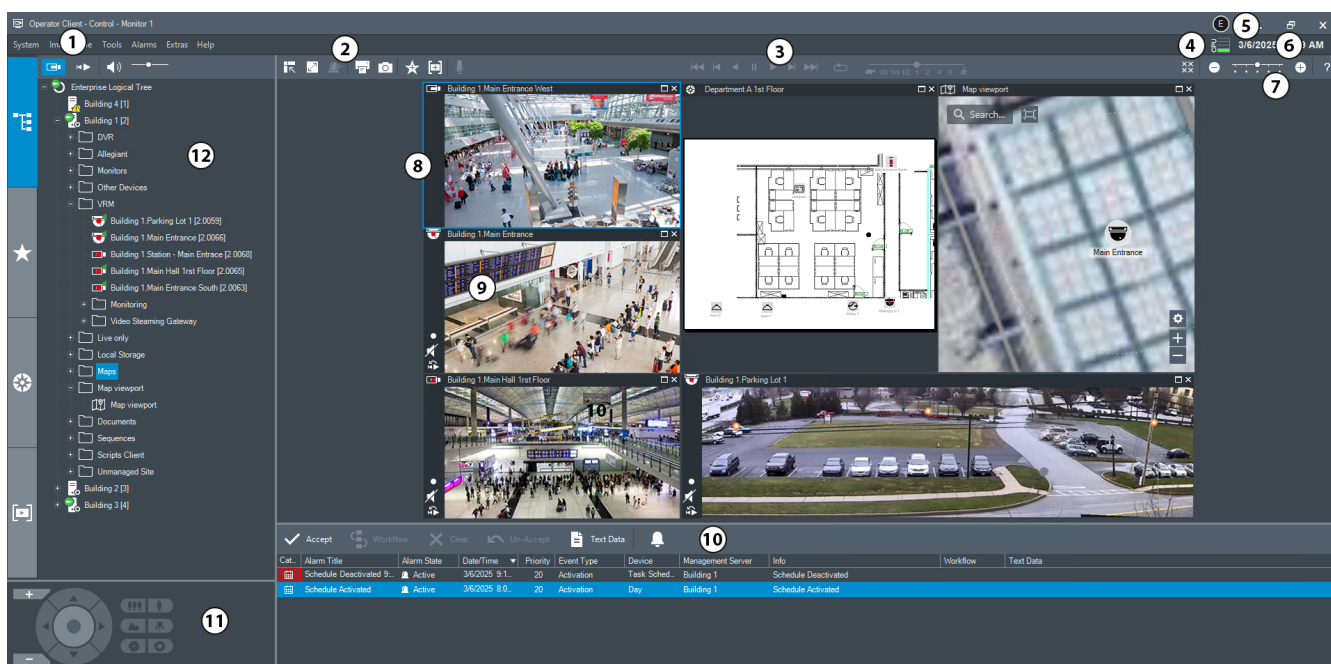
Po skonfigurowaniu każdej z kart należy zapisać konfigurację, klikając przycisk  w menu Narzędzia.

Aby wyświetlić zmiany w programie BVMS Operator Client, kliknąć  .



1	Pasek menu	Umożliwia wybór polecenia z menu.
2	Pasek kart	Umożliwia skonfigurowanie wszystkich koniecznych etapów procesu od lewej do prawej.
3	Pasek narzędzi	Zawiera dostępne przyciski zależne do aktywnej karty. Umieszczenie wskaźnika myszy na ikonie umożliwia wyświetlenie informacji o określonym narzędziu.
4	Pasek wyszukiwania	Umożliwia wyszukiwanie określonego urządzenia i odpowiadających mu elementów nadrzędnych w drzewie urządzeń.
5	Ikona pomocy	Wyświetla pomoc online do programu BVMS Configuration Client.
6	Okno wyboru	Hierarchiczna lista wszystkich urządzeń dostępnych w systemie.
7	Okno konfiguracji	Umożliwia skonfigurowanie wybranego urządzenia.

BVMS Operator Client



1	Pasek menu	Umożliwia wybór polecenia z menu.
2	Pasek narzędzi	Wyświetla dostępne przyciski. Przesunięcie wskaźnika myszy na ikonę umożliwia wyświetlenie informacji o określonym narzędziu.
3	Pulpit odtwarzania	Umożliwia sterowanie natychmiastowym odtwarzaniem obrazu, sekwencją kamery lub sekwencją alarmów.
4	Wskaźnik obciążenia systemu	Wyświetla wykorzystanie procesora.
5	Ikona logowania użytkownika	Wyświetla pierwszą literę nazwy zalogowanego użytkownika. Po najechaniu kursorem na ikonę wyświetlana jest nazwa użytkownika i odpowiadająca jej grupa użytkowników. Jeśli skonfigurowano tę opcję w Configuration Client, wyświetlana jest również pełna nazwa i opis użytkownika (dostępne tylko dla użytkowników zalogowanych jako BVMS). Opcja jest niedostępna dla użytkowników zalogowanych jako Windows, LDAP lub przez zewnętrznego Identity provider). W przypadku podwójnej autoryzacji wyświetlana jest ikona logowania dla każdego zalogowanego użytkownika, pokazująca informacje o nim oraz odpowiednią grupę podwójnej autoryzacji.
6	Wybór strefy czasowej	Umożliwia wybranie wpisu strefy czasowej, która będzie wyświetlana w większości pól związanych z czasem. Opcja dostępna tylko wtedy, gdy przynajmniej jeden serwer Management Server lub jedna unmanaged site w drzewie logicznym znajduje się w innej strefie czasowej niż komputer z programem Operator Client.
7	Elementy sterujące w okienkach obrazu	Umożliwiają wybór niezbędnej liczby okienek obrazu oraz zamykanie ich wszystkich naraz.
8	Okno obrazu	Umożliwia wyświetlanie okienek obrazu. Umożliwia rozmieszczenie okienek obrazu.
9	Okienko obrazu	Umożliwia wyświetlenie obrazu z kamery, mapy, obrazu lub dokumentu (pliku HTML).
10	 Okno Lista alarmów	Wyświetla wszystkie alarmy generowane przez system. Umożliwia zaakceptowanie lub zresetowanie alarmu albo uruchomienie procesu, na przykład przez wysłanie wiadomości e-mail do osoby zajmującej się obsługą systemu. Lista alarmów nie jest wyświetlana, gdy zostanie utracone połączenie z serwerem Management Server.
11	 Okno Sterowanie PTZ	Umożliwia sterowanie kamerą PTZ.

12	 Okno Drzewo logiczne	Wyświetla urządzenia, do których ma dostęp dana grupa użytkowników. Umożliwia wybranie urządzenia w celu przypisania go do okienka obrazu.
	 Okno Drzewo Ulubionych	Umożliwia uporządkowanie w żądany sposób urządzeń w oknie Drzewo logiczne.
	 Okno Znaczniki	Umożliwia zarządzanie znacznikami.
	 Okno Mapa	Wyświetla mapę obszaru. Umożliwia przeciągnięcie mapy w celu wyświetlenia określonego jej fragmentu. Jeśli jest włączone, mapa jest wyświetlana automatycznie dla każdej kamery, z której obraz pojawia się w okienku obrazu. W tym przypadku kamera musi być skonfigurowana na mapie.

3.1

Wersje BVMS

Różne wersje BVMS zapewniają pełną skalowalność, co pozwala na rozbudowę systemu dozorowego w zależności od potrzeb.

Dostępne są następujące wersje BVMS:

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

BVMS Viewer i BVMS Professional są produktami dostępnymi wyłącznie w postaci oprogramowania.

Nie można ich używać na urządzeniach Bosch DIVAR IP.

Systemy BVMS Lite i BVMS Plus mogą być używane na urządzeniach Bosch DIVAR IP lub jako samo oprogramowanie na dowolnym innym sprzęcie

Szczegółowe informacje na temat poszczególnych wersji BVMS można znaleźć w witrynie

www.boschsecurity.com oraz w Skróconym poradniku wyboru BVMS:

[Skrócony poradnik wyboru systemu BVMS.](#)

3.2

Omówienie aktywacji licencji systemu BVMS

W tym rozdziale omówiono sposób aktywacji licencji systemu BVMS.

Zamawianie licencji

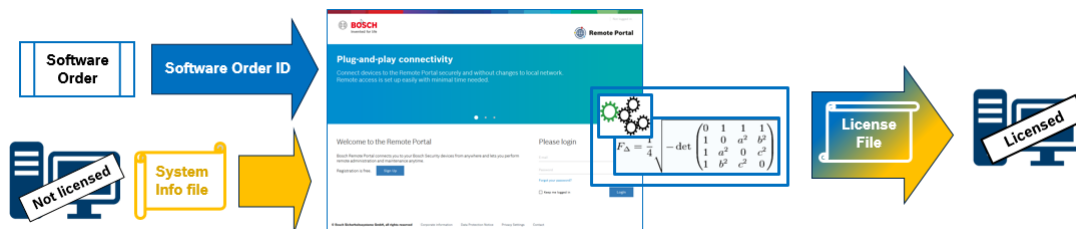
- Licencję należy zamówić za pośrednictwem działu zamówień Bosch.
- W potwierdzeniu zamówienia znajduje się nowy identyfikator zamówienia oprogramowania, który będzie wymagany do późniejszej aktywacji oprogramowania.
- Od wersji BVMS 11.0 licencje podstawowe i rozszerzające na system BVMS nie są już zależne od wersji.

Aktywacja licencji

- W miejsce Bosch Remote Portal (<https://www.remote.boschsecurity.com>) wprowadzono rozwiązanie Bosch **Manager licencji**.
- Wymaga jest rejestracja nowego użytkownika w Bosch Remote Portal.

- W celu aktywacji licencji obowiązkowe jest przekazanie pliku z informacjami o systemie oraz identyfikatora zamówienia oprogramowania.
- W wyniku tej operacji Remote Portal udostępni plik licencji i szczegółowe instrukcje dotyczące aktywacji. Ten plik licencji należy umieścić w zainstalowanym systemie BVMS.
- Proces aktywacji określa datę rozpoczęcia okresu obowiązywania usługi Software Assurance. Data zakończenia świadczenia tej usługi jest widoczna w obszarze **Manager licencji** programu BVMS Configuration Client.

Proces aktywacji licencji na oprogramowanie



Aby aktywować licencje na oprogramowanie, należy wykonać następujące czynności:

1. Zamówienie oprogramowania
 - Zamówić oprogramowanie zgodnie ze standardowym procesem zamawiania Bosch.
 - Zamówienia na oprogramowanie mogą obejmować jeden lub wiele produktów w jednej wersji lub wielu wersjach.
2. Odebranie identyfikatora zamówienia oprogramowania
 - Wynikiem zamówienia jest potwierdzenie zamówienia oprogramowania zawierające identyfikator zamówienia oprogramowania.
 - Identyfikator zamówienia oprogramowania umożliwia podłączenie zainstalowanego oprogramowania (w systemie operacyjnym i sprzęcie) do zamówionych produktów.
3. Aktywacja licencji
 - Do aktywacji licencji konieczne jest podanie pliku z informacjami o systemie odpowiadający unikalnej kombinacji systemu operacyjnego i sprzętu, na którym zainstalowane jest oprogramowanie.
 - W wyniku aktywacji następuje połączenie identyfikatora zamówienia oprogramowania z zainstalowanym oprogramowaniem oraz utworzenie pliku licencyjnego.
 - Aktywacja definiuje atrybuty systemu, takie jak data rozpoczęcia i zakończenia okresu świadczenia usługi Software Assurance.
4. Aktywacja oprogramowania
 - W celu aktywacji oprogramowania należy dodać plik licencyjny do zainstalowanego oprogramowania.
 - Pliki licencji pozwalają korzystać z funkcji systemu BVMS w zależności od tego, które elementy zostały aktywowane.

Uwaga!



Plik licencyjny zawiera następujące dane aktywacyjne:

- wersja produktu BVMS
- dozwolona wersja BVMS
- data wygaśnięcia dostępu do usługi Software Assurance
- Liczba licencji rozszerzających lub na funkcje

Patrz

- Aktywacja licencji na oprogramowanie, Strona 75

4 Ogólne informacje o systemie



Uwaga!

W niniejszym dokumencie opisano niektóre funkcje, które nie są dostępne w programie BVMS Viewer.

Szczegółowe informacje na temat poszczególnych wersji systemu BVMS znajdują się na stronie www.boschsecurity.com oraz w Skróconym poradniku wyboru systemu BVMS: [Skrócony poradnik wyboru systemu BVMS](#).

Jeżeli użytkownik ma zamiar instalować i konfigurować system BVMS, powinien wziąć udział w szkoleniu dotyczącym systemu BVMS.

Informacje na temat obsługiwanych wersji oprogramowania układowego i sprzętu oraz inne ważne dane znajdują się w Informacjach o wersji dotyczących najnowszej aktualizacji systemu BVMS.

Informacje na temat komputerów, na których można zainstalować system BVMS, znajdują się w arkuszach danych stacji roboczych i serwerów firmy Bosch.

W jednym komputerze można opcjonalnie zainstalować następujące moduły oprogramowania BVMS.

Ważne komponenty

Element	Opis
Management Server (do wybrania w ustawieniach)	Zarządzanie strumieniami danych, zarządzanie alarmami, zarządzanie priorytetami, zarządzanie rejestrem, zarządzanie użytkownikami, zarządzanie stanem urządzeń. Dodatkowa licencja Enterprise System: zarządzanie grupami użytkowników Enterprise User Group i kontami Enterprise Account.
Config Wizard	Łatwa i szybka konfiguracja systemu zapisu.
Configuration Client (do wybrania w ustawieniach)	Konfiguracja systemu i administracja systemem dla modułu Operator Client.
Operator Client (do wybrania w ustawieniach)	Monitorowanie na żywo, przeglądanie i odtwarzanie nagrań, alarmy i jednoczesny dostęp do wielu komputerów typu Management Server.
Video Recording Manager (do wybrania w ustawieniach)	Przekazywanie do nadajników informacji o dostępnych pojemnościach urządzeń iSCSI, przy jednoczesnym zapewnieniu zrównoważenia obciążenia pomiędzy wieloma urządzeniami iSCSI. Strumieniowe odtwarzanie danych audio i wideo z urządzeń iSCSI w programach Operator Client.
Web Client	Do podglądu obrazów na żywo oraz ich odtwarzania można używać przeglądarki Internetowej.
Aplikacja mobilna	Aplikacja mobilna umożliwia urządzeniom iPhone i iPad dostęp do podglądu obrazów na żywo oraz ich odtwarzania.
Bosch Video Streaming Gateway (do wybrania w ustawieniach)	Umożliwia integrację kamer innych producentów, na przykład z sieciami o małej szerokości pasma.
Cameo SDK (do wybrania w ustawieniach)	Zestaw Cameo SDK umożliwia osadzanie pochodzących z systemu BVMS okienek obrazów wyświetlanych na żywo i odtwarzanych w zewnętrznych aplikacjach innych firm. Do Okienek obrazu mają zastosowanie uprawnienia użytkownika w

Element	Opis
	systemie BVMS. Zestaw Cameo SDK oferuje podzbiór funkcji BVMS Operator Client umożliwiających tworzenie aplikacji zbliżonych do programu Operator Client.
Client Enterprise SDK	Zestaw Client Enterprise SDK umożliwia kontrolowanie i monitorowanie zachowania aplikacji Operator Client systemu Enterprise System przez aplikacje zewnętrzne. Zestaw SDK umożliwia przeglądanie urządzeń dostępnych poprzez działające, połączone programy Operator Client oraz sterowanie pewnymi funkcjami interfejsu użytkownika.
Client SDK / Server SDK	Zestaw Server SDK umożliwia kontrolowanie i monitorowanie serwera Management Server za pomocą skryptów i aplikacji zewnętrznych. Korzystanie z tych interfejsów jest możliwe przy użyciu ważnego konta administratora. Zestaw Client SDK umożliwia kontrolę i monitorowanie programu Operator Client za pomocą zewnętrznych aplikacji i skryptów (w ramach powiązanej konfiguracji serwera).

4.1 Wymagania sprzętowe

Zapoznać się z arkuszem danych BVMS. Dostępne są także karty katalogowe dotyczące platform komputerowych.

4.2 Wymagania w zakresie oprogramowania

Nie można zainstalować aplikacji BVMS Viewer w miejscu, w którym zainstalowany jest jakikolwiek inny komponent BVMS.

Zapoznać się z arkuszem danych BVMS.

4.3 Wymagania licencyjne

Zapoznać się z arkuszem danych BVMS w celu uzyskania informacji o dostępnych licencjach.

5 Pojęcia



Uwaga!

Program BVMS Viewer zapewnia tylko podstawowe funkcje. Funkcje zaawansowane udostępnia program BVMS Professional. Aby uzyskać szczegółowe informacje na temat różnych wersji systemu BVMS, należy odwiedzić witrynę www.boschsecurity.com i zobaczyć skrócony poradnik wyboru systemu BVMS: [Skrócony poradnik wyboru systemu BVMS](#).

Niniejszy rozdział zawiera podstawowe informacje na temat wybranych zagadnień.

5.1 Założenia projektowe systemu BVMS

Jeden system Management Server, Strona 24

Pojedynczy system BVMS Management Server umożliwia zarządzanie, monitorowanie i sterowanie nawet 2000 kamer/nadajników.

Enterprise System., Strona 25

Enterprise Management Server zapewnia jednoczesny dostęp do wielu jednostek typu Management Servers. Enterprise System zapewnia pełny dostęp do zdarzeń i alarmów z poziomu wielu podsystemów.

Server Lookup, Strona 26

Funkcja Server Lookup służy do wyświetlenia listy serwerów BVMS Management Servers dostępnych dla klienta BVMS Operator Client. Operator może wybrać serwer z listy dostępnych serwerów. Klient połączony z serwerem Management Server ma pełny dostęp do serwera Management Server.

Unmanaged site, Strona 28

Urządzenia można pogrupować w unmanaged sites. Urządzenia w unmanaged sites nie będą monitorowane przez Management Server. Management Server zawiera listę unmanaged sites dla klienta Operator Client. Operator może połączyć się na żądanie z lokalizacją i uzyskać dostęp do podglądu danych wideo na żywo oraz do zarejestrowanych danych wideo. Koncepcja unmanaged site nie uwzględnia obsługi zdarzeń ani alarmów.

5.1.1 Jeden system Management Server

- Pojedynczy BVMS Management Server może zarządzać nawet 2000 kanałów.
- BVMS Management Server umożliwia zarządzanie i sterowanie całym systemem oraz monitorowanie go.
- BVMS Operator Client jest podłączony do serwera Management Server i odbiera zdarzenia oraz alarmy z serwera BVMS Management Server, a także umożliwia wyświetlanie na żywo i odtwarzanie.
- W większości przypadków wszystkie urządzenia znajdują się w jednej sieci lokalnej o dużej szerokości pasma i małym opóźnieniu.

Zadania:

- Konfigurowanie danych
- Rejestr zdarzeń (dziennik zdarzeń)
- Profile użytkowników
- Priorytety użytkowników
- Licencjonowanie
- Zarządzanie zdarzeniami i alarmami

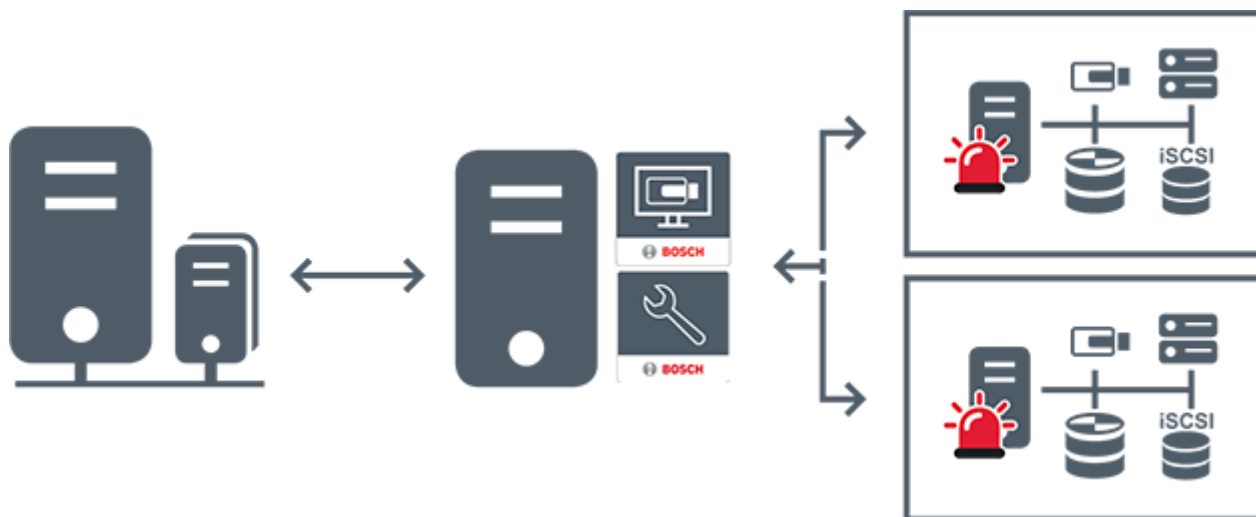


	Wyświetlanie na żywo, odtwarzanie, zdarzenia, alarmy
	Management Server
	Operator Client / Configuration Client
	Kamery
	VRM
	iSCSI
	Inne urządzenia

5.1.2

Enterprise System.

- Celem systemu BVMS Enterprise System jest zapewnienie użytkownikowi klienta Operator Client jednoczesnego dostępu do wielu serwerów Management Servers (podsystemów).
- Stacje klienckie połączone z serwerem Enterprise posiadają pełny dostęp do wszystkich kamer i nagrań z podsystemów.
- Stacje klienckie połączone z serwerem Enterprise posiadają pełne dane na temat stanu zdarzeń i alarmów we wszystkich podsystemach w czasie rzeczywistym.
- Typowe obszary zastosowań:
 - Metra
 - Lotniska



	Wyświetlanie na żywo, odtwarzanie, zdarzenia, alarmy
	BVMS Enterprise Management Server
	BVMS Operator Client / Configuration Client
	Podsystem BVMS

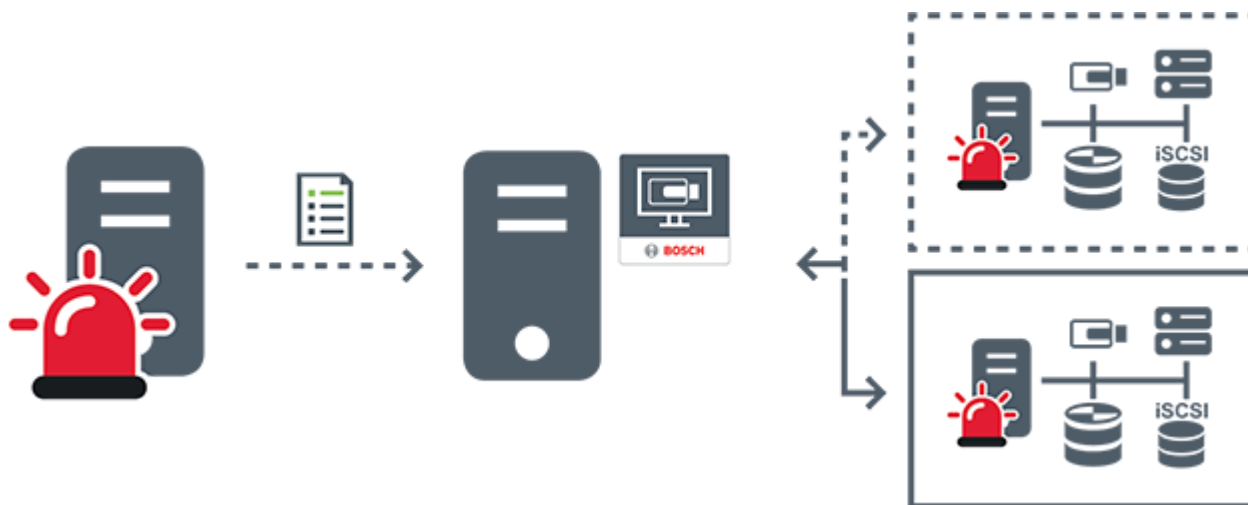
Patrz

- Tworzenie Enterprise System, Strona 85
- Konfigurowanie funkcji listy serwerów dla systemu Enterprise System, Strona 85
- Konfigurowanie użytkowników, uprawnień i dostępu Enterprise, Strona 351
- Dostęp do systemu, Strona 74

5.1.3**Server Lookup**

- Funkcja BVMS Server Lookup umożliwia operatorom nawiązywanie połączenia z serwerem BVMS Management Server wybranym z podanej listy serwerów.
- Pojedynczy użytkownik programu Configuration Client lub Operator Client może kolejno nawiązywać połączenia z wieloma punktami dostępowymi systemu.
- Punktami dostępowymi systemu mogą być serwery Management Server i Enterprise Management Server.
- Funkcja Server Lookup wykorzystuje dedykowany serwer Management Server do obsługi listy serwerów.
- Funkcje Server Lookup oraz Management Server lub Enterprise Management Server mogą być uruchomione na jednym komputerze.
- Program Server Lookup umożliwia odszukiwanie punktów dostępowych systemu na podstawie ich nazw lub opisów.

- Po podłączeniu do serwera Management Server program Operator Client odbiera alarmy i zdarzenia z serwera BVMS Management Server i umożliwia wyświetlanie danych na żywo lub ich odtwarzanie



	Na żądanie na żywo, odtwarzanie, zdarzenia, alarmy — podłączony
	Na żądanie na żywo, odtwarzanie, zdarzenia, alarmy — niepodłączony
	Management Server
	Lista serwerów
	Operator Client
	Podłączony system BVMS z listy serwerów
	Niepodłączony system BVMS z listy serwerów

Patrz

- Konfigurowanie funkcji Server Lookup, Strona 129
- Strona listy serwerów/książki adresowej, Strona 128
- Używanie funkcji Server Lookup, Strona 74
- Eksportowanie listy serwerów, Strona 130
- Importowanie listy serwerów, Strona 130

5.1.4

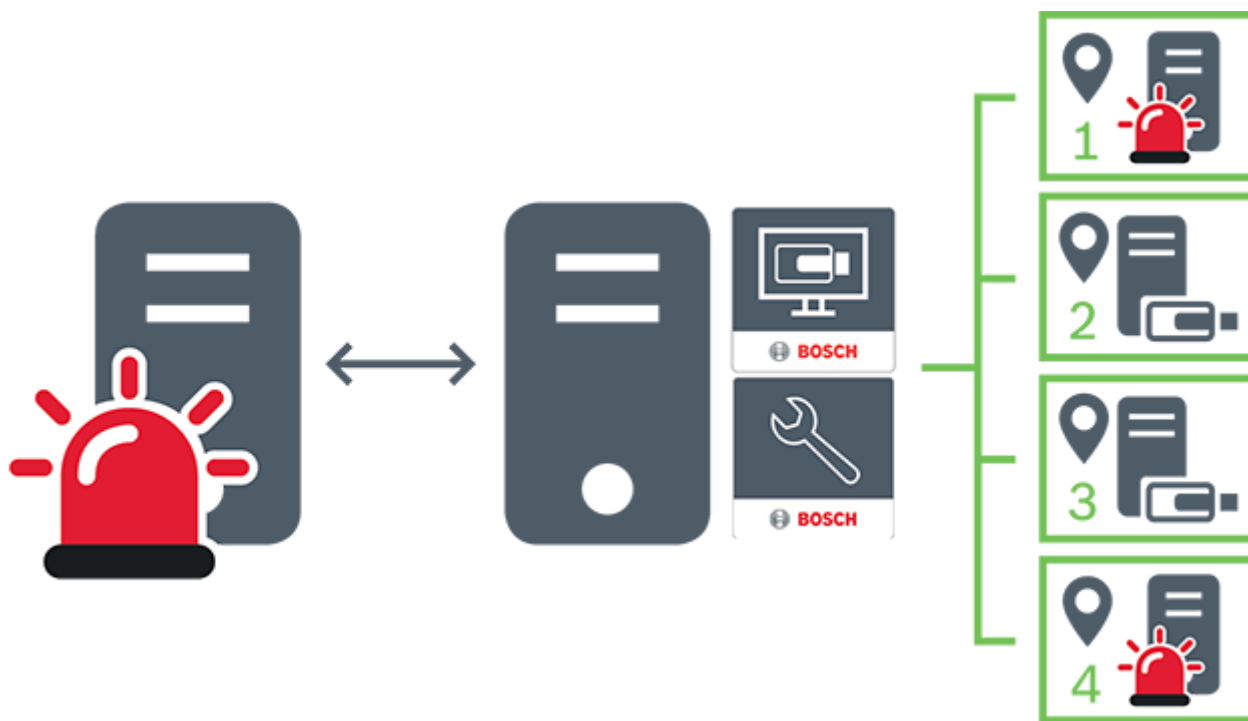
Unmanaged site

- Opcja projektu systemu w systemie BVMS o dużej liczbie małych podsystemów.
- Umożliwia skonfigurowanie maksymalnie 9999 lokalizacji na jednym serwerze BVMS Management Server.
- Operatorzy mogą korzystać z dostępu do danych wizyjnych na żywo lub z nagrań z maksymalnie 20 sites jednocześnie.
- W celu ułatwienia nawigacji lokalizacje sites można pogrupować w foldery lub umieścić na mapach. Wstępnie zdefiniowane nazwa użytkownika i hasło ułatwiają operatorom szybkie nawiązywanie połączenia z lokalizacją site.

Koncepcja unmanaged site obsługuje systemy BVMS oparte na IP, a także analogiczne rozwiązania DVR:

- Rejestratory analogowe Bosch DIVAR AN 3000/5000.
- rejestratory DIVAR hybrid,
- rejestratory DIVAR network,
- Rejestracja w oparciu o IP za pomocą jednostek DIP 3000/7000.
- Pojedynczy system serwera BVMS Management Server.

Aby dodać lokalizację site do lokalizacji monitorowanych centralnie, konieczna jest licencja (jedna) na lokalizację site, niezależnie od liczby kanałów w danej lokalizacji site.



	Wyświetlanie na żywo, odtwarzanie, zdarzenia, alarmy
	Ruch związany z podglądem na żywo na żądanie i odtwarzaniem wideo
	Management Server

	Operator Client / Configuration Client
	site
	DVR

Patrz

– Ręczne dodawanie lokalizacji *unmanaged site*, Strona 212

5.2**Zapis**

W tym rozdziale wyjaśniono różne funkcje związane z nagrywaniem i odtwarzaniem w systemie.

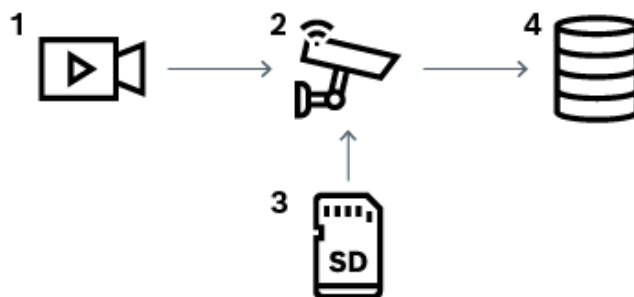
5.2.1**Automatyczne uzupełnianie sieciowe (Automated Network Replenishment, ANR)****Uwaga!**

Program BVMS Viewer zapewnia tylko podstawowe funkcje. Funkcje zaawansowane udostępnia program BVMS Professional. Aby uzyskać szczegółowe informacje na temat różnych wersji systemu BVMS, należy odwiedzić witrynę www.boschsecurity.com i zobaczyć skrócony poradnik wyboru systemu BVMS: [Skrócony poradnik wyboru systemu BVMS](#).

Przeznaczenie

W przypadku awarii sieci lub centralnego systemu zapisu funkcja ANR zapewnia, że nadajnik przekaże lokalnie buforowane dane z okresu trwania awarii do centralnego systemu zapisu po jej usunięciu.

Poniższy rysunek przedstawia przesyłanie danych wideo po usunięciu awarii sieci lub systemu zapisu.



1	Sygnał wizyjny
2	Koder, sieć IP
3	Karta SD (bufor pierścieniowy)

4	Docelowy iSCSI (centralny system zapisu)

Przykład: działanie w przypadku awarii sieci

Jeśli sieć ulegnie niespodziewanej awarii, funkcja ANR uzupełni centralny system zapisu zbuforowanymi lokalnie zapisami, gdy sieć będzie ponownie dostępna.

Przykład: zapisywanie danych wideo, gdy sieć jest niedostępna

Pociąg metra nie ma połączenia z centralnym systemem zapisu, gdy znajduje się pomiędzy stacjami. Zbuforowane dane mogą być przesłane do centralnego systemu zapisu tylko podczas normalnego zatrzymania się na stacji.

Należy upewnić się, że czas wymagany do przesłania zbuforowanych danych nie przekracza czasu postoju.

Przykład: funkcja ANR do zapisu alarmowego

Zapis przed wystąpieniem alarmu jest zapamiętywany lokalnie. Zapis przed wystąpieniem alarmu jest przesyłany do centralnego systemu zapisu tylko w przypadku wystąpienia alarmu. Jeśli nie wystąpi żaden alarm, nieaktualne zapisy sprzed wystąpienia alarmu nie są przesyłane do centralnego systemu zapisu i nie obciążają sieci.

Ograniczenia**Uwaga!**

Jeśli nadajnik ma ustawione hasła dla użytkownika i danych na żywo, nie można przesłać danych zapisanych na lokalnym nośniku. W razie potrzeby należy usunąć te hasła.

Funkcja ANR działa tylko z zapisem VRM.

Funkcja ANR nie działa z nadajnikiem, w którego przypadku skonfigurowano bezpieczne połączenie do wyświetlania obrazu na żywo.

Aby użyć funkcji ANR, należy skonfigurować nośnik zapisu nadajnika.

Nadajnik konfigurowany do użycia funkcji ANR musi mieć wersję oprogramowania układowego 5.90 lub nowszą. Nie wszystkie rodzaje nadajników obsługują funkcję ANR.

Funkcji ANR nie można używać w przypadku stosowania zapisu podwójnego.

System zapisu iSCSI musi być odpowiednio skonfigurowany.

Poniżej przedstawiono możliwe przyczyny braku możliwości skonfigurowania funkcji ANR:

- Nadajnik jest niedostępny (zły adres IP, awaria sieci itd.).
- Nośnik zapisu nadajnika jest niedostępny lub tylko do odczytu.
- Zła wersja oprogramowania układowego.
- Nadajnik nie obsługuje funkcji ANR.
- Zapis podwójny jest aktywny.

Patrz

- Konfiguracja urządzenia iSCSI, Strona 192
- Konfigurowanie nośnika zapisu nadajnika, Strona 84
- Konfigurowanie funkcji ANR, Strona 302

5.2.2**Zapis podwójny / awaryjny****Przeznaczenie**

Główny VRM zarządza zapisem z kamer działających w systemie. Programu pomocniczego VRM używa się do podwójnego zapisu obrazów z kamery.

Podwójny zapis pozwala zapisywać dane wideo z jednej kamery w różnych lokalizacjach.

Zapisu podwójnego używa się zwykle w przypadku różnych ustawień strumienia i trybów zapisywania. Specjalnym przypadkiem podwójnego zapisu jest zapisywanie nadmiarowe, tzn. nagrywanie tego samego sygnału wizyjnego w różnych miejscach.

Zapisywanie podwójne jest wykonywane przy użyciu 2 serwerów VRM zarządzających wieloma urządzeniami iSCSI, które mogą być umieszczone w różnych lokalizacjach.

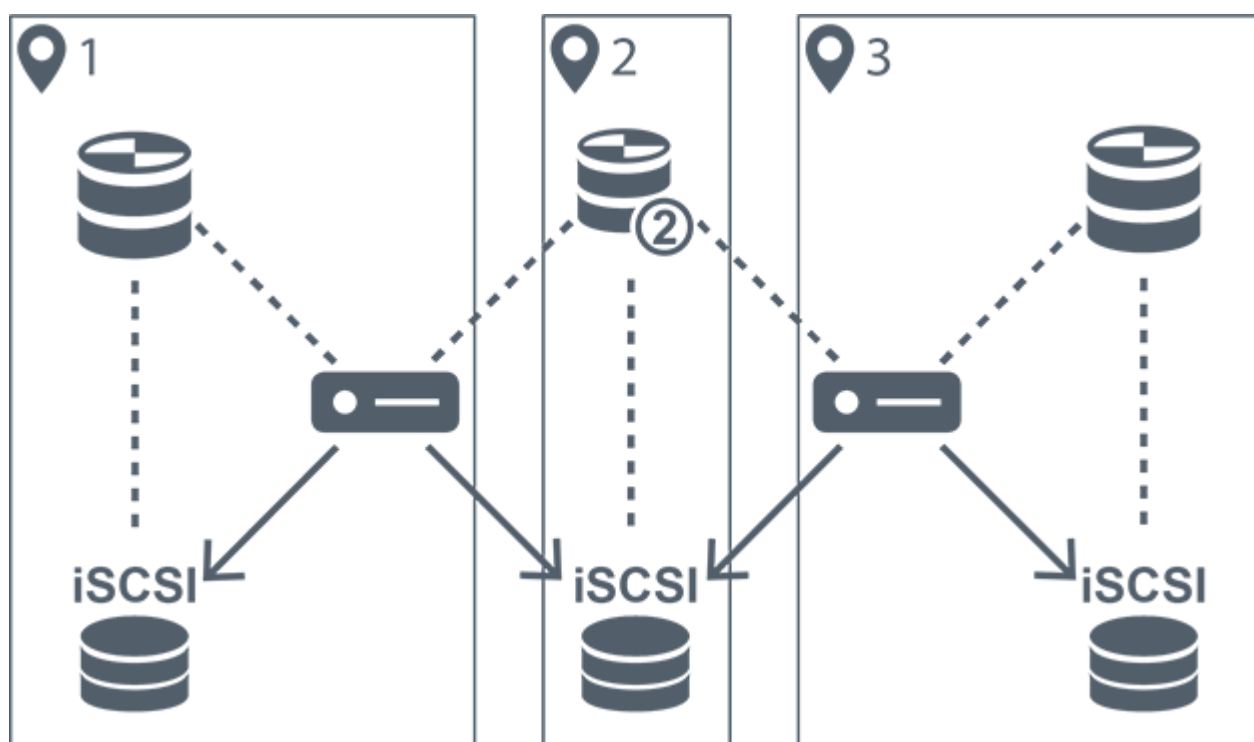
Pomocniczy VRM może zarządzać drugim zapisywaniem w wielu podstawowych VRM.

Użytkownik może wybierać pomiędzy zapisywaniem zarządzanym przez podstawowy lub pomocniczy VRM. W przypadku pojedynczej kamery użytkownik może przełączać na zapisywanie przez pomocniczy/podstawowy VRM. Może także wyświetlać równocześnie zapisy z tej samej kamery zarządzanej przez podstawowy i pomocniczy VRM.

Aby umożliwić zapis podwójny, należy podczas konfiguracji zainstalować pomocniczy VRM.

Awaryjny VRM jest używany, aby kontynuować zapis po awarii podstawowego VRM lub pomocniczego komputera VRM.

Poniższy rysunek przedstawia przykład scenariusza podwójnego zapisu:



1	Lokalizacja 1		Nadajnik
2	Lokalizacja centralna		Urządzenie pamięci masowej iSCSI
3	Lokalizacja 2		Złącze sterowania
	Główny rejestrator VRM		Strumień wizyjny
	Pomocniczy VRM		

Ograniczenia

Podwójnego zapisu nie można używać przy stosowaniu funkcji ANR.

Urządzenie Cameo SDK obsługuje tylko odtwarzanie z zapisu podstawowego.

Patrz

- Konfigurowanie podwójnego zapisu w tabeli kamery, Strona 303
- Dodawanie nadmiarowego urządzenia VRM, Strona 176
- Ręczne dodawanie awaryjnego VRM, Strona 175
- strona Kamery, Strona 285

5.2.3

Tryby zapisu VRM

W tym rozdziale są przedstawione rysunki ilustrujące możliwe tryby zapisu VRM.

Lista możliwych trybów zapisu VRM:

- Zapis podstawowy VRM
- Zapis na nadmiarowym VRM
- Zapis pomocniczy VRM
- Zapis awaryjny VRM

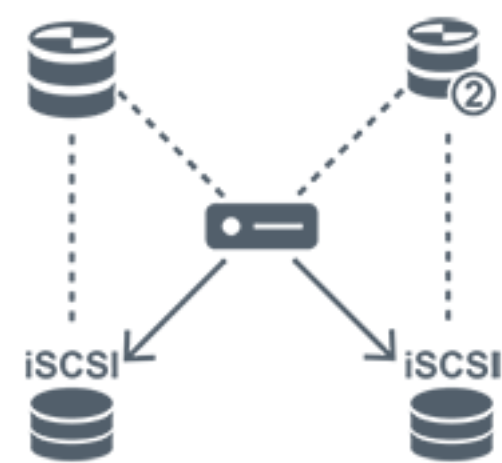
Informacje o zapisie ANR są podane w rozdziale Automatyczne uzupełnianie sieciowe (Automated Network Replenishment, ANR), Strona 29.

Zapis podstawowy VRM



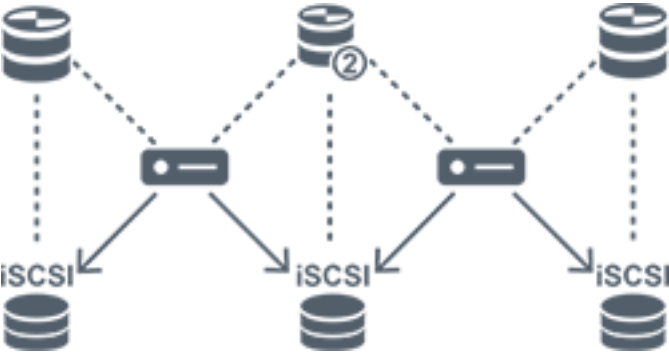
	Główny rejestrator VRM		Złącze sterowania
	Urządzenie pamięci masowej iSCSI		Strumień wizyjny
	Nadajnik		

Zapis na nadmiarowym VRM



	Główny rejestrator VRM		Pomocniczy VRM
	Urządzenie pamięci masowej iSCSI		Złącze sterowania
	Nadajnik	→	Strumień wizyjny

Zapis pomocniczy VRM



	Główny rejestrator VRM		Pomocniczy VRM
	Urządzenie pamięci masowej iSCSI		Złącze sterowania
	Nadajnik	→	Strumień wizyjny

Zapis awaryjny VRM



	Główny rejestrator VRM		Podstawowy awaryjny VRM
	Urządzenie pamięci masowej iSCSI		Nadajnik
-----	Złącze sterowania	→	Strumień wizyjny

5.2.4

Odtwarzanie zapisanych źródeł VRM

Poniższe rysunki przedstawiają okienka obrazu z odtworzonymi wszystkimi możliwymi źródłami VRM. Na każdym rysunku jako przykład odtwarzania przedstawiono urządzenie pamięci masowej, instancję programu VRM (jeśli jest dostępna) i fragment okienka obrazu. Jeśli to możliwe, źródło zapisu jest przedstawione w postaci odpowiedniej ikony na pasku okienka obrazu.

- Odtwarzanie zapisu pojedynczego, Strona 34
- Odtwarzanie podwójnego zapisu VRM, Strona 35
- Odtwarzanie podstawowego zapisu VRM z awaryjnym VRM, Strona 35
- Odtwarzanie pomocniczego zapisu VRM z awaryjnym VRM, Strona 36
- Automatyczne uzupełnianie sieciowe (Automatic Network Replenishment), Strona 37

Odtwarzanie zapisu pojedynczego

To okienko obrazu pojawia się, gdy tylko podstawowy VRM jest skonfigurowany. Nie można wybrać innego źródła nagrania.

-----> W przypadku konfiguracji dla tej stacji roboczej odtwarzanie jest wykonywane bezpośrednio przez urządzenie pamięci masowej iSCSI.



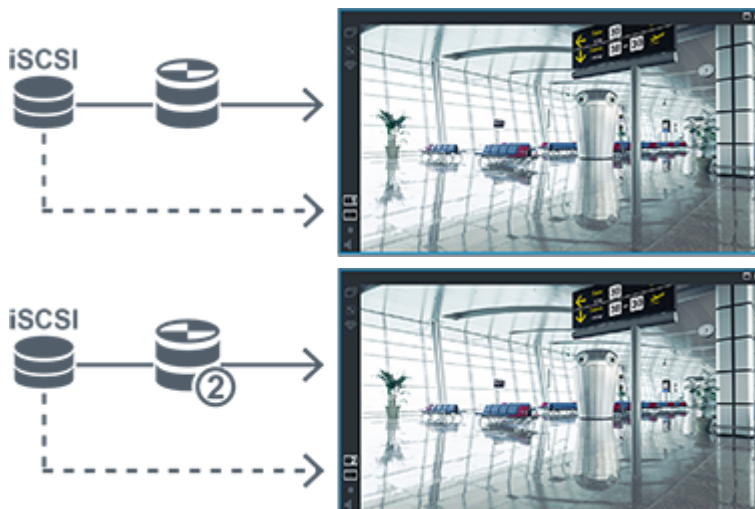
	Urządzenie pamięci masowej iSCSI

	Główny rejestrator VRM

Odtwarzanie podwójnego zapisu VRM

Skonfigurowany jest podstawowy VRM i pomocniczy VRM. Kliknij ikonę źródła zapisu, aby wyświetlić podstawowe i pomocnicze odtwarzanie.

W przypadku konfiguracji dla tej stacji roboczej odtwarzanie jest wykonywane bezpośrednio przez urządzenie pamięci masowej iSCSI.



	Urządzenie pamięci masowej iSCSI
	Główny rejestrator VRM
	Pomocniczy VRM

Odtwarzanie podstawowego zapisu VRM z awaryjnym VRM

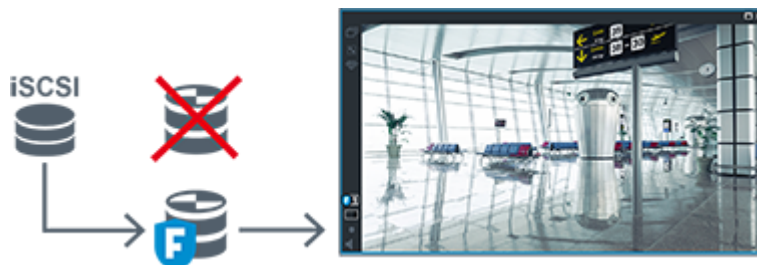
Gdy działa podstawowy VRM, wykonuje on też odtwarzanie. Awaryjny VRM działa tylko w stanie bezczynności.

W przypadku konfiguracji dla tej stacji roboczej odtwarzanie jest wykonywane bezpośrednio przez urządzenie pamięci masowej iSCSI.

Jeśli jest skonfigurowany pomocniczy VRM lub zapisywanie ANR, można przełączać źródła zapisu.



Jeśli podstawowy VRM nie jest podłączony, odtwarzanie jest wykonywane przez skonfigurowany awaryjny VRM. Zamknij to okienko obrazu i ponownie wyświetl obraz z kamery w jakimś okienku obrazu:



Jeśli nie jest podłączony ani podstawowy, ani opcjonalny awaryjny podstawowy VRM, odtwarzanie jest wykonywane przez nadajnik. Zamknij to okienko obrazu i ponownie wyświetl obraz z kamery w jakimś okienku obrazu:



	Urządzenie pamięci masowej iSCSI
	Główny rejestrator VRM
	Podstawowy awaryjny VRM
	Nadajnik

Odtwarzanie przez nadajnik dotyczy tylko ograniczonego czasu zapisu.

Odtwarzanie pomocniczego zapisu VRM z awaryjnym VRM

Gdy działa pomocniczy VRM, wykonuje on też odtwarzanie. Awaryjny VRM działa tylko w stanie bezczynności.

W przypadku konfiguracji dla tej stacji roboczej odtwarzanie jest wykonywane bezpośrednio przez urządzenie pamięci masowej iSCSI.



Jeśli pomocniczy VRM nie jest podłączony, odtwarzanie jest wykonywane przez skonfigurowany awaryjny VRM. Zamknij to okienko obrazu i ponownie wyświetl obraz z kamery w jakimś okienku obrazu:



Jeśli nie jest podłączony ani pomocniczy, ani opcjonalny awaryjny pomocniczy VRM, odtwarzanie jest wykonywane przez nadajnik. Zamknij to okienko obrazu i przeciągnij kamerę do jakiegoś okienka obrazu:



	Urządzenie pamięci masowej iSCSI
	Główny rejestrator VRM
	Pomocniczy awaryjny VRM
	Nadajnik

Odtwarzanie przez nadajnik dotyczy tylko ograniczonego czasu zapisu.

Automatyczne uzupełnianie sieciowe (Automatic Network Replenishment)

Skonfigurowana jest funkcja ANR. Kliknij ikonę źródła zapisu, aby wyświetlić odtwarzanie podstawowe (awaryjne odtwarzanie podstawowe, podstawowe odtwarzanie przez nadajnik) lub odtwarzanie ANR.

W przypadku konfiguracji dla tej stacji roboczej odtwarzanie jest wykonywane bezpośrednio przez urządzenie pamięci masowej iSCSI.





	Urządzenie pamięci masowej iSCSI
	Główny rejestrator VRM
	Karta SD

5.2.5

Przegląd zdarzeń związanych z przechowywaniem danych

W tym rozdziale opisano różne zdarzenia związane z przechowywaniem danych.

Stan magazynu buforowania

W przypadku awarii sieci lub centralnego systemu zapisu funkcja ANR zapewnia, że nadajnik przekaże lokalnie buforowane dane z okresu trwania awarii do centralnego systemu zapisu po jej usunięciu.

Możliwe stany pamięci bufora to:

- **Stan nośnika pamięci nieznany**
- **Stan magazynu OK**
- **Stan magazynu Krytyczny poziom zapełnienia buforu**
- **Stan nośnika pamięci - awaria**

Przepełnienie magazynu buforowania

To zdarzenie oznacza, że bufor pamięci jest zapełniony i nagrywane dane nie są już przesyłane do centralnej pamięci masowej.

Stan nośnika pamięci / Stan magazynu pomocniczego

Stan nośnika pamięci wskazuje stan połączenia między kamerą a centralną pamięcią masową.

Zdarzenie **Stan nośnika pamięci - awaria** jest wyzwalane w przypadku utraty przez kamerę łączności z centralną pamięcią masową. Jeśli brak łączności trwa tylko krótką chwilę, zdarzenie to nie musi oznaczać utraty danych wizyjnych.

Możliwe stany pamięci masowej to:

- **Stan nośnika pamięci nieznany**
- **Stan magazynu OK**
- **Stan nośnika pamięci - awaria**

Stan monitora zapisu / Stan pomocniczego monitora zapisu

To zdarzenie wskazuje, że nagrywanie jest monitorowane. Dopóki kamera może buforować zapis w pamięci RAM, nie jest wyzwalany żaden alarm. Zdarzenie **Stan monitora zapisu powoduje utratę zapisanych materiałów** jest wyzwalane tylko wtedy, gdy w ciągu dwóch ostatnich minut dane wizyjne nie mogą być dłużej buforowane w pamięci RAM i zostaną utracone. Zdarzenie to określa również czas, w którym nastąpiła utrata danych wizyjnych.

Możliwe stany monitora zapisu to:

- **Nieznany stan monitora zapisu**
- **Stan monitora zapisu prawidłowy**

- **Stan monitora zapisu powoduje utratę zapisanych materiałów**

Patrz

- *Automatyczne uzupełnianie sieciowe (Automated Network Replenishment, ANR), Strona 29*
- *Konfiguracja zdarzeń i alarmów, Strona 318*

5.3

Obsługa alarmów

Alarmy mogą być konfigurowane osobno w celu obsługi przez jedną lub więcej grup użytkowników. Kiedy wystąpi alarm, pojawia się on na liście alarmów wszystkich użytkowników w grupach użytkowników skonfigurowanych do odbioru tego typu alarmu. Kiedy jeden z tych użytkowników zaczyna obsługiwać alarm, znika on z listy alarmów pozostałych użytkowników.

Alarmy są wyświetlane na monitorze alarmowym stacji roboczej. Ten sposób działania został opisany w poniższych punktach.

Przebieg alarmów

1. Alarm jest wyzwalany w systemie.
2. Powiadomienie o alarmie pojawia się na liście alarmów wszystkich użytkowników skonfigurowanych do obsługi tego typu alarmu. Obraz alarmu jest niezwłocznie wyświetlany na skonfigurowanych monitorach. Jeśli jest to automatycznie wyświetlany alarm, obraz alarmu jest automatycznie wyświetlany na monitorach alarmowych stacji roboczej programu Operator Client.
Jeśli alarm jest skonfigurowany na automatyczne resetowanie, zostanie on usunięty z okna Lista alarmów po upływie czasu automatycznego resetowania (konfigurowanego w oknie Configuration Client).
Na monitorach każdy podgląd obrazu w widoku poczwórnym z nadajników VIP XD jest chwilowo zastępowany przez wyświetlanie pełnoekranowe.
3. Jeden z użytkowników akceptuje alarm. Obraz alarmowy jest następnie wyświetlany na stacji roboczej tego użytkownika (jeśli nie jest już wyświetlany za pomocą funkcji automatycznego wyświetlania). Alarm jest usuwany ze wszystkich list alarmów, a wyświetlanie obrazów alarmowych zostaje zakończone.
4. Użytkownik, który zaakceptował alarm, uruchamia sekwencję zadań, które mogą obejmować czytanie planu działania oraz wprowadzanie komentarzy. Ten krok jest opcjonalny – wymagania dotyczące sekwencji zadań mogą być konfigurowane przez administratora.
5. Na końcu użytkownik resetuje alarm. Spowoduje to usunięcie alarmu z listy alarmów oraz zakończenie wyświetlania obrazów alarmowych.
W grupie monitorów monitory powracają do wyświetlania obrazu z tych kamer, które znajdowały się w trybie podglądu przed wystąpieniem alarmu.

Okno obrazów alarmowych

1. Aby wyświetlić obraz alarmowy, okno obrazów alarmowych zastępuje okno obrazu w trybie podglądu bieżącego lub trybie odtwarzania na monitorze skonfigurowanym do wyświetlania alarmów.
2. Każdy alarm zajmuje rząd okien Okienko obrazu. Do każdego alarmu można przypisać maks. 5 okienek obrazu. Mogą one wyświetlać obraz bieżący, mapy lub odtwarzać obrazy.
W grupie monitorów każdy alarm może przywołać obraz z kamer w rzędzie monitorów. Liczba kamer w rzędzie jest ograniczona liczbą kolumn w grupie monitorów. Monitory w rzędzie, które nie są używane do podglądu obrazów alarmowych, mogą być skonfigurowane na wyświetlanie bieżącego obrazu lub pustego ekranu.
3. Alarmy o wyższym priorytecie są wyświetlane nad alarmami o niższym priorytecie zarówno w rzędach monitorów, jak i w rzędach monitorów alarmowych stacji roboczej programu Operator Client.

4. Jeśli okno obrazów alarmowych jest całkowicie wypełnione rzędami obrazów alarmowych, a musi być wyświetlony kolejny alarm, alarmy o najniższym priorytecie są grupowane w dolnym rzędzie okna obrazów alarmowych. Użytkownik może przełączać pomiędzy zgrupowanymi alarmami za pomocą elementów sterujących z lewej strony rzędu obrazów alarmowych. Użytkownik może przełączać pomiędzy zgrupowanymi alarmami w grupach monitorów alarmowych za pomocą przycisków sterujących w oknie **Monitory** monitora stacji roboczej programu Operator Client. Zaalarmowane monitory są oznaczone za pomocą czerwonych ikon z migającymi diodami LED.
Nazwa, godzina i data alarmu mogą być opcjonalnie wyświetlane na wszystkich monitorach lub tylko na pierwszym monitorze w rzędzie obrazów alarmowych.
5. Dla alarmów o takim samym priorytecie administrator może skonfigurować kolejność:
 - Tryb Last-in-First-out (LIFO): w tej konfiguracji nowe alarmy są wstawiane nad starszymi alarmami o takim samym priorytecie.
 - Tryb First-in-First-out (FIFO): w tej konfiguracji nowe alarmy są wstawiane pod starszymi alarmami o takim samym priorytecie.
6. Rząd obrazów alarmowych może pojawić się w oknie obrazów alarmowych w jeden z dwóch sposobów:
 - Kiedy jest generowany (automatyczne wyświetlanie). Sytuacja ta ma miejsce, gdy priorytet alarmu jest wyższy niż priorytet wyświetlacza.
 - Kiedy alarm został zaakceptowany. Sytuacja ta ma miejsce, gdy priorytet alarmu jest niższy niż priorytet wyświetlacza.

Alarmy wyświetlane automatycznie

Alarmy mogą być skonfigurowane na automatyczne wyświetlanie w oknie obrazów alarmowych w oparciu o priorytet alarmu. Każdy podgląd obrazu bieżącego lub odtwarzania w grupie użytkowników także ma przypisany priorytet. Kiedy otrzymywane alarmy posiadają wyższy priorytet niż podgląd użytkownika, alarm powoduje automatyczne wyświetlenie rzędu obrazów alarmowych w oknie obrazów alarmowych. Jeśli okno obrazów alarmowych nie jest aktualnie wyświetlane, automatycznie zastępuje ono okno podglądu bieżącego lub okno odtwarzania na monitorze obsługującym alarmy. Chociaż automatycznie wyświetlane alarmy są wyświetlane w oknie obrazów alarmowych, nie są one automatycznie akceptowane. Mogą być one wyświetlane jednocześnie na kilku monitorach użytkowników. Kiedy użytkownik zaakceptuje automatycznie wyświetlany alarm, jest on automatycznie usuwany ze wszystkich list alarmów użytkowników, a podgląd obrazów alarmowych zostaje zamknięty.

Obsługa alarmów w przypadku wyłączenia systemu

W przypadku wyłączenia serwera wszystkie aktywne alarmy zostają zachowane. Alarmy są przywracane i wyświetlane ponownie w oknie **Lista alarmów** po ponownym uruchomieniu systemu. Po ponownym uruchomieniu systemu alarmy w stanie **Przyjęty** lub **Etapy pracy** są automatycznie resetowane do stanu **Aktywny**. Komentarze wprowadzone dla alarmów w stanie **Etapy pracy** zostają zachowane.



Uwaga!

Dane alarmów są automatycznie zapisywane co minutę, więc w najgorszym przypadku można utracić dane zebrane w ciągu jednej minuty.

Patrz

- Konfigurowanie dla alarmu czasów trwania okresu przed i po wystąpieniu alarmu, Strona 323

5.4 Włączanie/wyłączanie analizy zawartości obrazu (Video Analysis)

Użytkownicy należący do grupy, z odpowiednimi uprawnieniami, mogą tymczasowo włączać lub wyłączać analizę zawartości obrazu (Video Analysis) w wybranych kamerach.

Konfigurowanie uprawnień w Configuration Client:

- Okno główne > **Grupy użytkowników** > karta **Grupy użytkowników** >  > karta **Uprawnienia do obsługi** > karta **Funkcje operatora** > **Aktywacja/Dezaktywacja Video Analysis**
lub
- Okno główne > **Grupy użytkowników** > karta **Enterprise User Groups** >  > karta **Uprawnienia do obsługi** > karta **Funkcje operatora** > **Aktywacja/Dezaktywacja Video Analysis**

W Operator Client funkcja analizy zawartości obrazu (Video Analysis) jest domyślnie aktywna we wszystkich kamerach. Funkcję można wyłączyć w jednej kamerze albo w wielu kamerach.

Wyłączanie funkcji analizy zawartości obrazu dla pojedynczej kamery:

1. W Operator Client przejść do wybranej kamery w drzewie logicznym, drzewie ulubionych, oknie obrazów lub na mapie witryny.
2. Kliknąć prawym przyciskiem myszy kamerę, a następnie wybrać opcję **Wyłącz analizę zawartości obrazu**.
Funkcja analizy zawartości obrazu (Video Analysis) obrazu jest wyłączona, a na kamerze wyświetlana  jest ikona nakładki.

Wyłączanie funkcji analizy zawartości obrazu (Video Analysis) dla pojedynczej kamery:

1. W Operator Client przejść do folderu w drzewie logicznym lub drzewie ulubionych, który zawiera wybrane kamery.
2. Kliknąć folder prawym przyciskiem myszy, a następnie wybrać opcję **Wyłącz analizę zawartości obrazu**.
Funkcja analizy zawartości obrazu (Video Analysis) zostanie wyłączona dla wszystkich kamer w folderze, a na ich obrazach pojawi się ikona nakładki .

Aktywowanie analizy zawartości obrazu (Video Analysis) dla kamery ze stanem: Analiza zawartości obrazu: Wyłączona:

1. W Operator Client przejść do wybranej kamery w drzewie logicznym, drzewie ulubionych, oknie obrazów lub na mapie witryny.
2. Kliknąć kamerę prawym przyciskiem myszy, a następnie wybrać opcję **Włącz analizę zawartości obrazu**.
Po włączeniu funkcji analiza zawartości obrazu (Video Analysis) zostaje włączona, a ikona nakładki  znika z obrazu kamery.

Aktywowanie analizy zawartości obrazu (Video Analysis) dla wielu kamer ze stanem: Analiza zawartości obrazu: Wyłączona:

1. W Operator Client przejść do folderu w drzewie logicznym lub drzewie ulubionych, który zawiera wybrane kamery.

2. Kliknąć folder prawym przyciskiem myszy, a następnie wybrać opcję **Włącz analizę zawartości obrazu**.

Analiza zawartości obrazu (Video Analysis) zostanie włączona we wszystkich kamerach w folderze, a ikona nakładki  zniknie z ich obrazu.

**Uwaga!**

Włączanie i wyłączanie analizy zawartości obrazu (Video Analysis) w Operator Client jest możliwe tylko wtedy, gdy Operator Client jest połączony z Central Server.

**Uwaga!**

Aktywacji / dezaktywacji analizy zawartości obrazu (Video Analysis) nie jest obsługiwana przez kodery zgodne z profilem ONVIF-G.

**Uwaga!**

Po ponownym uruchomieniu Operator Client lub Central Server zostanie zachowana ostatnia konfiguracja.

5.5

Mapowanie zdarzeń ONVIF

**Uwaga!**

Należy pamiętać, że ta funkcja wkrótce zostanie wyłączona.

Należy korzystać z narzędzia ONVIF Camera Event Driver Tool do łatwego mapowania zdarzeń ONVIF.

Patrz *Uruchamianie narzędzia ONVIF Camera Event Driver Tool za pomocą Configuration Client*, Strona 208.

Przeznaczenie

Celem jest odwzorowanie zdarzeń ONVIF na zdarzenia BVMS. Dzięki temu zdarzenia ONVIF mogą wywoływać alarmy i zapis w systemie BVMS.

Można definiować domyślne odwzorowania zdarzeń obowiązujące tylko w przypadku określonego urządzenia ONVIF, wszystkich urządzeń ONVIF tego samego producenta i modelu lub wszystkich urządzeń ONVIF tego samego producenta. Domyślne odwzorowania zdarzeń są przypisywane automatycznie do wszystkich odpowiednich nadajników ONVIF, które zostały dodane za pomocą Kreatora skanowania systemu BVMS lub ręcznie.

Po dodaniu nadajnika ONVIF do konfiguracji systemu BVMS bez połączenia z tym nadajnikiem ONVIF nie są przypisywane żadne odwzorowania zdarzeń. Odwzorowania zdarzeń można zaktualizować w takim nadajniku ONVIF, korzystając z innego nadajnika ONVIF tego samego producenta i (lub) modelu, który został już dodany.

Odwzorowania zdarzeń można definiować dla następujących źródeł:

- Nadajnik ONVIF
- Kamery tego nadajnika ONVIF
- Przekazniki tego nadajnika ONVIF
- Wejścia tego nadajnika ONVIF

Przykład

W kamerze ONVIF występuje zdarzenie detekcji ruchu. Zdarzenie to powinno wyzwolić zdarzenie **Wykryto ruch** w systemie BVMS.

Aby tak się stało, należy wprowadzić dla tej kamery ONVIF następujące ustawienia:

- Temat zdarzenia ONVIF (*MotionDetection*)
- Element danych zdarzenia ONVIF (*motion*)
- Rodzaj danych zdarzenia ONVIF (*boolean*)
- Wartość danych zdarzenia ONVIF (*true*)

Uwaga: nie wystarczy tylko skonfigurować zdarzenie **Wykryto ruch**. Należy również skonfigurować zdarzenie **Ruch zatrzymany**. Zdarzenia należy zawsze konfigurować parami.

Importowanie i eksportowanie tablicy odwzorowań

Tablicę odwzorowań można wyeksportować na komputerze, na jakim została utworzona, a następnie zaimportować ją na innym komputerze, na którym jest niedostępna.

Nieprawidłowości w działaniu i ich usuwanie

Można tworzyć pliki rejestru pomagające w rozwiązywaniu problemów.

Patrz

- Konfigurowanie tabeli odwzorowań ONVIF, Strona 241
- Włączanie rejestrowania zdarzeń ONVIF, Strona 379
- Strona ONVIF Encoder Events (Zdarzenia nadajników ONVIF), Strona 237

5.6

Wylogowanie w przypadku braku aktywności

Przeznaczenie

Celem funkcji wylogowania w przypadku braku aktywności jest ochrona programu Operator Client lub Configuration Client podczas nieobecności operatora bądź administratora.

Można skonfigurować grupę użytkowników tak, aby wylogowanie z programu Operator Client następowało automatycznie po określonym czasie braku aktywności.

W przypadku programu Configuration Client nie są dostępne żadne grupy użytkowników. Ustawienie wylogowania w przypadku braku aktywności jest przeznaczone tylko dla użytkownika **admin**.

Wszystkie działania na klawiaturze, myszy i na klawiaturze CCTV wpływają na określony czas braku aktywności, po którym nastąpi wylogowanie. Automatyczne działania programu Operator Client nie wpływają na ten czas. Automatyczne działania programu Configuration Client, np. przesyłanie oprogramowania układowego czy konfigurowanie połączenia iSCSI, zapobiegają wylogowaniu w wyniku braku aktywności.

Można także skonfigurować wylogowanie w przypadku braku aktywności programu Web Client w systemie BVMS.

Na krótko przed wylogowaniem w wyniku braku aktywności pojawia się okno dialogowe, które monituje użytkownika o aktywność, aby zapobiec wylogowaniu.

Rejestr zawiera zapisy wylogowań, które nastąpiły w wyniku braku aktywności.

Przykład

Jeśli stacja robocza jest dostępna publicznie, wylogowanie w przypadku braku aktywności ogranicza ryzyko uzyskania za jej pomocą dostępu do programu Operator Client przez nieupoważnione osoby.

Członek grupy administratorów powinien być wylogowany automatycznie po określonym czasie nieaktywności, ale funkcjonariusz (grupa operatorów) może oglądać wideo bez interakcji z systemem i nie musi być wylogowany w przypadku braku aktywności.

Ograniczenia

Program Client SDK nie obsługuje funkcji wylogowania w przypadku braku aktywności, tzn. czynności w programie Client SDK nie wpływają na czas wylogowania.

Patrz

- Okno dialogowe Opcje (menu Ustawienia), Strona 120
- Strona funkcji operatora, Strona 337

5.7 Program Operator Client niezależny od wersji

W przypadku trybu zgodności zarówno aplikacja Operator Client, jak i Management Server muszą być w wersji 5.5 lub nowszej.

Użytkownik programu Operator Client może pomyślnie zalogować się na serwerze Management Server, na którym działa starsza wersja oprogramowania.

Jeśli serwer udostępnia nowszą konfigurację niż dostępna na stacji roboczej z programem Operator Client, nowsza wersja jest automatycznie kopiowana na stację roboczą. Użytkownik może decydować o pobraniu nowej konfiguracji.

Program Operator Client udostępnia ograniczony zestaw funkcji i ma połączenie z tym serwerem Management Server.

Po zalogowaniu się na serwerze Management Server z poprzednią wersją oprogramowania dostępne są następujące funkcje związane z serwerem Management Server:

- Preferencje użytkownika
- Rozpoczynanie zapisu ręcznego
- Wyświetlanie stanów urządzeń
- Przełączanie stanów przekaźnika
- Wyszukiwanie w rejestrze
- Wyszukiwanie zdarzeń jest niemożliwe.
- Server Lookup
- Zdalny eksport

5.7.1 Praca w trybie zgodności



: Ten stan programu Operator Client jest wyświetlany w przypadku trybu zgodności.

W przypadku wersji nowszych niż 5.5, gdy program Management Server jest w wersji niższej program Operator Client będzie działał w trybie zgodności.

W przypadku wersji nowszych niż 10.0 program Operator Client będzie działał w trybie zgodności w następujących przypadkach:

- Program Operator Client nie połączył się ze wszystkimi usługami komunikacyjnymi.
- Przykład: program Management Server jest włączony i działa, ale usługa WebServiceHost jest wyłączona.
- Wystąpiły zmiany w interfejsie komunikacyjnym między programami Operator Client i Management Server

Przyczyną braku niektórych funkcji w Operator Client mogą być jedynie zmiany interfejsu semantycznego lub częściowe wyłączenie usług.

5.8 Tryby podglądu kamery panoramicznej

W tym rozdziale przedstawiono tryby podglądu kamery panoramicznej dostępne w systemie BVMS.

Dostępne są następujące tryby podglądu:

- Widok okręgu
- Widok panoramy
- Widok przycięty

Tryby widoków panorama i przycięcie są tworzone przez proces prostowania obrazu w systemie BVMS. Autonomiczne korygowanie zniekształceń przez kamerę nie jest stosowane.

Administrator musi skonfigurować położenie zamontowania kamery panoramicznej w programie Configuration Client.

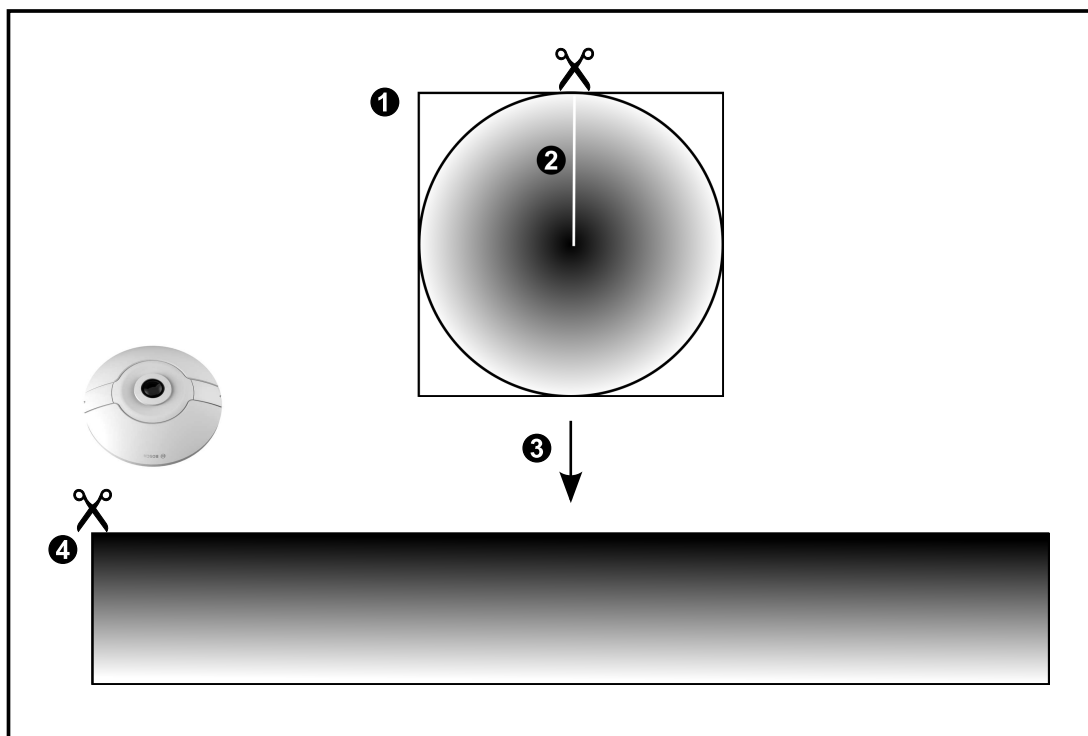
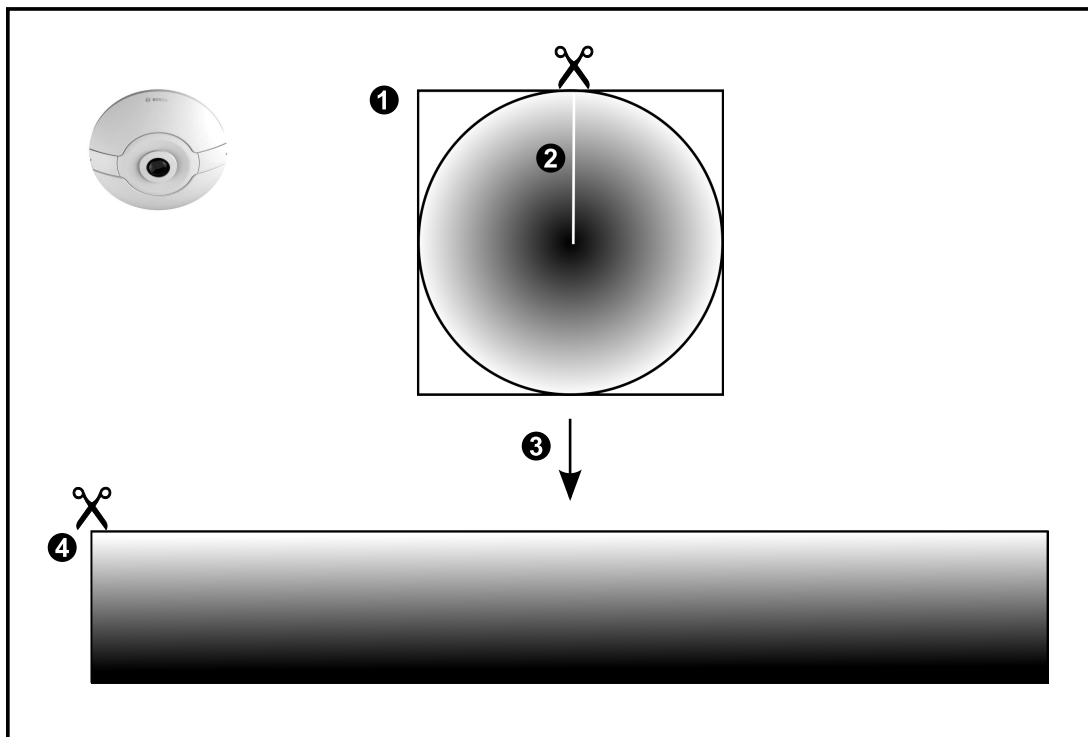
W razie potrzeby można zmienić rozmiar okienka obrazu kamery. Format okienka obrazu nie ogranicza się tylko do współczynników kształtu 4:3 lub 16:9.

Patrz

- Konfigurowanie predefiniowanych położeń i funkcji dodatkowych, Strona 300

5.8.1**Kamera panoramiczna 360° do montażu podłogowego lub sufitowego**

Poniższy rysunek przedstawia prostowanie obrazu w kamerze 360° montowanej na podłodze lub suficie.

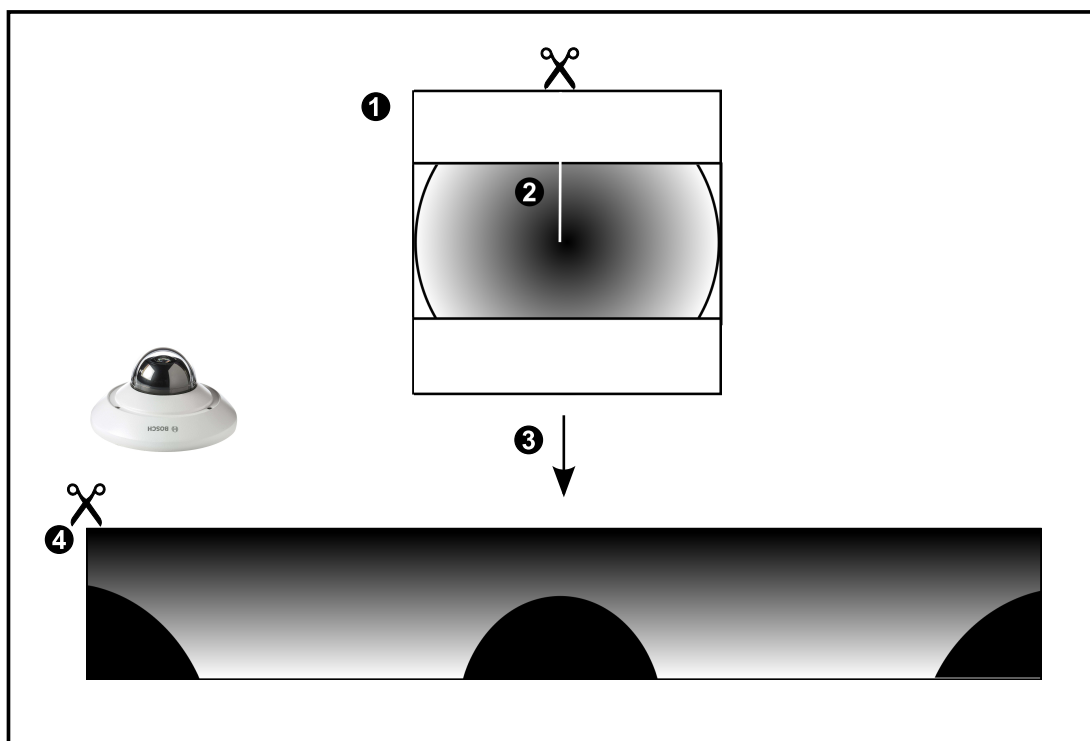
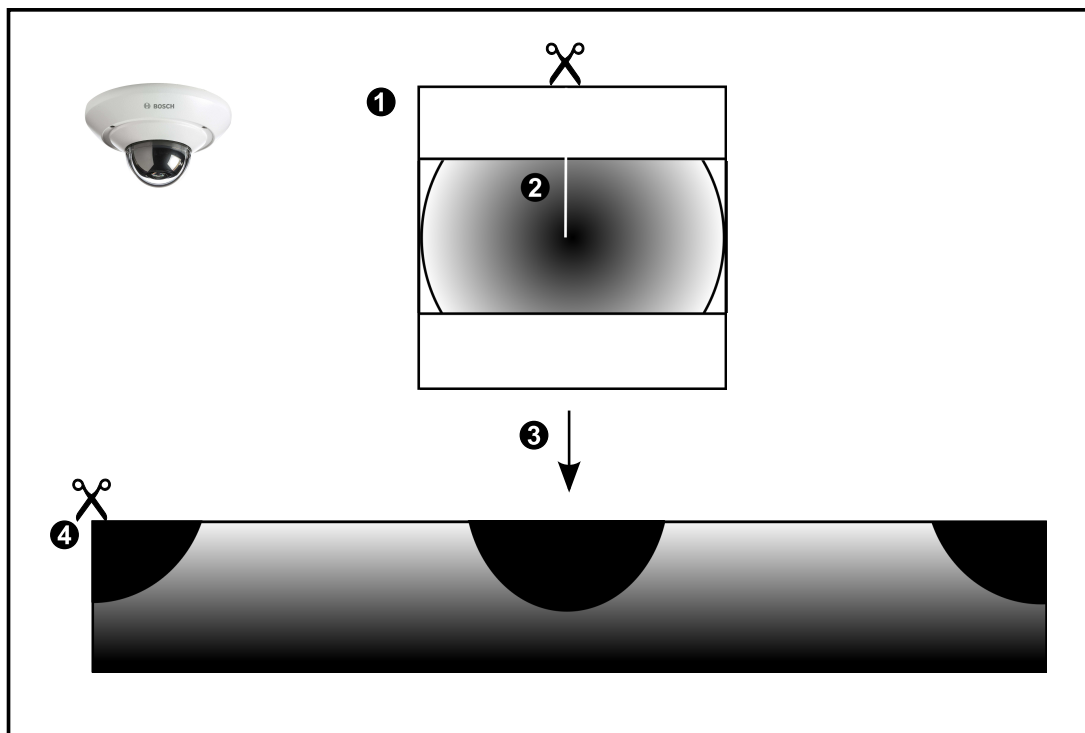


1	Pełny obraz kolisty	3	Prostowanie obrazu
2	Linia wycięcia (operator może zmienić jej położenie, jeżeli obraz nie jest przybliżony)	4	Widok panoramy

5.8.2

Kamera panoramiczna 180° do montażu podłogowego lub sufitowego

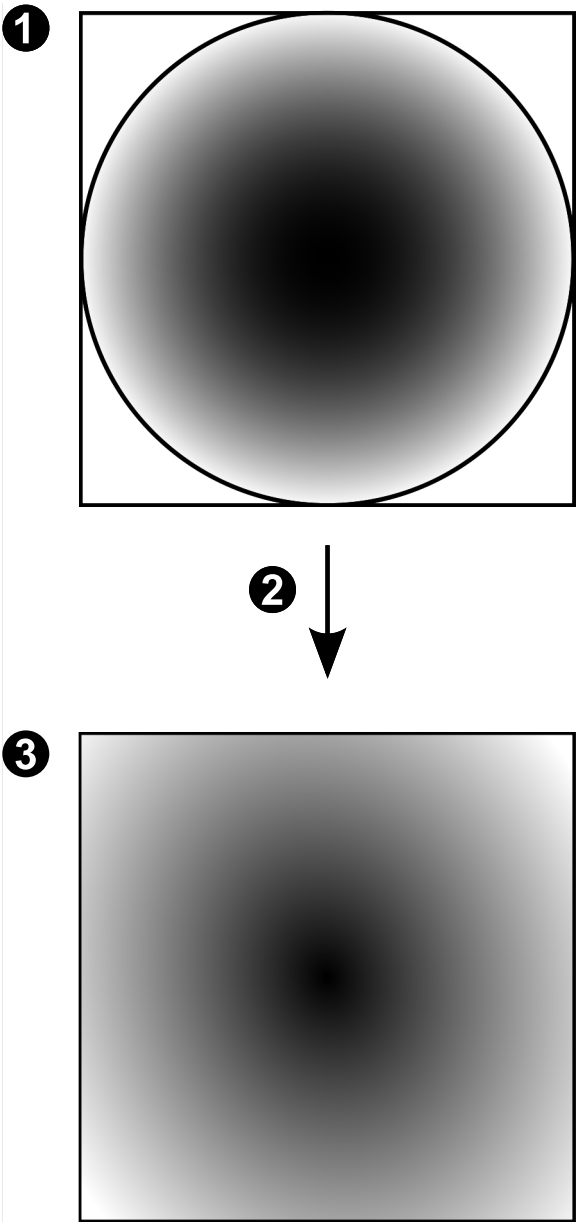
Poniższy rysunek przedstawia prostowanie obrazu w kamerze 180° montowanej na podłodze lub suficie.



1	Pełny obraz kolisty	3	Korygowanie zniekształceń
2	Linia wycięcia (operator może zmienić jej położenie, jeżeli obraz nie jest przybliżony)	4	Widok panoramy

5.8.3 Kamera panoramiczna 360° do montażu ściennego

Poniższy rysunek przedstawia prostowanie obrazu w kamerze 360° montowanej na ścianie.

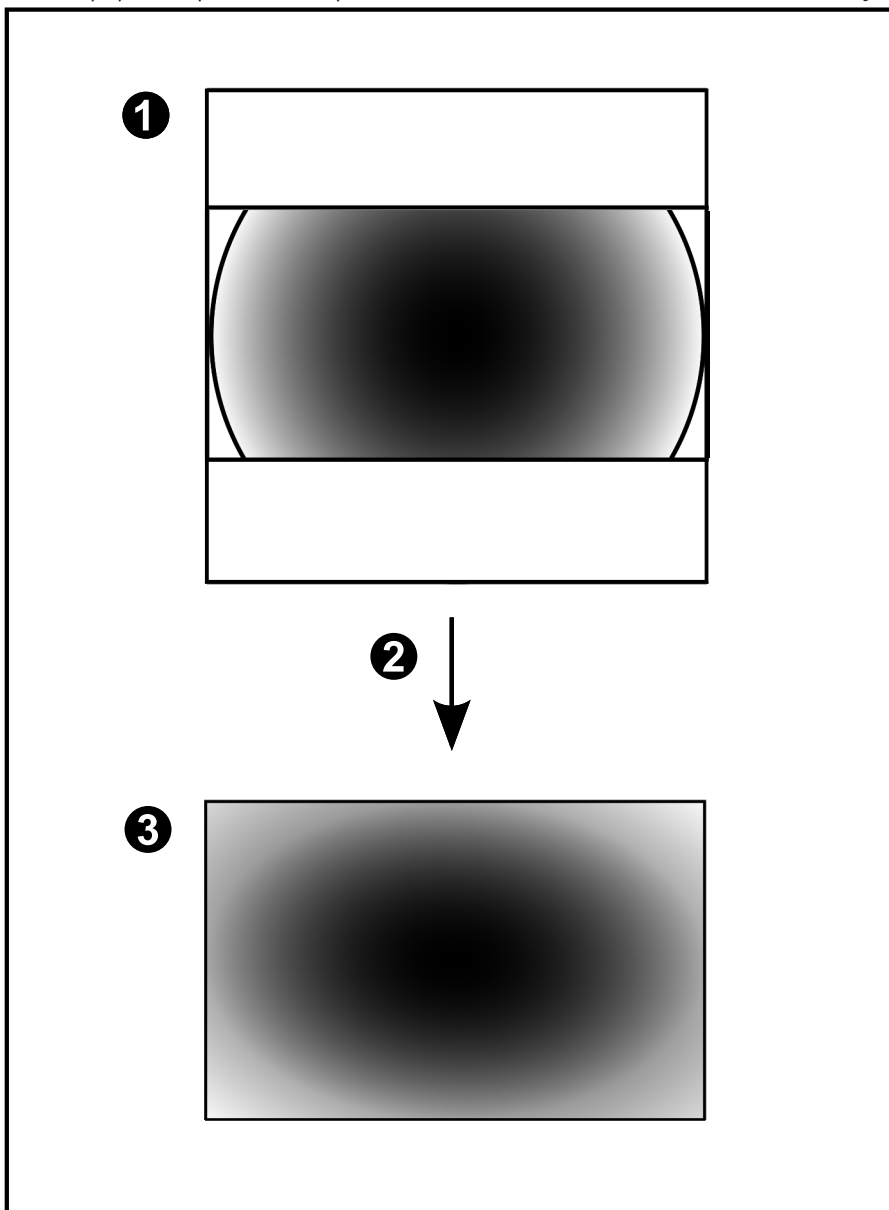


1	Pełny obraz kolisty	3	Widok panoramy
2	Korygowanie zniekształceń		

5.8.4

Kamera panoramiczna 180° do montażu ściennego

Poniższy rysunek przedstawia prostowanie obrazu w kamerze 180° montowanej na ścianie.



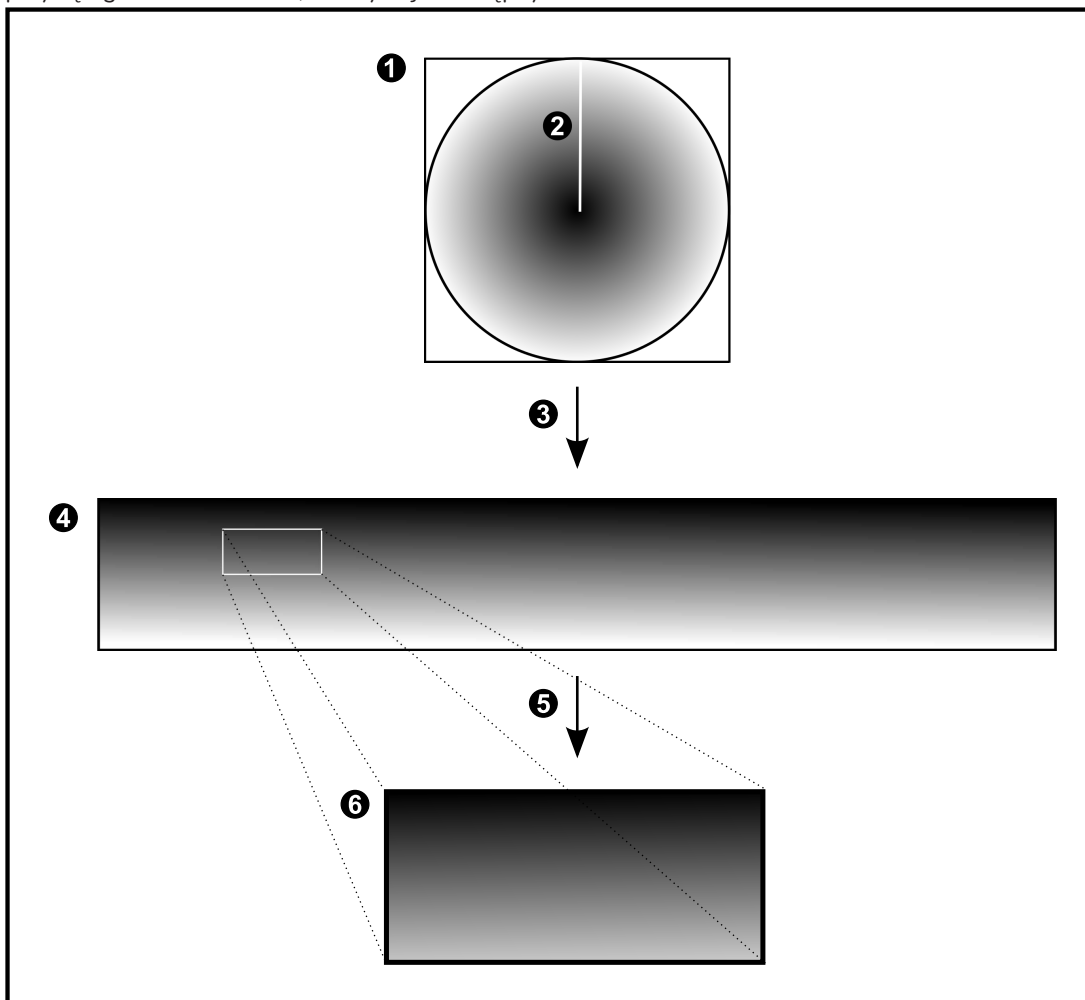
1	Pełny obraz kolisty	3	Widok panoramy
2	Korygowanie zniekształceń		

5.8.5

Przycięty widok w kamerze panoramicznej

Poniższy rysunek przedstawia przycinanie obrazu w kamerze 360° montowanej na podłodze lub suficie.

Obszar prostoliniowy używany do przycięcia znajduje się w pozycji stałej. Aby zmienić fragment przyciętego okienka obrazu, skorzystaj z dostępnych elementów sterowania PTZ.



1	Pełny obraz kolisty	4	Widok panoramy
2	Linia wycięcia (operator może zmienić jej położenie, jeżeli obraz nie jest przybliżony)	5	Przycinanie
3	Prostowanie obrazu	6	Okno przyciętego obrazu

5.9 Tunelowanie SSH

System BVMS zapewnia zdalną łączność dzięki zastosowaniu tunelowania Secure Shell (SSH). Tunelowanie SSH tworzy zaszyfrowany tunel ustanowiony przez połączenia gniazda protokołu SSH. Takiego zaszyfrowanego tunelu można używać do transportu zarówno ruchu szyfrowanego, jak i niezaszyfrowanego. Implementacja protokołu SSH firmy Bosch również korzysta z protokołu Omni-Path będącego wysoko wydajnym protokołem komunikacyjnym o małym opóźnieniu opracowanym przez firmę intel.

Aspekty techniczne i ograniczenia

- Tunelowanie SSH wykorzystuje port 5322. Nie można modyfikować tego portu.
- Usługa SSH musi być zainstalowana na tym samym serwerze co system BVMS Management Server.
- (Enterprise) Konta użytkowników muszą mieć skonfigurowane hasła. (Enterprise) Z konta użytkowników bez hasła nie można zalogować się za pomocą połączenia SSH.
- Kamery z obsługą lokalnego urządzenia pamięci masowej nie obsługują połączenia SSH.
- Program Configuration Client nie może nawiązać połączenia zdalnie za pośrednictwem SSH. Połączenie programu Configuration Client należy przeprowadzić za pomocą mapowania portów.
- Program Operator Client sprawdza połączenia z usługą SSH co 15 sekund. Jeśli połączenie zostało przerwane, Operator Client ponownie testuje połączenie co minutę.

Mapowanie portów

- ▶ Należy skonfigurować jeden port do przekazywania dalej portu 5322 BVMS Management Server w celu wykorzystywania go do połączeń wewnętrznych i zewnętrznych. To jest jedyne mapowanie portu, jakie musi być wykonane w całym systemie. Mapowanie portów w systemie BVMS nie jest wymagane.

Szyfrowanie komunikacji

Po nawiązaniu połączenia za pomocą tunelu SSH cała komunikacja między programem BVMS Management Server a zdalnym klientem jest szyfrowana.

5.10 Wielościeżkowość

System BVMS udostępnia wielościeżkowość dla systemów w konfiguracji z dwoma kontrolerami. Wielościeżkowość jest techniką zapewniania odporności na błędy, która polega na zdefiniowaniu więcej niż jednej ścieżki fizycznej między kamerą a jej urządzeniami pamięci iSCSI poprzez zastosowanie nadmiarowych połączeń sieciowych. Podczas korzystania z wielościeżkowości zapisywanie i odtwarzanie danych wideo jest możliwe nawet w przypadku awarii kontrolera iSCSI.

Warunki wstępne i ograniczenia

- Zainstalowana jednostka iSCSI z dwoma kontrolerami NetApp E2800.
- Oprogramowanie układowe 6.43 umożliwia urządzeniom zapis na E2800 w celu zapewnienia alternatywnych ścieżek.
- VRM 3.71 do monitorowania i rejestrowania z obsługą wielościeżkowości.
- Po dwa porty fizyczne iSCSI skonfigurowane dla każdego kontrolera: RJ45 2x2 lub światłowodowe 2x2.
- W celu osiągnięcia pełnej wydajności wymagana jest szybkość łącza na poziomie 10 Gb/s.
- Tryb Dual-Simplex używany w E2700 nie jest już obsługiwany.

Więcej informacji na temat instalacji systemu DSA E2800 Full Duplex można znaleźć w instrukcji instalacji DSA E-Series E2800.

5.11 Open ID Connect (OIDC) i Identity Provider (IdP)

System BVMS obsługuje uwierzytelnianie za pośrednictwem usług zewnętrznego dostawcy uwierzytelniania. Uwierzytelnianie jest obsługiwane za pośrednictwem wstępnie skonfigurowanego Identity provider (IdP) za pomocą połączenia Open ID Connect (OIDC), a zadanie autoryzacji wykonuje system BVMS.

Przydaje się to w przypadku dużych grup Enterprise, gdzie trzeba zarządzać pojedynczymi użytkownikami indywidualnie. Poprzez mapowanie grup użytkowników do grup IdP użytkownicy otrzymują dostęp według potrzeb.

Patrz

- Okno dialogowe *Opcje* (menu *Ustawienia*), Strona 120
- strona *Grupy użytkowników*, Strona 328

5.12 Rozpoznawanie tablic rejestracyjnych

Najnowsze kamery firmy Bosch z Intelligent Video Analytics (IVA) Pro obsługą rozpoznawania tablic rejestracyjnych.

Aby móc rozpoznawać tablice rejestracyjne pojazdów, w kamerze musi być zainstalowana specjalna licencja. Nie ma potrzeby aktywowania licencji w systemie BVMS.

W zależności od tego, jaka licencja została zainstalowana, kamera będzie wysyłać tylko dane odczytane z tablicy rejestracyjnej oraz kod kraju oraz typ i model pojazdu.

Ustawienia LPR należy skonfigurować na stronie internetowej kamery.

W oprogramowaniu Configuration Client systemu BVMS można skonfigurować odpowiednie zdarzenia i alarmy w odniesieniu do odczytanych tablic rejestracyjnych, a także wyszukiwać zeskanowane tablice rejestracyjne w dzienniku.



Uwaga!

W przypadku zdarzenia LPR do zapisu nie można dodać opisu.



Uwaga!

Gdy pojazd przejeżdża obok, kamera potrzebuje do 3 sekund na zeskanowanie tablicy rejestracyjnej. Następnie BVMS tworzy zdarzenie LPR z odpowiednim znacznikiem czasu.

Ze względu na opóźnienie detekcji należy podczas konfigurowania ustawień zapisu kamery ustawić zapis przedalarmowy na minimum 5 sekund.

Patrz

- Strona *rozpoznawania tablic rejestracyjnych*, Strona 257
- strona *Zdarzenia*, Strona 305

6 Obsługiwany sprzęt



Uwaga!

Nie należy podłączać urządzeń do więcej niż jednego systemu BVMS! Może to powodować powstawanie luk w nagraniach i innych niepożądanych efektów.

Z systemem BVMS mogą współpracować następujące urządzenia:

- Mobilne urządzenia klienckie z obsługą wideo, takie jak iPhone lub iPad, poprzez usługę DynDNS
- Różne kamery IP, nadajniki i kamery ONVIF (na żywo lub za pośrednictwem bramy Video Streaming Gateway)
Połączone za pośrednictwem sieci
- Nadajniki podglądu bieżącego z lokalną pamięcią masową
Połączone za pośrednictwem sieci
- Urządzenia pamięci masowej iSCSI
Połączone za pośrednictwem sieci
- Kamery analogowe
Podłączone do nadajników,
- Dekodery
Połączone za pośrednictwem sieci
- Monitory
Dołączone do dekodera, do krosownicy Bosch Allegiant lub do stacji roboczej-klienta systemu BVMS
- Krosownica Bosch Allegiant (wersja oprogramowania układowego: 8.75 lub nowsza, wersja oprogramowania MCS: 2.80 lub nowsza)
Dołączona do portu COM komputera typu Management Server lub do komputera zdalnego oraz nadajnika sieciowego przyłączonego do sieci.
- Klawiatura KBD-Universal XF
Podłączona do portu USB stacji roboczej systemu BVMS
- Klawiatura Bosch IntuiKey
Podłączona do portu COM stacji roboczej BVMS (wersja oprogramowania układowego: 1.82 lub nowsza) lub do odbiornika sprzętowego (VIP XD).
Jeśli klawiatura jest podłączona do stacji roboczej, użytkownik może za jej pomocą sterować całym systemem. Jeśli klawiatura jest podłączona do odbiornika VIP XD, użytkownik może sterować za jej pomocą tylko monitorami.
- Serwer pocztowy SMTP
Połączone za pośrednictwem sieci
- POS
Połączone za pośrednictwem sieci
- ATM
Połączone za pośrednictwem sieci
- Urządzenie monitoringu sieci
Połączone za pośrednictwem sieci
- Moduły wejścia / wyjścia
Połączone za pośrednictwem sieci
Obsługiwane są tylko urządzenia ADAM.

Wszystkie urządzenia połączone z siecią są dołączone do przełącznika. Komputery oprogramowania BVMS są także dołączone do tego urządzenia.

6.1 Instalowanie urządzeń

System BVMS obsługuje następujące składniki sprzętowe:

- Klawiatura KBD-Universal XF
 - Klawiatura Bosch IntuiKey
 - Krosownica Bosch Allegiant z kamerami i monitorem: podłączona do portu COM jednego z komputerów w sieci oraz do nadajników sieciowych
 - Nadajniki z kamerami analogowymi
 - Nadajniki z obsługą lokalnego urządzenia pamięci masowej
 - Kamery sieciowe i kamery sieciowe AutoDome
 - Monitory dołączone do dekodera (możliwe jest zastosowanie grup monitorów do przetwarzania alarmów)
 - Systemy DVR z kamerami
 - Urządzenia ATM/POS
 - Moduły we/wy
- Obsługiwane są wyłącznie urządzenia ADAM.

6.2 Instalowanie klawiatury KBD Universal XF



Uwaga!

Należy zapoznać się z instrukcją obsługi dostarczaną z klawiaturą KBD-Universal XF dostępną w katalogu produktów online.

Dalsze informacje

Więcej informacji, dokumentację i oprogramowanie do pobrania można znaleźć na stronie www.boschsecurity.com lub na stronie danego produktu.

Z systemem BVMS mogą współpracować następujące urządzenia:

- Mobilne urządzenia klienckie z obsługą wideo, takie jak iPhone lub iPad, poprzez usługę DynDNS
- Różne kamery IP, nadajniki i kamery ONVIF (na żywo lub za pośrednictwem bramy Video Streaming Gateway)
Połączone za pośrednictwem sieci
- Nadajniki podglądu bieżącego z lokalną pamięcią masową
Połączone za pośrednictwem sieci
- Urządzenia pamięci masowej iSCSI
Połączone za pośrednictwem sieci
- Kamery analogowe
Podłączone do nadajników,
- Dekodery
Połączone za pośrednictwem sieci
- Monitory
Dołączone do dekodera, do krosownicy Bosch Allegiant lub do stacji roboczej-klienta systemu BVMS
- Krosownica Bosch Allegiant (wersja oprogramowania układowego: 8.75 lub nowsza, wersja oprogramowania MCS: 2.80 lub nowsza)
Dołączona do portu COM komputera typu Management Server lub do komputera zdalnego oraz nadajnika sieciowego przyłączonego do sieci.

6.3 Podłączanie klawiatury Bosch IntuiKey do systemu BVMS

W tym rozdziale przedstawiono podstawowe informacje o konfigurowaniu klawiatury Bosch IntuiKey.

6.3.1

Możliwe sposoby podłączenia klawiatury Bosch IntuiKey

Klawiaturę Bosch IntuiKey można podłączyć do portu COM stacji roboczej systemu BVMS (scenariusz 1) lub do odbiornika sprzętowego (np. VIP XD, scenariusz 2).

Jeśli klawiatura zostanie dołączona do stacji roboczej systemu BVMS, użytkownik może sterować całym systemem. Jeśli klawiatura zostanie dołączona do odbiornika, użytkownik może sterować tylko monitorami analogowymi dołączonymi do systemu.

W przypadku podłączenia klawiatury do stacji roboczej Enterprise Operator Client użytkownik może sterować kamerami wybranego serwera Management Server, naciskając najpierw klawisz serwera w celu wprowadzenia numeru tego serwera, a następnie wprowadzając numer kamery.

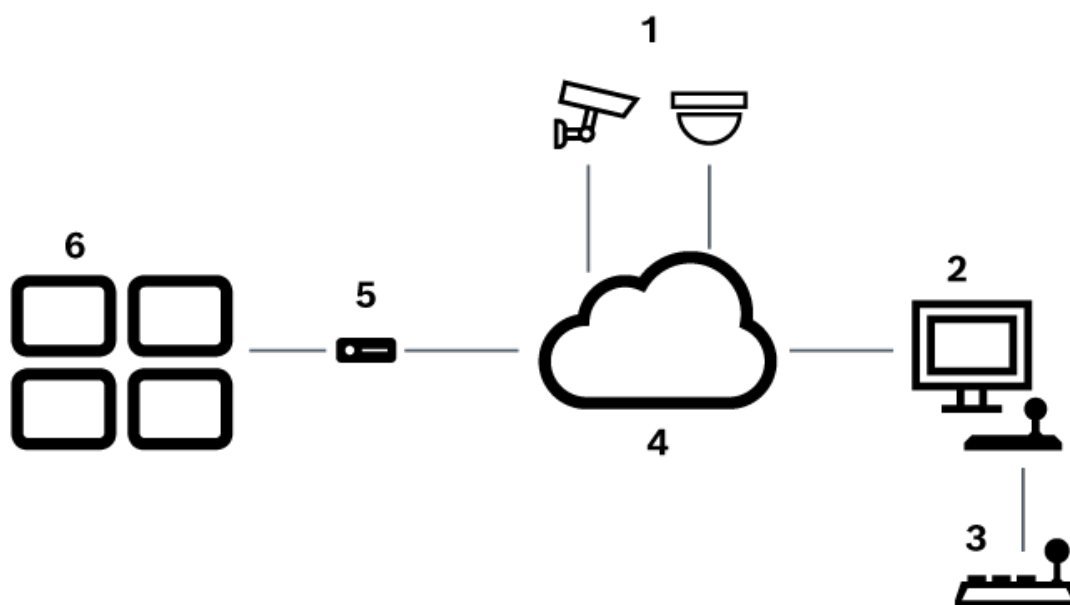


Uwaga!

Do połączenia klawiatury Bosch IntuiKey ze stacją roboczą systemu BVMS należy użyć specjalnego kabla Bosch.

Do połączenia klawiatury Bosch IntuiKey z odbiornikiem VIP XD wymagany jest kabel łączący port szeregowy COM klawiatury z interfejsem szeregowym odbiornika. Aby uzyskać informacje o połączeniach, patrz Podłączanie klawiatury CCTV do odbiornika.

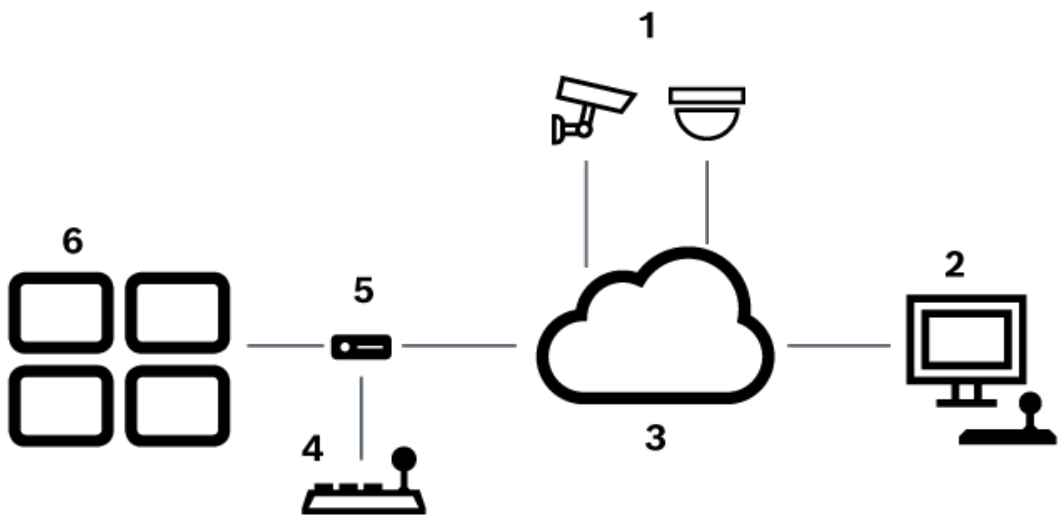
Klawiatura Bosch IntuiKey podłączona do stacji roboczej systemu BVMS



Rysunek 6.1: Sposób 1: klawiatura Bosch IntuiKey podłączona do stacji roboczej systemu Bosch Video Management System

1	Różne kamery dołączone do sieci za pomocą nadajników
2	Stacja robocza systemu BVMS
3	Klawiatura Bosch IntuiKey
4	Sieć systemu BVMS
5	Dekoder
6	Monitory

Klawiatura Bosch IntuiKey podłączona do odbiornika



Rysunek 6.2: Scenariusz 2: klawiatura Bosch IntuiKey podłączona do odbiornika

1	Różne kamery dołączone do sieci za pomocą nadajników
2	Stacja robocza systemu BVMS
3	Sieć systemu BVMS
4	Klawiatura Bosch IntuiKey
5	Dekoder
6	Monitory

Zapoznać się z odnośnikami, aby uzyskać szczegółowe informacje na temat dostępnych okien:

- Strona Przypisz klawiaturę, Strona 156

Zapoznać się z odnośnikami, aby uzyskać informacje na temat dostępnych szczegółowych instrukcji:

- Konfigurowanie klawiatury Bosch IntuiKey (strona Ustawienia) (stacja robocza), Strona 137
- Konfigurowanie klawiatury Bosch IntuiKey (odbiornik), Strona 145
- Konfigurowanie odbiornika podłączonego do klawiatury Bosch IntuiKey, Strona 145

Patrz

- Strona Przypisz klawiaturę, Strona 156

6.3.2 Podłączanie klawiatury Bosch IntuiKey do odbiornika

Konfigurowanie odbiornika

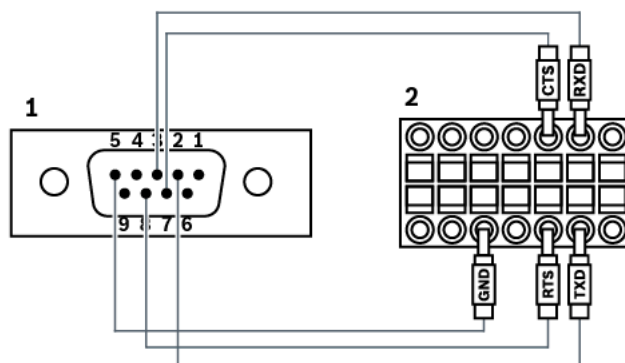
Patrz Konfigurowanie odbiornika podłączonego do klawiatury Bosch IntuiKey, Strona 145 , aby uzyskać szczegółowe informacje.

Połączenia między portem COM a odbiornikiem VIP XD

Poniższa tabela zawiera spis połączeń pomiędzy adapterem RS-232 i interfejsem szeregowym odbiornika VIP XD:

Adapter RS-232	Interfejs szeregowy odbiornika VIP XD
1	
2	TX
3	RX
4	
5	GND
6	
7	CTS
8	RTS
9	

Poniższy rysunek pokazuje rozmieszczenie styków standardowego adaptera RS-232 (1) oraz rozmieszczenie styków adaptera szeregowego odbiornika (2):



6.3.3

Aktualizacja oprogramowania układowego klawiatury Bosch IntuiKey

1. Na dowolnym komputerze PC zainstalować program IntuiKey downloader.
2. Uruchomić program do aktualizacji oprogramowania układowego IntuiKey.
3. Podłączyć klawiaturę do komputera PC za pomocą odpowiedniego kabla szeregowego (skontaktować się z Działem obsługi klienta firmy Bosch, jeśli taki kabel nie jest dostępny).
4. Na klawiaturze nacisnąć przycisk ekranowy Keyboard Control, a następnie Firmware Upgrade.
5. Wprowadzić hasło: jednocześnie 0 i 1.
Klawiatura znajduje się w trybie ładowania oprogramowania.
6. W komputerze PC kliknąć przycisk Browse, aby wybrać plik z oprogramowaniem układowym, na przykład kbd.s20
7. Ustawić port COM.
8. Kliknąć przycisk Download, aby pobrać oprogramowanie układowe.
Na wyświetlaczu klawiatury widoczny jest komunikat Programming.
Nie należy naciskać teraz przycisku Clr. W przeciwnym wypadku klawiatura nie będzie działała po restarcie (patrz poniższa uwaga).

9. Kliknąć przycisk Browse, aby wybrać język: na przykład 8900_EN_..s20
Na wyświetlaczu klawiatury widoczny jest komunikat Programming.
10. Zamknąć program do aktualizacji oprogramowania układowego IntuiKey.
11. Nacisnąć na klawiaturze przycisk Clr, aby zakończyć.
Klawiatura zostanie zrestartowana. Poczekać kilka sekund, aż pojawi się menu służące do wyboru języka klawiatury.
12. Wybrać żądany język za pomocą przycisku ekranowego.
Pojawi się domyślny ekran startowy.

**Uwaga!**

Aby bezpośrednio uruchomić tryb pobierania, można odłączyć zasilanie z klawiatury, nacisnąć równocześnie klawisze 0 i 1, ponownie włączyć zasilanie i zwolnić klawisze 0 oraz 1.

6.4

Podłączanie krosownicy Bosch Allegiant do systemu BVMS

Interfejs krosownicy BVMSAllegiant zapewnia płynny dostęp do kamer krosownicy analogowej z poziomu interfejsu Operator Client. Kamery Allegiant wyglądają praktycznie tak samo jak kamery sieciowe. Jedyną różnicą jest umieszczony na kamerze niewielki symbol siatki informujący, że jest to urządzenie Allegiant. Użytkownik może wyświetlać obraz z kamer za pomocą tych samych funkcji, jakie są dostępne dla kamer sieciowych. Oba typy kamer znajdują się w drzewie logicznym i mapach obszaru, a użytkownicy mogą dodawać je do drzew ulubionych. W oknie podglądu jest obsługiwane sterowanie kamerami PTZ dołączonymi do krosownicy Allegiant, a użytkownik może łatwo wyświetlać kamery Allegiant na monitorach dołączonych do dekodatorów sieciowych.

System BVMS zapewnia interfejs do krosownicy wizyjnej poprzez aplikację Allegiant MCS (Master Control Software). Oprogramowanie MCS w tym przypadku pracuje niewidocznie w tle. Oferuje ono wydajny, sterowany zdarzeniami interfejs do krosownicy Allegiant. Zapewnia szybką odpowiedź w czasie rzeczywistym z krosownicy Allegiant do systemu BVMS. Jeśli więc na przykład uszkodzony kabel koncentryczny spowoduje zanik sygnału wizyjnego w krosownicy Allegiant, system BVMS jest natychmiast o tym powiadamiany. Dodatkowo system BVMS można zaprogramować tak, aby reagował na alarmy krosownicy Allegiant.

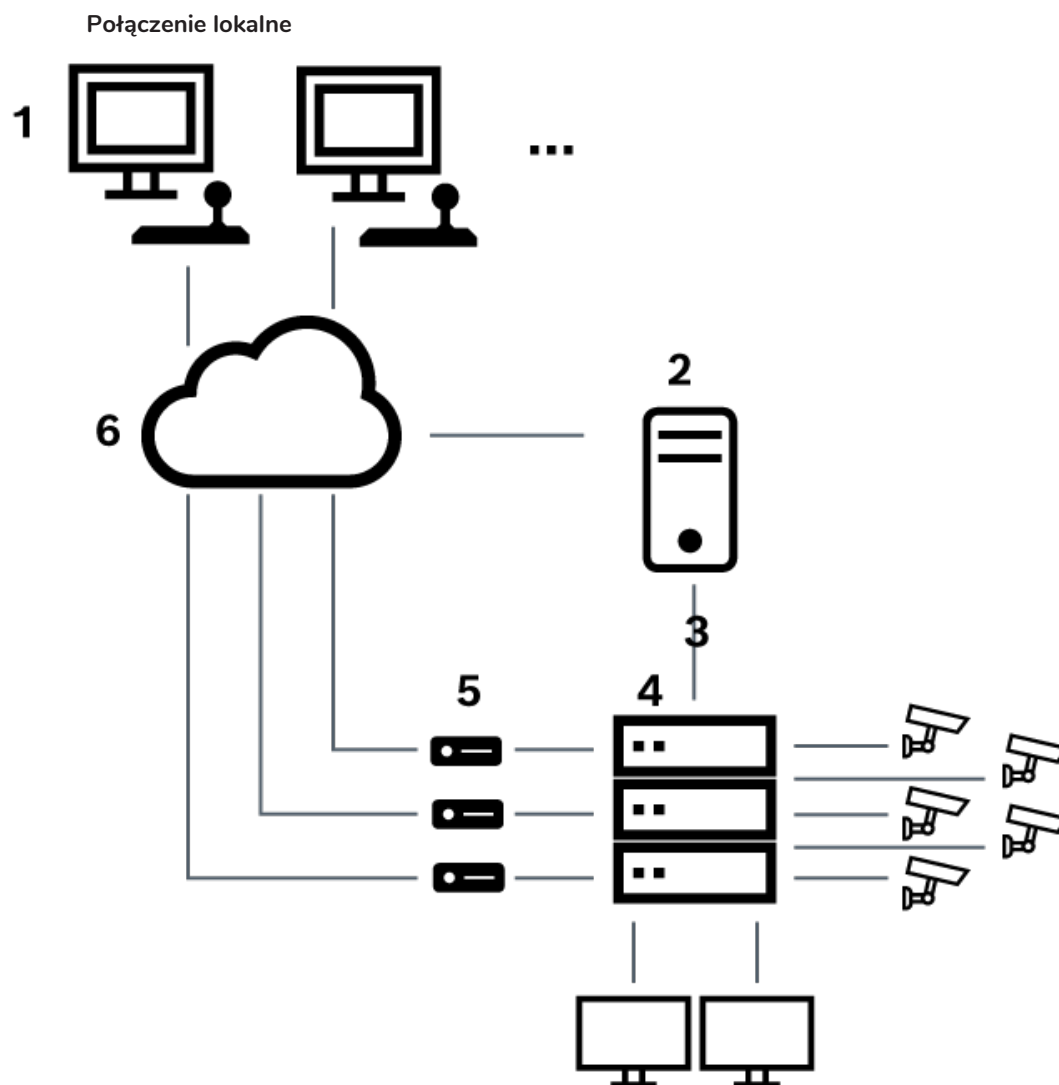
6.4.1

Połączenia krosownicy Bosch Allegiant – informacje ogólne

Warunkiem połączenia systemu BVMS z krosownicami Allegiant jest odpowiednie skonfigurowanie kanału sterującego łączącego system BVMS i urządzenie Allegiant.

Możliwe są dwa rozwiązania:

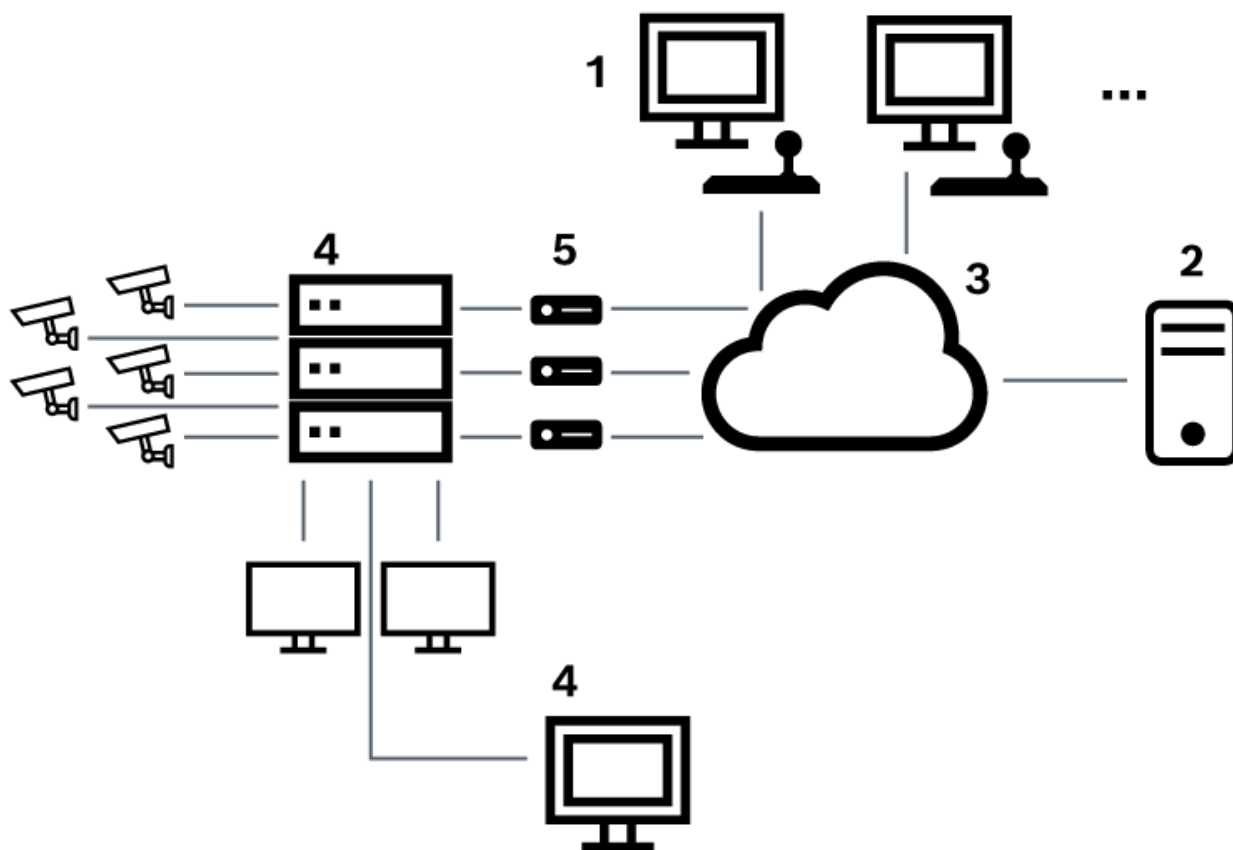
- Połączenie lokalne
Krosownicą Allegiant steruje Management Server.
- Połączenie zdalne
Krosownicą Allegiant steruje oddzielny komputer Bosch Allegiant przyłączony do sieci.



Rysunek 6.3: Lokalne połączenie systemu BVMS z krosownicą Bosch Allegiant

1	Stacje robocze klienta systemu BVMS
2	Management Server z oprogramowaniem Master Control Software
3	Połączenie RS-232
4	Krosownica Allegiant
5	Nadajniki
6	Sieć

Połączenie zdalne



Rysunek 6.4: Zdalne połączenie systemu BVMS z krosownicą Bosch Allegiant

1	Stacje robocze klienta systemu BVMS
2	Management Server z oprogramowaniem Master Control Software
3	Sieć
4	Komputer PC Allegiant z oprogramowaniem Master Control Software
5	Połączenie RS-232
6	Nadajniki
7	Krosownica Allegiant

6.4.2

Konfiguracja kanału sterującego

Aby skonfigurować kanał sterujący, należy wykonać następujące działania:

- Gniazda połączeniowe
- Instalacja oprogramowania
- Utworzenie pliku konfiguracyjnego Allegiant
- Dodanie krosownicy Allegiant do systemu BVMS

- Konfiguracja nazw użytkownika

Gniazda połączeniowe

BVMS z krosownicą Allegiant należy podłączyć jeden komputer za pomocą portu szeregowego (RS-232) do portu konsoli krosownicy Allegiant (przy użyciu specjalnego przewodu firmy Bosch). Może to być komputer typu Management Server wchodzący w skład systemu BVMS lub dowolny inny komputer PC przyłączony do sieci.

Instalacja oprogramowania Allegiant Master Control Software

1. Zatrzymaj usługę Management Server, jeśli jest uruchomiona (klikając kolejno opcje **Start > Panel sterowania > Usługi >** kliknij prawym przyciskiem myszy opcję BVMS Management Server > **Zatrzymaj**)
2. Zainstaluj oprogramowanie Allegiant Master Control Software na Management Server i komputerze PC Allegiant (jeśli jest używany).
3. Zdalny komputer Allegiant należy skonfigurować tak, aby program Allegiant Network Host (Id_alghw.exe) uruchamiał się wraz z systemem operacyjnym. Spowoduje to uruchomienie niezbędnych usług Allegiant, umożliwiających innym komputerom PC w sieci dostęp do krosownicy Allegiant. Oprogramowanie pracuje w sposób niewidoczny. Podłączenie klucza sprzętowego do tego komputera nie jest konieczne.
Aby usługa uruchamiała się automatycznie podczas procedury uruchamiania komputera, skopiuj łącznie do pliku Id_alghw.exe do folderu Autostart komputera.

Tworzenie pliku konfiguracyjnego Bosch Allegiant

1. Za pomocą oprogramowania Allegiant Master Control Software utwórz plik konfiguracyjny Allegiant, który określa parametry komputera podłączonego do krosownicy Allegiant. Do tego zadania wymagany jest klucz zabezpieczający Master Control.
2. W menu Transfer kliknij pozycję Communication Setup. Na liście Current Host wprowadź nazwę DNS komputera podłączonego do krosownicy Allegiant, a następnie wprowadź parametry portu szeregowego (numer portu COM, prędkość transmisji itp.) połączony z krosownicą Allegiant. Umożliwi to oprogramowaniu Master Control Software zainstalowanemu na komputerze typu Management Server lub innym komputerze nawiązywanie połączenia z systemem Allegiant. Jeśli konfiguracja się nie powiodła, upewnij się, że oprogramowanie Master Control Software lub program Allegiant Network Host są uruchomione na komputerze dołączonym do krosownicy Allegiant, a zabezpieczenia sieci pozwalają na zdalny dostęp do tego komputera.
3. W menu Transfer kliknij pozycję Upload. Zaznacz wszystkie tabele i kliknij przycisk Upload. Aby zapisać plik konfiguracyjny, wybierz katalog.
4. Wyjdź z oprogramowania Master Control Software.

Dodawanie krosownicy Bosch Allegiant do systemu BVMS

1. Uruchom usługę Management Server wchodzącą w skład systemu BVMS, uruchom program Configuration Client i dodaj urządzenie Allegiant, wskazując odpowiedni plik konfiguracyjny (szczegółowe instrukcje zawiera rozdział Dodawanie urządzenia).
2. Upewnij się, że plik konfiguracyjny oprogramowania Allegiant Master Control Software używany w systemie BVMS odpowiada bieżącej konfiguracji krosownicy Allegiant.
System BVMS uruchamia wymagane komponenty oprogramowania Master Control Software niewidocznie w tle.

Konfiguracja nazwy użytkownika do logowania do usług Allegiant

Jeśli krosownica Allegiant jest podłączona do komputera sieciowego, a nie do komputera typu Management Server, należy się upewnić, że usługi Allegiant na tym komputerze PC i komputerze typu Management Server wykorzystują podczas logowania to samo konto użytkownika. Ten użytkownik musi być członkiem grupy administratorów.

Więcej informacji znajduje się w dokumentacji

Zapoznać się z odnośnikami, aby uzyskać szczegółowe informacje na temat dostępnych okien:

- strona Krosownice wizyjne, Strona 134

Zapoznać się z odnośnikami, aby uzyskać informacje na temat dostępnych szczegółowych instrukcji:

- Konfigurowanie urządzenia Bosch Allegiant, Strona 134

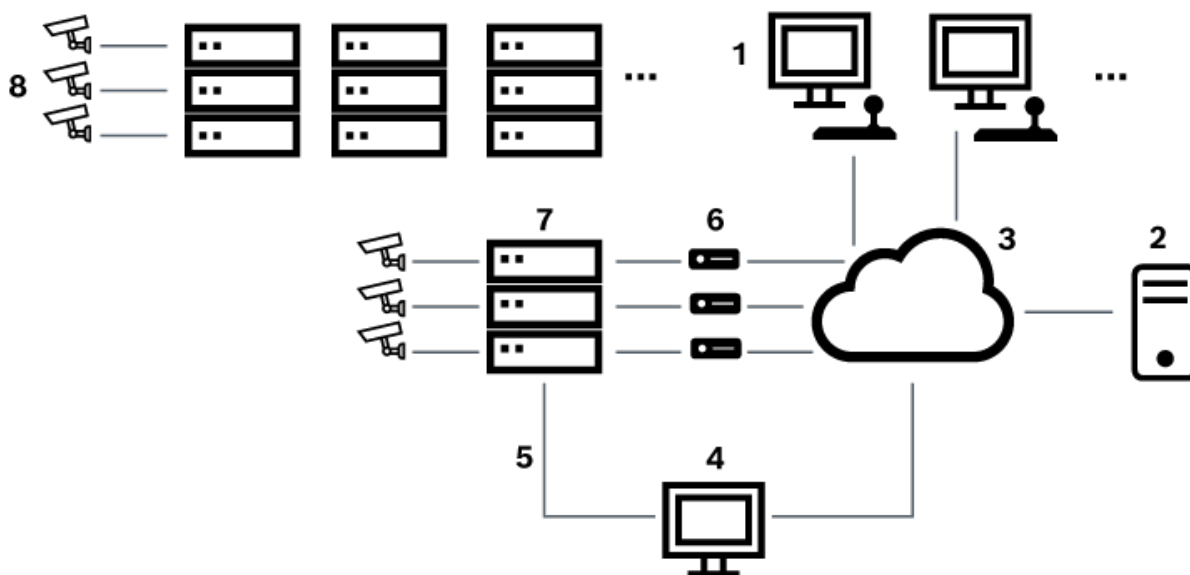
Patrz

- strona Krosownice wizyjne, Strona 134

6.4.3**Koncepcja systemu satelitarnego Bosch Allegiant**

Krosownica Allegiant umożliwia połączenie ze sobą kilku systemów Allegiant za pomocą systemu satelitarnego. W tym przypadku kilka systemów Allegiant jest widocznych dla systemu BVMS jako jeden, duży system, zapewniający dostęp do wszystkich kamer we wszystkich systemach.

W systemie satelitarnym Allegiant wyjścia monitorów satelitarnych krosownic podrzędnych Allegiant są połączone z wejściami wizyjnymi w krosownicy głównej Allegiant. To połączenie jest nazywane linią połączenia. Ponadto między krosownicą główną i podrzędną jest tworzony kanał sterujący. Kiedy kamera z podrzędnej krosownicy Allegiant jest wywoływana przez główną krosownicę Allegiant, do krosownicy podrzędnej jest wysyłane polecenie nakazujące przełączenie żądanej kamery na linię połączenia. W tym samym czasie główna krosownica Allegiant przełącza wejście linii na wymagane wyjście monitora głównej krosownicy Allegiant. To działanie kończy tworzenie połączenia wizyjnego z żądanej kamery systemu podrzędnego do wybranego monitora systemu głównego.



Rysunek 6.5: System Bosch Allegiant rozbudowany o przełączniki satelitarne

1	Stacje robocze klienta systemu BVMS
2	Management Server z oprogramowaniem Master Control Software
3	Sieć
4	Komputer PC Allegiant z oprogramowaniem Master Control Software
5	Połączenie RS-232
6	Nadajniki
7	Krosownica Allegiant

8	Krosownica satelitarna Allegiant

Koncepcja systemu satelitarnego może być tak zastosowana, że krosownica Allegiant może być zarówno krosownicą główną, jak i satelitarną. W ten sposób krosownica Allegiant może mieć dostęp do obrazów z kamer z innych krosownic. Wymagane jest tylko połączenie linii połączeń oraz linii sterujących w obydwu kierunkach i prawidłowe skonfigurowanie tabel Allegiant.

Koncepcję można rozszerzać bez ograniczeń na wiele systemów Allegiant. System Allegiant może posiadać wiele systemów podrzędnych oraz może być systemem podrzędnym dołączonym do wielu systemów głównych. Użytkownik może zaprogramować tabele Allegiant, aby umożliwić lub zabronić użytkownikom dostęp do obrazów z kamer zgodnie z wymaganiami każdej z lokalizacji.

6.5

Polecenia CCL systemu Allegiant obsługiwane w systemie BVMS

W celu korzystania z poleceń CCL należy zapoznać się z instrukcją użytkownika poleceń CCL. Jest ona dostępna w Internetowym katalogu produktów, w sekcji dokumentacji poszczególnych krosownic LTC Allegiant.

Obsługiwane polecenia	Opis	Uwagi
Przełączanie/sekwencja		
LCM	Przełączanie kamery logicznej na monitor	Polecenia LCM, LCM+ i LCM- są równoważne.
LCMP	Przełącz kamerę logiczną na monitor z wywołaniem położenia zaprogramowanego	
MON+CAM	Przełącz kamerę fizyczną na monitor	
MON-RUN	Uruchom sekwencję według numeru monitora	
MON-HOLD	Wstrzymaj sekwencję według numeru monitora	
SEQ-REQ	Żądanie sekwencji	
SEQ-ULD	Usuń sekwencję z pamięci	
Dekoder/sterownik		
R/D	Podstawowe polecenia sterujące	
REMOTE-ACTION	Polecenia jednoczesnego obrotu, pochylenia i powiększenia	
REMOTE-TGL	Polecenia przełączanego obrotu, pochylenia i powiększenia	
PREPOS-SET	Ustawienie położenia zaprogramowanego	

Obsługiwane polecenia	Opis	Uwagi
Przełączanie/sekwencja		
PREPOS	Wywołanie położenia zaprogramowanego	
AUX-ON AUX-OFF	Dodatkowe polecenia sterujące – Dodatkowe wł. – Dodatkowe wył.	
VARSPEED_PTZ	Polecenia zmiennej prędkości	
Alarm		Służy do kontroli wirtualnych wejść. Przykładowo polecenie „+alarm 1” zamyka wirtualne wejście 1, a „-alarm 1” otwiera wirtualne wejście 1
+ALARM	Aktywuj alarm	Otwarcie wejścia wirtualnego w systemie BVMS.
-ALARM	Dezaktywuj alarm	Zamknięcie wejścia wirtualnego w systemie BVMS.
System		
TC8x00>HEX	Ustaw tryb szesnastkowy	
TC8x00>DECIMAL	Ustaw tryb dziesiętny	

7 Rozpoczęcie pracy

Niniejszy rozdział zawiera informacje o rozpoczynaniu pracy z systemem BVMS.

7.1 Instalacja modułów oprogramowania

**Uwaga!**

Należy zainstalować wszystkie moduły oprogramowania na komputerze przeznaczonym do współpracy z tymi modułami.

Aby zainstalować, należy:

Zamknąć aplikację Configuration Client przed uruchomieniem konfiguracji systemu BVMS.

1. Uruchomić plik Setup.exe lub uruchom opcję Setup (Instalacja) BVMS w oknie powitalnym.
2. W kolejnym oknie dialogowym wybrać moduły przeznaczone do zainstalowania na danym komputerze.
3. Postępować zgodnie ze wskazówkami wyświetlanymi na ekranie.

7.2 Używanie kreatora Config Wizard

Config Wizard umożliwia szybką i łatwą konfigurację mniejszego systemu. Config Wizard pomaga uzyskać skonfigurowany system obejmujący VRM, system iSCSI, kamery, profile zapisu oraz grupy użytkowników.

W przypadku standardowych instalacji oprogramowania systemy iSCSI muszą zostać dodane ręcznie. Konfiguracja grup użytkowników i ich uprawnień przebiega automatycznie. Można dodawać i usuwać użytkowników oraz ustawiać hasła.

Config Wizard ma dostęp do serwera Management Server tylko na komputerze lokalnym.

Uaktywnioną konfigurację można zapisać jako kopię zapasową i zaimportować ją w późniejszym czasie. Po zaimportowaniu konfiguracja może zostać zmodyfikowana.

Program Config Wizard automatycznie dodaje lokalny system VRM zarówno w przypadku standardowej instalacji oprogramowania, jak i DIVAR IP.

W przypadku DIVAR IP lokalne urządzenie iSCSI jest również dodawane automatycznie, jeśli nie było wcześniej dostępne.

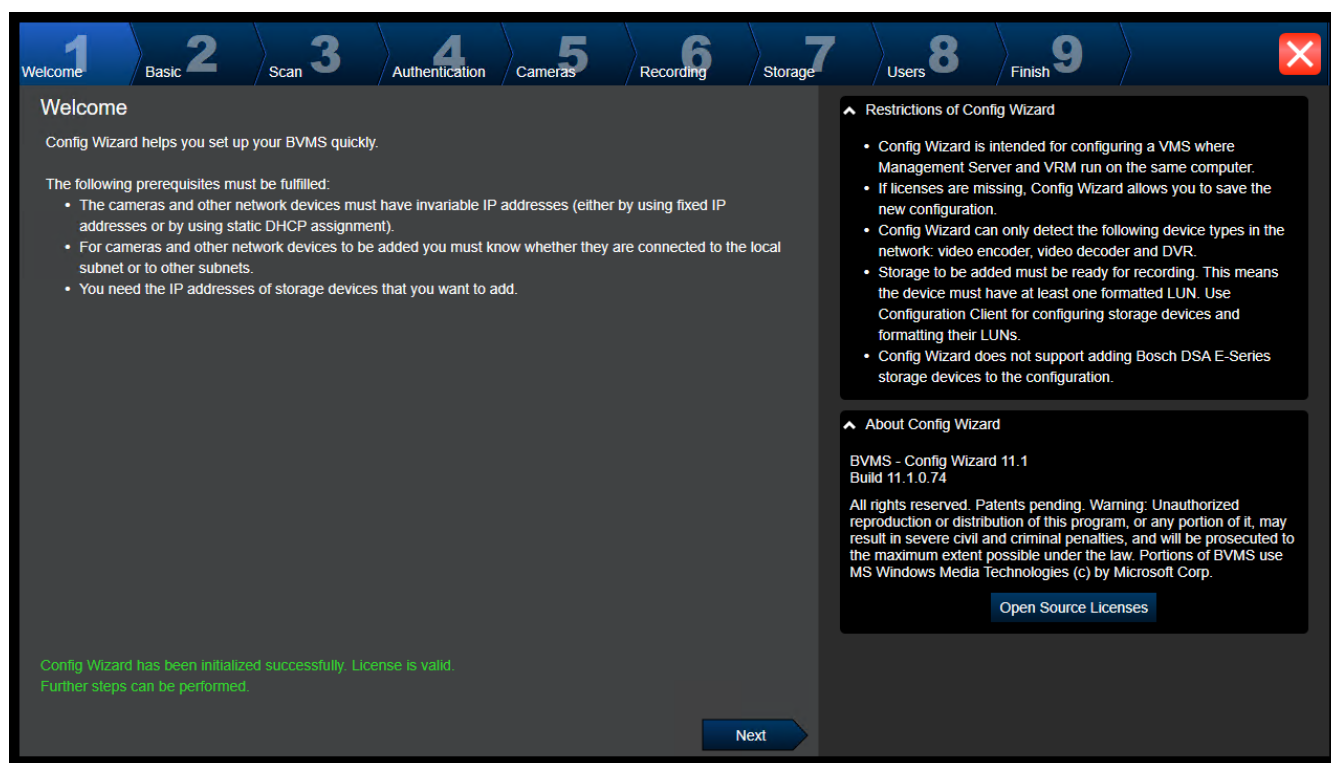
**Uwaga!**

Aby używać dekodatorów w systemie, należy upewnić się, że wszystkie nadajniki mają to samo hasło dla poziomu autoryzacji użytkownika user.

Aby uruchomić program Config Wizard:

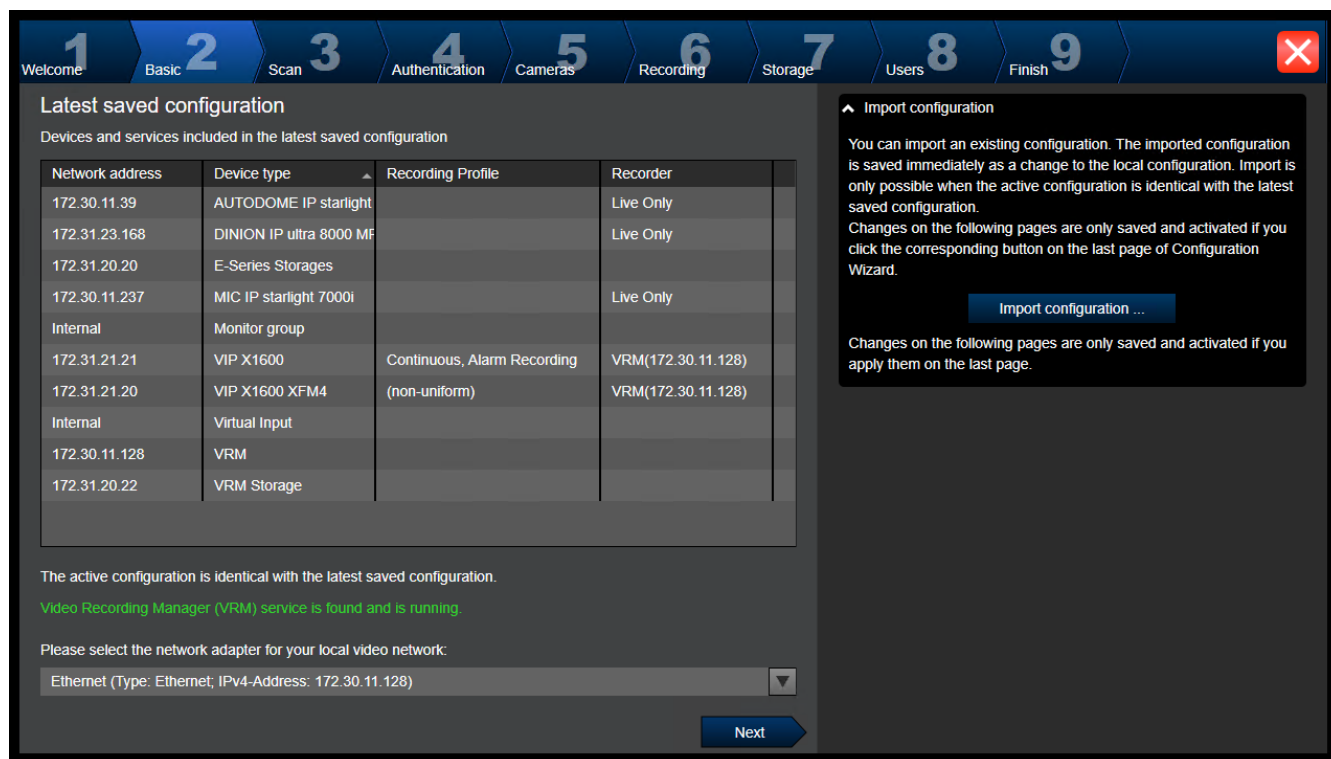
- ▶ Kliknij kolejno opcje **Uruchom** > **Wszystkie programy** > BVMS > Config Wizard
- Zostanie wyświetlona strona Welcome.

Strona Welcome



► Kliknij przycisk **Next**, aby kontynuować.

Strona Basic



Na tej stronie jest wyświetlana ostatnia zapisana konfiguracja. Można zmienić istniejącą konfigurację, importując plik BVMS. Po kliknięciu opcji **Next** zmiana zostanie zapisana, lecz konfiguracja nie będzie aktywna.

Użytkownik może wybrać w systemie kartę sieciową komputera, który jest połączony z urządzeniami wizyjnymi (kamerami sieciowymi, nadajnikami, odbiornikami, systemami pamięci masowej iSCSI). Adres IP wybranej karty sieciowej będzie adresem IP urządzeń VRM i VSG oraz lokalnego systemu pamięci masowej iSCSI.

Kliknąć przycisk **Port Mapping**, aby wprowadzić publiczny adres IP lub nazwę DNS, jeśli ma być możliwy dostęp do systemu za pośrednictwem Internetu.

Strona 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
☒	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
☐	Dinion IP 5000i IR	172.31.23.95	00-07-5f-93-cf-bb	DINION IP 5000i IR
☐	Dinion IP Starlight 6000 HD	172.31.23.145	00-07-5f-8d-21-d3	DINION IP starlight 6000 HD

Next

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

Scan options

Range of network scan:

☐ Local subnet only (recommended)

☐ Across subnets

Rescan network

Change network addresses

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

Change IP Addresses

Uwaga:

Skanowanie w poszukiwaniu urządzeń może trochę potrwać. Skanowanie można anulować.

Wszystkie urządzenia, które zostały już wykryte podczas skanowania, są wyświetlone w tabeli.

Na tej stronie są wyświetlane wszystkie urządzenia wideo nieuwzględnione w ostatnio zapisanej konfiguracji.

Usuń zaznaczenia pól wyboru przy urządzeniach, których nie chcesz dodawać do konfiguracji, i kliknij przycisk **Next**.

Jeśli wybrane urządzenia nie należą do tego samego zakresu adresów IP co system DIVAR IP, można zmienić adres IP urządzenia, wprowadzając adres początkowy zakresu adresów IP urządzenia.

Strona 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-1600XFM (172.31.22.4)	172.31.22.4	service		🔒
VIPX-1600XFM (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.

▼ Change default password

Show passwords Set Initial Passwords Next

Ta strona jest używana do uwierzytelniania urządzeń wideo chronionych hasłem. Aby w łatwy sposób uwierzytelniać tym samym hasłem wiele urządzeń, można użyć funkcji schowka (CTRL+C, CTRL+V):

1. Kliknij polecenie **Show passwords**.
2. Wybierz wiersz z uwierzytelnionym urządzeniem (z ikoną zielonej kłódki), naciśnij klawisze CTRL+C, wybierz wiersze z czerwoną kłódką i naciśnij klawisze CTRL+V.

Jeśli użytkownik przez kilka sekund nie wprowadzi żadnego znaku w polu hasła lub kliknie poza polem, sprawdzenie hasła następuje automatycznie.

Można wprowadzić globalne hasło domyślne do wszystkich urządzeń, które nie są obecnie chronione hasłem.

Jeśli urządzenie wymaga hasła początkowego, wyświetlony zostanie symbol ⚠.

Aby ustawić hasło początkowe:

1. Wprowadzić hasło w polu **Password**.
2. Kliknąć polecenie **Set Initial Passwords**.

Hasło początkowe zostanie ustawione.

Uwaga: dopóki nie ustawiono hasła początkowego dla wszystkich urządzeń na liście, które tego wymagają, nie można kontynuować.

3. Kliknąć przycisk **Next**, aby kontynuować.

Strona 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

Ta strona umożliwia zarządzanie kamerami należącymi do systemu.

Strona 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

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

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

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

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

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

Motion Alarm Recording in Recording Profiles

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

Next

Na tej stronie wyświetlane są tylko nowo dodane kamery. Po uaktywnieniu tej konfiguracji nie można zmieniać przypisania profili tych kamer.

Zapis ruchu można włączać w profilach zapisu z uaktywnionym zapisem zwykłym i alarmowym. Zapis zwykły i alarmowy można w razie potrzeby skonfigurować w programie Configuration Client (w oknie dialogowym **Ustawienia zaplanowanego zapisu**).

Funkcja VCA jest włączana automatycznie w przypadku każdej nowo dodanej kamery.

Strona Storage

The screenshot shows the 'Add storage' configuration window. The top navigation bar includes steps: 1 Welcome, 2 Basic, 3 Scan, 4 Authentication, 5 Cameras, 6 Recording, 7 Storage (active), 8 Users, and 9 Finish. The main content area is titled 'Add storage' and features a table with columns 'IP address' and 'Storage type'. A 'Next' button is located at the bottom right. A text box on the right states: '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.'

Ta strona umożliwia dodawanie kolejnych urządzeń pamięci masowej iSCSI.

Strona Users

Na tej stronie można dodać nowych użytkowników do istniejących grup użytkowników.

- ▶ Dla każdego nowego użytkownika należy wprowadzić nazwę użytkownika, opis i ustawić hasło.

Strong password policy

Pole wyboru **Strong password policy** jest wstępnie zaznaczone dla wszystkich nowo utworzonych grup użytkowników.

Zalecamy zachować to ustawienie w celu zwiększenia ochrony przed nieautoryzowanym dostępem komputera.

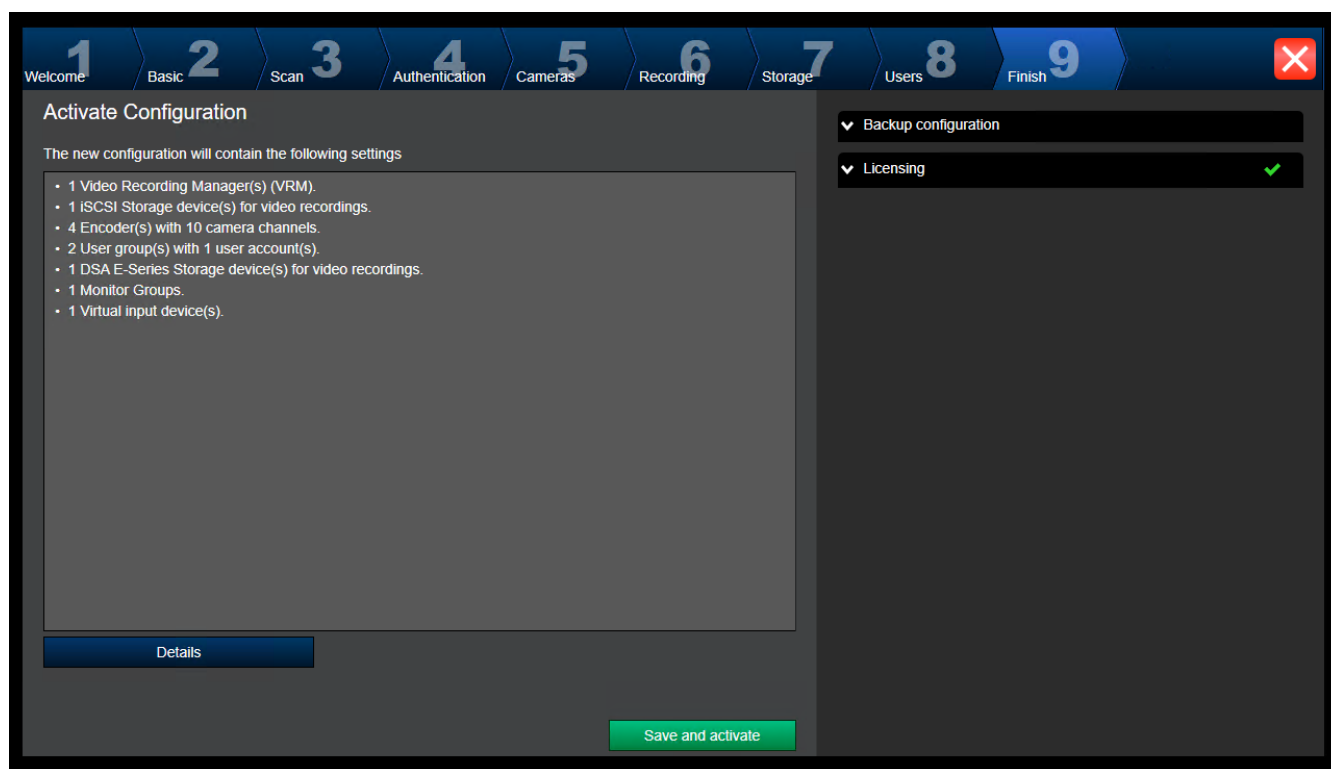
Mają zastosowanie następujące reguły:

- Minimalna długość hasła dla grupy użytkowników jest skonfigurowana na stronie **Zasady konta**.
- Nie należy używać jednego z poprzedniej haseł.
- Należy zastosować co najmniej jedną dużą literę (od A do Z).
- Należy zastosować co najmniej jedną cyfrę (od 0 do 9).
- Należy zastosować co najmniej jeden znak specjalny (np. ! \$ # %).
- ▶ Kliknąć przycisk **Apply**, aby zastosować ustawienia, a następnie przycisk **Next**, aby kontynuować.

Uwaga: pomimo włączenia opcji **Strong password policy** nie będzie można kontynuować, dopóki hasła nie zostaną ustawione dla wszystkich użytkowników. Aby kontynuować, ustawić brakujące hasła.

Do dodawania grup użytkowników i zmiany ich uprawnień służy program Configuration Client.

Strona Finish



Przed uaktywnieniem konfiguracji trzeba wykonać następujące zadania:

- Wprowadzić globalne hasło domyślne do wszystkich urządzeń, które nie są obecnie chronione hasłem.
- Uaktywnić pakiet licencji (w razie potrzeby).

Globalne hasło domyślne

Jeśli w programie Configuration Client wyłączona jest opcja **Enforce password protection on activation (Ustawienia -> Opcje)**, uaktywnienie nie wymaga wprowadzenia globalnego hasła domyślnego.

Licencjonowanie

Rozwinąć węzeł **Licensing** i kliknąć element **License Wizard**, aby sprawdzić lub uaktywnić pakiet licencji.

Kliknięcie przycisku **Save and activate** powoduje aktywowanie konfiguracji.

Po udanym uaktywnieniu pojawia się ponownie strona **Finish**. Następnie w razie potrzeby można zachować kopię zapasową konfiguracji: należy kliknąć opcję **Save backup copy**.

Kliknięcie przycisku **Save and activate** powoduje aktywowanie konfiguracji.

Po udanym uaktywnieniu pojawia się ponownie strona **Zakończ**. Następnie w razie potrzeby można zachować kopię zapasową konfiguracji: należy kliknąć opcję **Save backup copy**.

7.3

Uruchamianie programu Configuration Client



Uwaga!

Tylko użytkownik będący administratorem może logować się do programu Configuration Client.

Domyślną nazwą administratora jest Admin. Tylko ten użytkownik może zalogować się do programu Configuration Client podczas uruchamiania programu Configuration Client po raz pierwszy.

Po uruchomieniu programu Configuration Client można zmienić nazwę użytkownika Admin i zmienić hasło.

Uwaga:

Nie można uruchomić programu Configuration Client, jeśli inny użytkownik już uruchomił program Configuration Client na innym komputerze.

Aby uruchomić program Configuration Client:

1. W menu **Start** wybrać **Programy** > BVMS > Configuration Client.
Zostanie wyświetlone okno dialogowe logowania.
2. W polu **Nazwa użytkownika:** wprowadzić swoją nazwę użytkownika.
Po pierwszym uruchomieniu aplikacji w polu nazwy użytkownika wpisać Admin. Podanie hasła nie jest wymagane.
3. Wpisać hasło w polu **Hasło:**.
4. Kliknij **OK**.
Aplikacja zostanie uruchomiona.

Przy pierwszym uruchomieniu programu Configuration Client przez użytkownika-administratora, zostanie wyświetlone okno dialogowe **Naruszono politykę haseł** z prośbą o ustawienie hasła dla konta użytkownika administratora. Bezwzględnie zaleca się zachowanie tego ustawienia i ustawienie dla konta użytkownika administratora silnego hasła, zgodnego z zasadami polityki haseł.

Patrz

- Zasady silnych haseł , Strona 351
- Konfigurowanie grupy administratorów, Strona 356

7.4

Wybieranie wersji językowej modułu Configuration Client

Wersję językową programu Configuration Client wybiera się niezależnie od analogicznych ustawień wybranych w systemie operacyjnym Windows.

Konfiguracja żądanej wersji językowej:

1. W menu **Ustawienia** kliknąć **Opcje**.
Zostanie wyświetlone okno dialogowe **Opcje**.
2. Na liście **Język** należy wybrać żądany język.
W przypadku zaznaczenia opcji **Język systemu** zostanie wybrany taki sam język, jaki jest używany w systemie Windows komputera.
3. Kliknąć **OK**.
Wersja językowa zostanie zmieniona po zamknięciu i ponownym uruchomieniu aplikacji.

7.5

Wybieranie wersji językowej modułu Operator Client

Dla modułu Operator Client można wybrać inną wersję językową niż dla systemu Windows i programu Configuration Client. Stosowne ustawienia wybiera się w programie Configuration Client.

Konfiguracja żądanej wersji językowej:

1. Kliknij **Grupy użytkowników** >  . Kliknij kartę **Właściwości grupy użytkowników**. Kliknij kartę **Uprawnienia do obsługi**.
2. Zaznacz żadaną opcję na liście **Język**.
3. Kliknij  , aby zapisać ustawienia.



4. Kliknij , aby uaktywnić konfigurację.
Uruchom ponownie Operator Client.

7.6

Skanowanie w poszukiwaniu urządzeń

Okno główne > **Urządzenia**

Można skanować w poszukiwaniu poniższych urządzeń, aby dodać je za pomocą okna dialogowego kreatora **BVMS Scan Wizard**:

- Urządzenia VRM
- Nadajniki
- Nadajniki podglądu bieżącego i z lokalną pamięcią masową
- Nadajniki podglądu bieżącego ONVIF
- Nadajniki z obsługą lokalnego urządzenia pamięci masowej
- Dekodery
- Urządzenia Video Streaming Gateway (VSG)
- Urządzenia DVR

Aby dodać urządzenia poprzez skanowanie, należy przejrzeć informacje na temat tych urządzeń dostępne w rozdziale strona *Urządzenia*, Strona 124.

Patrz

- Dodawanie urządzeń VRM poprzez skanowanie; Strona 169
- Dodawanie urządzenia ONVIF tylko do podglądu bieżącego za pomocą skanowania, Strona 236
- Dodawanie urządzeń podglądu bieżącego poprzez skanowanie, Strona 209
- Dodawanie urządzenia, Strona 125

7.7

Dostęp do systemu

W celu uzyskania dostępu do systemu należy wykonać następujące czynności:

1. W celu wybrania adresu sieciowego dla żądanego systemu należy wykonać jedną z poniższych czynności:
 - Kliknij zaznaczoną pozycję na liście.
 - Wpisz ręcznie adres sieci.
 - Wybierz adres sieciowy za pomocą funkcji Server Lookup.
2. Zaloguj się w żądanym systemie:
 - System z jednym serwerem
 - System Enterprise System

7.8

Używanie funkcji Server Lookup

- Funkcja BVMS Server Lookup umożliwia operatorom nawiązywanie połączenia z serwerem BVMS Management Server wybranym z podanej listy serwerów.
- Pojedynczy użytkownik programu Configuration Client lub Operator Client może kolejno nawiązywać połączenia z wieloma punktami dostępowymi systemu.
- Punktami dostępowymi systemu mogą być serwery Management Server i Enterprise Management Server.
- Funkcja Server Lookup wykorzystuje dedykowany serwer Management Server do obsługi listy serwerów.
- Funkcje Server Lookup oraz Management Server lub Enterprise Management Server mogą być uruchomione na jednym komputerze.

- Program Server Lookup umożliwia odszukiwanie punktów dostępowych systemu na podstawie ich nazw lub opisów.
- Po połączeniu do serwera Management Server program Operator Client odbiera alarmy i zdarzenia z serwera BVMS Management Server i umożliwia wyświetlanie danych na żywo lub ich odtwarzanie

W celu uzyskania dostępu:

1. Uruchomić program Operator Client lub Configuration Client.
Zostanie wyświetlone okno dialogowe logowania.
2. Na liście **Połączenie:** wybrać w przypadku programu Configuration Client opcję **<Książka adresowa...>** lub w przypadku programu Operator Client — opcję **<Książka adresowa...>**.
Jeśli w przypadku danego serwera skonfigurowano prywatny i publiczny adres IP, będzie to odpowiednio oznaczone.
Po pierwszym wybraniu opcji **<Książka adresowa...>** lub **<Książka adresowa...>** zostanie wyświetlone okno dialogowe **Server lookup**.
3. W polu **Adres serwera (Enterprise) Management Server:** należy wpisać prawidłowy adres sieciowy żądanego serwera.
4. Wprowadzić prawidłową nazwę użytkownika i hasło.
5. W razie potrzeby kliknąć **Pamiętaj ustawienia**.
6. Kliknąć **OK**.
Zostanie wyświetlone okno dialogowe **Server lookup**.
7. Wybrać żądany serwer.
8. Kliknąć **OK**.
9. Jeśli wybrany serwer posiada zarówno prywatny, jak i publiczny adres sieciowy, zostanie wyświetlony monit z pytaniem, czy użytkownik korzysta z komputera znajdującego się w sieci prywatnej wybranego serwera.
Nazwa serwera jest dodawana do listy **Połączenie:** w oknie dialogowym logowania.
10. Należy zaznaczyć ten serwer na liście **Połączenie:** i kliknąć **OK**.
Jeśli pole **Pamiętaj ustawienia** zostało wybrane, można będzie w razie ponownej chęci skorzystania z niego wybrać ten serwer bezpośrednio.

7.9 Aktywacja licencji na oprogramowanie

Podczas instalowania BVMS po raz pierwszy musisz aktywować licencje dla zamówionych pakietów oprogramowania, w tym pakietu podstawowego oraz wszelkich rozszerzeń i/lub funkcji opcjonalnych.

Aby aktywować system:

1. Uruchomić program BVMS Configuration Client.
2. W menu **Narzędzia** kliknąć **Manager licencji...**
Zostanie wyświetlone okno dialogowe **Manager licencji**.
3. Kliknąć **Dodaj**, aby dodać licencje.
Zostanie wyświetlone okno dialogowe **Dodaj licencję**.
4. Postępować zgodnie z instrukcjami wyświetlanymi w oknie dialogowym.
5. Po pomyślnej aktywacji, zamknąć okno dialogowe **Dodaj licencję**.
6. Zamknąć okno dialogowe **Manager licencji**.

Dalsze informacje można znaleźć w odpowiedniej dokumentacji licencji na system BVMS.

Patrz

- Okno dialogowe *Inspektor licencji* (menu **Narzędzia**), Strona 77
- Okno dialogowe *Manager licencji* (menu **Narzędzia**), Strona 76

- Okno dialogowe Dodawanie licencji, Strona 77
- Omówienie aktywacji licencji systemu BVMS, Strona 20

7.9.1

Okno dialogowe Manager licencji (menu Narzędzia)

Okno dialogowe > menu **Narzędzia** > polecenie **Manager licencji...**

Umożliwia zarejestrowanie licencji zamówionego pakietu BVMS oraz jego aktualizację o nowe funkcje.

Stan licencji

W tym obszarze wyświetlany jest stan licencji.

Odcisk palca systemu

Dla celów pomocniczych zalecamy podanie **Odcisk palca systemu**.

Lokalizacja instalacji

Podczas aktywacji licencji podstawowej w Bosch Remote Portal należy podać informacje o miejscu instalacji systemu. Te informacje są dostępne tutaj.

Uwaga: te informacje można również podać w innych licencjach, ale tutaj wyświetlane są tylko informacje podane w licencji podstawowej.

Licencje

1. Kliknąć **Dodaj**, aby dodać licencje.
Zostanie wyświetlone okno dialogowe **Dodaj licencję**.
2. Postępować zgodnie z instrukcjami wyświetlanymi w oknie dialogowym.

Ważna licencja

Wyświetla działającą licencję podstawową, która została aktywowana.

Funkcje

- ▶ Kliknij polecenie **License Inspector...**
Pojawi się okno dialogowe **Inspektor licencji**.

Wyświetla ilość licencjonowanych funkcji, które są aktualnie zainstalowane.

Można sprawdzić, czy liczba zainstalowanych licencji systemu BVMS przekracza liczbę licencji zakupionych.

Zainstalowana wersja oprogramowania BVMS

Wyświetla aktualnie zainstalowaną wersję systemu BVMS, np. 11.0.

Wersje oprogramowania BVMS z licencjami

Wyświetla wszystkie wersje BVMS które są zawarte i obsługiwane w aktualnie dostarczonym pliku licencyjnym.

Na przykład: BVMS 11.0 i wszystkie wersje poboczne BVMS 11.x

Data uaktywnienia

Wyświetla datę aktywacji zainstalowanej wersji systemu BVMS.

Data ważności

Wyświetla datę ważności zainstalowanej wersji systemu BVMS. Data ważności ma zastosowanie tylko w przypadku instalacji licencji awaryjnej lub licencji na prezentację sprzedażową.

Software Maintenance Agreement

Data ważności

Jeśli została zakupiona i aktywowana dowolna umowa Software Maintenance Agreement, w tym miejscu wyświetlana jest data ważności.

Patrz

- Aktywacja licencji na oprogramowanie, Strona 75
- Okno dialogowe Dodawanie licencji, Strona 77
- Okno dialogowe Inspektor licencji (menu Narzędzia), Strona 77

7.9.1.1

Okno dialogowe Dodawanie licencji

Okno główne > menu **Narzędzia** > polecenie **Manager licencji...** > **Licencje** > **Dodaj**

Umożliwia dodanie zakupionych licencji lub licencji demonstracyjnych z poziomu witryny Bosch Remote Portal remote.boschsecurity.com do systemu BVMS.

Aby dodać swoje licencje, postępuj zgodnie z instrukcjami w oknie dialogowym.

Dalsze informacje można znaleźć w odpowiedniej dokumentacji licencji na system BVMS.

7.9.2

Okno dialogowe Dodawanie licencji

Okno główne > menu **Narzędzia** > polecenie **Manager licencji...** > **Licencje** > **Dodaj**

Umożliwia dodanie zakupionych licencji lub licencji demonstracyjnych z poziomu witryny Bosch Remote Portal remote.boschsecurity.com do systemu BVMS.

Aby dodać swoje licencje, postępuj zgodnie z instrukcjami w oknie dialogowym.

Dalsze informacje można znaleźć w odpowiedniej dokumentacji licencji na system BVMS.

7.9.3

Okno dialogowe Inspektor licencji (menu Narzędzia)

Okno główne > menu **Narzędzia**, kliknąć polecenie **License Inspector...** > okno dialogowe **Inspektor licencji**

Wyświetla ilość licencjonowanych funkcji, które są aktualnie zainstalowane.

Można sprawdzić, czy liczba zainstalowanych licencji systemu BVMS przekracza liczbę licencji zakupionych.

Uwaga: jeśli bieżąca konfiguracja systemu przekracza limity aktualnie zainstalowanych licencji, nie można aktywować konfiguracji.

7.10

Utrzymanie systemu BVMS

Ten rozdział zawiera informacje o konserwacji niedawno zainstalowanego lub uaktualnionego systemu BVMS.

W tym celu wykonaj poniższe działania:

- Wyeksportuj konfigurację systemu BVMS i ustawienia użytkownika. Historia wersji (wszystkie wcześniejsze aktywowane wersje konfiguracji) nie jest eksportowana. Zaleca się aktywowanie konfiguracji przed jej eksportowaniem.
 - Zobacz opis procedury w punkcie *Aby eksportować dane konfiguracyjne, należy:*, Strona 77.

LUB

- Wykonaj kopię zapasową pliku elements.bvms. Jest to wymagane, aby przywrócić serwer (Enterprise) Management Server wraz z historią wersji. Nie obejmuje to ustawień użytkownika.
 - Zobacz opis procedury w punkcie *Aby wykonać kopię zapasową:*, Strona 78.
- Zapisz plik konfiguracji VRM (config.xml)
 - Zobacz opis procedury w punkcie *Aby zapisać konfigurację VRM:*, Strona 78.

Tak wyeksportowana konfiguracja nie zachowuje historii systemu. Cofnięcie nie jest możliwe.

Cała konfiguracja systemu wraz z pełną historią zmian jest zapisana w jednym pliku:

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

Aby eksportować dane konfiguracyjne, należy:

1. W menu **System** kliknąć **Eksportuj konfigurację....**
Zostanie wyświetlone okno dialogowe **Eksportuj plik konfiguracyjny**.



Uwaga: Jeśli bieżąca kopia robocza konfiguracji nie jest uaktywniona (jest aktywne), należy zamiast uaktywnionej konfiguracji wyeksportować tę kopię roboczą.

2. Kliknąć **Zapisz**.

3. Wprowadzić nazwę pliku.
Aktualna konfiguracja zostanie wyeksportowana. Zostanie utworzony plik .zip z bazą danych i danymi użytkowników.

Aby wykonać kopię zapasową:

1. Zatrzymaj usługę BVMS **Central Server** na serwerze (Enterprise) Management Server.
2. Skopiuj plik elements.bvms do katalogu kopii zapasowej.
3. Uruchom usługę BVMS **Central Server** na serwerze (Enterprise) Management Server.

Konfiguracja VRM została zapisana w pojedynczym zaszyfrowanym pliku config.xml.

Plik ten można skopiować i zapisać w celu utworzenia kopii zapasowej, gdy usługa VRM działa ponownie.

Plik jest zaszyfrowany i zawiera wszystkie niezbędne dane VRM, takie jak:

- Dane użytkownika
- Wszystkie urządzenia systemu i ich odpowiednie ustawienia VRM

Części konfiguracji VRM są zapisane także w konfiguracji systemu BVMS. Wszelkie zmiany dokonane w tych danych są zapisywane do pliku config.xml po aktywacji konfiguracji systemu BVMS.

Poniższe ustawienia nie są zapisywane w konfiguracji systemu BVMS:

- **Ustawienia VRM > Ustawienia główne**
- **Sieć > SNMP**
- **Serwis > Zaawansowane**
- **Preferencje zapisu**
- **Balans obciążenia**

Wszelkie zmiany dokonane na tych stronach są natychmiast zapisywane na serwerze VRM, ale nie są zapisywane w konfiguracji systemu BVMS.

Aby zapisać konfigurację VRM:

- ▶ Skopiuj plik Config.xml do bezpiecznej lokalizacji.
Plik ten można znaleźć w następującym katalogu na podstawowym VRM:
C:\ProgramData\Bosch\VRM\primary
Plik ten można znaleźć w następującym katalogu na pomocniczym VRM:
C:\ProgramData\Bosch\VRM\secondary

7.11

Wymiana urządzenia

Niniejszy rozdział zawiera informacje o sposobie naprawy systemu, gdy na przykład urządzenie uległo awarii i trzeba je wymienić.

Wymagania

Należy uprzednio wykonać zadania związane z utrzymywaniem systemu.

Patrz

- Utrzymanie systemu BVMS, Strona 77

7.11.1

Wymiana MS / EMS

Nie ma różnic w wymianie Management Server i Enterprise Management Server.

Można albo przywrócić konfigurację starego serwera Management Server, albo Enterprise Management Server lub zaimportować konfigurację wyeksportowaną.

Po przywróceniu konfiguracji identyfikator serwera (Server ID) pozostaje niezmieniony.

Po zaimportowaniu konfiguracji identyfikator serwera otrzymuje wartość z nowego systemu. Nowa wartość identyfikatora serwera jest potrzebna, gdy chce się tworzyć Enterprise System, używając wyeksportowanej konfiguracji, którą importuje się dla każdego serwera Management Server jako szablon. Każdy serwer Management Server w tym systemie Enterprise System musi mieć unikatowy numer serwera.

Można importować i eksportować konfigurację oraz ustawienia użytkownika w tej konfiguracji.

Ustawienia użytkownika obejmują użytkowników dodanych w tej konfiguracji wraz z ich ustawieniami w programie Operator Client, takimi jak rozmiar okna i Ulubione.

Uwaga: Importowanie konfiguracji nie przywraca historii wersji starych konfiguracji. Podczas importowania konfiguracji nie są importowane ustawienia użytkownika. Wyeksportowane ustawienia użytkownika należy przywrócić ręcznie.

Aby zaimportować konfigurację:

1. W menu **System** kliknąć **Import configuration ...**.
Zostanie wyświetlone okno dialogowe **Importuj plik konfiguracyjny**.
2. Wybrać plik do zaimportowania i kliknąć opcję **Otwórz**.
Zostanie wyświetlone okno dialogowe **Importuj konfigurację**.
3. Wprowadzić odpowiednie hasło i kliknąć **OK**.
Program Configuration Client zostanie uruchomiony ponownie. Konieczne będzie ponowne zalogowanie się.
Zaimportowana konfiguracja nie będzie uaktywniona, ale można będzie edytować ją w programie Configuration Client.

Aby przywrócić wyeksportowaną konfigurację:

Dostęp do tego pliku (kopiowanie, usuwanie) jest możliwy tylko wtedy, gdy usługa BVMS **Central Server** jest zatrzymana.

1. Zatrzymaj usługę BVMS **Central Server** na serwerze (Enterprise) Management Server.
2. W razie potrzeby zmień nazwę kopii zapasowej na Elements.bvms.
3. Zamień istniejący plik Elements.bvms.
4. Uruchom usługę BVMS **Central Server** na serwerze (Enterprise) Management Server.

Uwaga: Aby zresetować system do pustej konfiguracji, należy zatrzymać tę usługę i usunąć plik Elements.bvms.

Pozostałe pliki konfiguracji:

- Elements.bvms.bak (od wersji V.2.2): automatyczna kopia zapasowa ostatniej aktywacji zawiera historię wersji. Późniejsze zmiany konfiguracji, które nie zostały aktywowane, nie są uwzględniane.
- Elements_Backup*****.bvms: konfiguracja ze starszej wersji. Ten plik jest tworzony po aktualizacji oprogramowania.

Aby przywrócić wyeksportowane ustawienia użytkownika:

1. Rozpakuj plik zip utworzony podczas eksportu w ramach utrzymywania systemu.
Plik *export.bvms* i katalog *UserData* zostaną wydodrężnione.
2. Na żądanym serwerze (Enterprise) Management Server: skopiuj katalog *UserData* do lokalizacji *C:\ProgramData\Bosch\VMS*.

7.11.2

Wymiana VRM

Warunki wstępne

- Zainstalowany system operacyjny z prawidłowymi ustawieniami sieci i właściwą wersją VRM.

Aby wymienić urządzenie VRM na BVMS:

1. Uruchom program BVMS Configuration Client.
2. W drzewie urządzeń wybierz urządzenie VRM.

3. Wykonaj ustawienia na poniższych stronach, zapisz je i aktywuj konfigurację:

- Okno główne > **Urządzenia** > rozwiń  > rozwiń  > rozwiń 
- Okno główne > **Urządzenia** > rozwiń  > rozwiń  > **Ustawienia VRM** > **Ustawienia główne**
- Okno główne > **Urządzenia** > rozwiń  > rozwiń  > **Sieć** > **SNMP**
- Okno główne > **Urządzenia** > rozwiń  > rozwiń  > **Serwis** > **Zaawansowane**
- Okno główne > **Urządzenia** > rozwiń  > rozwiń  > rozwiń  > **Ustawienia zaawansowane** > **Preferencje zapisu**
- Okno główne > **Urządzenia** > rozwiń  > rozwiń  > rozwiń  > **iSCSI** > **Balans obciążenia**

Aby wymienić urządzenie VRM na BVMS:

Oryginalna kopia zapasowa config.xml dla urządzenia VRM zawiera wszystkie ustawienia konfiguracji (żadne dalsze ustawienia nie są wymagane).

1. Zatrzymaj usługę **Video Recording Manager**.
2. Skopiuj plik config.xml na nowy serwer.
3. Uruchom usługę **Video Recording Manager**.

Aby wymienić urządzenie iSCSI (zaplanowana awaria):

1. Dodaj nowe urządzenie iSCSI.
2. Używając programu Configuration Manager na urządzeniu iSCSI, które ma być wymienione, skonfiguruj wszystkie numery LUN jako tylko do odczytu.

Uwaga: Stare urządzenie iSCSI można usunąć, gdy stare zapisy nie są już potrzebne.



Uwaga!

Po skonfigurowaniu nowego urządzenia iSCSI zaleca się użycie tego samego hasła CHAP, które funkcjonowało dla starego urządzenia.

W przypadku użycia nowego hasła CHAP należy ustawić to hasło CHAP jako hasło CHAP dla całego systemu i przypisać je do wszystkich urządzeń iSCSI.

W przeciwnym wypadku uwierzytelnianie w iSCSI oraz odtwarzanie bezpośrednio z urządzenia iSCSI będzie niemożliwe.

7.11.3

Wymiana nadajnika lub dekodera



Uwaga!

Nie należy usuwać urządzenia z drzewa urządzeń, jeśli chce się zachować zawarte na nim zapisy. Aby wymienić to urządzenie, należy wymienić sprzęt.

Wymiana nadajnika/dekodera na ten sam typ

Warunkiem koniecznym jest urządzenie z domyślnym ustawieniem fabrycznym (adres IP = 192.168.0.1).

1. Odłącz stare urządzenie od sieci.
2. Nie usuwać urządzenia z drzewa urządzeń w programie Configuration Client systemu BVMS! Usunięcie urządzenia z VRM spowoduje utratę zapisów.
3. Podłącz do sieci nowe urządzenie tego samego typu.

**Uwaga!**

W następnym etapie potrzebny będzie wspomniany wyżej adres IP. Z adresem IP przypisanym przez DHCP nie można będzie wykonać skanowania w poszukiwaniu urządzeń.

4. Configuration Client: W menu **Urządzenie** kliknąć **Inicjujące skanowanie urządzeń....**
Zostanie wyświetlone okno dialogowe **Inicjujące skanowanie urządzeń**.
5. Kliknąć komórkę, aby zmienić wymagany adres. W przypadku zmiany wielu urządzeń wybrać żądane rzędy. Za pomocą klawiszy CTRL lub SHIFT można wybrać wiele urządzeń równocześnie. Następnie kliknąć prawym przyciskiem myszy zaznaczone wiersze i wybrać **Ustaw adresy IP...** lub kliknąć **Ustaw maskę podsieci...**, aby zmienić odpowiednie wartości. Wpisać odpowiednią maskę podsieci i adres IP.
Maska podsieci i adres IP muszą być identyczne jak w zastępowanym urządzeniu.
6. Kliknąć **OK**.
7. Po kilku sekundach w drzewie urządzeń będą dostępne ustawienia urządzenia.
8. Zmienić wszystkie wymagane ustawienia urządzenia, które nie są definiowane przez system BVMS (patrz informacje poniżej).
9. Zapisać i aktywować.

Uwagi:

- Podczas początkowego skanowania urządzeń są znajdowane tylko urządzenia z domyślnym adresem IP (192.168.0.1) lub zduplikowanym adresem IP.
- Nie należy używać skanowania VRM do domyślnych urządzeń, ponieważ nie będzie można potem zmienić ich adresu IP.

Wymiana nadajnika z adresem IP przypisanym przez DHCP:

Warunkiem koniecznym jest, aby był to domyślny fabryczny nadajnik (z adresem IP przypisywanym przez DHCP).

1. Podłącz nadajnik bezpośrednio do portu sieci Ethernet komputera.
2. Zapisz konfigurację TCP/IPv4 karty sieciowej, aby przywrócić ją później.
3. Na karcie sieciowej komputera skonfiguruj następujący stały adres IP i maskę podsieci:
192.168.0.2
255.255.255.0
4. Uruchom przeglądarkę Internet Explorer.
5. Na pasku **Adres** wpisz 192.168.0.1.
Pojawi się strona sieci Web urządzenia.
6. Kliknij **Ustawienia**, a następnie **Sieć**.
7. Na stronie **Sieć** wybierz na liście **DHCP** opcję **Off**.
8. W polach **Adres IP**, **Maska podsieci** i **Adres bramy** wpisz odpowiednie dla danej sieci wartości.
9. Kliknij **Ustaw i uruchom ponownie**.
10. Przywróć konfigurację karty sieciowej.

Wymiana nadajnika/dekodera na inny typ

- Odłącz stare urządzenie od sieci.
- Nie usuwać urządzenia z drzewa urządzeń w programie Configuration Client systemu BVMS!
- Podłączyć do sieci urządzenie nowego typu.

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > rozwiń  > kliknij prawym

przyciskiem myszy  > kliknij okno dialogowe **Edytuj nadajnik** > okno dialogowe **Edytuj nadajnik**
lub

Okno główne > **Urządzenia** > Rozwiń  > Kliknij prawym przyciskiem myszy  > Kliknij **Edytuj nadajnik** > Okno dialogowe **Edytuj nadajnik**
lub

Okno główne > **Urządzenia** > Rozwiń  > Kliknij prawym przyciskiem myszy  > Kliknij **Edytuj nadajnik** > Okno dialogowe **Edytuj nadajnik**
lub

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > kliknij prawym przyciskiem myszy  > kliknij **Edytuj odbiornik** > okno dialogowe **Edytuj odbiornik**

Po zakończeniu rozbudowy urządzenia można zaktualizować informacje dotyczące jego wydajności.

Tekst komunikatu informuje, czy pobrane dane o wydajności urządzenia są zgodne z informacjami zapisanymi w BVMS.

Aby zaktualizować program:

1. Kliknij **OK**.
Zostanie wyświetlone okno komunikatu zawierające wiadomość:
Jeśli zatwierdzisz informacje dotyczące wydajności urządzenia, ustawienia zapisu i ustawienia zdarzeń tego urządzenia mogą ulec zmianie. Sprawdź ustawienia tego urządzenia.
2. Kliknij **OK**.
Informacje o wydajności urządzenia zostały zaktualizowane.

Wymiana kamery VSG

Wymieniając kamerę VSG, należy się upewnić, że nowa kamera ma taki sam typ, adres IP i profil ONVIF, jak stara.

Ponadto przed wymianą starej kamery AXIS w nowej kamerze AXIS należy za pomocą interfejsu Web kamery VSG wybrać następujące ustawienia:

- Ustawić hasło dla użytkownika typu root
- Skonfigurować synchronizację czasową
- Wyłącz łącze adresu lokalnego
- Utwórz użytkownika ONVIF
- Wyłącz ochronę przed atakiem metodą powtórzeń

Ustawienia regulowane przez system BVMS

Nadajniki i dekodery skonfigurowane w systemie BVMS są sterowane z poziomu BVMS Server i dlatego nie można ich współużytkować z innymi aplikacjami.

Za pomocą programu BVMS Device Monitor można sprawdzić, które urządzenia różnią się konfiguracją od konfiguracji systemu BVMS.

Oprogramowanie BVMS Configuration Client udostępnia strony do konfiguracji wszystkich urządzeń BVIP.

Zakres ustawień zależy od konkretnego modelu urządzenia BVIP (np. VIPX 1600 XFM4).

System BVMS kontroluje wszystkie ustawienia BVIP wymagane do bezproblemowego zintegrowania urządzeń z systemem BVMS.

Ustawienia regulowane przez system BVMS:

- Nazwa kamery
- Ustawienia serwera czasu
- Zarządzanie zapisami (profile, czasy przechowywania, harmonogramy)
- Definicje ustawień jakości
- Hasła

Zapisane w konfiguracji systemu BVMS, ale bez możliwości zmiany z poziomu urządzeń:

- Adres IP (adres IP można zmienić w oknie dialogowym konfiguracji urządzeń IP systemu BVMS)
- Nazwy przekaźników/wejść (wyświetlane są różnice pomiędzy nazwami w urządzeniu a nazwami skonfigurowanymi w systemie BVMS)

Zdarzenia systemowe w przypadku rozbieżności w konfiguracji urządzenia

- W przypadku gdy konfiguracja urządzenia zostanie poprawiona w trakcie okresowego sprawdzania, generowane są zdarzenia SystemInfo.
- Gdy rozbieżność konfiguracji urządzenia zostanie wykryta po raz pierwszy, generowane są zdarzenia SystemWarning. Kolejne sprawdzenia nie generują tego zdarzenia do czasu, aż konfiguracja zostanie poprawiona w trakcie wykonywania okresowej korekty.
- Gdy podczas aktywacji okresowego sprawdzania zostanie wykryty błąd konfiguracji, generowane są zdarzenia SytemError. Kolejne sprawdzenia nie generują tego zdarzenia do czasu, aż konfiguracja zostanie poprawiona w trakcie wykonywania okresowej korekty.

7.11.4

Wymiana stacji roboczej Operator Client

Aby wymienić stację roboczą Operator Client:

1. Wymień komputer.
2. Uruchom konfigurację BVMS nowego komputera.
3. Na liście komponentów, które mają być zainstalowane, wybierz Operator Client.
W razie potrzeby wybierz inne komponenty, które były zainstalowane na wymienianym komputerze.
4. Zainstaluj oprogramowanie.

7.11.5

Testy końcowe

Aby sprawdzić wymianę MS/EMS i stacji roboczej Operator Client:

1. Uaktywnij konfigurację.
2. Uruchom program Operator Client.
3. Sprawdź drzewo logiczne w programie Operator Client.
Musi być ono identyczne z drzewem logicznym w programie Configuration Client.

Aby sprawdzić wymianę VRM:

- ▶ Uruchom VRM Monitor i sprawdź aktywne zapisy.

7.11.6

Odzyskiwanie DIVAR IP

Zobacz w podręczniku instalacji DIVAR IP. W rozdziale dotyczącym odzyskiwania jednostki znajduje się opis wymaganych czynności.

7.12

Konfiguracja synchronizacji czasowej



Uwaga!

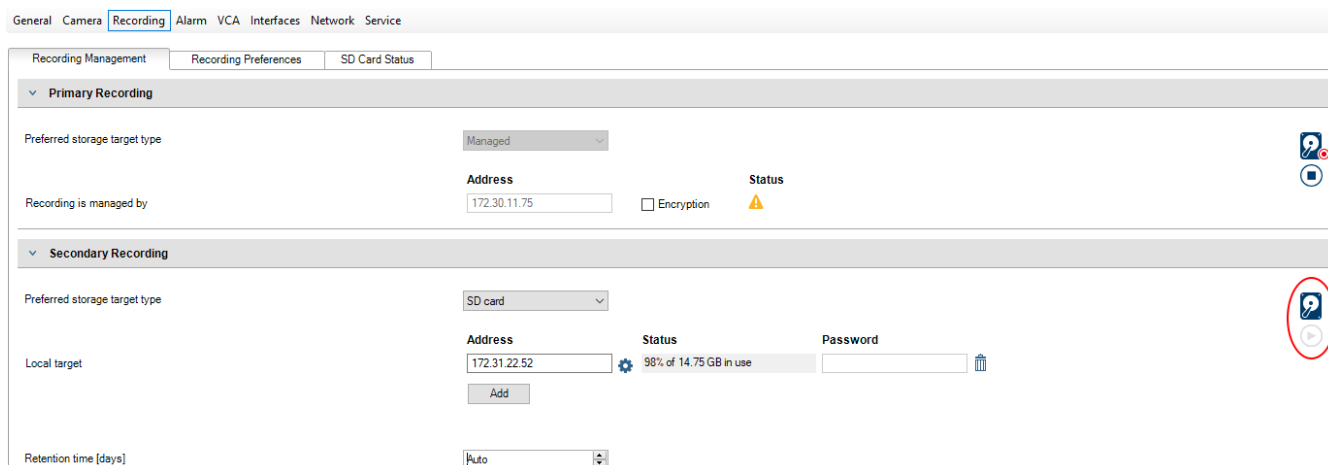
Upewnić się, że czas wszystkich komputerów systemu BVMS jest zsynchronizowany z serwerem Management Server. W przeciwnym razie może dojść do utraty zarejestrowanych danych wizyjnych. Na komputerze typu Management Server należy odpowiednio skonfigurować oprogramowanie serwera czasu. Z kolei na innym komputerze należy skonfigurować adres IP serwera Management Server jako serwera czasu. W tym celu należy posłużyć się standardowymi procedurami obsługi systemu Windows.

7.13 Konfigurowanie nośnika zapisu nadajnika

Okno główne > **Urządzenia** > rozwiń  > rozwiń  >  >  > **Ustawienia zaawansowane** > **Zarządzanie zapisem**

Uwaga: Należy się upewnić, że żądane kamery tego nadajnika są dodane do drzewa logicznego. Nośnik zapisu nadajnika należy skonfigurować pod kątem użycia funkcji ANR.

Uwaga: aby skonfigurować nośnik zapisu nadajnika, który został już dodany do systemu i jest zapisany przez usługę VRM, należy upewnić się, że zapis pomocniczy jest zatrzymany:



The screenshot shows the 'Recording Management' tab in the BVMS configuration client. It is divided into 'Primary Recording' and 'Secondary Recording' sections. In the Primary Recording section, the 'Preferred storage target type' is set to 'Managed'. Below it, 'Recording is managed by' shows an address of 172.30.11.75 and a status icon. In the Secondary Recording section, the 'Preferred storage target type' is set to 'SD card'. Below it, 'Local target' shows an address of 172.31.22.52, a status of 98% of 14.75 GB in use, and a password field. A red circle highlights the 'Add' button in the Secondary Recording section.

Funkcja ANR działa tylko na nadajnikach z oprogramowaniem układowym w wersji 5.90 lub wyższej. Nie wszystkie typy nadajników obsługują funkcję ANR, nawet jeśli mają zainstalowaną prawidłową wersję oprogramowania układowego.

Aby skonfigurować nośnik zapisu nadajnika, należy:

1. W obszarze **Zapis pomocniczy** na liście **Preferowany typ miejsca docelowego zapisu** wybrać nośnik zapisu. W zależności od typu urządzenia dostępne będą różne nośniki.
2. W razie potrzeby kliknąć przycisk ..., aby sformatować nośnik zapisu. Po udanym zakończeniu formatowania nośnik zapisu jest gotowy do użycia za pomocą funkcji ANR.
3. Skonfiguruj funkcję ANR pod kątem nadajnika na stronie **Kamery i zapis**.

Patrz

- Strona Zarządzanie zapisem, Strona 233
- Konfigurowanie funkcji ANR, Strona 302

8 Tworzenie Enterprise System

Wykonaj następujące zadania, aby utworzyć System Enterprise na serwerze Enterprise Management Server i wielu komputerach Management Server:

1. Konfigurowanie funkcji listy serwerów dla systemu Enterprise System, Strona 85
2. Tworzenie grupy Enterprise User Group, Strona 86
3. Tworzenie konta Enterprise Account, Strona 86

Aby można było używać systemu Enterprise System, wymagane jest posiadanie ważnych licencji.

Patrz

- Enterprise System., Strona 25

8.1 Konfigurowanie funkcji listy serwerów dla systemu Enterprise System

Okno główne > **Urządzenia** > **System Enterprise** > **Lista serwerów/książka adresowa**

Należy skonfigurować wiele komputerów z serwerem Management Server na liście serwerów odpowiedniego serwera Management Server.

Aby umożliwić jednoczesny dostęp, należy skonfigurować jedną lub więcej grup Enterprise User Groups. Spowoduje to zmianę tego serwera Management Server w Enterprise Management Server. Użytkownik programu Operator Client może zalogować się, używając nazwy użytkownika Enterprise User Group w celu uzyskania jednoczesnego dostępu do komputerów Management Server skonfigurowanych na liście serwerów.

Uprawnienia dotyczące obsługi są konfigurowane w serwerze Enterprise Management Server w sekcji **Grupy użytkowników**, na karcie Enterprise User Group.

Uprawnienia dotyczące urządzeń są konfigurowane w każdym serwerze Management Server w sekcji **Grupy użytkowników**, na karcie Enterprise Access.

- Kliknij , aby zapisać ustawienia.
- Kliknij , aby cofnąć ostatnią zmianę.
- Kliknij , aby uaktywnić konfigurację.

Aby dodać serwery:

1. Kliknąć **Dodaj serwer**.
Zostanie wyświetlone okno dialogowe **Dodaj serwer**.
2. Wpisać nazwę wyświetlaną na serwerze i wpisać adres sieci prywatnej (nazwa DNS lub adres IP).

Uwaga: w przypadku korzystania z połączenia SSH wprowadzić adres w następującym formacie:

ssh://IP or servername:5322

3. Kliknąć **OK**.
4. Powtarzaj te czynności, aż zostaną dodane wszystkie żądane komputery typu Management Server.

Aby dodać kolumny:

- ▶ Kliknąć prawym przyciskiem myszy nagłówek tabeli i kliknąć **Dodaj kolumnę**.

Można dodać maks. 10 kolumn.

Aby usunąć kolumnę, kliknąć prawym przyciskiem myszy żądaną kolumnę i kliknąć **Usuń kolumnę**.

⇒ Podczas eksportowania listy serwerów dodane kolumny zostaną również wyeksportowane. Komputery z serwerem Management Server są skonfigurowane do użycia funkcji Enterprise System.

Patrz

- Enterprise System., Strona 25
- Strona listy serwerów/książki adresowej, Strona 128
- strona Grupy użytkowników, Strona 328
- Używanie funkcji Server Lookup, Strona 74

8.2

Tworzenie grupy Enterprise User Group

Okno główne > **Grupy użytkowników**

Użytkownik wykonuje zadanie polegające na utworzeniu konta Enterprise User Group dla Enterprise System na serwerze Enterprise Management Server.

Celem utworzenia grupy użytkowników Enterprise User Group wraz z użytkownikami jest skonfigurowanie ich uprawnień dotyczących obsługi. Te uprawnienia dotyczące obsługi są dostępne w aplikacji Operator Client, która jest połączona z serwerem zarządzającym Enterprise Management Server. Przykładem uprawnienia dotyczącego obsługi jest interfejs użytkownika monitora alarmowego.

Aby utworzyć grupę Enterprise User Group:

1. Kliknij kartę **Enterprise User Groups**.

Uwaga: Karta **Enterprise User Groups** jest dostępna tylko wówczas, gdy występuje odpowiednia licencja oraz co najmniej jeden komputer z serwerem Management Server został skonfigurowany w oknie **Urządzenia > System Enterprise > Lista serwerów/książka adresowa**.

2. Kliknij .

Zostanie wyświetlone okno dialogowe **Nowa grupa użytkowników Enterprise User Group**.

3. Wpisz nazwę i opis.
4. Kliknij przycisk **OK**.

Grupa Enterprise User Group zostanie dodana do odpowiedniego drzewa.

5. Kliknij nową grupę Enterprise prawym przyciskiem myszy i kliknij pozycję **Zmień nazwę**.
6. Wpisz żadaną nazwę i naciśnij klawisz ENTER.
7. Na stronie **Uprawnienia do obsługi** skonfiguruj według potrzeb uprawnienia dotyczące obsługi oraz dostęp do serwera dla skonfigurowanych komputerów typu Management Server.

Patrz

- strona Właściwości grupy użytkowników, Strona 330
- Strona funkcji operatora, Strona 337
- strona Priorytety, Strona 341
- strona Interfejs użytkownika, Strona 341
- Strona Dostęp do serwera, Strona 342

8.3

Tworzenie konta Enterprise Account

Okno główne > **Grupy użytkowników**

**Uwaga!**

Przed dodaniem Enterprise Account należy skonfigurować co najmniej jedno urządzenie w Drzewie urządzeń.

Użytkownik wykonuje zadanie polegające na utworzeniu konta Enterprise Account na serwerze Management Server. Należy powtórzyć to zadanie dla każdego serwera Management Server, który jest częścią systemu Enterprise System.

Celem utworzenia konta Enterprise Account jest skonfigurowanie uprawnień dotyczących urządzeń dla aplikacji Operator Client korzystającej z systemu Enterprise System.

Aby utworzyć grupę Enterprise Account:

1. Kliknąć kartę **Dostęp Enterprise**.
2. Kliknąć .
Zostanie wyświetlone okno dialogowe **Nowe konto Enterprise Account**.
3. Wpisać nazwę i opis.
4. Pole wyboru **Przy następnym logowaniu użytkownik musi zmienić hasło** jest wstępnie zaznaczone dla wszystkich nowo utworzonych kont użytkowników.
Wpisać klucz z zachowaniem zasad polityki kluczy, a następnie go potwierdzić.
5. Kliknąć przycisk **OK**.
Nowe konto Enterprise Account zostanie dodane do odpowiedniego drzewa.
6. Kliknąć prawym przyciskiem myszy nowe konto Enterprise Account, a następnie kliknąć opcję **Zmień nazwę**.
7. Wpisać żadaną nazwę i naciśnij klawisz ENTER.
8. Na stronie **Uprawnienia urządzenia** skonfigurować według wymagań dane uwierzytelniające oraz uprawnienia urządzeń.

Patrz

- Zasady silnych haseł, Strona 351
- Strona Dane uwierzytelniające, Strona 336
- strona Drzewo logiczne, Strona 337
- strona Zdarzenia i alarmy, Strona 336
- Strona Priorytety sterowania, Strona 334
- strona Uprawnienia kamery, Strona 333
- strona Uprawnienia odbiornika, Strona 335

8.4 Uwierzytelnianie za pomocą tokenów

Konto Enterprise Account umożliwia zarządzanym komputerom klienckim systemu Enterprise dostęp do programu Management Server skonfigurowanego na liście kontroli dostępu do serwerów w programie Enterprise Management Server.

Konto Enterprise Account jest zabezpieczone kluczem. W przypadku zmiany klucza należy go zmienić również w programach Management Server i Enterprise Management Server. Dodatkowo trzeba aktywować zmienioną konfigurację.

Jeśli do komputera z programem Enterprise Management Server podłączono dużą liczbę komputerów z programem Management Server, może to być czasochłonne.

Dlatego zamiast zabezpieczać konto Enterprise Account za pomocą nazwy użytkownika i klucza można skonfigurować uwierzytelnianie za pomocą tokenów.

1. Program Enterprise Management Server tworzy token.
2. Token jest podpisywany za pomocą certyfikatu o nazwie Token Issuer.
3. Management Server przyznaje dostęp, gdy token jest prawidłowy.
Management Server udziela dostępu tylko pod warunkiem, że w programie Management Server skonfigurowano ufanie certyfikatowi Token Issuer.

Warunki wstępne

Do podpisania i uwierzytelnienia tokena jest potrzebny certyfikat lub łańcuch certyfikatów.

Uwaga: Certyfikaty nie są generowane ani instalowane przez program BVMS. Należy je dostarczyć i zainstalować niezależnie. Program BVMS może używać certyfikatów zainstalowanych w magazynie Windows Certificate Store.

Komputery, na których będą instalowane programy Enterprise Management Server i Management Server, mają różne wymagania wstępne. Poniżej wyjaśniono, które środowiska wymagają poszczególnych certyfikatów.

Certyfikat

- Enterprise Management Server potrzebuje certyfikatu i jego klucza prywatnego.
- Management Server potrzebuje certyfikatu.

Łańcuch certyfikatów

Łańcuch certyfikatów rozpoczyna się od certyfikatu Root, którym można podpisać inny certyfikat. Następnie można ponownie użyć tego certyfikatu do podpisania kolejnego certyfikatu. Długość łańcuchów certyfikatów można określić samodzielnie.

- Enterprise Management Server wymaga całego łańcucha certyfikatów. Ostatni certyfikat w łańcuchu (Token Issuer) wymaga klucza prywatnego.
- Management Server wymaga tylko części łańcucha certyfikatów, zależnie od skonfigurowanych ustawień tokena dostępu.

Aby skonfigurować uwierzytelnianie za pomocą tokenów, należy wykonać następujące czynności:

1. Skonfigurowanie programu Enterprise Management Server
 - Zdefiniowanie uwierzytelniania za pomocą tokena dostępu na koncie Enterprise Accounts
 - Skonfigurowanie ustawień tokena dostępu
2. Skonfigurowanie programu Management Server
 - Określenie zaufanych certyfikatów
 - Zablokowanie dostępu do programu Enterprise Account za pomocą klucza

Szczegółowe informacje z poszczególnych tematów można znaleźć w raporcie technicznym Uwierzytelnianie za pomocą tokenów.

Patrz

- Okno dialogowe Ustawienia tokena dostępu (menu Ustawienia), Strona 118
- Strona Dostęp do serwera, Strona 342

9 Konfiguracja skryptów poleceń

W niniejszym rozdziale opisano, jak skonfigurować skrypty poleceń. Skrypty poleceń występują w różnych miejscach systemu BVMS.

1. Kliknij , aby zapisać ustawienia.
2. Kliknij , aby cofnąć ostatnią zmianę.
3. Kliknij , aby uaktywnić konfigurację.



Uwaga!

Skrypty serwerów są aktywowane podczas ponownego uruchamiania usługi Management Server, nawet jeśli nie zostały aktywowane przez program Configuration Client.

9.1 Zarządzanie skryptami poleceń

Okno główne

Użytkownik może utworzyć skrypt poleceń, używając następujących języków skryptów:

- C#
- VB.Net

Nie można zmienić języka skryptu w istniejącym skrypcie poleceń.

Użytkownik może utworzyć Skrypt klienta lub Skrypt serwera.

Do każdego skryptu można dodać scriptlet.

Aby uzyskać pomoc przy wprowadzaniu kodu, kliknij w oknie dialogowym **Edytor skryptów poleceń**

ikonę  . Spowoduje to wyświetlenie pomocy dotyczącej opracowanego przez firmę Bosch interfejsu API skryptu.

Aby dodać scriptlet serwera:

1. W menu **Narzędzia** kliknij polecenie **Edytor Skryptów poleceń....**
Jeśli nie został jeszcze utworzony żaden skrypt poleceń, pojawi się okno dialogowe **Wybierz język skryptu**.
2. Wybierz odpowiednią pozycję na liście **Język skryptu**.
Pojawi się okno dialogowe **Edytor skryptów poleceń**.
3. W lewym okienku okna dialogowego **Edytor skryptów poleceń** kliknij prawym przyciskiem myszy opcję **ServerScript**, a następnie kliknij polecenie **Nowy scriptlet**.
Zostanie dodany nowy scriptlet.
4. Wprowadzić kod użytkownika.

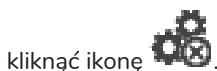
Aby dodać scriptlet klienta:

1. W menu **Narzędzia** kliknij polecenie **Edytor Skryptów poleceń....**
Jeśli nie został jeszcze utworzony żaden skrypt poleceń, pojawi się okno dialogowe **Wybierz język skryptu**.
2. Wybierz odpowiednią pozycję na liście **Język skryptu**.
Pojawi się okno dialogowe **Edytor skryptów poleceń**.
3. W lewym okienku okna dialogowego **Edytor skryptów poleceń** kliknij prawym przyciskiem myszy opcję **ClientScript**, a następnie kliknij polecenie **Nowy scriptlet**.
Zostanie dodany nowy scriptlet.
4. Wprowadzić kod użytkownika.

Aby usunąć scriptlet:

1. Otworzyć okno dialogowe **Edytor skryptów poleceń**.

2. W razie potrzeby kliknąć kartę **Skrypt serwera** lub kartę **Skrypt klienta**.
3. W drzewie zdarzeń kliknąć odpowiednie zdarzenie prawym przyciskiem myszy, a następnie



kliknąć ikonę

Scriptlet zostanie usunięty.

Aby zamknąć okno dialogowe Edytor skryptów poleceń:

- ▶ Kliknąć przycisk .

Patrz

- Okno dialogowe Edytor skryptu poleceń, Strona 307

9.2 Konfigurowanie opcji automatycznego wykonywania skryptu poleceń

Okno główne > **Alarmy** >  lub  > kolumna **Opcje alarmu** > ...

Użytkownik konfiguruje skrypt poleceń klienta do uruchomienia w następujących przypadkach:

- Stacja robocza jest uruchamiana.
- Użytkownik akceptuje alarm.

Aby skonfigurować skrypt poleceń przy uruchomieniu stacji roboczej, należy:

Patrz Konfiguracja skryptu poleceń wykonywanego przy uruchomieniu.

Aby skonfigurować skrypt poleceń po przyjęciu alarmu przez użytkownika, należy:

1. Kliknąć kartę **Etapy pracy**.
2. Na liście **Wykonaj następujący Skrypt klienta, kiedy alarm został przyjęty**: zaznaczyć żądany skrypt klienta.
Skrypt zostanie uruchomiony w chwili przyjęcia wybranego alarmu przez użytkownika.

Patrz

- Okno dialogowe Opcje alarmu, Strona 313
- Konfigurowanie startowego skryptu poleceń (strona ustawień), Strona 91

9.3 Importowanie skryptu poleceń

Okno główne

Użytkownik może importować skrypty poleceń, które zostały utworzone na innym komputerze. Plik musi być napisany w tym samym języku skryptu, jaki jest używany w systemie użytkownika.

Aby importować skrypt poleceń, należy:

1. W menu **Narzędzia** kliknąć polecenie **Edytor Skryptów poleceń...**
Pojawi się okno dialogowe **Edytor skryptów poleceń**.
2. Kliknąć ikonę .
3. Zaznaczyć żądany plik skryptu i kliknąć przycisk **OK**.

Patrz

- Okno dialogowe Edytor skryptu poleceń, Strona 307

9.4 Eksportowanie skryptu poleceń

Okno główne

Użytkownik może eksportować skrypty poleceń, które zostały utworzone na innym komputerze.

Aby wyeksportować skrypt poleceń, należy:

1. W menu **Narzędzia** kliknąć polecenie **Edytor Skryptów poleceń...**
Pojawi się okno dialogowe **Edytor skryptów poleceń**.
2. Kliknąć ikonę .
Pojawi się okno dialogowe zapisywania plików.
3. Wprowadzić nazwę pliku skryptu i kliknąć przycisk **OK**.

Patrz

- Okno dialogowe Edytor skryptu poleceń, Strona 307

9.5

Konfigurowanie startowego skryptu poleceń (strona ustawień)

Okno główne > **Urządzenia** > rozwinąć  >  > strona **Ustawienia**

Skrypt poleceń można skonfigurować tak, aby był wykonywany podczas uruchamiania programu Operator Client zainstalowanego na wybranej stacji roboczej.

Użytkownik musi utworzyć odpowiedni skrypt poleceń.

Aby utworzyć skrypt poleceń, patrz *Zarządzanie skryptami poleceń*, Strona 89.

Aby skonfigurować skrypt wykonywany przy uruchomieniu, należy:

- ▶ Na liście **Skrypt startowy**: zaznaczyć żądany skrypt poleceń.

Patrz

- strona Stacja robocza, Strona 136

10 Zarządzanie danymi konfiguracyjnymi

Okno główne

Użytkownik musi uaktywnić bieżącą konfigurację, aby obowiązywała dla programu Management Server and Operator Client. System przypomina o uaktywnieniu podczas wyłączania oprogramowania Configuration Client.

Każda uaktywniona konfiguracja jest zapisywana wraz z datą oraz opisem, jeśli jest wymagany. W każdym momencie użytkownik może przywrócić ostatnio uaktywnioną konfigurację. Wszystkie konfiguracje zapisane w międzyczasie zostaną utracone.

Bieżącą konfigurację można eksportować w postaci pliku konfiguracyjnego, który następnie można importować. Powoduje to przywrócenie wyeksportowanej konfiguracji. Wszystkie konfiguracje zapisane w międzyczasie są tracone.

- Kliknij , aby zapisać ustawienia.
- Kliknij , aby cofnąć ostatnią zmianę.
- Kliknij , aby uaktywnić konfigurację.

10.1 Uaktywnienie konfiguracji roboczej

Okno główne

Aktywować bieżącą konfigurację. Aktywowana konfiguracja jest stosowana w programie Operator Client po kolejnym uruchomieniu, jeżeli została zaakceptowana przez użytkownika. Jeżeli aktywacja zostanie wymuszona, wszystkie otwarte programy Operator Client w sieci są zamykane i uruchamiane ponownie. Użytkownik każdej kopii Operator Client zwykle nie musi się logować ponownie.

Możliwe jest ustawienie opóźnionego czasu aktywacji. W przypadku skonfigurowania opóźnionego czasu aktywacji konfiguracja robocza nie zostaje uaktywniona od razu, ale po upływie ustawionego czasu. Jeśli użytkownik skonfiguruje inny czas aktywacji później (bez względu na to, czy jest to czas opóźniony czy nie), ten czas będzie teraz aktywny. Pierwszy skonfigurowany czas aktywacji zostaje usunięty.

Po zamknięciu system Configuration Client przypomina o uaktywnieniu bieżącej kopii roboczej konfiguracji.

Nie można aktywować konfiguracji, która zawiera urządzenie niechronione hasłem.



Uwaga!

Jeśli aktywacja zostanie wymuszona, wszystkie programy Operator Client są uruchamiane ponownie po jej aktywowaniu. Należy unikać niepotrzebnych aktywacji. Aktywacje najlepiej przeprowadzać w nocy lub podczas okresów o niskiej aktywności.



Uwaga!

Jeśli system zawiera urządzenia, które nie są chronione hasłem, przed aktywacją należy je zabezpieczyć. Wymuszanie hasła można jednak wyłączyć.

Aby uaktywnić bieżącą konfigurację roboczą:

1. Kliknąć .
Zostanie wyświetlone okno dialogowe **Uaktywnij konfigurację**.
Jeśli konfiguracja zawiera urządzenia, które nie są chronione hasłem, nie można wykonać aktywacji. W takim przypadku wyświetli się okno dialogowe **Ochrona urządzeń przy użyciu hasła domyślnego...**
Należy postępować zgodnie z instrukcjami widocznymi w oknie dialogowym i kliknąć **Zastosuj**.
Ponownie wyświetli się okno dialogowe **Uaktywnij konfigurację**.
2. W razie potrzeby wprowadzić opóźniony czas aktywacji. Domyślnie jako czas aktywacji jest ustawiany czas bieżący. Jeśli nie zostanie zmieniony opóźniony czas aktywacji, aktywacja jest realizowana od razu.
W razie potrzeby kliknąć opcję **Wymuś aktyw. wsz. progr. Operator Client**, aby ją zaznaczyć.
3. Wprowadzić opis i kliknąć przycisk **OK**.
Bieżąca konfiguracja zostanie uaktywniona.
W przypadku wymuszenia aktywacji każda stacja robocza Operator Client podłączona do sieci jest natychmiast uruchamiana ponownie. Niepodłączona stacja robocza jest uruchomiona ponownie zaraz po ponownym podłączeniu.
Jeśli został skonfigurowany opóźniony czas aktywacji, konfiguracja zostanie uaktywniona później.

Uwaga: opóźniona aktywacja nie jest wykonywana tak długo, jak użytkownik jest zalogowany w Configuration Client.

Patrz

- Ochrona urządzenia za pomocą okna dialogowego *Globalne hasło domyślne* (menu *Sprzęt*), Strona 105
- Okno dialogowe *Uaktywnij konfigurację* (menu *System*), Strona 104

10.2

Uaktywnienie konfiguracji

Okno główne

Istnieje możliwość uaktywnienia (przywrócenia) jednej z poprzednich wersji konfiguracji zapisanych wcześniej.

Aby uaktywnić konfigurację:

1. W menu **System** kliknąć **Manager uaktywnienia...**
Zostanie wyświetlone okno dialogowe **Manager uaktywnienia**.
2. Na liście zaznaczyć konfigurację, która ma być uaktywniona.
3. Kliknąć **Uaktywnij**.
Zostanie wyświetlone okno komunikatu.
4. Kliknąć **OK**.
Zostanie wyświetlone okno dialogowe **Uaktywnij konfigurację**.
5. W razie potrzeby kliknąć opcję **Wymuś aktyw. wsz. progr. Operator Client**, aby ją zaznaczyć.
Wszystkie stacje robocze Operator Client zostaną automatycznie ponownie uruchomione w celu aktywowania nowej konfiguracji. Użytkownik nie może odrzucić nowej konfiguracji.
Jeśli opcja **Wymuś aktyw. wsz. progr. Operator Client** nie zostanie zaznaczona, w każdej stacji roboczej Operator Client na kilka sekund zostanie wyświetlone okno dialogowe. Użytkownik może wówczas odrzucić lub zaakceptować nową konfigurację. Jeżeli użytkownik nie dokona żadnego wyboru przez kilka sekund, okno dialogowe zostanie zamknięte. Nowa konfiguracja nie jest wówczas akceptowana.

Patrz

- Okno dialogowe *Uaktywnij konfigurację* (menu System), Strona 104
- Okno dialogowe *Manager uaktywnienia* (menu System), Strona 103

10.3

Eksportowanie danych konfiguracyjnych

Okno główne

Użytkownik może eksportować dane konfiguracyjne urządzenia obsługiwane przez system BVMS w postaci pliku .zip. Plik .zip zawiera plik bazy danych (*Export.bvms*) oraz dane użytkownika (plik .*dat*).

Pliki te mogą posłużyć do przywrócenia wyeksportowanej wcześniej konfiguracji systemu na tym samym serwerze (Enterprise) Management Server lub do zaimportowania jej na inny serwer (Enterprise) Management Server. Plik danych użytkowników nie może być importowany, ale można go wykorzystać do ręcznego przywrócenia konfiguracji użytkowników.

Aby eksportować dane konfiguracyjne, należy:

1. W menu **System** kliknąć **Eksportuj konfigurację....**
Zostanie wyświetlone okno dialogowe **Eksportuj plik konfiguracyjny**.



Uwaga: Jeśli bieżąca kopia robocza konfiguracji nie jest uaktywniona (jest aktywne), należy zamiast uaktywnionej konfiguracji wyeksportować tę kopię roboczą.

2. Kliknąć **Zapisz**.
3. Wprowadzić nazwę pliku.
Aktualna konfiguracja zostanie wyeksportowana. Zostanie utworzony plik .zip z bazą danych i danymi użytkowników.

Patrz

- Importowanie danych konfiguracyjnych, Strona 94

10.4

Importowanie danych konfiguracyjnych

Okno główne

Możliwe są trzy scenariusze użycia:

- Import konfiguracji, która została wcześniej wyeksportowana z tego samego serwera (wykonano kopię zapasową)
- Import szablonu konfiguracji, który został przygotowany i wyeksportowany z innego serwera
- Import konfiguracji wcześniejszej wersji BVMS.

Import konfiguracji jest możliwy tylko pod warunkiem, że ostatnie zmiany w bieżącej kopii roboczej zostały zapisane i uaktywnione.

Do importu danych konfiguracji konieczne jest posiadanie odpowiedniego hasła.

Nie można importować danych użytkowników.

Aby zaimportować konfigurację:

1. W menu **System** kliknąć **Import configuration**
Zostanie wyświetlone okno dialogowe **Importuj plik konfiguracyjny**.
2. Wybrać plik do zaimportowania i kliknąć opcję **Otwórz**.
Zostanie wyświetlone okno dialogowe **Importuj konfigurację**.

3. Wprowadzić odpowiednie hasło i kliknąć **OK**.
Program Configuration Client zostanie uruchomiony ponownie. Konieczne będzie ponowne zalogowanie się.
Zaimportowana konfiguracja nie będzie uaktywniona, ale można będzie edytować ją w programie Configuration Client.

**Uwaga!**

Aby kontynuować edycję konfiguracji, która została uaktywniona dla danego serwera Management Server, należy w oknie dialogowym **Uaktywnij konfigurację** przeprowadzić przebieg ponowny.

Patrz

– Eksportowanie danych konfiguracyjnych, Strona 94

10.5

Eksportowanie danych konfiguracyjnych do aplikacji serwera OPC

Okno główne

Można wyeksportować dane konfiguracji urządzenia systemu BVMS w postaci pliku XML, aby następnie zaimportować je do aplikacji serwera OPC. Plik musi znajdować się w katalogu bin instalacji systemu BVMS.

Informacje na temat konfiguracji połączenia BVMS–BIS można znaleźć w podręczniku instalacji połączenia BVMS–BIS i notatkach technicznych dotyczących serwera OPC systemu BVMS.

**Uwaga!**

Serwer BIS i BVMS Management Server należy zainstalować na dwóch różnych komputerach. Jeśli oba serwery uruchomione są na tym samym komputerze, spada wydajność systemu. Dodatkowo może wystąpić poważny konflikt oprogramowania.

Aby eksportować dane konfiguracyjne, należy:

1. W menu **System** kliknąć **Eksportuj informacje o urządzeniu dla systemu OPC**.
Zostanie wyświetlone okno dialogowe **Eksportuj plik informacji o urządzeniu**.
2. Wprowadzić nazwę pliku i kliknąć przycisk **Zapisz**.
Plik zostanie zapisany.
Teraz można go zaimportować do aplikacji serwera OPC.

10.6

Sprawdzanie stanu nadajników/dekoderów

Okno główne > menu **Urządzenie** > polecenie **Monitor urządzenia...** > okno dialogowe **Monitor urządzenia**

Można sprawdzić stan wszystkich aktywowanych nadajników/dekoderów w drzewie urządzeń.

Patrz

– Okno dialogowe Monitor urządzeń (menu Sprzęt), Strona 110

10.7

Konfigurowanie monitorowania SNMP

Okno główne

Aby przeprowadzić konfigurację:

1. W menu **Ustawienia** kliknij pozycję **Ustawienia SNMP...**
Pojawi się okno dialogowe **Ustawienia SNMP**.
2. Wykonaj żądane ustawienia i kliknij **OK**.

Aby wyłączyć SNMP GetRequest:

- ▶ Usuń zawartość pola **Port SNMP GET**.
System BVMS nie nasłuchuje już protokołu SNMP GetRequest.

Patrz

- Okno dialogowe *Ustawienia SNMP* (menu *Ustawienia*), Strona 115

10.8

Tworzenie raportów

Okno główne

Możesz utworzyć pojedynczy raport w celu zapisania ustawień konfiguracji w specjalnym oknie dialogowym albo utworzyć wszystkie raporty konfiguracyjne jednocześnie.

Aby utworzyć pojedynczy raport:

1. W menu **Raporty** kliknij żądane polecenie.
Zostanie wyświetlone związane z nim okno dialogowe.
2. Kliknij **Eksport CSV**.
3. Wprowadź ścieżkę i nazwę pliku dla nowego raportu.
4. Aby sprawdzić zawartość pliku CSV, otwórz go w programie Microsoft Excel lub w innym arkuszu kalkulacyjnym.

Aby utworzyć wszystkie raporty konfiguracyjne jednocześnie:

1. W menu **Raporty** kliknij pozycję **Eksportuj wszystkie raporty**
2. Zaznacz folder docelowy, w którym chcesz zapisać raporty, i kliknij przycisk **OK**.
Raporty zostaną utworzone i zapisane w żądanym folderze. Pasek postępu pokazuje postęp zapisywania.

Patrz

- Okno dialogowe *Harmonogramy zapisu*, Strona 113
- Okno dialogowe *Harmonogramy zadań*, Strona 113
- Okno dialogowe *Parametry kamer i zapisu*, Strona 113
- Okno dialogowe *Ustawienia jakości strumienia*, Strona 113
- Okno dialogowe *Ustawienia zdarzeń*, Strona 113
- Okno dialogowe *Ustawienia zdarzeń złożonych*, Strona 113
- Okno dialogowe *Ustawienia alarmowe*, Strona 113
- Okno dialogowe *Skonfigurowani użytkownicy*, Strona 114
- Okno dialogowe *Grupy i konta użytkowników*, Strona 114
- Okno dialogowe *Uprawnienia do obsługi*, Strona 114

11 Przykładowe konfiguracje

W tym rozdziale przedstawiono przykładowe konfiguracje wybranych urządzeń wchodzących w skład systemu BVMS.

11.1 Dodawanie interfejsu do ATM/POS-Bridge firmy Bosch

W tym przykładzie opisano, jak skonfigurować interfejs Bosch ATM/POS Bridge.

ATM/POS Bridge — konfigurowanie

1. Upewnij się, że urządzenie jest zasilane.
2. Aby skonfigurować adres IP i maskę podsieci urządzenia, należy podłączyć je do portu COM komputera za pomocą kabla RS232 (należy użyć kabla określonego przez firmę Bosch). Szczegółowe informacje można znaleźć w instrukcji instalacji urządzenia Bosch ATM/POS Bridge.
3. Zainicjuj na komputerze sesję programu Hyperterminal (w typowej konfiguracji należy kliknąć kolejno opcje: **Start > Programy > Akcesoria > Komunikacja > Hyperterminal**).
4. Wpisać nazwę sesji i kliknąć przycisk **OK**.
5. Wybrać numer portu COM i kliknąć przycisk **OK**.
6. Wybrać następujące ustawienia portu COM:
 - 9600 bitów/s
 - 8 bitów danych
 - Bez parzystości
 - 1 bit stopu
 - Sprzętowe sterowanie przepływemKliknąć przycisk **OK**.
7. Naciśnąć klawisz F1 w celu wyświetlenia menu opcji systemowych urządzenia.
8. Wpisać cyfrę „1”, aby móc skonfigurować adres IP i maskę podsieci.
9. Pozostaw domyślne ustawienia portów:
 - port1: **4201**
 - port2: **4200**

Dodawanie urządzenia ATM/POS Bridge do BVMS

1. Przyłącz urządzenie do sieci systemu BVMS.
2. Uruchom aplikację Configuration Client.
3. Kliknij opcję **Urządzenia**, rozwiń drzewo logiczne, rozwiń opcję , kliknij prawym przyciskiem myszy  i kliknij opcję **Dodaj interfejs do ATM/POS-Bridge firmy Bosch**. Pojawi się okno dialogowe **Dodaj interfejs do ATM/POS-Bridge firmy Bosch**.
4. Wpisz żadaną nazwę i wprowadź ustawienia, które zostały skonfigurowane wcześniej.
5. Kliknij kartę **Wejścia** i wybierz żądane wejścia.
6. Kliknij , aby zapisać ustawienia.
7. Kliknij **Zdarzenia**.
8. Rozwiń , rozwiń **Wejście interfejsu do POS**, kliknij **Wejście danych**.
9. Z listy **Wyzwól alarm** wybierz opcję **Zawsze**, aby mieć pewność, że w razie wystąpienia określonego zdarzenia zawsze będzie wyzwalany alarm. Można także wybrać harmonogram, dzięki czemu alarm będzie wyzwalany tylko w przypadku wystąpienia zdarzenia w określonym przedziale czasu.

10. Kliknij , aby zapisać ustawienia.
11. Kliknij **Alarmy**.
12. Skonfiguruj żądane ustawienia alarmu powiązanego z określonym zdarzeniem.
13. Kliknij ikonę , aby zapisać ustawienia, a następnie kliknij ikonę  w celu uaktywnienia konfiguracji.
14. Wykonaj test, aby sprawdzić, czy wybrano właściwe ustawienia alarmu.

11.2 Dodawanie wejścia alarmowego do urządzenia Bosch Allegiant

Po zintegrowaniu urządzenia Bosch Allegiant z systemem BVMS należy dodać także wejścia alarmowe.

1. W drzewie urządzeń kliknij pozycję odpowiadającą urządzeniu Allegiant.
2. Kliknij kartę **Wejścia** i kliknij **Dodaj wejście**.
3. Dodaj żądane wejścia alarmowe.
4. Kliknij **Zdarzenia**.
5. W drzewie zdarzeń rozwiń **Urządzenia Allegiant**, rozwiń **Wejście Allegiant** i kliknij **Wejście zamknięte** lub **Wejście otwarte** (w zależności od rodzaju aplikacji).
6. Z listy **Wyzwól alarm** wybierz opcję **Zawsze**, aby mieć pewność, że w razie wystąpienia określonego zdarzenia zawsze będzie wyzwalany alarm. Można także wybrać harmonogram, dzięki czemu alarm będzie wyzwalany tylko w przypadku wystąpienia zdarzenia w określonym przedziale czasu.

7. Kliknij ikonę , aby zapisać ustawienia, a następnie kliknij ikonę  w celu uaktywnienia konfiguracji.
8. Wykonaj test, aby sprawdzić, czy wybrano właściwe ustawienia alarmu.

11.3 Dodanie i konfiguracja 2 kamer sieciowych Dinion z zapisem VRM

Ta część opisuje, jak dodać 2 kamery sieciowe Dinion z zapisem VRM, jak skonfigurować różne ustawienia zapisu, a także jak skonfigurować dla tych kamer funkcję Wyszukiwania na podstawie ruchu w obrazie.

Warunek:

Program VRM i urządzenia iSCSI są odpowiednio skonfigurowane.

Oznacza to, że:

- Oprogramowanie VRM jest dodane do Drzewa urządzeń.
- Urządzenie iSCSI ze skonfigurowanym urządzeniem docelowym i numerem LUN jest przypisane do programu VRM.

Aby dodać kamery IP do programu VRM:

Okno główne > **Urządzenia** > rozwiń 

1. Kliknij prawym przyciskiem myszy  i kliknij **Dodaj nadajnik**.
Zostanie wyświetlone okno dialogowe **Dodaj nadajnik**.
2. Wpisz adres IP kamery IP i wybierz typ nadajnika (Dinion IP).
Kliknij **OK**.
Powtórz ten krok dla kolejnej kamery IP.

Aby dodać kamery sieciowe do drzewa logicznego:

Okno główne > **Mapy i struktura**

- ▶ Przeciągnij kamery do drzewa logicznego.

Aby zmienić właściwości kamery:

Okno główne > **Kamery i zapis** >  > karta 

1. W kolumnie **Obraz bieżący** skonfiguruj jakość podglądu bieżącego. W przypadku tych urządzeń jakość podglądu bieżącego można ustawić tylko odnośnie do poszczególnych kamer; konfiguracja zależna od harmonogramu nie jest dostępna.
2. Dokonaj odpowiednich ustawień w innych kolumnach.

Aby skonfigurować ustawienia zapisu dla kamery:

1. Kliknij .
2. Wybierz odpowiednią rodzinę urządzeń.
3. Wybierz odpowiednie dostępne ustawienia zapisu.
4. Wybierz odpowiedni harmonogram zapisu, na przykład **Dzień**.
5. W obszarze **Zapis ciągły lub alarmu wstępnego** wybierz żądany tryb zapisu, strumień i jakość. Wybranie trybu **Przed alarmem** spowoduje udostępnienie parametru **Czas trwania**, w którym można wybrać czas w sekundach, z jakim rozpocznie się zapis alarmowy przed faktycznym wyemitowaniem alarmu.
6. W obszarze **Zapis alarmowy** w kolumnie **Czas trwania** kliknij komórkę i wpisz w sekundach żądany czas trwania zapisu po wyemitowaniu alarmu.
7. Powtórz powyższe czynności, aby wprowadzić ustawienia zapisu dla kamery z innej rodziny urządzeń.

12

Globalne okna systemu Configuration Client

**Uwaga!**

Program BVMS Viewer zapewnia tylko podstawowe funkcje. Funkcje zaawansowane udostępnia program BVMS Professional. Aby uzyskać szczegółowe informacje na temat różnych wersji systemu BVMS, należy odwiedzić witrynę www.boschsecurity.com i zobaczyć skrócony poradnik wyboru systemu BVMS: [Skrócony poradnik wyboru systemu BVMS](#).

Niniejszy rozdział zawiera informacje o niektórych podstawowych oknach aplikacji dostępnych w systemie BVMSConfiguration Client.

12.1

Okno konfiguracji

Okno główne

Umożliwia konfigurowanie systemu. Przyciski na pasku narzędzi reprezentują różne strony, które należy skonfigurować, aby system mógł pracować. Ich sekwencja odpowiada zalecanej kolejności procesu konfiguracji.

- ▶ Kliknij element drzewa, aby wyświetlić dostępne strony właściwości.

Urządzenia	Kliknij, aby wyświetlić stronę Urządzenia zawierającą wszystkie urządzenia dołączone do systemu.
Mapy i struktura	Kliknij, aby wyświetlić stronę Mapy i struktura zawierającą Drzewo logiczne, Drzewo urządzeń oraz mapy.
Harmonogramy	Kliknij, aby wyświetlić stronę Harmonogramy zapisu i Harmonogramy zadań .
Kamery i zapis	Kliknij, aby wyświetlić stronę Kamery i zapis zawierającą Tabele kamery oraz ustawienia zapisu wszystkich kamer.
Zdarzenia	Kliknij, aby wyświetlić stronę Zdarzenia .
Alarmy	Kliknij, aby wyświetlić stronę Alarmy .
Grupy użytkowników	Kliknij, aby wyświetlić stronę Grupy użytkowników zawierającą wszystkich użytkowników.
	Kliknij, aby zapisać zmienione ustawienia bieżącego okna.
	Kliknij, aby przywrócić zapisane ustawienia bieżącego okna. Uwaga: Zostaną przywrócone tylko ustawienia wprowadzone w programie BVMS, a nie bezpośrednio na urządzeniu. Może to spowodować, że urządzenia przestaną być dostępne.
	Kliknij, aby wyświetlić okno dialogowe Uaktywnij konfigurację .
	Kliknij, aby usunąć zaznaczony element. (Nie jest dostępne na każdej stronie).

	Kliknij, aby zmienić nazwę zaznaczonego elementu. (Nie jest dostępne na każdej stronie).
	Kliknij, aby wyświetlić pomoc na temat bieżącego okna.
	Kliknij, aby zaktualizować informacje o stanie wszystkich urządzeń i w razie potrzeby również informacje o ich wydajności (nie dostępne na każdej stronie). Można zaktualizować stan pojedynczego urządzenia: kliknij prawym przyciskiem myszy urządzenie i kliknij przycisk Odśwież stan . Uwaga: w przypadku dużego systemu zawierającego kilka tysięcy skonfigurowanych urządzeń proces aktualizacji stanów urządzeń i informacji o ich wydajności może trwać długo.

12.2

Polecenia menu

Polecenia menu System

Zapisz zmiany	Zapisuje wszystkie zmiany dokonane na stronie.
Cofnij wszystkie zmiany na stronie	Przywraca ostatnio zapisane ustawienia strony.
Manager uaktywnienia...	Wyświetla okno dialogowe Manager uaktywnienia .
Eksportuj konfigurację...	Wyświetla okno dialogowe Eksportuj plik konfiguracyjny .
Importuj konfigurację...	Wyświetla okno dialogowe Importuj plik konfiguracyjny .
Eksportuj informacje o urządzeniu dla systemu OPC	Wyświetla okno dialogowe pozwalające utworzyć plik konfiguracyjny, który można zaimportować do systemu zarządzania pochodzącego od innego dostawcy.
Zakończ	Kończy pracę z programem.

Polecenia menu Urządzenie

Inicjujące skanowanie urządzeń...	Wyświetla okno dialogowe Inicjujące skanowanie urządzeń .
Ochrona urządzeń przy użyciu hasła domyślnego...	Wyświetla okno dialogowe Ochrona urządzeń przy użyciu globalnego hasła domyślnego .
Chroń nośniki iSCSI za pomocą hasła CHAP...	Wyświetla okno dialogowe Chroń nośniki iSCSI za pomocą hasła CHAP .
Zmień hasła urządzenia...	Wyświetla okno dialogowe Zmień hasła urządzenia .
Aktualizuj oprogramowanie układowe urządzenia...	Wyświetla okno dialogowe Aktualizuj oprogramowanie układowe urządzenia .
Zmień adres IP urządzenia i ustawienia sieciowe...	Wyświetla okno dialogowe Zmień adres IP urządzenia i ustawienia sieciowe .
Monitor urządzenia...	Wyświetla okno dialogowe Monitor urządzenia .

Polecenia menu Narzędzia

Edytor Skryptów poleceń...	Wyświetla okno dialogowe Edytor skryptów poleceń .
Manager zasobów...	Wyświetla okno dialogowe Manager zasobów .
Kreator sekwencji...	Wyświetla okno dialogowe Kreator sekwencji .
Manager licencji...	Wyświetla okno dialogowe Manager licencji .
License Inspector...	Wyświetla okno dialogowe Inspektor licencji .
Monitorowanie stacji roboczej...	Wyświetla okno dialogowe Monitorowanie stacji roboczej .

Polecenia menu Raporty

Eksport wszystkich raportów...	Wybrać folder docelowy do zapisania raportów.
Harmonogramy zapisu...	Wyświetla okno dialogowe raportu Harmonogramy zapisu .
Ustawienia zaplanowanego zapisu...	Wyświetla okno dialogowe raportu Ustawienia zaplanowanego zapisu .
Harmonogramy zadań...	Wyświetla okno dialogowe raportu Harmonogramy zadań .
Parametry kamer i zapisu...	Wyświetla okno dialogowe raportu Parametry kamer i nagrywania .
Ustawienia jakości strumienia...	Wyświetla okno dialogowe raportu Ustawienia jakości strumienia .
Ustawienia zdarzenia...	Wyświetla okno dialogowe raportu Ustawienia zdarzenia .
Ustawienia zdarzenia złożonego...	Wyświetla okno dialogowe raportu Ustawienia zdarzenia złożonego .
Ustawienia alarmowe...	Wyświetla okno dialogowe raportu Ustawienia alarmowe .
Skonfigurowani użytkownicy...	Wyświetla okno dialogowe raportu Skonfigurowani użytkownicy .
Grupy i konta użytkowników...	Wyświetla okno dialogowe raportu Grupy i konta użytkowników .
Uprawnienia urządzenia...	Wyświetla okno dialogowe raportu Uprawnienia urządzenia .
Uprawnienia do obsługi...	Wyświetla okno dialogowe raportu Uprawnienia do obsługi .
Uprawnienia konfiguracji...	Wyświetla okno dialogowe raportu Uprawnienia konfiguracji .
Uprawnienia grup użytkowników...	Wyświetla okno dialogowe raportu Uprawnienia grupy użytkowników .
Ustawienia zabezpieczeń...	Wyświetla okno dialogowe raportu Ustawienia zabezpieczeń .

Uprawnienia do aplikacji...	Wyświetla okno dialogowe raportu Uprawnienia do aplikacji .
Pominięte urządzenia...	Wyświetla okno dialogowe raportu Pominięte urządzenia .

Polecenia menu Ustawienia

Ustawienia alarmowe...	Wyświetla okno dialogowe Ustawienia alarmowe .
Ustawienia SNMP...	Wyświetla okno dialogowe Ustawienia SNMP .
Ustawienia serwera LDAP...	Wyświetla okno dialogowe Ustawienia serwera LDAP .
Określ kolejność grup użytkowników w usłudze LDAP...	Wyświetla okno dialogowe Określ kolejność grup użytkowników w usłudze LDAP...
Ustawienia tokena dostępu...	Wyświetla okno dialogowe Ustawienia tokena dostępu .
Ustawienia zaufanych certyfikatów...	Wyświetla okno dialogowe Ustawienia zaufanych certyfikatów . Uwaga: Menu Ustawienia zaufanych certyfikatów... jest dostępne tylko po uruchomieniu programu Configuration Client za pomocą poświadczeń administratora, a użytkownik, który się zaloguje, ma uprawnienie Konfiguruj grupy użytkowników/Enterprise Accounts .
Ustaw jakość zapisu...	Wyświetla okno dialogowe Ustawienia jakości strumienia .
Opcje	Wyświetla okno dialogowe Opcje .

Polecenia menu Pomoc

Wyświetl pomoc	Wyświetla okno dialogowe pomocy aplikacji BVMS.
Informacje	Wyświetla okno dialogowe zawierające informacje o zainstalowanym systemie, np. numer wersji.

12.3

Okno dialogowe Manager uaktywnienia (menu System)

Okno dialogowe > menu **System** > polecenie **Manager uaktywnienia...**

Umożliwia uaktywnienie bieżącej konfiguracji lub przywrócenie poprzedniej konfiguracji.

Activation Manager



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

Date & Time	User	Description
Working Copy		
11/25/2021 2:01:01 PM	TECHDOC-01 : Admin	
11/17/2021 11:09:06 AM	TECHDOC-01 : SYSTEM	Migrated to Version: 11.1.0.335
11/2/2021 12:35:57 PM	TECHDOC-01 : SYSTEM	Migrated to Version: 11.1.0.301
10/11/2021 2:41:12 PM	TECHDOC-01 : SYSTEM	Added event type data to configuration (BVMS version 11.1.0.232)
10/11/2021 2:40:58 PM	TECHDOC-01 : SYSTEM	Migrated to Version: 11.1.0.232
7/26/2021 6:01:33 PM	TECHDOC-01 : Admin	
7/26/2021 2:39:38 PM	TECHDOC-01 : SYSTEM	Migrated to Version: 11.1.0.74
5/11/2021 12:43:21 PM	TECHDOC-01 : SYSTEM	Migrated to Version: 11.0.0.1001
3/29/2021 2:31:47 PM	TECHDOC-01 : Admin	
3/18/2021 1:08:18 PM	TECHDOC-01 : Admin	
3/18/2021 1:05:00 PM	TECHDOC-01 : Admin	
3/18/2021 1:04:02 PM	TECHDOC-01 : Admin	
3/18/2021 1:01:44 PM	TECHDOC-01 : Admin	

↑ Exported configuration

● Currently active configuration

↓ Imported configuration

↓ Rollback: This configuration will be removed after activation

☐ Generate new Management Server ID

Activate

Cancel

Uaktywnij

Kliknij, aby wyświetlić okno dialogowe **Uaktywnij konfigurację**.

Patrz

- Uaktywnienie konfiguracji roboczej, Strona 92
- Uaktywnienie konfiguracji, Strona 93

12.4

Okno dialogowe Uaktywnij konfigurację (menu System)



Okno główne >

Umożliwia wprowadzenie opisu dla kopii roboczej konfiguracji, która ma być uaktywniona.

Ustaw czas opóźnionego uaktywnienia

Kliknij, aby wybrać opóźniony czas aktywacji.

Uwaga: opóźniona aktywacja nie jest wykonywana tak długo, jak użytkownik jest zalogowany w Configuration Client.

Wymuś aktyw. wsz. progr. Operator Client

W przypadku zaznaczenia tej opcji wszystkie stacje robocze Operator Client zostaną automatycznie ponownie uruchomione w celu aktywowania nowej konfiguracji. Użytkownik nie może odrzucić nowej konfiguracji.

W przypadku niezaznaczenia opcji w każdej stacji roboczej Operator Client na kilka sekund zostanie wyświetlone okno dialogowe. Użytkownik może wówczas odrzucić lub zaakceptować nową konfigurację. Jeżeli użytkownik nie dokona żadnego wyboru przez kilka sekund, okno dialogowe zostanie zamknięte. Nowa konfiguracja nie jest wówczas akceptowana.

Patrz

- Uaktywnienie konfiguracji roboczej, Strona 92

12.5

Okno dialogowe Inicjujące skanowanie urządzeń (menu Sprzęt)

Okno główne > menu **Urządzenie**, kliknąć polecenie **Inicjujące skanowanie urządzeń...**

Wyświetla urządzenia, które mają zduplikowane adresy IP lub domyślny adres IP (192.168.0.1).
Umożliwia zmianę takich adresów IP oraz masek podsieci.
Przed zmianą adresu IP konieczne jest wprowadzenie prawidłowej maski podsieci.

12.6

Ochrona urządzenia za pomocą okna dialogowego Globalne hasło domyślne (menu Sprzęt)

Okno dialogowe > menu **Urządzenie** > polecenie **Ochrona urządzeń przy użyciu hasła domyślnego...** lub



Okno główne >

To okno dialogowe pojawi się, gdy jest oczekiwanie na jakąś aktywację i konfiguracja zawiera urządzenia, które nie są chronione hasłem. Pozwala ono wprowadzić globalne hasło domyślne, które będzie stosowane do wszystkich wymagających tego urządzeń.

Aktualizuj stany i wydajność

Kliknij, aby ponownie wykonać skanowanie w poszukiwaniu urządzeń, które nie są chronione hasłem.

Global default password

Wpisz hasło, które będzie używane dla wszystkich niechronionych obecnie urządzeń.

Pokaż hasła

Kliknij, aby aktywować wszystkie hasła widoczne w tym oknie dialogowym.

Enforce password protection on activation

Kliknij to pole wyboru, aby je zaznaczyć. Jeśli globalne hasło domyślne zostało aktywowane, musi być ono używane dla wszystkich urządzeń, które nie są chronione hasłem.

Zastosuj

Kliknąć, aby zastosować globalne hasło domyślne.

Zostanie wyświetlone okno dialogowe **Zmianie haseł**. Zmiany haseł są notowane.

Kliknąć **OK**, aby zamknąć okno.

Po uruchomieniu aktywacji konfiguracji zostanie wyświetlone okno dialogowe **Manager uaktywnienia**.

Patrz

– Uaktywnienie konfiguracji roboczej, Strona 92

12.7

Chroń magazyny iSCSI za pomocą okna dialogowego Hasło CHAP (menu Sprzęt)

Użyj tego okna dialogowego, aby ustawić hasła CHAP na urządzeniach iSCSI i VRM. System automatycznie przenosi te hasła na konta **Użytkownik** i **Lokalizacja docelowa** nadajników, dekodatorów i urządzeń VSG.

W przypadku nowo dodanych urządzeń hasła są ustawiane automatycznie po aktywacji konfiguracji.

Uwaga: ustawienie pustego hasła CHAP powoduje usunięcie hasła CHAP na urządzeniach iSCSI i VRM.

**Uwaga!**

- We wszystkich urządzeniach DSA E-Series hasło CHAP jest ustawiane automatycznie.
- Urządzenia VRM wysyłają hasło CHAP do nadajników. Jednak aby następował zapis, należy ustawić hasło CHAP w odpowiednim urządzeniu iSCSI.
- We wszystkich urządzeniach DIVAR IP hasło CHAP trzeba ustawiać ręcznie. Więcej instrukcji można znaleźć w podręczniku obsługi urządzeń DIVAR IP. Bez ustawienia hasła zapis się zatrzyma lub odtwarzanie nie będzie działać.

Globalne hasło CHAP

Wpisać hasło CHAP iSCSI, które są niezbędne do przeprowadzenia uwierzytelnienia na urządzeniu pamięci masowej iSCSI oraz włączenia bezpośredniego odtwarzania z iSCSI.

Potwierdź globalne hasło CHAP

Potwierdzić hasło CHAP iSCSI.

Pokaż hasło

Kliknij, aby włączyć opcję wyświetlania wprowadzonego hasła. Uważaj, aby osoby postronne nie poznały tego hasła.

Zastosuj

Kliknąć, aby zastosować hasło CHAP.

Uwaga: sprawdzić wynik operacji. W niektórych urządzeniach może wystąpić konieczność ręcznego ustawienia hasła CHAP iSCSI.

12.8

Okno dialogowe zmiany hasła urządzenia (menu Urządzenie)

Okno główne > **Urządzenia** >  **Zmień hasła urządzenia** > okno dialogowe **Zmień hasła urządzenia**

LUB

Okno główne > menu **Urządzenie** > polecenie **Zmień hasła urządzenia...** > okno dialogowe **Zmień hasła urządzenia**



Kliknąć, aby odświeżyć informacje o stanie wszystkich urządzeń. Można odświeżyć stan pojedynczego urządzenia: należy kliknąć prawym przyciskiem myszy urządzenie i kliknąć przycisk **Odśwież stan**.

Uwaga: w przypadku dużego systemu zawierającego kilka tysięcy skonfigurowanych urządzeń proces odświeżania stanów może trwać długo.



Kliknąć, aby zaznaczyć wszystkie dostępne urządzenia jednocześnie.

Pokaż hasła

Zaznaczyć pole wyboru, jeśli skonfigurowane hasła mają być wyświetlane w wersji możliwej do odczytu.

Aby wyszukać elementy:

- ▶ W polu wyszukiwania wpisz ciąg znaków i naciśnij przycisk ENTER aby przefiltrować wyświetlone elementy.
Pojawią się tylko elementy zawierające łańcuch i odpowiadające im elementy nadrzędne (tylko w drzewach). Zostanie podana liczba odfiltrowanych elementów oraz całkowita liczba elementów.

Uwaga: ciąg znaków należy otoczyć cudzysłowem, aby znaleźć go precyzyjnie. Na przykład wpisanie "Camera 1" odfiltruje kamery o tej nazwie, a nie camera 201.

Uwaga: wyszukiwanie haseł jest możliwe tylko przy zaznaczonym polu wyboru **Pokaż hasła**.

Tabela umożliwia ustawienie następujących właściwości dostępnych urządzeń sieciowych:

- Hasło „service”
- Hasło „user”
- Hasło „live”
- Docelowe hasło

Aby zmienić hasło urządzeń sieciowych, należy:

1. Zaznaczyć żądane urządzenie.
2. Kliknąć prawym przyciskiem myszy zaznaczone urządzenie, a następnie kliknąć **Edytuj hasło....**
Pojawi się okno dialogowe **Zmień hasła urządzenia**.
3. Zaznaczyć żądany tym hasła.
4. Wprowadzić nowe hasło.
5. Kliknąć przycisk **OK**.
Nowe hasło zostanie zaktualizowane w wybranym urządzeniu.

Aby zmienić ustawienia dla wielu urządzeń, należy:

Patrz *Konfiguracja wielu nadajników / odbiorników*, Strona 230.

12.9

Okno dialogowe aktualizacji oprogramowania układowego urządzenia (menu Urządzenie)

Okno główne > menu **Urządzenie** > polecenie **Aktualizuj oprogramowanie układowe urządzenia...** > okno dialogowe **Aktualizuj oprogramowanie układowe urządzenia**



Kliknąć, aby odświeżyć informacje o stanie wszystkich urządzeń. Można odświeżyć stan pojedynczego urządzenia: należy kliknąć prawym przyciskiem myszy urządzenie i kliknąć przycisk **Odśwież stan**.

Uwaga: w przypadku dużego systemu zawierającego kilka tysięcy skonfigurowanych urządzeń proces odświeżania stanów może trwać długo.



Kliknąć, aby zaznaczyć wszystkie dostępne urządzenia jednocześnie.



Kliknąć, aby zaktualizować wersję oprogramowania układowego.

Aby wyszukać elementy:

- ▶ W polu wyszukiwania wpisz ciąg znaków i naciśnij przycisk ENTER aby przefiltrować wyświetlone elementy.
Pojawią się tylko elementy zawierające łańcuch i odpowiadające im elementy nadrzędne (tylko w drzewach). Zostanie podana liczba odfiltrowanych elementów oraz całkowita liczba elementów.

Uwaga: ciąg znaków należy otoczyć cudzysłowem, aby znaleźć go precyzyjnie. Na przykład wpisanie "Camera 1" odfiltruje kamery o tej nazwie, a nie camera 201.

Aby zaktualizować wersję oprogramowania układowego, należy:

1. Zaznaczyć żądane urządzenie.
2. Kliknąć przycisk **Aktualizuj oprogramowanie układowe**. Zostanie wyświetlone okno informacyjne Configuration Client.
3. Kliknąć przycisk **OK**.
Zostanie otwarty Eksplorator plików.
4. Wybierać plik zawierający aktualizację.
5. Kliknij przycisk **Otwórz**.
Zostanie wyświetlone okno **Stan przesłania oprogramowania układowego**.
6. Kliknij **Uruchom**, aby rozpocząć przesyłanie danych.
7. Kliknąć **Zamknij**.
Oprogramowanie układowe jest zaktualizowane.

Aby zmienić ustawienia dla wielu urządzeń, należy:

Patrz Konfiguracja wielu nadajników / odbiorników, Strona 230.

12.10

Okno dialogowe zmieniania ustawień sieciowych urządzenia i sieci (menu Urządzenie)

Okno główne > menu **Urządzenie** > polecenie **Zmień adres IP urządzenia i ustawienia sieciowe...** > okno dialogowe **Zmień adres IP urządzenia i ustawienia sieciowe**



Kliknąć, aby odświeżyć informacje o stanie wszystkich urządzeń. Można odświeżyć stan pojedynczego urządzenia: należy kliknąć prawym przyciskiem myszy urządzenie i kliknąć przycisk **Odśwież stan**.

Uwaga: w przypadku dużego systemu zawierającego kilka tysięcy skonfigurowanych urządzeń proces odświeżania stanów może trwać długo.



Kliknąć, aby zaznaczyć wszystkie dostępne urządzenia jednocześnie.

Aby wyszukać elementy:

- ▶ W polu wyszukiwania wpisz ciąg znaków i naciśnij przycisk ENTER aby przefiltrować wyświetlone elementy.
Pojawią się tylko elementy zawierające łańcuch i odpowiadające im elementy nadrzędne (tylko w drzewach). Zostanie podana liczba odfiltrowanych elementów oraz całkowita liczba elementów.

Uwaga: ciąg znaków należy otoczyć cudzysłowem, aby znaleźć go precyzyjnie. Na przykład wpisanie "Camera 1" odfiltruje kamery o tej nazwie, a nie camera 201.

Tabela umożliwia ustawienie następujących właściwości dostępnych urządzeń sieciowych:

- Nazwa urządzenia
- Adres IP
- Maskę podsieci
- Adres IP bramy



Uwaga!

Zamiast używać poleceń można wprowadzić odpowiednie ustawienia w żądanym polu.

Aby ustawić nazwę wyświetlaną urządzeń sieciowych, należy:

1. Zaznaczyć żądane urządzenie.
2. Kliknąć prawym przyciskiem myszy zaznaczone urządzenie, a następnie wybrać **Ustaw wyświetlanie nazw...** Pojawi się okno dialogowe **Ustaw wyświetlanie nazw**.
3. W polu **Rozpocznij z:** wprowadzić pierwszy ciąg.
4. Kliknąć **Oblicz**. W polu **Zakończ z:** wyświetlany jest ostatni ciąg z zakresu wybranego urządzenia.
5. Kliknąć **OK**.
6. W oknie dialogowym **Zmień adres IP urządzenia i ustawienia sieciowe** kliknąć **Zastosuj**. Obliczona nazwa zostanie zaktualizowana dla wybranego urządzenia.

Okno dialogowe Ustaw wyświetlanie nazw

Rozpocznij z:

Wprowadzić pierwszą nazwę.

Zakończ z:

Wyświetla ostatnią nazwę dla wybranych urządzeń po kliknięciu przycisku **Oblicz**.

Oblicz

Kliknąć, aby obliczyć zakres wyświetlanych nazw dla wybranych urządzeń.

Aby ustawić adres IP urządzeń IP, należy:

1. Zaznaczyć żądane urządzenie.
2. Kliknąć prawym przyciskiem myszy zaznaczone urządzenie, a następnie wybrać **Ustaw adresy IP...** Pojawi się okno dialogowe **Ustaw adresy IP**.
3. W polu **Rozpocznij z:** wprowadzić adres IP.
4. Kliknąć **Oblicz**. W polu **Zakończ z:** wyświetlany jest ostatni adres IP z zakresu dla wybranego urządzenia.
5. Kliknąć **OK**.
6. W oknie dialogowym **Zmień adres IP urządzenia i ustawienia sieciowe** kliknąć **Zastosuj**. Adres IP wybranego urządzenia zostanie zaktualizowany.

Okno dialogowe Ustaw adres IP

Rozpocznij z:

Wprowadzić pierwszy adres IP.

Zakończ z:

Wyświetla ostatni adres IP dla wybranych urządzeń po kliknięciu przycisku **Oblicz**.

Oblicz

Kliknąć, aby obliczyć zakres adresów IP dla wybranych urządzeń.

Aby ustawić maskę podsieci/identyfikator bramy urządzeń sieciowych, należy:

1. Kliknąć w żądanym polu.
 2. Wprowadzić odpowiednią wartość.
 3. Kliknąć przycisk **Zastosuj**.
- Nowa wartość zostanie zaktualizowana w wybranym urządzeniu.

Zastosuj

Kliknij, aby skonfigurować urządzenia za pomocą wprowadzonych wartości bez zamykania okna dialogowego.

Aby zmienić ustawienia dla wielu urządzeń, należy:

Patrz *Konfiguracja wielu nadajników / odbiorników*, Strona 230.

12.11

Okno dialogowe Monitor urządzeń (menu Sprzęt)

Okno główne > menu **Urządzenie** > polecenie **Monitor urządzenia...** > okno dialogowe **Monitor urządzenia**

Pozwala sprawdzić stan nadajników/odbiorników w drzewie urządzeń, które są aktywne w systemie BVMS.

Wyświetlana nazwa

Nazwa urządzenia, która została skonfigurowana w systemie BVMS.

Adres sieciowy

Adres IP urządzenia.

Stan

Można wyświetlić następujące stany:

- **Skonfigurowane**: konfiguracja urządzenia została aktywowana.
- **Niezgodność konfiguracji**: konfiguracja urządzenia nie została aktywowana.
- **Nieznane**: nie można było określić stanu.
- **Niepołączony**: niepodłączone.

Ostatnia kontrola

Data i czas rozpoczęcia dialogu oraz wykonania sprawdzenia. Podczas wyświetlania tego okna dialogowego urządzenia nie są ponownie sprawdzane.

Patrz

- *Sprawdzanie stanu nadajników/dekoderów*, Strona 95

12.12

Okno dialogowe Edytor skryptu poleceń (menu Narzędzia)

Aby uzyskać więcej informacji, patrz *Okno dialogowe Edytor skryptu poleceń*, Strona 307.

Patrz

- *Okno dialogowe Edytor skryptu poleceń*, Strona 307

12.13 Okno dialogowe Manager zasobów (menu Narzędzia)

Aby uzyskać więcej informacji, patrz Okno dialogowe Manager zasobów, Strona 263.

Patrz

- Okno dialogowe Manager zasobów, Strona 263

12.14 Okno dialogowe Budowa sekwencji (menu Narzędzia)

Aby uzyskać więcej informacji, patrz Okno dialogowe Budowa sekwencji, Strona 266.

Patrz

- Okno dialogowe Budowa sekwencji, Strona 266

12.15 Okno dialogowe Manager licencji (menu Narzędzia)

Okno dialogowe > menu **Narzędzia** > polecenie **Manager licencji...**

Umożliwia zarejestrowanie licencji zamówionego pakietu BVMS oraz jego aktualizację o nowe funkcje.

Stan licencji

W tym obszarze wyświetlany jest stan licencji.

Odcisk palca systemu

Dla celów pomocniczych zalecamy podanie **Odcisk palca systemu**.

Lokalizacja instalacji

Podczas aktywacji licencji podstawowej w Bosch Remote Portal należy podać informacje o miejscu instalacji systemu. Te informacje są dostępne tutaj.

Uwaga: te informacje można również podać w innych licencjach, ale tutaj wyświetlane są tylko informacje podane w licencji podstawowej.

Licencje

1. Kliknąć **Dodaj**, aby dodać licencje.
Zostanie wyświetlone okno dialogowe **Dodaj licencję**.
2. Postępować zgodnie z instrukcjami wyświetlanymi w oknie dialogowym.

Ważna licencja

Wyświetla działającą licencję podstawową, która została aktywowana.

Funkcje

- ▶ Kliknij polecenie **License Inspector....**
Pojawi się okno dialogowe **Inspektor licencji**.

Wyświetla ilość licencjonowanych funkcji, które są aktualnie zainstalowane.

Można sprawdzić, czy liczba zainstalowanych licencji systemu BVMS przekracza liczbę licencji zakupionych.

Zainstalowana wersja oprogramowania BVMS

Wyświetla aktualnie zainstalowaną wersję systemu BVMS, np. 11.0.

Wersje oprogramowania BVMS z licencjami

Wyświetla wszystkie wersje BVMS które są zawarte i obsługiwane w aktualnie dostarczonym pliku licencyjnym.

Na przykład: BVMS 11.0 i wszystkie wersje poboczne BVMS 11.x

Data uaktywnienia

Wyświetla datę aktywacji zainstalowanej wersji systemu BVMS.

Data ważności

Wyświetla datę ważności zainstalowanej wersji systemu BVMS. Data ważności ma zastosowanie tylko w przypadku instalacji licencji awaryjnej lub licencji na prezentację sprzedażową.

Software Maintenance Agreement**Data ważności**

Jeśli została zakupiona i aktywowana dowolna umowa Software Maintenance Agreement, w tym miejscu wyświetlana jest data ważności.

Patrz

- Aktywacja licencji na oprogramowanie, Strona 75
- Okno dialogowe Dodawanie licencji, Strona 112
- Okno dialogowe Inspektor licencji (menu Narzędzia), Strona 112

12.15.1**Okno dialogowe Dodawanie licencji**

Okno główne > menu **Narzędzia** > polecenie **Manager licencji...** > **Licencje** > **Dodaj**

Umożliwia dodanie zakupionych licencji lub licencji demonstracyjnych z poziomu witryny Bosch Remote Portal remote.boschsecurity.com do systemu BVMS.

Aby dodać swoje licencje, postępuj zgodnie z instrukcjami w oknie dialogowym.

Dalsze informacje można znaleźć w odpowiedniej dokumentacji licencji na system BVMS.

12.16**Okno dialogowe Inspektor licencji (menu Narzędzia)**

Okno główne > menu **Narzędzia**, kliknąć polecenie **License Inspector...** > okno dialogowe **Inspektor licencji**

Wyświetla ilość licencjonowanych funkcji, które są aktualnie zainstalowane.

Można sprawdzić, czy liczba zainstalowanych licencji systemu BVMS przekracza liczbę licencji zakupionych.

Uwaga: jeśli bieżąca konfiguracja systemu przekracza limity aktualnie zainstalowanych licencji, nie można aktywować konfiguracji.

12.17**Okno dialogowe Monitorowanie stacji roboczej (menu Narzędzia)**

Okno główne > menu **Narzędzia** > polecenie **Monitorowanie stacji roboczej...** > okno dialogowe **Monitorowanie stacji roboczej**

Wyświetla listę wszystkich stacji roboczych, które są aktualnie połączone z serwerem BVMS Management Server.

Uwaga: na liście wyświetleni są wszyscy podłączeni klienci Operator Clients i Cameo SDK.

Aby odłączyć stację roboczą:

1. Wybierz z listy odpowiednią pozycję.
2. Kliknij polecenie **Rozłącz**.

Uwaga: funkcja jest aktywna tylko wtedy, gdy użytkownik ma odpowiednie uprawnienia.

3. Kliknij pozycję **Tak**.

Pozycja zostanie usunięta, gdy właściwy klient Operator Client wyloguje się pomyślnie.

Uwaga: można odłączyć tylko stacje robocze Operator Client.

12.18 Okna dialogowe raportów (menu Raporty)

W tym rozdziale opisano wszystkie okna dialogowe służące do konfigurowania raportów.

Patrz

- Tworzenie raportów, Strona 96

12.18.1 Okno dialogowe Harmonogramy zapisu

Okno dialogowe > menu **Raporty** > polecenie **Harmonogramy zapisu...**

Zawiera listę skonfigurowanych harmonogramów zapisu.

- ▶ Aby zapisać wszystkie informacje z tego okna dialogowego w pliku CSV, kliknij **Eksport CSV**.

12.18.2 Okno dialogowe Ustawienia zaplanowanego zapisu

Okno dialogowe > menu **Raporty** > polecenie **Ustawienia zaplanowanego zapisu...**

Zawiera listę ustawień zaplanowanego zapisu.

- ▶ Aby zapisać wszystkie informacje z tego okna dialogowego w pliku CSV, kliknij **Eksport CSV**.

12.18.3 Okno dialogowe Harmonogramy zadań

Okno dialogowe > menu **Raporty** > polecenie **Harmonogramy zadań...**

Zawiera listę skonfigurowanych harmonogramów zadań.

- ▶ Aby zapisać wszystkie informacje z tego okna dialogowego w pliku CSV, kliknij **Eksport CSV**.

12.18.4 Okno dialogowe Parametry kamer i zapisu

Okno dialogowe > menu **Raporty** > polecenie **Parametry kamer i zapisu...**

Zawiera listę parametrów zapisu skonfigurowanych w tabeli kamery i w tabeli zapisu.

- ▶ Aby zapisać wszystkie informacje z tego okna dialogowego w pliku CSV, kliknij **Eksport CSV**.

12.18.5 Okno dialogowe Ustawienia jakości strumienia

Okno dialogowe > menu **Raporty** > polecenie **Ustawienia jakości strumienia...**

Zawiera listę skonfigurowanych ustawień jakości strumienia dla wszystkich kamer.

- ▶ Aby zapisać wszystkie informacje z tego okna dialogowego w pliku CSV, kliknij **Eksport CSV**.

12.18.6 Okno dialogowe Ustawienia zdarzeń

Okno dialogowe > menu **Raporty** > polecenie **Ustawienia zdarzenia złożonego...**

Zawiera listę zdarzeń ze skonfigurowanym harmonogramem wyzwalania alarmu.

- ▶ Aby zapisać wszystkie informacje z tego okna dialogowego w pliku CSV, kliknij **Eksport CSV**.

12.18.7 Okno dialogowe Ustawienia zdarzeń złożonych

Okno dialogowe > menu **Raporty** > polecenie **Ustawienia zdarzenia złożonego...**

Zawiera listę wszystkich zdarzeń złożonych.

- ▶ Aby zapisać wszystkie informacje z tego okna dialogowego w pliku CSV, kliknij **Eksport CSV**.

12.18.8 Okno dialogowe Ustawienia alarmowe

Okno dialogowe > menu **Raporty** > polecenie **Ustawienia alarmowe...**

Zawiera listę wszystkich ustawień skonfigurowanych alarmów, łącznie z ustawieniami z okna dialogowego **Opcje alarmu**.

- ▶ Aby zapisać wszystkie informacje z tego okna dialogowego w pliku CSV, kliknij **Eksport CSV**.

- 12.18.9 Okno dialogowe Skonfigurowani użytkownicy**
Okno dialogowe > menu **Raporty** > polecenie **Skonfigurowani użytkownicy...**
Zawiera listę użytkowników, którzy są uprawnieni do logowania się w programie Operator Client.
▶ Aby zapisać wszystkie informacje z tego okna dialogowego w pliku CSV, kliknij **Eksport CSV**.
- 12.18.10 Okno dialogowe Grupy i konta użytkowników**
Okno dialogowe > menu **Raporty** > polecenie **Grupy i konta użytkowników...**
Zawiera listę skonfigurowanych grup użytkowników, Enterprise Accounts i Enterprise User Groups grup podwójnej autoryzacji.
▶ Aby zapisać wszystkie informacje z tego okna dialogowego w pliku CSV, kliknij **Eksport CSV**.
- 12.18.11 Okno dialogowe Uprawnienia urządzenia**
Okno dialogowe > menu **Raporty** > polecenie **Uprawnienia urządzenia...**
Zawiera listę uprawnień poszczególnych grup użytkowników do korzystania ze skonfigurowanych urządzeń.
▶ Aby zapisać wszystkie informacje z tego okna dialogowego w pliku CSV, kliknij **Eksport CSV**.
- 12.18.12 Okno dialogowe Uprawnienia do obsługi**
Okno dialogowe > menu **Raporty** > polecenie **Uprawnienia do obsługi...**
Zawiera listę uprawnień poszczególnych grup użytkowników do korzystania z programu Operator Client.
▶ Aby zapisać wszystkie informacje z tego okna dialogowego w pliku CSV, kliknij **Eksport CSV**.
- 12.18.13 Konfigurowanie okna dialogowego Uprawnienia**
Okno dialogowe > menu **Raporty** > polecenie **Uprawnienia konfiguracji...**
Zawiera listę uprawnień poszczególnych grup użytkowników do korzystania z programu Configuration Client.
▶ Aby zapisać wszystkie informacje z tego okna dialogowego w pliku CSV, kliknij **Eksport CSV**.
- 12.18.14 Okno dialogowe Uprawnienia grupy użytkowników**
Okno dialogowe > menu **Raporty** > polecenie **Uprawnienia grup użytkowników...**
Zawiera listę uprawnień do konfigurowania grup użytkowników w poszczególnych grupach użytkowników.
▶ Aby zapisać wszystkie informacje z tego okna dialogowego w pliku CSV, kliknij **Eksport CSV**.
- 12.18.15 Okno dialogowe Ustawienia zabezpieczeń**
Okno dialogowe > menu **Raporty** > polecenie **Ustawienia zabezpieczeń...**
Wyświetla listę skonfigurowanych ustawień zabezpieczeń dla każdej grupy użytkowników i Enterprise User Groups.
▶ Aby zapisać wszystkie informacje z tego okna dialogowego w pliku CSV, kliknij **Eksport CSV**.
- 12.18.16 Okno dialogowe Uprawnienia aplikacji**
Okno główne > menu **Raporty** > polecenie **Uprawnienia do aplikacji...**

Wyświetla listę wszystkich grup użytkowników i ich uprawnień do aplikacji.
▶ Aby zapisać wszystkie informacje z tego okna dialogowego w pliku CSV, kliknij **Eksport CSV**.
- 12.18.17 Okno dialogowe Wyłączone urządzenia**
Okno dialogowe > menu **Raporty** > polecenie **Pominięte urządzenia...**

Wyświetla listę wszystkich skonfigurowanych wyłączonych urządzeń.

- ▶ Aby zapisać wszystkie informacje z tego okna dialogowego w pliku CSV, kliknij **Eksport CSV**.

12.19 Okno dialogowe Ustawienia alarmów (menu Ustawienia)

Patrz Okno dialogowe Ustawienia alarmowe, Strona 311, aby uzyskać szczegółowe informacje.

12.20 Okno dialogowe Ustawienia SNMP (menu Ustawienia)

Okno dialogowe > menu **Ustawienia** > polecenie **Ustawienia SNMP...**

Pozwala skonfigurować monitorowanie SNMP na komputerze Management Server. Można określić, które zdarzenia wysyłają komunikat trap SNMP, dodatkowe informacje o systemie i adresy IP komputerów, które będą otrzymywać komunikaty trap SNMP z systemu BVMS.

Serwer wyśle komunikat trap SNMP, gdy wystąpi określone zdarzenie. Komunikaty trap można otrzymywać przez odbiornik SNMP w programie Configuration Client za pomocą narzędzia **Narzędzie do rejestrowania komunikatów Trap SNMP**. Można także używać innego oprogramowania odbierającego komunikaty trap SNMP.

Agent SNMP w systemie BVMS obsługuje funkcję SNMP GetRequest. Gdy oprogramowanie menedżera SNMP (np. iReasoning MIB Browser) wyśle komunikat SNMP GetRequest do serwera BVMS Management Server, wówczas Management Server wyśle odpowiedni komunikat odpowiedzi. Plik MIB znajduje się w następującej lokalizacji:

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

Obsługiwane są tylko wersje SNMPv1 i v2.

Uwaga: Protokoły SNMPv1 i SNMPv2 nie są całkowicie zgodne. Ponadto nie zalecamy jednoczesnego używania protokołów SNMPv1 i SNMPv2.

Port SNMP GET

Wpisz numer portu dla SNMP GetRequest. Jest to port, na którym agent SNMP systemu BVMS Management Server nasłuchuje komunikatów SNMP GetRequest.

Uwaga: System BVMS nie używa standardowego portu nr 161 dla SNMP GetRequest, ponieważ ten port może być używany przez agenta SNMP komputera, na którym jest zainstalowany system BVMS Management Server.

Wartością domyślną jest 12544.

Kontakt systemu

Wprowadź dane kontaktowe dotyczące systemu BVMS. Można wyszukać te informacje przez SNMP GetRequest, używając OID .1.3.6.1.2.1.1.4.

Opis systemu

Wprowadź opis systemu BVMS. Można wyszukać te informacje przez SNMP GetRequest, używając OID .1.3.6.1.2.1.1.5.

Lokalizacja systemu

Wprowadź lokalizację systemu BVMS. Dane powinny określać fizyczną lokalizację serwera, np. numer budynku, numer sali, numer stelaża itd.

Można wyszukać te informacje przez SNMP GetRequest, używając OID .1.3.6.1.2.1.1.6.

Odbiorniki komunikatów Trap

Wprowadź adres IP komputera, do którego system BVMS będzie domyślnie wysyłać komunikaty trap SNMP.

Filtr komunikatów Trap

Kliknąć i wybrać zdarzenia w drzewie zdarzeń, aby przefiltrować wysłane komunikaty trap SNMP.

Patrz

– Konfigurowanie monitorowania SNMP, Strona 95

12.21**Okno dialogowe Ustawienia serwera LDAP (menu Ustawienia)**

Okno dialogowe > menu **Ustawienia** > polecenie **Ustawienia serwera LDAP...**

Wprowadzić ustawienia serwera LDAP, które zostały skonfigurowane poza systemem BVMS.

Potrzebna będzie pomoc administratora sieci, który skonfiguruje serwer LDAP dla poniższych opcji.

Konieczne jest wypełnienie wszystkich pól poza polami w pozycji **Testuj użytkownika / grupę użytkowników**.

Ustawienia serwera LDAP**Serwer LDAP**

Wpisać nazwę lub adres IP serwera LDAP.

Port

Wprowadzić numer portu serwera LDAP (domyślny HTTP: 389, HTTPS: 636)

Zabezpiecz połączenie

Zaznaczyć pole wyboru, aby włączyć bezpieczną transmisję danych.

Mechanizm uwierzytelniania

Funkcja negocjowania automatycznie wybiera odpowiedni protokół uwierzytelniania.

W prosty sposób przesyła poświadczenia logowania w postaci niezaszyfrowanej za pomocą zwykłego tekstu.

Uwierzytelnianie przez proxy**Anonimowy**

Pozwala logować się jako gość. Wybrać tę opcję, jeśli serwer LDAP obsługuje ją i nie można skonfigurować określonego użytkownika serwera proxy.

Użyj następujących poświadczeń**Nazwa użytkownika**

Wprowadzić niepowtarzalną nazwę użytkownika proxy. Użytkownik ten musi umożliwić dostęp do serwera LDAP użytkownikom tej grupy użytkowników systemu BVMS.

Hasło

Wprowadzić hasło użytkownika proxy.

Test

Kliknąć, aby sprawdzić, czy użytkownik proxy posiada dostęp do serwera LDAP.

Podstawa LDAP dla użytkownika

Wprowadzić niepowtarzalną nazwę (DN = distinguished name) ścieżki LDAP, w której będzie wyszukiwany użytkownik.

Przykład DN podstawy LDAP: CN=Users,DC=Security,DC=MyCompany,DC=com

Filtr dla użytkownika

Wybrać filtr używany do wyszukiwania niepowtarzalnej nazwy użytkownika. Dostępne są predefiniowane przykłady. W miejsce zmiennej %username% wstawić faktyczną nazwę użytkownika.

Podstawa LDAP dla grupy

Wprowadzić niepowtarzalną nazwę ścieżki LDAP, w której będą wyszukiwane grupy.

Przykład DN podstawy LDAP: CN=Users,DC=Security,DC=MyCompany,DC=com

Filtr wyszukiwania członka grupy

Wybrać filtr służący do wyszukiwania członka grupy.

Dostępne są predefiniowane przykłady. W miejsce zmiennej %usernameDN% wstawić faktyczną nazwę użytkownika oraz jego niepowtarzalną nazwę (DN).

Filtr wyszukiwania grupy

Nie pozostawiać tego pola pustego. Jeśli pole będzie puste, nie będzie można przypisać grupy LDAP do grupy użytkowników systemu BVMS.

Zaznaczyć filtr, aby odszukać grupę użytkowników.

Dostępne są predefiniowane przykłady.

Testuj użytkownika / grupę użytkowników

Parametry w tym oknie dialogowym nie są zapisywane po kliknięciu **OK**. Służą one jedynie do przeprowadzenia testu.

Nazwa użytkownika

Wprowadzić nazwę testowanego użytkownika. Pominąć DN.

Hasło

Wprowadzić hasło testowanego użytkownika.

Testuj użytkownika

Kliknąć, aby sprawdzić, czy kombinacja nazwy użytkownika i hasła jest prawidłowa.

Grupa (DN)

Wprowadzić niepowtarzalną nazwę grupy, do której jest przypisany użytkownik.

Testuj grupę

Kliknąć, aby sprawdzić przypisanie użytkownika do grupy.

Patrz

– Wybieranie skojarzonej grupy LDAP, Strona 357

12.21.1

Przypisywanie grupy LDAP

Grupę LDAP kojarzy się z grupą użytkowników BVMS, aby zapewnić użytkownikom tej grupy LDAP dostęp do programu Operator Client. Użytkownicy z tej grupy LDAP posiadają uprawnienia dostępu grupy użytkowników, w której skonfigurowana została grupa LDAP.

Do wprowadzenia tych ustawień będzie najprawdopodobniej potrzebna pomoc administratora sieci, który jest odpowiedzialny za obsługę serwera LDAP.

Grupy LDAP są konfigurowane w standardowych grupach użytkowników lub Enterprise User Groups.



Uwaga!

Jeśli grupa LDAP jest skojarzona z grupą użytkowników BVMS, użytkownicy tej grupy LDAP mogą uruchomić Operator Client za pomocą funkcji pojedynczego logowania.



Uwaga!

Użytkownik LDAP może być skojarzony z więcej niż jedną grupą użytkowników LDAP, które z kolei są skojarzone z określoną grupą użytkowników BVMS.

Użytkownik LDAP otrzymuje uprawnienia grupy użytkowników BVMS, która znajduje się na wyższym miejscu listy niż inne grupy użytkowników LDAP skojarzone z tym użytkownikiem LDAP.

Aby przypisać grupę LDAP:

1. Kliknąć **Ustawienia serwera LDAP...**

Zostanie wyświetlone okno dialogowe **Ustawienia serwera LDAP**.

2. Wpisać ustawienia serwera LDAP i kliknąć **OK**.

Kliknąć poniższy odnośnik do wybranego okna programu, aby uzyskać szczegółowe informacje o różnych polach.

Patrz

- Okno dialogowe Ustawienia serwera LDAP (menu Ustawienia), Strona 116
- strona Właściwości grupy użytkowników, Strona 330

12.22**Okno dialogowe Definiowanie kolejności grup użytkowników LDAP (menu Ustawienia)**

Wyświetla listę **Zmień kolejność grup użytkowników w usłudze LDAP**. Na liście będą pokazane grupy użytkowników LDAP ze skojarzonymi BVMSgrupami użytkowników oraz Enterprise User Groups. Przeciągając i upuszczając lub używając strzałek w górę i w dół można zmieniać kolejność grup.

**Uwaga!**

Użytkownik LDAP może być skojarzony z więcej niż jedną grupą użytkowników LDAP, które z kolei są skojarzone z określoną grupą użytkowników BVMS.

Użytkownik LDAP otrzymuje uprawnienia grupy użytkowników BVMS, która znajduje się na wyższym miejscu listy niż inne grupy użytkowników LDAP skojarzone z tym użytkownikiem LDAP.

12.23**Okno dialogowe Ustawienia tokena dostępu (menu Ustawienia)**

Okno dialogowe > menu **Ustawienia** > polecenie **Ustawienia tokena dostępu...**

Jeśli skonfigurowano logowanie do programu Management Server za pomocą tokena dostępu, najpierw należy zdefiniować ustawienia tokena.

Token jest tworzony w programie Enterprise Management Server i musi zostać podpisany za pomocą certyfikatu z magazynu certyfikatów na lokalnym komputerze. Należy precyzyjnie zidentyfikować dostępne certyfikaty, aby ustalić, który z nich ma zostać użyty.

Uwaga: Oprogramowanie BVMS nie obsługuje certyfikatów, które używają algorytmu bezpiecznego tworzenia skrótów SHA-1 i mają klucz krótszy niż 2048 bitów.

Właściwości certyfikatu podpisywania

Wpisz ciąg właściwości identyfikujących odpowiedni certyfikat.

Uwaga: Jeśli więcej niż jeden ważny certyfikat spełnia kryteriom, zostanie użyty najnowszy.

Aby wpisać prawidłowy ciąg właściwości w polu **Właściwości certyfikatu podpisywania**, przestrzegaj następujących reguł:

- Ciąg zawiera jeden lub wiele warunków.
- Warunki są rozdzielone średnikami (;).
- Warunki to pary nazwy właściwości certyfikatu i oczekiwanej wartości, rozdzielone znakiem równości (=).
- Nazwy właściwości certyfikatów mogą składać się z jednej lub wielu części, rozdzielonych kropką (.).
- W nazwach właściwości certyfikatów i oczekiwanych wartościach nie jest uwzględniana wielkość liter.

Przykłady:

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

- Część Nazwa pospolita (CN) w nazwie podmiotu certyfikatu musi mieć wartość *BVMS Token Issuer*.

- Dodatkowo część Nazwa pospolita w nazwie podmiotu certyfikatu w obiekcie nadrzędnym certyfikatu musi mieć wartość *BVMS Intermediate*. Obiektem nadrzędnym jest certyfikat użyty do podpisania bieżącego certyfikatu.

Parent.Thumbprint=A95FF7C6EC374127174D3AFA8EA67C94E8E66C3F

- Odcisk palca nadrzędnego obiektu certyfikatu musi mieć format jak niżej.

Lista obsługiwanych nazw właściwości certyfikatów:

Nazwa	Zwracany typ
Thumbprint	String
SerialNumber	String
SubjectName	Distinguished name of subject
IssuerName	Distinguished name of issuer
Parent	Certyfikat użyty do podpisania obecnego certyfikatu (urząd certyfikacji wystawcy)

Lista obsługiwanych nazw właściwości w nazwie wyróżniającej:

Nazwa	Zwracany typ
CN	Ciąg tekstowy: nazwa pospolita
OU	Ciąg tekstowy: nazwa jednostki organizacyjnej
O	Ciąg tekstowy: nazwa organizacji
L	Ciąg: nazwa lokalizacji
S	Ciąg: nazwa stanu/prowincji/województwa
C	Ciąg tekstowy: nazwa kraju

Przykłady użycia nazwy wyróżniającej:

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

Łańcuch certyfikatów

Zaznacz pole wyboru, aby dołączyć łańcuch certyfikatów.

Uwaga: Jeśli na komputerze z programem Management Server jest zainstalowany dokładnie ten sam certyfikat, nie trzeba koniecznie dołączać łańcucha certyfikatów.

Liczba dołączonych certyfikatów

Wpisz dokładną liczbę certyfikatów, które są uwzględnione w tokenie dostępu.

Uwaga: Pod żadnym pozorem nie uwzględniaj certyfikatu Root.

Okres ważności tokena dostępu

Wpisz czas w godzinach określający okres ważności tokenów po ich utworzeniu przez program Enterprise Management Server.

Patrz

- Uwierzytelnianie za pomocą tokenów, Strona 87

12.24**Okno dialogowe Ustawienia zaufanych certyfikatów (menu Ustawienia)**

Okno dialogowe > menu **Ustawienia** > polecenie **Ustawienia zaufanych certyfikatów...**

W tym oknie dialogowym można wprowadzić odcisk palca certyfikatu używany przez program Management Server do uwierzytelniania tokena dostępu.

Uwaga: Menu **Ustawienia zaufanych certyfikatów...** jest dostępne tylko wtedy, gdy program Configuration Client zostanie uruchomiony za pomocą uprawnień administratora, a logujący się użytkownik ma uprawnienie **Konfiguruj grupy użytkowników/Enterprise Accounts**.

Odcisk palca lub zaufany certyfikat

Pokazuje już skonfigurowany odcisk palca, a jeśli w rejestrze nie można odnaleźć konfiguracji, to pusty odcisk palca. Wpisz lub zmień odcisk palca certyfikatu głównego.

Podany odcisk zostanie zapisany w ścieżce `HKEY_LOCAL_MACHINE\SOFTWARE\Bosch Sicherheitssysteme GmbH\Bosch Video Management System\TrustedCertificates` w kluczu „BvmsTrustedCertificate”.

Uwaga: Podczas eksportowania konfiguracji odcisk nie jest do niej dołączany.

Uwaga: Oprogramowanie BVMS nie obsługuje certyfikatów, które używają algorytmu bezpiecznego tworzenia skrótów SHA-1 i mają klucz krótszy niż 2048 bitów.

12.25**Okno dialogowe Opcje (menu Ustawienia)**

Uwaga: niektóre funkcje wymagają zakupu odpowiedniej licencji.

Okno dialogowe > menu **Ustawienia** > polecenie **Opcje**

Ogólne**Configuration Client****Język**

Umożliwia skonfigurowanie wersji językowej programu Configuration Client. W przypadku zaznaczenia opcji **Język systemu** zostanie wybrany taki sam język, jaki jest używany w systemie Windows.

To ustawienie jest włączone po ponownym uruchomieniu programu Configuration Client.

Automatyczne wylogowanie

Umożliwia skonfigurowanie funkcji automatycznego wylogowywania z programu Configuration Client. Program Configuration Client wyloguje się po ustalonym okresie.

Po wylogowaniu z powodu braku aktywności zmiany wprowadzone na stronach konfiguracji poniższych urządzeń na stronie **Urządzenia** nie są automatycznie zapisywane, więc ulegają utracie:

- Nadajniki
- Dekodery
- Urządzenia VRM
- Urządzenia iSCSI
- Urządzenia VSG

Pozostałe oczekujące zmiany w konfiguracji są automatycznie zapisywane.

Uwaga: zmiany wprowadzane w oknach dialogowych, które nie zostały zatwierdzone kliknięciem przycisku **OK**, nie są zapisywane.

Scan options

Umożliwia skonfigurowanie możliwości skanowania konkretnej podsieci lub wielu podsieci w poszukiwaniu urządzeń.

Operator Client

Wielokrotne logowanie

Zezwalaj na wielokrotne logowanie tego samego użytkownika

Umożliwia użytkownikowi programu Web Client systemu BVMS SDK, aplikacji mobilnej systemu BVMS, BVMS lub programu Operator Client wielokrotne, jednocześnie logowanie za pomocą tej samej nazwy użytkownika.

Central Server

Ciąg połączenia bazy danych

Umożliwia skonfigurowanie ciągu połączenia dla bazy danych Rejestr.



Uwaga!

Ciąg należy zmienić tylko w przypadku, kiedy użytkownik chce skonfigurować zdalny serwer SQL dla rejestru i jest zaznajomiony z technologią serwera SQL.

Okres przechowywania

Umożliwia zdefiniowanie maksymalnego czasu przechowywania wpisów w rejestrze. Po upływie tego zdefiniowanego czasu przechowywania wpisy są automatycznie usuwane.

To ustawienie jest włączone po uaktywnieniu konfiguracji.

Urządzenia

Grupa monitorów

Pozwala wybrać ustawienia, które umożliwiają użytkownikom kontrolowanie wszystkich grup monitorów za pomocą poszczególnych komputerów klienckich systemu BVMS. Z tego powodu nie jest wymagane skonfigurowanie tego komputera jako stacji roboczej w drzewie urządzeń.

Wybór strumienia z odbiornika

Pozwala skonfigurować system tak, aby wszystkie dekodery w systemie używały zgodnego strumienia, a niekoniecznie strumienia podglądu na żywo.

To ustawienie jest włączone po uaktywnieniu konfiguracji.

Monitorowanie układu grupy i przydziału kamer

Możesz wybrać, czy po ponownym uruchomieniu Central Server układ grupy monitorów i ustawienia przypisania kamery mają być resetowane do ustawień domyślnych czy też zachować ostatnie ustawienia wprowadzone w Operator Client.

Jeśli chcesz zachować ostatnie ustawienia, zaznacz pole wyboru **Zachowaj ustawienia po ponownym uruchomieniu Central Server**.

Uwaga: Sekwencja kamer rozpocznie się od pierwszej kamery w sekwencji.

Serwer czasu nadajnika

Umożliwia skonfigurowanie ustawień serwera czasu w odniesieniu do nadajników. Domyślnie używany jest adres IP Central Server.

Funkcje systemowe

Audit Trail

Do edytowania ustawień wymienionych poniżej są potrzebne uprawnienia:

Audit Trail

Włączanie i wyłączanie funkcji Audit Trail.

Uwaga: Strona Audit Trail jest dostępna w aplikacji Configuration Client tylko po włączeniu tej funkcji.

Maksymalny okres przechowywania

Umożliwia zdefiniowanie maksymalnego czasu przechowywania wpisów funkcji Audit Trail. Po upływie tego zdefiniowanego czasu przechowywania wpisy są automatycznie usuwane.

Język

Należy wybrać żadaną wersję językową wpisów funkcji Audit Trail.

Wyjątek: Wszystkie wpisy funkcji Audit Trail z kategorii filtrowania **Urządzenia (konfiguracja kamery)** będą wyświetlane w języku skonfigurowanym dla aplikacji Configuration Client.

Uwaga: Bazę danych funkcji Audit Trail należy zainstalować poprzez jej zaznaczenie w instalatorze programu BVMS (opcjonalna funkcja instalatora).

Ustawienia funkcji Audit Trail są włączane dopiero po uaktywnieniu konfiguracji.

Mapy

Typ mapy tła

Umożliwia wybranie typu mapy tła dla mapy globalnej. Jeśli jest dostęp do Internetu (tryb online), dostępne są następujące typy map:

- **Mapa ulic HERE**
- **Mapa ulic HERE**
- **Mapa satelitarna HERE**

Jeśli nie ma dostępu do Internetu (tryb offline), wybrać **Brak**.



Uwaga!

Jeśli zmienisz typ mapy tła z offline (**Brak**) na online (mapy **HERE**), sprawdź, czy położenie map podrzędnych i punktów aktywnych kamery jest wciąż prawidłowe.

Map-based tracking assistant

Włącz funkcję systemową

Umożliwia skonfigurowanie, aby użytkownik programu Operator Client mógł używać opcji Map-based tracking assistant.

Wyświetlacz stanu zaawansowanego

Wyłącz kolorowanie miejsc aktywnych na mapach

Umożliwia skonfigurowanie wyłączenia migania aktywnych miejsc na mapach.

Włącz zaawansowane wyświetlanie stanu (kolorowanie miejsc aktywnych na mapach w zależności od stanu)

Umożliwia konfigurowanie wszystkich zdarzeń stanu w taki sposób, aby miejsca aktywne urządzeń należące do danego zdarzenia były wyświetlane z odpowiednim kolorem tła i migały po wystąpieniu tego zdarzenia.

Włącz zaawansowane wyświetlanie alarmu (kolorowanie miejsc aktywnych na mapach w zależności od alarmu)

Umożliwia konfigurowanie wszystkich alarmów w taki sposób, aby miejsca aktywne urządzeń należące do danego alarmu były wyświetlane z odpowiednim kolorem tła i migały po wystąpieniu tego alarmu.

Określanie zaawansowanego wyświetlania stanu jest możliwe dopiero po zapisaniu konfiguracji.

Miejsca aktywne są wyświetlane na mapie w programie Operator Client po uaktywnieniu konfiguracji.

Privacy overlay**Włącz funkcję systemową**

Umożliwia skonfigurowanie, aby użytkownik programu Operator Client mógł eksportować wideo przy użyciu opcji Privacy overlay.

Identity provider**Identity provider**

Wybierz dostawcę tożsamości. Po dokonaniu wyboru wyświetlane są dalsze opcje.

Tenant ID (dla dostawcy tożsamości Microsoft)

Wprowadź informacje zewnętrznego dostawcy tożsamości.

To pole jest opcjonalne.

***URL wystawcy (dla dostawcy tożsamości Amazon Federation)**

Wprowadź informacje zewnętrznego dostawcy tożsamości.

***Application ID**

Wprowadź informacje zewnętrznego dostawcy tożsamości.

Application secret

To pole należy wypełnić, aby użyć ciągu poufnego do identyfikacji połączenia z usługą zewnętrznego dostawcy tożsamości.

To pole jest opcjonalne.

Adres zewnętrzny

W razie potrzeby wpisz w tym polu zewnętrzny adres sieciowy połączenia przekierowywanego do BVMS Management Server, np. połączenie SSH lub internetowe.

To pole jest opcjonalne.

Kliknąć przycisk **OK**, aby zapisać zmiany.

Przetwarzanie metadanych**Wizualizacja obiektów na mapie**

Zaznacz pole wyboru, aby włączyć funkcję śledzenia obiektów w ustawieniach ogólnych.

Po włączeniu tej funkcji, na stronie **Kamery i zapis** w zakładce  pojawi się kolumna **Śledzenie obiektów**, w której można indywidualnie włączyć lub wyłączyć tę funkcję dla wybranych kamer.

**Uwaga!**

Funkcja śledzenia obiektów jest dostępna wyłącznie dla kamer z platformą CPP6 lub nowszą, dodanych do drzewa logicznego oraz do mapy globalnej.

Patrz

– strona Kamery, Strona 285

13 strona Urządzenia

Okno główne > **Urządzenia**



Uwaga!

Program BVMS Viewer nie obsługuje odbiorników.

Wyświetla okna Drzewo urządzeń i strony konfiguracji.

Liczba pozycji poniżej wpisu jest wyświetlana w nawiasach kwadratowych.

Umożliwia skonfigurowanie dostępnych urządzeń, takich jak nadajniki ONVIF, urządzenia Bosch Video Streaming Gateway, nadajniki, dekodery, VRM, nadajniki lokalnej pamięci masowej, matryce analogowe lub urządzenia peryferyjne, takie jak ATM/POS Bridge.

Uwaga:

Urządzenia są reprezentowane na drzewie i pogrupowane na podstawie fizycznej struktury sieci oraz kategorii urządzeń.

Źródła sygnału wizyjnego, takie jak nadajniki, są zgrupowane pod modułami VRM.

Aby wyszukać elementy:

- ▶ W polu wyszukiwania wpisz ciąg znaków i naciśnij przycisk ENTER aby przefiltrować wyświetlone elementy.
Pojawią się tylko elementy zawierające łańcuch i odpowiadające im elementy nadrzędne (tylko w drzewach). Zostanie podana liczba odfiltrowanych elementów oraz całkowita liczba elementów.

Uwaga: ciąg znaków należy otoczyć cudzysłowem, aby znaleźć go precyzyjnie. Na przykład wpisanie "Camera 1" odfiltruje kamery o tej nazwie, a nie camera 201.

- ▶ Kliknąć element drzewa, aby wyświetlić odpowiednią stronę.

13.1 Aktualizowanie stanów i informacji o wydajności urządzeń

Okno główne > **Urządzenia**

Na przykład po aktualizacji oprogramowania układowego może być konieczne zsynchronizowanie wydajności wszystkich skonfigurowanych dekoderek, nadajników i VSG. Dzięki tej funkcji informacji o wydajności poszczególnych urządzeń są porównywane z informacjami o wydajności już zapisanymi w BVMS. Informacje o wydajności wszystkich urządzeń w drzewie można aktualizować jednocześnie. Istnieje również możliwość skopiowania listy urządzeń, których informacje o wydajności zostały zmienione w schowku. Następnie można wkleić listę, na przykład do edytora tekstu, aby szczegółowo zbadać zmiany.

Lista urządzeń ze schowka ma postać pliku CSV i zawiera następujące informacje:

- Urządzenie
- Typ urządzenia
- Adres IP

Uwaga: w przypadku dużego systemu zawierającego kilka tysięcy skonfigurowanych urządzeń proces odświeżania stanów urządzeń i aktualizacji informacji o ich wydajności może trwać długo.



Uwaga!

Informacje o wydajności są pobierane tylko w odniesieniu do urządzeń osiągalnych. Aby sprawdzić, czy urządzenie jest nieosiągalne, należy sprawdzić stan urządzenia.

Aby zaktualizować stany i informacje o wydajności urządzeń:

1. Kliknąć .
Zostanie wyświetlone okno dialogowe **Aktualizuj wydajność urządzenia**. Informacje o stanie wszystkich urządzeń są aktualizowane i pobierane są ich informacje o ich wydajności.
Jeśli informacje o wydajności urządzeń nie są aktualne, odpowiednie urządzenia są wyświetlane na liście i przycisk **Aktualizuj** jest aktywny.
 2. W razie potrzeby kliknąć **Kopiuj listę urządzeń do schowka**.
 3. Kliknąć **Aktualizuj**.
 4. Kliknąć **OK**.
- ⇒ Informacje o wydajności urządzenia są teraz zaktualizowane.



Uwaga!

Informacje o stanie wszystkich urządzeń będą zawsze aktualizowane, nawet jeśli anulujesz okno dialogowe **Aktualizowanie informacji o wydajności urządzeń**.

13.2

Zmienianie hasła urządzeń sieciowych

Okno główne > **Urządzenia** >  **Zmień hasła urządzenia** > okno dialogowe **Zmień hasła urządzenia**

LUB

Okno główne > menu **Urządzenie** > polecenie **Zmień hasła urządzenia...** > okno dialogowe **Zmień hasła urządzenia**

Aby zmienić hasło urządzeń sieciowych, należy:

1. Zaznaczyć żądane urządzenie.
2. Kliknąć prawym przyciskiem myszy zaznaczone urządzenie, a następnie kliknąć **Edytuj hasło...**
Pojawi się okno dialogowe **Zmień hasła urządzenia**.
3. Zaznaczyć żądany tym hasła.
4. Wprowadzić nowe hasło.
5. Kliknąć przycisk **OK**.
Nowe hasło zostanie zaktualizowane w wybranym urządzeniu.

Aby uzyskać więcej informacji, patrz Okno dialogowe zmiany hasła urządzenia (menu Urządzenie), Strona 106.

Aby zmienić ustawienia dla wielu urządzeń, należy:

Patrz Konfiguracja wielu nadajników / odbiorników, Strona 230.

Patrz

- Okno dialogowe zmiany hasła urządzenia (menu Urządzenie), Strona 106

13.3

Dodawanie urządzenia

Okno główne > **Urządzenia**

Aby ręcznie dodać następujące urządzenia do drzewa urządzeń, należy znać adres sieciowy urządzenia:

- Sieciowe urządzenie wizyjne firmy Bosch
- Krosownica analogowa
Warunkiem dodania urządzenia Bosch Allegiant jest wskazanie właściwego pliku konfiguracyjnego Allegiant.

- Stacja robocza systemu BVMS
Stacja robocza musi mieć zainstalowane oprogramowanie Operator Client.
- Urządzenie komunikacyjne
- Urządzenie Bosch ATM/POS Bridge DTP
- Wirtualne wejście
- Urządzenie monitoringu sieci
- Klawiatura Bosch IntuiKey
- Klawiatura KBD-Universal XF
- Grupa monitorów
- Moduł wejścia-wyjścia
- Emulacja poleceń CCL urządzenia Allegiant
- Centrala alarmowa firmy Bosch
- Urządzenie analizy oparte na serwerze
- Systemy kontroli dostępu firmy Bosch

Można skanować w poszukiwaniu poniższych urządzeń, aby dodać je za pomocą okna dialogowego kreatora **BVMS Scan Wizard**:

- Urządzenia VRM
- Nadajniki
- Nadajniki podglądu bieżącego i z lokalną pamięcią masową
- Nadajniki podglądu bieżącego ONVIF
- Nadajniki z obsługą lokalnego urządzenia pamięci masowej
- Dekodery
- Urządzenia Video Streaming Gateway (VSG)
- Urządzenia DVR



Uwaga!

Po dodaniu urządzenia należy kliknąć przycisk , aby zapisać ustawienia.



Uwaga!

Dodać rejestrator DVR za pomocą konta administratora urządzenia. Korzystanie z konta użytkownika cyfrowego rejestratora wizyjnego z ograniczonymi uprawnieniami może skutkować dostępem do funkcji bezużytecznych w systemie BVMS, takich jak sterowanie kamerą PTZ.

Okno dialogowe BVMS Scan Wizard

Okno główne > **Urządzenia** > rozwiń opcję > kliknij prawym przyciskiem myszy > kliknij opcję **Skanuj w poszukiwaniu nadajników** > okno dialogowe **BVMS Scan Wizard**

Okno główne > **Urządzenia** > rozwiń opcję > kliknij prawym przyciskiem myszy > kliknij opcję **Skanuj w poszukiwaniu bram Video Streaming Gateway** > okno dialogowe **BVMS Scan Wizard**

Okno główne > **Urządzenia** > kliknij prawym przyciskiem myszy > kliknij opcję **Skanuj w poszukiwaniu nadajników tylko podglądu bieżącego** > okno dialogowe **BVMS Scan Wizard**

Okno główne > **Urządzenia** > kliknij prawym przyciskiem myszy  > kliknij opcję **Skanuj w poszukiwaniu nadajników z pamięcią lokalną** > okno dialogowe **BVMS Scan Wizard**

Okno główne > **Urządzenia** > rozwiń opcję  > rozwiń opcję  > kliknij prawym przyciskiem

myszy  > kliknij opcję **Wyszukaj dekodery** > okno dialogowe **BVMS Scan Wizard**

To okno dialogowe umożliwia w jednej procedurze wykonanie skanowania w poszukiwaniu urządzeń dostępnych w sieci, skonfigurowanie ich i dodanie do systemu.

Użyj

Kliknij, aby wybrać urządzenie dodawane do systemu.

Typ (brak dla urządzeń VSG)

Wyświetla typ urządzenia.

Wyświetlana nazwa

Wyświetla nazwę urządzenia wprowadzoną w drzewie urządzeń.

Adres sieciowy

Wyświetla adres IP urządzenia.

Nazwa użytkownika

Wyświetla nazwę użytkownika, która została skonfigurowana na tym urządzeniu.

Hasło

Wprowadź hasło, które umożliwia uwierzytelnienie w urządzeniu.

Stan

Pokazuje stan uwierzytelniania.



: pomyślne



: nieudane

Okno główne > **Urządzenia** > kliknij prawym przyciskiem myszy  > kliknij opcję **Skanuj w poszukiwaniu urządzeń VRM** > okno dialogowe **BVMS Scan Wizard**



Uwaga!

Aby skonfigurować pomocniczy VRM, należy najpierw zainstalować na komputerze odpowiednie oprogramowanie. Uruchom program Setup.exe i wybierz **Pomocniczy VRM**.

Rola

Wybierz odpowiednią pozycję na liście.

Poniższa tabela przedstawia dostępne role urządzenia VRM:

Rola/typ	Główny rejestrator VRM	Pomocniczy VRM
Podstawowy (normalny)	X	
Pomocniczy (normalny)		X
Podstawowy awaryjny	X	
Pomocniczy awaryjny		X
Redundantny		X

Do podstawowego VRM można dodać urządzenia VRM pełniące następujące role:

- Awaryjny VRM
- Nadmiarowy VRM

Do pomocniczego VRM można dodać urządzenia VRM pełniące następujące role:

- Awaryjny VRM

Główny VRM

Na liście zaznacz żądaną pozycję.

Nazwa użytkownika

Wyświetla nazwę użytkownika, która została skonfigurowana na urządzeniu.

Można wpisać inną nazwę użytkownika, jeśli jest to wymagane.

Patrz

- Dodawanie urządzeń VRM poprzez skanowanie:, Strona 169
- Dodawanie nadajnika do puli VRM, Strona 218
- Dodawanie nadajnika udostępniającego tylko podgląd bieżący, Strona 218
- Dodawanie nadajnika z pamięcią lokalną, Strona 218
- Skanowanie w poszukiwaniu urządzeń, Strona 74

13.4

Strona listy serwerów/książki adresowej

Okno główne > **Urządzenia** > **System Enterprise** > **Lista serwerów/książka adresowa**

W celu umożliwienia jednoczesnego dostępu w systemie BVMS Enterprise System można dodać wiele komputerów z serwerem Management Server. Ponadto można dodać wiele komputerów z serwerem Management Server, aby zapewnić sekwencyjny dostęp do funkcji Server Lookup.

Do listy serwerów można dodawać dalsze kolumny. Dzięki nim można wprowadzać więcej informacji, które mogą wyszukiwać użytkownicy podczas korzystania z funkcji Server Lookup. Dodane kolumny będą też widoczne na stronie **Dostęp do serwera** (okno główne > **Grupy użytkowników** > karta

Enterprise User Groups >  > karta **Dostęp do serwera**).

Dodaj serwer

Kliknij **Dodaj serwer**, aby wyświetlić okno dialogowe.

Usuń serwer

Kliknąć, aby usunąć wpisy Management Server.

Management Server

Wyświetla nazwy wszystkich dodanych komputerów Management Server. Użytkownik może zmienić każdy wpis.

Uwaga: używając połączenia SSH, należy wprowadzić adres w następującym formacie:

SSH://IP lub nazwa_serwera:5322

Prywatny adres sieciowy

Wyświetlane są prywatne adresy sieciowe wszystkich dodanych komputerów Management Server. Użytkownik może zmienić każdy wpis.

Numer serwera

Wyświetla numery logiczne wszystkich dodanych komputerów Management Server. Użytkownik może zmienić każdy wpis.

Opis serwera

Wprowadzić opis dla tego konta Management Server. Ten opis jest potrzebny do znajdowania pozycji na liście wszystkich dostępnych serwerów, gdy użytkownik chce wyłączonego dostępu do serwera Management Server, na przykład w celu wyjaśnienia alarmu mającego źródło w innym systemie zarządzania.

Kliknij, aby uzyskać szczegółowe instrukcje:

- Konfigurowanie funkcji listy serwerów dla systemu Enterprise System, Strona 85
- Konfigurowanie funkcji Server Lookup, Strona 129
- Eksportowanie listy serwerów, Strona 130
- Importowanie listy serwerów, Strona 130

Patrz

- Tunelowanie SSH, Strona 51

13.4.1**Okno dialogowe Dodaj serwer**

Okno główne > **Urządzenia** > **System Enterprise** > **Lista serwerów/książka adresowa**

Nazwa serwera

Wpisz wyświetlaną nazwę serwera Management Server.

Uwaga: używając połączenia SSH, należy wprowadzić adres w następującym formacie:

SSH://IP lub nazwa_serwera:5322

Prywatny adres sieciowy

Wpisz prywatny adres IP lub nazwę serwera DNS Management Server.

Adres sieci publicznej

Wpisz adres sieci publicznej.

Opis serwera

Wpisać opis dla Management Server.

13.4.2**Konfigurowanie funkcji Server Lookup**

W przypadku funkcji Server Lookup użytkownik Operator Client lub Configuration Client loguje się z użyciem nazwy użytkownika normalnej grupy użytkowników, a nie jako użytkownik grupy Enterprise User Group.

Patrz

- Server Lookup, Strona 26
- Strona listy serwerów/książki adresowej, Strona 128
- Używanie funkcji Server Lookup, Strona 74

13.4.3**Konfigurowanie listy serwerów**

Okno główne > **Urządzenia** > **System Enterprise** > **Lista serwerów/książka adresowa**

Aby dodać serwery:

1. Kliknąć **Dodaj serwer**.
Zostanie wyświetlone okno dialogowe **Dodaj serwer**.

2. Wpisać nazwę wyświetlaną na serwerze i wpisać adres sieci prywatnej (nazwa DNS lub adres IP).

Uwaga: w przypadku korzystania z połączenia SSH wprowadzić adres w następującym formacie:

ssh://IP or servername:5322

3. Kliknij **OK**.
4. Powtarzaj te czynności, aż zostaną dodane wszystkie żądane komputery typu Management Server.

Aby dodać kolumny:

- ▶ Kliknąć prawym przyciskiem myszy nagłówek tabeli i kliknąć **Dodaj kolumnę**.
Można dodać maks. 10 kolumn.
Aby usunąć kolumnę, kliknąć prawym przyciskiem myszy żądaną kolumnę i kliknąć **Usuń kolumnę**.
- ⇒ Podczas eksportowania listy serwerów dodane kolumny zostaną również wyeksportowane.

Patrz

- Konfigurowanie funkcji listy serwerów dla systemu Enterprise System, Strona 85

13.4.4

Eksportowanie listy serwerów

Okno główne > **Urządzenia** > **System Enterprise** > **Lista serwerów/książka adresowa**

Można wyeksportować listę serwerów i wszystkie skonfigurowane właściwości, aby dokonać edycji i zaimportować dane w późniejszym czasie.

Edytując wyeksportowany plik csv w edytorze zewnętrznym, należy uwzględnić ograniczenia opisane w rozdziale Lista serwerów.

Aby wyeksportować dane:

1. Kliknij prawym przyciskiem myszy nagłówek tabeli i wybierz **Eksportuj listę serwerów...**
 2. Wprowadź nazwę pliku eksportu i kliknij przycisk **Zapisz**.
- ⇒ Wszystkie kolumny listy serwerów zostaną wyeksportowane do pliku csv.

Tematy pokrewne

- Server Lookup, Strona 26
- Lista serwerów
- Strona listy serwerów/książki adresowej, Strona 128

13.4.5

Importowanie listy serwerów

Okno główne > **Urządzenia** > **System Enterprise** > **Lista serwerów/książka adresowa**

Edytując wyeksportowany plik csv w edytorze zewnętrznym, należy uwzględnić ograniczenia opisane w rozdziale Lista serwerów.

Aby zaimportować dane:

1. Kliknij prawym przyciskiem myszy nagłówek tabeli i wybierz **Importuj listę serwerów...**
2. Wybierz żądany plik i kliknij przycisk **Otwórz**.

Tematy pokrewne

- Server Lookup, Strona 26
- Lista serwerów
- Strona listy serwerów/książki adresowej, Strona 128

13.5

Strona DVR (cyfrowego rejestratora wizyjnego)



Okno główne > **Urządzenia** >

Wyświetla strony właściwości wybranego urządzenia DVR.
Umożliwia integrację urządzenia DVR z systemem użytkownika.
► Kliknąć kartę, aby wyświetlić odpowiednią stronę właściwości.

**Uwaga!**

Rejestrator DVR nie podlega odrębnej konfiguracji, lecz jest konfigurowany jako element zintegrowany z systemem BVMS.

**Uwaga!**

Dodać rejestrator DVR za pomocą konta administratora urządzenia. Korzystanie z konta użytkownika cyfrowego rejestratora wizyjnego z ograniczonymi uprawnieniami może skutkować dostępem do funkcji bezużytecznych w systemie BVMS, takich jak sterowanie kamerą PTZ.

Patrz

- urządzenia DVR, Strona 131
- Konfiguracja zintegrowanego rejestratora DVR, Strona 133

13.5.1

urządzenia DVR

W tym rozdziale znajdują się podstawowe informacje o urządzeniach DVR, które mogą być zintegrowane z systemem BVMS.

Część modeli urządzeń DVR umożliwia nagrywanie z nadajników/kamer sieciowych. Pozostałe modele rejestratorów DVR obsługują wyłącznie kamery analogowe.

Pojedynczy nadajnik lub kamera sieciowa nie może być elementem konfiguracji dwóch systemów wizyjnych (rejestratorów DVR lub systemów zarządzania obrazem).

Nadajniki/kamery sieciowe połączone do urządzenia DVR, które jest już zintegrowane z systemem BVMS nie będą wykrywane przez proces skanowania sieci systemu BVMS. Odnosi się to do skanowania sieci rozpoczętego z poziomu programu Configuration Client lub kreatora Config Wizard. W przypadku, gdy urządzenie DVR z podłączonymi nadajnikami/kamerami sieciowymi zostanie zintegrowane z systemem BVMS, a te nadajniki lub kamery sieciowe zostały wcześniej dodane do systemu BVMS, wyświetlane jest ostrzeżenie. Należy usunąć te nadajniki/kamery sieciowe z konfiguracji DVR lub z systemu BVMS.

Config Wizard nie dodaje do konfiguracji urządzeń DVR z podłączonymi kamerami sieciowymi, które powodują konflikt.

Urządzenia DVR mogą obsługiwać ograniczoną liczbę jednoczesnych połączeń. Ta wartość oznacza maksymalną liczbę użytkowników programu Operator Client, którzy mogą jednocześnie wyświetlać obraz z tego urządzenia DVR, aby nie dochodziło do ukazania się czarnego Okienka obrazu.

**Uwaga!**

Dodać rejestrator DVR za pomocą konta administratora urządzenia. Korzystanie z konta użytkownika cyfrowego rejestratora wizyjnego z ograniczonymi uprawnieniami może skutkować dostępem do funkcji bezużytecznych w systemie BVMS, takich jak sterowanie kamerą PTZ.

**Uwaga!**

DIVAR AN 3000/5000: przy usuwaniu danych wizyjnych z cyfrowego rejestratora wizyjnego należy pamiętać, że zawsze kasowana jest co najmniej godzina materiału wideo. Na przykład po wybraniu przedziału czasu od 6:50 do 7:05 zostaną tak naprawdę usunięte dane wizyjne obejmujące okres od 6:00 do 8:00.

Rejestratory sieciowe i hybrydowe HD serii 700 firmy Bosch: usuwanie rozpoczyna się zawsze od początku nagrań ze wszystkich kamer wyświetlanych w programie Operator Client i kończy we wprowadzonym przez użytkownika punkcie czasowym.

Patrz

- Strona DVR (cyfrowego rejestratora wizyjnego), Strona 130
- Konfiguracja zintegrowanego rejestratora DVR, Strona 133

13.5.2

Dodawanie urządzenia DVR poprzez skanowanie

Aby poprzez skanowanie dodać urządzenia DVR:

1. Kliknij prawym przyciskiem myszy , a następnie kliknij **Skanuj w poszukiwaniu urządzeń DVR**.

Zostanie wyświetlone okno dialogowe **BVMS Scan Wizard**.

2. Zaznacz pola wyboru odpowiadające urządzeniom, które mają zostać dodane.
3. Kliknij **Dalej >>**.

Zostanie wyświetlone okno dialogowe kreatora **Uwierzytelnianie urządzeń**.

4. Wpisać hasło w przypadku każdego urządzenia, które jest nim chronione.
Jeśli przez kilka sekund nie wprowadzisz żadnego znaku w polu hasła lub klikniesz poza tym polem, sprawdzenie hasła następuje automatycznie.
Jeśli hasło do wszystkich urządzeń jest identyczne, można wpisać je w pierwszym polu **Hasło**.
Następnie kliknąć to pole prawym przyciskiem myszy i wybrać opcję **Kopiuj komórkę do kolumny**.

Udane logowanie jest oznaczane w kolumnie **Stan** ikoną .

Nieudane próby logowania są oznaczane ikoną .

5. Kliknąć **Zakończ**.
Urządzenie zostanie dodane do drzewa urządzeń.

13.5.3

Dodanie okna dialogowego DVR

Okno główne > **Urządzenia** > rozwinąć  >  > **Dodaj urządzenie DVR**
Umożliwia ręczne dodanie urządzenia DVR.

Adres/port sieciowy

Wpisz adres IP systemu DVR. Jeśli jest to wymagane, zmień numer portu.

Nazwa użytkownika:

Należy tu wpisać nazwę użytkownika stosowaną do nawiązywania połączenia z cyfrowym rejestratorem wizyjnym.

Hasło:

Należy tu wpisać hasło służące do nawiązywania połączenia z cyfrowym rejestratorem wizyjnym.

Bezpieczeństwo

Pole wyboru **Zabezpiecz połączenie** jest domyślnie zaznaczone.

Jeśli połączenie bezpieczne jest niemożliwe, zostanie wyświetlony odpowiedni komunikat. Kliknąć, aby usunąć zaznaczenie.

**Uwaga!**

Jeśli pole wyboru **Bezpieczne połączenie** jest zaznaczone, połączenia związane z poleceniami i sterowaniem są bezpieczne. Strumieniowe przesyłanie danych wideo nie jest zabezpieczone.

Patrz

– Dodawanie urządzenia, Strona 125

13.5.4**Karta Ustawienia**

Okno główne > **Urządzenia** > > karta **Ustawienia**

Wyświetla ustawienia sieciowe urządzenia DVR dołączonego do systemu. Umożliwia zmianę ustawień, jeśli jest to wymagane.

13.5.5**Karta Kamery**

Okno główne > **Urządzenia** > > karta **Kamery**

Wyświetla wszystkie kanały wizyjne urządzenia DVR jako kamery. Umożliwia usuwanie kamer. Wejście wizyjne wyłączone w urządzeniu DVR jest w systemie BVMS widoczne jako aktywna kamera, ponieważ mogą istnieć związane z nim wcześniejsze zapisy.

13.5.6**Karta wejść**

Okno główne > **Urządzenia** > > karta **Wejścia**

Wyświetla wszystkie wejścia urządzenia DVR.

Umożliwia usuwanie pozycji.

13.5.7**Karta Przekazniki**

Okno główne > **Urządzenia** > > karta **Przekazniki**

Wyświetla wszystkie przekazniki urządzenia DVR. Umożliwia usuwanie pozycji.

13.5.8**Konfiguracja zintegrowanego rejestratora DVR**

Okno główne > **Urządzenia** > rozwinąć > >

**Uwaga!**

Dodać rejestrator DVR za pomocą konta administratora urządzenia. Korzystanie z konta użytkownika cyfrowego rejestratora wizyjnego z ograniczonymi uprawnieniami może skutkować dostępem do funkcji bezużytecznych w systemie BVMS, takich jak sterowanie kamerą PTZ.

**Uwaga!**

Rejestrator DVR nie podlega odrębnej konfiguracji, lecz jest konfigurowany jako element zintegrowany z systemem BVMS.

Aby usunąć element:

1. Kliknąć kartę **Ustawienia**, a następnie kartę **Kamery**, kartę **Wejścia** lub kartę **Przekazniki**.
2. Kliknąć element prawym przyciskiem myszy i wybrać polecenie **Usuń**. Element zostanie usunięty.

**Uwaga!**

Aby przywrócić usunięty element, kliknąć prawym przyciskiem myszy urządzenie DVR i kliknąć **Ponownie skanuj urządzenie DVR**.

Aby zmienić nazwę urządzenia DVR:

1. Kliknąć prawym przyciskiem myszy urządzenie DVR, a następnie kliknąć **Zmień nazwę**.
2. Wprowadzić nową nazwę dla urządzenia.

Patrz

- Dodawanie urządzenia, Strona 125
- Strona DVR (cyfrowego rejestratora wizyjnego), Strona 130

13.6

strona Krosownicy wizyjnej

Okno główne > **Urządzenia** >  > 

Wyświetla strony właściwości urządzenia Bosch Allegiant.

Podczas tej procedury nie konfiguruje się samego urządzenia Bosch Allegiant, a jedynie jego właściwości powiązane z systemem BVMS. Informacje o łączeniu urządzenia Allegiant z systemem BVMS znajdują się w rozdziale **Pojęcia** w Pomocy ekranowej. Niniejszy rozdział zawiera podstawowe informacje na temat wybranych zagadnień.

Dodatkowo możliwa jest konfiguracja priorytetów sterowania dla linii połączeń Allegiant.

- ▶ Kliknij kartę, aby wyświetlić odpowiednią stronę właściwości.

Patrz

- Konfigurowanie urządzenia Bosch Allegiant, Strona 134
- Podłączanie krosownicy Bosch Allegiant do systemu BVMS, Strona 58

13.6.1

Dodawanie urządzenia Bosch Allegiant

Aby dodać urządzenie Bosch Allegiant:

1. Kliknąć prawym przyciskiem myszy  i kliknąć **Dodaj urządzenie Allegiant**.
przycisk **Otwórz** Zostanie wyświetlone okno dialogowe.
2. Wybierz właściwy plik konfiguracyjny Allegiant i kliknij przycisk **OK**.
Urządzenie Bosch Allegiant zostanie dodane do systemu.

Uwaga: Do systemu można dodać tylko jedną krosownicę Bosch Allegiant.

13.6.2

Konfigurowanie urządzenia Bosch Allegiant

Okno główne > **Urządzenia** > rozwinąć  > 

Podczas tej procedury nie konfiguruje się samego urządzenia Bosch Allegiant, a jedynie jego właściwości powiązane z systemem BVMS.

Aby przypisać wyjście do nadajnika, należy:

1. Kliknąć kartę **Wyjścia**.
2. W kolumnie **Używanie** kliknąć **Linia cyfrowa** w żądanych komórkach.
3. W kolumnie **Nadajnik** zaznaczyć żądany nadajnik.

Dodawanie wejścia do urządzenia Bosch Allegiant:

1. Kliknąć kartę **Wejścia**.

2. Kliknąć **Dodaj wejścia**. W tabeli zostanie dodany nowy wiersz.
3. Wprowadzić żądane ustawienia w komórkach.

Usuwanie wejścia:

1. Kliknąć kartę **Wejścia**.
2. Kliknąć żądany wiersz tabeli.
3. Kliknąć **Usuń wejście**. Wiersz zostanie usunięty z tabeli.

Patrz

- Podłączanie klawiatury Bosch IntuiKey do systemu BVMS, Strona 54
- strona Połączenie, Strona 136
- strona Kamery, Strona 136
- strona Wyjścia, Strona 135
- strona Wejścia, Strona 136

13.6.3

strona Wyjścia

Okno główne > **Urządzenia** > rozwinąć  >  > karta **Wyjścia**

Umożliwia skonfigurowanie sposobu używania wyjścia urządzenia Bosch Allegiant oraz przypisanie nadajnika do wyjścia.

Aby w systemie BVMS można było zapisywać sygnał wizyjny z wyjścia urządzenia Bosch Allegiant, należy przypisać nadajnik do wyjścia. Ten nadajnik musi być połączony z wyjściem.

Nr

Wyświetla numer wyjścia.

Nr logiczny urządzenia Allegiant

Wyświetla logiczny numer wyjścia urządzenia Allegiant.

Nr logiczny systemu BVMS

Pozwala zmienić numer logiczny wyjścia w systemie BVMS. Jeśli wprowadzisz już używany numer, pojawi się komunikat.

Nazwa

Wyświetla nazwę wyjścia.

Używanie

Umożliwia zmianę sposobu używania wyjścia.

W przypadku wybrania **Linia cyfrowa** możliwe jest przypisanie nadajnika do tego wyjścia w polu

Nadajnik. Wyjście urządzenia Allegiant staje się kompatybilne z siecią.

W przypadku wybrania opcji **Monitor Allegiant** w programie Operator Client użytkownik może przypisać sygnał kamery do monitora sprzętu. Sterowanie PTZ jest możliwe, jeśli kamera jest skonfigurowana jako kamera PTZ. W programie Operator Client użytkownik nie może przeciągnąć tej kamery do okienka obrazu.

W przypadku wybrania opcji **Nie używane** użytkownik nie może przypisać monitora do kamery systemu Allegiant.

Nadajnik

Umożliwia przypisanie wyjścia do nadajnika. Nadajnik można wybrać tylko po zaznaczeniu pola **Linia cyfrowa**. Nadajnik jest zablokowany dla drzewa logicznego. W przypadku przypisania nadajnika, który już znajduje się w drzewie logicznym, zostanie on stamtąd usunięty. W programie Operator Client użytkownik może przeciągnąć kamerę do okienka obrazu.

Patrz

- Konfigurowanie urządzenia Bosch Allegiant, Strona 134

13.6.4 strona Wejścia

Okno główne > **Urządzenia** > rozwinąć  >  > karta **Wejścia**
Umożliwia dodanie wejść do urządzenia Bosch Allegiant.

Dodaj wejście

Kliknij, aby dodać nowy wiersz w tabeli służący do określenia nowego wejścia.

Usuń wejście

Kliknij, aby usunąć wiersz z tabeli.

Nr wejścia

Wprowadź wymagany numer wejścia. Jeśli wprowadzisz już używany numer, pojawi się komunikat.

Wprowadź nazwę

Wprowadź wymaganą nazwę wejścia.

Patrz

– Konfigurowanie urządzenia Bosch Allegiant, Strona 134

13.6.5 strona Połączenie

Okno główne > **Urządzenia** > rozwinąć  >  > karta **Połączenie**

Wyświetla nazwę pliku konfiguracyjnego urządzenia Bosch Allegiant.

System BVMS odczytuje pliki konfiguracyjne w strukturalnym formacie zapisu danych wraz z nazwami i konfiguracją wszystkich kamer podłączonych do urządzenia Bosch Allegiant.

Aktualizuj konfigurację

Kliknij, aby wybrać zaktualizowany plik konfiguracyjny Bosch Allegiant.

Patrz

– Konfigurowanie urządzenia Bosch Allegiant, Strona 134

13.6.6 strona Kamery

Okno główne > **Urządzenia** > rozwinąć  >  > karta **Kamery**

Wyświetla tabelę kamer obejmującą kamery podłączone do urządzenia Bosch Allegiant.

Nr

Wyświetla kolejny numer kamery.

Nr logiczny urządzenia Allegiant

Wyświetla logiczny numer kamery.

Nazwa kamery

Wyświetla nazwę kamery.

Patrz

– Konfigurowanie urządzenia Bosch Allegiant, Strona 134

13.7 strona Stacja robocza

Okno główne > **Urządzenia** > rozwiń węzeł  > 

Stacja robocza musi mieć zainstalowane oprogramowanie Operator Client.

Umożliwia skonfigurowanie następujących ustawień stacji roboczej:

- Dodawanie klawiatury CCTV podłączonej do stacji roboczej z systemem Bosch Video Management System.
- Przypisywanie skryptu poleceń, który jest wykonywany podczas uruchamiania stacji roboczej.
- Wybór strumienia domyślnego do wyświetlania obrazu na żywo. Strumienie można wybierać z kamer dwu- i wielostrumieniowych.

Uwaga: klawiatura CCTV nie może być skonfigurowana do pracy z domyślną stacją roboczą. Jest to możliwe tylko w określonych skonfigurowanych stacjach roboczych.

Aby dodać klawiaturę Bosch IntuiKey, która jest podłączona do odbiornika, rozwinąć węzeł  i

kliknąć pozycję .

Patrz

- Ręczne dodawanie stacji roboczej, Strona 137
- Konfigurowanie startowego skryptu poleceń (strona ustawień), Strona 138

13.7.1

Ręczne dodawanie stacji roboczej

Aby dodać stację roboczą systemu BVMS, należy:

1. Prawym przyciskiem myszy kliknąć .
2. Kliknąć **Dodaj stację roboczą**.
Zostanie wyświetlone okno dialogowe **Dodaj stację roboczą**.
3. Wpisać odpowiednią wartość.
4. Kliknąć przycisk **OK**.

Stacja robocza  zostanie dodana do systemu.

Aby dodać domyślną stację roboczą systemu BVMS, należy:

- ▶ Prawym przyciskiem myszy kliknąć ikonę .
- Kliknąć przycisk **Dodaj domyślną stację roboczą**.

Stacja robocza  jest dodana do Twojego systemu.



Uwaga!

Można dodać tylko jedną pojedynczą domyślną stację roboczą.

Jeśli zostanie skonfigurowana domyślna stacja robocza, ustawienia dotyczą wszystkich stacji roboczych dołączonych do tego serwera i nie są konfigurowane osobno.

W przypadku skonfigurowania stacji roboczej będą stosowane ustawienia tej stacji, a nie ustawienia domyślnej stacji roboczej.

13.7.2

Konfigurowanie klawiatury Bosch IntuiKey (strona Ustawienia) (stacja robocza)

Okno główne > **Urządzenia** > rozwinąć  > 

Aby skonfigurować klawiaturę Bosch IntuiKey dołączoną do stacji roboczej, należy:

1. Kliknąć kartę **Ustawienia**.
2. W polu **Ustawienia klawiatury** skonfigurować żądane ustawienia.

Więcej informacji o różnych polach znajduje się w Pomocy ekranowej wybranego okna programu.

Patrz

– strona Stacja robocza, Strona 136

13.7.3**Konfigurowanie startowego skryptu poleceń (strona ustawień)**

Okno główne > **Urządzenia** > rozwinąć  >  > strona **Ustawienia**

Skrypt poleceń można skonfigurować tak, aby był wykonywany podczas uruchamiania programu Operator Client zainstalowanego na wybranej stacji roboczej.

Użytkownik musi utworzyć odpowiedni skrypt poleceń.

Aby utworzyć skrypt poleceń, patrz Zarządzanie skryptami poleceń, Strona 89.

Aby skonfigurować skrypt wykonywany przy uruchomieniu, należy:

- ▶ Na liście **Skrypt startowy**: zaznaczyć żądany skrypt poleceń.

Patrz

– strona Stacja robocza, Strona 136

13.7.4**strona Ustawienia**

Okno główne > **Urządzenia** > rozwinąć  >  > karta **Ustawienia**

Umożliwia skonfigurowanie skryptu, który jest wykonywany w momencie uruchomienia programu Operator Client na stacji roboczej.

Umożliwia skonfigurowanie protokołu TCP lub UDP jako protokołu transmisji dla wszystkich kamer wyświetlanych na stacji roboczej w trybie podglądu na żywo.

Pozwala określić, który strumień danych z urządzenia sieciowego ma być używany do wyświetlania obrazu bieżącego.

Umożliwia włączenie na danej stacji roboczej funkcji wyszukiwania na podstawie ruchu w obrazie.

Dodatkowo można skonfigurować klawiaturę dołączoną do tej stacji roboczej.

Adres sieciowy:

Wprowadzić nazwę DNS lub adres IP systemu stacji roboczej.

Skrypt startowy:

Należy tu wybrać żądany skrypt, który ma być wykonywany podczas uruchamiania programu Operator Client na stacji roboczej. Skrypt jest tworzony lub importowany ze strony **Zdarzenia**.

Domyślny protokół kamery:

Wybrać domyślny protokół transmisji używany przez wszystkie kamery, które są przypisane do Drzewa logicznego tej stacji roboczej.

Zastęp ustawienia ze strony "Kamera i zapis"

Zaznaczenie tego pola wyboru umożliwia wybieranie odpowiedniego strumienia danych do podglądu na żywo.

Uwaga: w przypadku cyfrowych rejestratorów wizyjnych, które dostarczają więcej niż 1 strumień (np. DIVAR AN 3000/5000), to pole wyboru powoduje również zmianę ustawienia ich strumienia na żywo. Ustawienia ich strumienia na żywo są niedostępne na stronie **Kamery i zapis**.

Strumień bieżący

Należy wybrać odpowiedni strumień do podglądu na żywo. Strumień można wybierać z kamer dwu- i wielostrumieniowych.

Po wybraniu opcji **Zoptymalizowany rozmiar okienka obrazu** rozdzielczość wyświetlanego obrazu z każdej kamery jest automatycznie dopasowywana do rozmiaru okienka obrazu, odpowiednio do rozdzielczości używanego monitora. Przydaje się to w przypadku wyświetlania obrazu z wielu kamer o wysokiej rozdzielczości, np. kamer 4K ultra HD. Dostosowanie rozdzielczości do okienka obrazu jest możliwe tylko w przypadku kamer przesyłających strumienie, których rozdzielczość można niezależnie konfigurować. Użytkownik programu Operator Client może zmieniać wybór strumienia dla każdej kamery z osobna.

Kamery dwustrumieniowe

Wybierz domyślny strumień do wyświetlania na żywo z kamer dwustrumieniowych.

Kamery wielostrumieniowe

Wybierz domyślny strumień do wyświetlania na żywo z kamer wielostrumieniowych.

Zamiast użyj strumienia transkodowanego, jeśli jest dostępny

Zaznaczenie tego pola wyboru włącza użycie strumienia transkodowanego, o ile jest dostępny.

Strumień transkodowany służy wtedy do podglądu na żywo zamiast wybranego strumienia.

Aby w systemie BVMS był dostępny strumień transkodowany, komputer z usługą VRM musi być wyposażony w transkoder sprzętowy.

Gdy obraz z kamery jest wyświetlany w trybie podglądu na żywo, używany jest domyślny strumień ustawiony dla stacji roboczej. Jeśli kamera nie dostarcza strumienia 2 lub usługa transkodowania (programowa lub sprzętowa) jest niedostępna, zostanie użyty strumień 1, nawet jeśli w ustawieniach stacji roboczej wybrana jest inna opcja.

Odtwarzaj bezpośrednio z pamięci masowej

Zaznacz pole wyboru, aby strumień wideo był przesyłany bezpośrednio z urządzenia pamięci masowej do tej stacji roboczej. Strumień nie jest teraz wysyłany za pośrednictwem oprogramowania VRM. Stacja robocza nadal musi nawiązywać połączenie z oprogramowaniem VRM w celu umożliwienia prawidłowego odtwarzania.

Uwaga: bezpośrednie odtwarzanie z urządzenia pamięci masowej iSCSI jest dostępne tylko wówczas, jeśli ustawiono globalne hasło CHAP iSCSI.

Pobierz obraz bieżący ze strumienia 1 Video Streaming Gateway dla kamer z obrazem bieżącym "Bezpośrednio z kamery"

Wyświetla listę urządzeń Video Streaming Gateway. Wybrać żądane pozycje, aby umożliwić przesyłanie danych wizyjnych między źródłem sygnału wizyjnego a stacją roboczą poprzez odcinki o niskiej przepustowości.

Uwaga: Jeśli wybierzesz pobieranie obrazu wideo na żywo z urządzenia Video Streaming Gateway, ustawienie **Obraz bieżący - Profil** na stronie **Kamery i zapis** przestanie działać. Zamiast tego do transmisji obrazu na żywo będzie również używane ustawienie **Zapis - Profil**.

Typ klawiatury:

Wybierz typ klawiatury dołączonej do stacji roboczej.

Port

Wybierz port COM, do którego będzie podłączana klawiatura.

Szybkość transmisji:

Wybrać maksymalną prędkość w bitach na sekundę (b/s), z którą mają być przesyłane dane przez port. Zwykle jest to maksymalna prędkość obsługiwana przez komputer lub urządzenie, z którym jest nawiązywana komunikacja.

Bity danych:

Wyświetla liczbę bitów danych dla każdego znaku, który jest odbierany i transmitowany.

Bity stopu:

Wyświetla czas pomiędzy każdym transmitowanym ciągiem znaków (czas jest podawany w bitach).

Parzystość:

Wyświetla rodzaj sprawdzania błędów używany dla wybranego portu.

Typ portu:

Wyświetla typ połączenia używanego do połączenia klawiatury Bosch IntuiKey ze stacją roboczą.

Patrz

- Konfigurowanie startowego skryptu poleceń (strona ustawień), Strona 138

13.7.5**Zmiana adresu sieciowego stacji roboczej**

Okno główne > **Urządzenia** > rozwiń 

Aby zmienić adres IP:

1. Kliknąć prawym przyciskiem myszy  i kliknąć **Zmień adres sieciowy**.
Zostanie wyświetlone okno dialogowe **Zmień adres sieciowy**.
2. Zmień zawartość pola zgodnie z potrzebami.

13.8**Strona Odbiorniki**

Okno główne > **Urządzenia** > rozwinąć  > 

Umożliwia dodanie i skonfigurowanie odbiorników.

**Uwaga!**

Program BVMS Viewer nie obsługuje odbiorników.

**Uwaga!**

Aby używać dekoderek w systemie, należy upewnić się, że wszystkie nadajniki mają to samo hasło dla poziomu autoryzacji użytkownika user.

Patrz

- Skanowanie w poszukiwaniu urządzeń, Strona 74
- Strona Bosch Encoder / Decoder / Camera (Nadajnik/odbiornik/kamera firmy Bosch), Strona 215

13.8.1**Ręczne dodawanie nadajnika**

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > kliknij prawym przyciskiem myszy



> kliknij **Dodaj nadajnik** > okno dialogowe **Dodaj nadajnik**

lub

Okno główne > **Urządzenia** > kliknij prawym przyciskiem myszy  > kliknij **Dodaj nadajnik** > okno dialogowe **Dodaj nadajnik**

lub

Okno główne > **Urządzenia** > kliknij prawym przyciskiem myszy  > kliknij **Dodaj nadajnik** > okno dialogowe **Dodaj nadajnik**

lub

Okno główne > **Urządzenia** > rozwiń  > kliknij prawym przyciskiem myszy  > kliknij **Dodaj odbiornik** > okno dialogowe **Dodaj nadajnik**

Umożliwia ręczne dodanie nadajnika. Jest to szczególnie użyteczne, gdy chce się dodać sieciowe urządzenie wizyjne firmy Bosch (tylko dla VRM).

Uwaga:

W przypadku dodawania nadajnika strumienia wideo firmy Bosch za pomocą funkcji <**Automatyczne wykrywanie**> to urządzenie musi być dostępne w sieci.

Aby dodać sieciowe urządzenie wizyjne firmy Bosch:

1. Rozwiń , rozwiń , kliknąć prawym przyciskiem myszy .
lub
Kliknąć prawym przyciskiem myszy .
lub
Kliknąć prawym przyciskiem myszy .
2. Kliknąć **Dodaj nadajnik**.
Zostanie wyświetlone okno dialogowe **Dodaj nadajnik**.
3. Wprowadzić prawidłowy adres IP.
4. Na liście zaznaczyć pozycję <**Automatyczne wykrywanie**>, wprowadź hasło dostępu do urządzenia i kliknij przycisk **Uwierzytelnij**.
Lub
Na liście zaznaczyć określony typ nadajnika lub <**Symbol zastępczy jednej kamery**>.
5. Kliknij **OK**.
Urządzenie zostanie dodane do systemu.

Ikona  oznacza błąd, którym należy się zająć. Więcej informacji o charakterze błędu uzyskasz z etykiety narzędzia.

Okno dialogowe Dodaj nadajnik

Adres sieciowy

Wpisz poprawny adres IP.

Numer portu

Wpisać numer portu urządzenia.

Typ nadajnika

W przypadku urządzeń, których typ jest znany, wybierz odpowiednią pozycję. Urządzenie nie musi być dostępne w sieci.

Dodając sieciowe urządzenie wizyjne firmy Bosch, zaznacz opcję <**Automatyczne wykrywanie**>.

Urządzenie musi być dostępne w sieci.

Aby dodać kamerę w konfiguracji offline, wybierz opcję <**Symbol zastępczy jednej kamery**>.

Nazwa użytkownika

Wyświetla nazwę użytkownika używaną w celu uwierzytelniania w urządzeniu.

Hasło

Wprowadź poprawne hasło używane do uwierzytelniania w urządzeniu.

Pokaż hasło

Kliknij, aby włączyć opcję wyświetlania wprowadzonego hasła. Uważaj, aby osoby postronne nie poznały tego hasła.

Uwierzytelnij

Kliknąć, aby uwierzytelnić w urządzeniu z wykorzystaniem wprowadzonych powyżej poświadczeń.

13.8.2**Okno dialogowe Edytuj nadajnik/odbiornik**

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > rozwiń  > kliknij prawym

przyciskiem myszy  > kliknij okno dialogowe **Edytuj nadajnik** > okno dialogowe **Edytuj nadajnik** lub

Okno główne > **Urządzenia** > Rozwiń  > Kliknij prawym przyciskiem myszy  > Kliknij **Edytuj nadajnik** > Okno dialogowe **Edytuj nadajnik** lub

Okno główne > **Urządzenia** > Rozwiń  > Kliknij prawym przyciskiem myszy  > Kliknij **Edytuj nadajnik** > Okno dialogowe **Edytuj nadajnik** lub

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > kliknij prawym przyciskiem myszy  > kliknij **Edytuj odbiornik** > okno dialogowe **Edytuj odbiornik**

Umożliwia sprawdzanie i aktualizowanie możliwości urządzenia. Po otwarciu tego okna nawiązywane jest połączenie z urządzeniem. Po weryfikacji hasła dane dotyczące wydajności urządzenia są porównywane z informacjami zapisanymi w BVMS.

Nazwa

Wyświetla nazwę urządzenia. Podczas dodawania sieciowego urządzenia wizyjnego firmy Bosch wygenerowana zostaje nazwa urządzenia. Jeśli jest to wymagane, należy zmienić wprowadzone dane.

Adres/port sieciowy

Wprowadź adres sieciowy urządzenia. Jeśli jest to wymagane, zmień numer portu.

Nazwa użytkownika

Wyświetla nazwę użytkownika używaną w celu uwierzytelniania w urządzeniu.

Hasło

Wprowadź poprawne hasło używane do uwierzytelniania w urządzeniu.

Pokaż hasło

Kliknij, aby włączyć opcję wyświetlania wprowadzonego hasła. Uważaj, aby osoby postronne nie poznały tego hasła.

Uwierzytelnij

Kliknąć, aby uwierzytelnić w urządzeniu z wykorzystaniem wprowadzonych powyżej poświadczeń.

Bezpieczeństwo

Pole wyboru **Zabezpiecz połączenie** jest domyślnie zaznaczone.

Jeśli połączenie bezpieczne jest niemożliwe, zostanie wyświetlony odpowiedni komunikat. Kliknąć, aby usunąć zaznaczenie.

Następujące odbiorniki obsługują bezpieczne połączenie:

- VJD 7000
- VJD 8000
- VIP XD HD

**Uwaga!**

Połączenie pomiędzy odbiornikiem i nadajnikiem jest bezpieczne, jeśli oba urządzenia zostały skonfigurowane z obsługą bezpiecznego połączenia.

Strumień wizyjny

UDP: umożliwia szyfrowany streaming multicast do obsługiwanych odbiorników.

TCP: umożliwia szyfrowany sstreaming unicast do obsługiwanych odbiorników.

Uwaga: Jeśli w nadajniku nie zostanie skonfigurowany adres multicast, odbiornik będzie przyjmował strumień w formie unicast.

**Uwaga!**

Oprogramowanie BVMS nie obsługuje kamer Bosch podłączonych do bramy VSG.
BVMS obsługuje szyfrowanie protokołem UDP tylko dla platform starszych niż CPP13.

Wydajność urządzenia

Wyświetlone informacje o wydajności urządzenia można sortować według kategorii lub alfabetycznie. Tekst komunikatu informuje, czy wykryte dane o wydajności urządzenia są zgodne z bieżącymi informacjami.

Kliknij przycisk **OK**, aby wprowadzić zmiany dotyczące wydajności urządzenia po jego rozbudowie.

Patrz

- Szyfrowanie obrazu wizyjnego na żywo (Edytuj nadajnik), Strona 221
- Aktualizacja informacji o funkcjach urządzenia (Edytuj nadajnik), Strona 222

13.8.3**Zmiana hasła nadajnika/dekodera (Zmień hasło / Wprowadź hasło)**

Okno główne > **Urządzenia** > rozwinąć  > rozwinąć  >  >  > 

lub

Okno główne > **Urządzenia** >  > 

lub

Okno główne > **Urządzenia** >  > 

lub

Okno główne > **Urządzenia** > Rozwiń  > Rozwiń  > 

Określ i zmień hasła osobno dla każdego z poziomów. Wpisz hasło (maks. 19 znaków bez znaków specjalnych) dla wybranego poziomu.

Aby zmienić hasło:

1. Kliknij prawym przyciskiem myszy , a następnie kliknij polecenie **Zmień hasło....**
Pojawi się okno dialogowe **Wprowadź hasło**.
2. Na liście **Wprowadź nazwę użytkownika** zaznacz żądane go użytkownika, dla którego chcesz zmienić hasło.
3. W polu **Wprowadź hasło dla użytkownika** wpisz nowe hasło.

4. Kliknij **OK**.

⇒ Hasło na urządzeniu zostanie natychmiast zmienione.

Hasło uniemożliwia dostęp do urządzenia osobom nieuprawnionym. Do kontroli dostępu można używać różnych poziomów autoryzacji.

Właściwa ochrona hasłem jest zagwarantowana tylko wówczas, gdy wszystkie wyższe poziomy autoryzacji są także chronione hasłem. Przydzielając hasła, należy zawsze zaczynać od najwyższego poziomu autoryzacji.

Można zdefiniować i zmienić hasło dla każdego z poziomów autoryzacji, jeśli użytkownik jest zalogowany do konta użytkownika „service”.

Urządzenie obsługuje trzy poziomy autoryzacji: service, user i live.

- Poziom service jest najwyższym poziomem autoryzacji. Po wprowadzeniu prawidłowego hasła użytkownik uzyskuje dostęp do wszystkich funkcji i może zmieniać wszystkie ustawienia konfiguracyjne.
- Poziom user jest średnim poziomem autoryzacji. Umożliwia on na przykład obsługę urządzenia, odtwarzanie nagrań oraz sterowanie kamerami, ale nie pozwala zmieniać ustawień konfiguracyjnych.
- Poziom live jest najniższym poziomem autoryzacji. Umożliwia on tylko podgląd obrazu wideo na żywo i przełączanie pomiędzy różnymi obrazami na żywo.

Dla dekodera następujący poziom autoryzacji zastępuje poziom autoryzacji live:

- destination password (dostępne tylko dla dekoderek)
- Używane do dostępu do nadajnika.

Patrz

- Dostarczanie hasła docelowego dla dekodera (Uwierzytelnij...), Strona 211

13.8.4

Profil odbiornika

Umożliwia ustawienie różnych opcji wyświetlania obrazu na monitorze VGA.

Nazwa monitora

Wprowadzić nazwę monitora. Nazwa monitora ułatwia identyfikację zdalnej lokalizacji monitora.

Należy użyć nazwy umożliwiającej łatwą i jednoznaczną identyfikację lokalizacji.

Kliknąć przycisk , aby uaktualnić nazwę w Drzewie urządzeń.

Standard

Wybrać wyjściowy sygnał wizyjny używanego monitora. Dostępne są opcje PAL i NTSC dotyczące monitorów analogowych, a ponadto można wybrać jedno z ośmiu fabrycznie skonfigurowanych ustawień dotyczących monitorów VGA.



Uwaga!

Wybranie opcji VGA, dla której określono parametry wykraczające poza zakres wartości obsługiwanych przez monitor, może doprowadzić do poważnego uszkodzenia monitora. Więcej informacji znajduje się w dokumentacji technicznej monitora.

Układ okna

Należy wybrać domyślny układ monitora.

Rozmiar okna VGA

Wprowadzić format obrazu (np. 4 × 3) lub fizyczny rozmiar ekranu w milimetrach. Na podstawie wprowadzonych tu ustawień urządzenie będzie mogło poprawnie wyskalować obraz, tak aby był on pozbawiony zniekształceń.

13.8.5

Wyświetl. na monitorze

Urządzenie rozpoznaje zakłócenia w transmisji sygnału i wyświetla ostrzeżenie na ekranie monitora.

Zakłócenia w transmisji obrazu

Wybrać opcję **Wł.**, aby urządzenie wyświetlało ostrzeżenie w przypadku wystąpienia zakłóceń w transmisji sygnału.

Czułość zakłóceń

Przesunąć suwak, aby ustawić poziom zakłóceń, którego przekroczenie będzie powodować wyświetlenie ostrzeżenia.

Tekst powiadomienia o zakłóceniach

Wpisać treść ostrzeżenia wyświetlanego na monitorze w przypadku przerwania połączenia. Maksymalna długość tekstu to 31 znaków.

13.8.6

Konfigurowanie klawiatury Bosch IntuiKey (odbiornik)

Okno główne > **Urządzenia** > rozwiń



Uwaga!

Klawiatury KBD-Universal XF nie można podłączyć do odbiornika.

Aby skonfigurować klawiaturę Bosch IntuiKey dołączonej do odbiornika, należy:

1. Kliknąć komórkę w kolumnie **Połączenie**, a następnie wybrać odpowiedni odbiornik. Można wybrać także stację roboczą, jeśli klawiatura Bosch IntuiKey jest podłączona do stacji roboczej.



Stacja robocza musi być skonfigurowana na stronie

2. W polu **Ustawienia połączenia** skonfigurować żądane ustawienia.

Więcej informacji o różnych polach znajduje się w Pomocy ekranowej wybranego okna programu.

Patrz

- Strona Przypisz klawiaturę, Strona 156
- Możliwe sposoby podłączenia klawiatury Bosch IntuiKey, Strona 55
- Podłączanie klawiatury Bosch IntuiKey do odbiornika, Strona 56

13.8.7

Konfigurowanie odbiornika podłączonego do klawiatury Bosch IntuiKey



Okno główne > **Urządzenia** > rozwinąć



> rozwinąć

W celu skonfigurowania odbiornika VIP XD podłączonego do klawiatury Bosch IntuiKey należy wykonać przedstawione poniżej czynności.

Aby skonfigurować odbiornik:

1. Kliknąć odpowiedni odbiornik, do którego ma być podłączona klawiatura Bosch IntuiKey.
2. Kliknąć kartę **Urządzenie peryferyjne**.
3. Upewnić się, że zostały wybrane następujące ustawienia:
 - Funkcja portu szeregowego: **Tryb transparentny**
 - Szyb. transm.: **19 200**
 - Bity stopu: **1**
 - Kontrola parzystości: **Brak**
 - Tryb interfejsu: **RS232**

- Tryb jednokierunkowy: **Wył.**

Patrz

- Możliwe sposoby podłączenia klawiatury Bosch IntuiKey, Strona 55
- Podłączanie klawiatury Bosch IntuiKey do odbiornika, Strona 56
- Aktualizacja oprogramowania układowego klawiatury Bosch IntuiKey, Strona 57

13.8.8

Usuń logo dekodera

Kliknij, aby usunąć logo skonfigurowane na stronie internetowej dekodera.

13.9

Strona Grupy monitorów

Okno główne > **Urządzenia** > Rozwiń



Pozwala dodać i skonfigurować grupy monitorów. Grupę monitorów przypisuje się do stacji roboczej

systemu BVMS w



Uwaga!

Nie można sterować grupą monitorów z poziomu programu Operator Client, gdy zostanie utracone połączenie z serwerem Central Server.

Patrz

- Ręczne dodawanie grupy monitorów, Strona 146
- Konfigurowanie grupy monitorów, Strona 146
- Konfigurowanie predefiniowanych położeń i funkcji dodatkowych, Strona 300
- Konfigurowanie alarmu, Strona 322
- Okno dialogowe Opcje alarmu, Strona 313
- Okno wyboru Wybierz zawartość okienka obrazu (MG), Strona 313

13.9.1

Ręczne dodawanie grupy monitorów

Okno główne > **Urządzenia** > Rozwiń



> Kliknij prawym przyciskiem myszy



> Kliknij

Dodaj grupę monitorów

1. Kliknąć **Dodaj grupę monitorów**.
Zostanie wyświetlone okno dialogowe **Dodaj grupę monitorów**. Wprowadzić nazwę nowej grupy monitorów.
2. Kliknąć OK.
Dana grupa monitorów zostanie dodana do systemu użytkownika.
3. Kliknij **Mapy i struktura**.
4. Przeciągnąć grupę monitorów do okna Drzewo logiczne.

13.9.2

Konfigurowanie grupy monitorów

Okno główne > **Urządzenia** > rozwinąć



>



**Uwaga!**

Nie można sterować grupą monitorów z poziomu programu Operator Client, gdy zostanie utracone połączenie z serwerem Central Server.

Można skonfigurować monitory w grupie monitorów w sposób logiczny, w rzędach i kolumnach. To rozmieszczenie nie musi odpowiadać fizycznemu układowi monitorów.

Aby skonfigurować grupę monitorów:

1. Przeciągnąć odpowiednie monitory z karty **Nieprzypisane monitory** do pola grup monitorów.
2. W karcie **Układ** wybrać odpowiedni układ.
3. Przeciągnąć dowolną dostępną kamerę z karty **Kamery** do okienka monitorów po lewej stronie. Numer logiczny kamery zostanie wyświetlony w postaci czarnej liczby na okienku monitora i zmieni się kolor tego okienka.
4. Zmienić odpowiednio numery logiczne okienek obrazu. Jeśli zostanie wprowadzony już używany numer, pojawi się komunikat.
5. W karcie **Opcje** można określić, czy nazwa i numer kamery mają być widoczne w okienku monitorów. Można także wybrać pozycję tych informacji.

Uwaga: W przypadku VIDEOJET decoder 7513, VIDEOJET decoder 7523 i VIDEOJET decoder 8000 te opcje są dostępne tylko po skonfigurowaniu odpowiednich ustawień dekodera.

Patrz

- Konfiguracja dekoderek do wyświetlania OSD, Strona 233

**Uwaga!**

Można określić, czy skonfigurowane ustawienia grupy monitorów powinny zostać przywrócone po ponownym uruchomieniu Central Server lub czy ostatnie ustawienia grupy monitorów wprowadzone w Operator Client powinny zostać zachowane.

Patrz Okno dialogowe *Opcje* (menu *Ustawienia*), Strona 120

Obraz na monitorze

Pogrubiona liczba w kolorze czarnym, jeśli jest wyświetlona, określa numer logiczny kamery inicjującej. Natomiast niewielka liczba w kolorze czarnym przedstawia numer logiczny monitora. Aby usunąć przypisanie kamery, kliknąć prawym przyciskiem myszy w okienku monitorów, a następnie kliknąć przycisk **Wyczyść okienko** lub przeciągnąć kamerę poza okienko obrazu.

Patrz

- Ręczne dodawanie grupy monitorów, Strona 146

13.10

strona Urządzenia komunikacyjne

Okno główne > **Urządzenia** > rozwiń  > 

Umożliwia dodanie lub skonfigurowanie urządzenia komunikacyjnego.

Można skonfigurować następujące urządzenie komunikacyjne:

- Adres e-mail

Patrz

- Konfiguracja urządzenia komunikacyjnego, Strona 149

13.10.1

Dodawanie serwera poczty elektronicznej/SMTP

Aby dodać urządzenie komunikacyjne:

1. Rozwinąć  , prawym przyciskiem myszy kliknąć  , a następnie kliknąć **Dodaj urządzenie e-mail / SMTP**.

Zostanie wyświetlone okno dialogowe **Dodaj urządzenie e-mail / SMTP**.

2. Wprowadzić odpowiednie ustawienia.
3. Kliknąć **OK**.

Urządzenie komunikacyjne zostanie dodane do systemu użytkownika.

Okno dialogowe Dodaj urządzenie e-mail / SMTP

Nazwa:

Wprowadzić nazwę serwera poczty elektronicznej.

13.10.2

strona Serwer SMTP

Okno główne > **Urządzenia** > rozwin  > rozwin  > 

Umożliwia skonfigurowanie ustawień poczty elektronicznej systemu. Na stronie **Zdarzenia** można przypisać zdarzenie do poczty elektronicznej. Kiedy wybrane zdarzenie wystąpi, system wysła wiadomość e-mail. Wiadomości e-mail nie można otrzymywać w systemie BVMS.

Nazwa serwera SMTP

Wprowadź nazwę serwera poczty elektronicznej. Niezbędne informacje można uzyskać u dostawcy usługi. Zwykle jest to adres IP lub nazwa DNS serwera poczty elektronicznej użytkownika.

Adres nadawcy

Należy tu wpisać adres e-mail, który posłuży jako adres nadawcy przy wysłaniu przez system wiadomości e-mail, np. w przypadku wystąpienia alarmu.

SSL/TLS

To pole wyboru należy zaznaczyć, aby włączyć użycie bezpiecznego połączenia SSL/TLS. W takim przypadku port sieciowy zmienia się automatycznie na 587.

Port

Należy tu wpisać numer portu sieciowego dla poczty wychodzącej. Niezbędne informacje na ten temat można uzyskać od usługodawcy.

Po wyłączeniu ustawienia **SSL/TLS** automatycznie wybierany jest port 25.

W razie potrzeby można wybrać inny port.

Limit czasu połączenia [s]

Wprowadź liczbę sekund nieaktywności, po której połączenie jest zrywane.

Uwierzytelnianie

Zaznacz pole wyboru żądanej metody uwierzytelniania. Niezbędne informacje można uzyskać u dostawcy usługi.

Nazwa użytkownika

Wprowadź nazwę użytkownika do uwierzytelniania na serwerze poczty elektronicznej. Niezbędne informacje można uzyskać u dostawcy usługi.

Hasło:

Wprowadź hasło do uwierzytelniania na serwerze poczty elektronicznej. Niezbędne informacje można uzyskać u dostawcy usługi.

Wyślij testową wiadomość e-mail

Kliknij, aby wyświetlić okno dialogowe **Wyślij testową wiadomość e-mail**.

Patrz

- Konfiguracja urządzenia komunikacyjnego, Strona 149

13.10.3**Konfiguracja urządzenia komunikacyjnego**

Okno główne > **Urządzenia** > rozwinąć  > rozwinąć 

Aby skonfigurować urządzenie komunikacyjne:

1. Kliknąć .
2. Wprowadzić odpowiednie ustawienia.

Więcej informacji o różnych polach znajduje się w Pomocy ekranowej wybranego okna programu.

Patrz

- Dodawanie serwera poczty elektronicznej/SMTP, Strona 148
- strona Serwer SMTP, Strona 148

13.10.4**Okno dialogowe Wyślij testową wiadomość e-mail**

Okno główne > **Urządzenia** > rozwiń  > rozwiń  >  > przycisk **Wyślij testową wiadomość e-mail**

Umożliwia wysłanie testowej wiadomości e-mail.

Od:

Wprowadź adres e-mail nadawcy.

Do

Wprowadź adres e-mail odbiorcy.

Temat

Wprowadź temat wiadomości e-mail.

Komunikat

Wprowadź tekst wiadomości.

Wyślij testową wiadomość e-mail

Kliknij, aby wysłać testową wiadomość e-mail.

Patrz

- Konfiguracja urządzenia komunikacyjnego, Strona 149

13.11**Strona ATM/POS-Bridge**

Okno główne > **Urządzenia** > rozwiń opcję  > 

Umożliwia dodawanie i konfigurowanie urządzeń peryferyjnych, np. ATM/POS Bridge Bosch.

Jeśli do jednego serwera ma być przypisanych kilka interfejsów, należy użyć różnych portów.

Patrz

- Dodawanie interfejsu do ATM/POS-Bridge firmy Bosch, Strona 97
- Konfiguracja urządzenia peryferyjnego, Strona 151

13.11.1

Ręczne dodawanie interfejsu do ATM/POS-Bridge firmy Bosch

Okno główne > **Urządzenia** > rozwiń opcję  > kliknij prawym przyciskiem myszy  > **Dodaj interfejs do ATM/POS-Bridge firmy Bosch**.

Umożliwia dodanie urządzenia ATM firmy Bosch.

Aby dodać urządzenie peryferyjne:

1. Rozwinąć , prawym przyciskiem myszy kliknąć , a następnie kliknąć polecenie **Dodaj interfejs do ATM/POS-Bridge firmy Bosch**.

Zostanie wyświetlone okno dialogowe **Dodaj interfejs do ATM/POS-Bridge firmy Bosch**.

2. Wprowadzić odpowiednie ustawienia.
3. Kliknąć **OK**.

Urządzenie peryferyjne zostanie dodane do systemu użytkownika.

Okno dialogowe Dodaj interfejs do ATM/POS-Bridge firmy Bosch

Nazwa:

Wprowadzić nazwę urządzenia.

Adres IP:

Wprowadź adres IP urządzenia.

Port 1

Należy tu wpisać odpowiedni numer portu pełniącego funkcję portu nasłuchowego dla urządzenia ATM/POS Bridge.

Port 2

Należy tu wpisać odpowiedni numer portu pełniącego funkcję portu nasłuchowego dla urządzenia BVMSManagement Server.

**Uwaga!**

Po dodaniu do systemu wielu urządzeń ATM/POS Bridges należy upewnić się, że numer portu 2 jest w każdym z nich inny. Wielokrotne używanie tego samego numeru dla portu 2 może doprowadzić do utraty danych przez ATM/POS.

Patrz

– Dodawanie interfejsu do ATM/POS-Bridge firmy Bosch, Strona 97

13.11.2

strona Interfejs do ATM/POS Bridge firmy Bosch

Okno główne > **Urządzenia** > rozwiń opcję  > rozwiń opcję  >  > karta **Interfejs do ATM/POS-Bridge firmy Bosch**

Umożliwia skonfigurowanie urządzenia ATM/POS Bridge firmy Bosch.

Adres IP:

Należy tu wpisać adres IP urządzenia.

Port 1

Należy tu wpisać odpowiedni numer portu pełniącego funkcję portu nasłuchowego dla urządzenia ATM/POS Bridge.

Port 2

Należy tu wpisać odpowiedni numer portu pełniącego funkcję portu nasłuchowego dla urządzenia BVMSManagement Server.

**Uwaga!**

Po dodaniu do systemu wielu urządzeń ATM/POS Bridges należy upewnić się, że numer portu 2 jest w każdym z nich inny. Wielokrotne używanie tego samego numeru dla portu 2 może doprowadzić do utraty danych przez ATM/POS.

Patrz

- Konfiguracja urządzenia peryferyjnego, Strona 151
- Dodawanie interfejsu do ATM/POS-Bridge firmy Bosch, Strona 97

13.11.3**Konfiguracja urządzenia peryferyjnego**

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > **Interfejs do ATM/POS-Bridge firmy Bosch**

lub

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > **Urządzenie DTP** > 

Aby skonfigurować urządzenie peryferyjne:

- ▶ Zmień wymagane ustawienia.

Kliknąć poniższy odnośnik do wybranego okna programu, aby uzyskać szczegółowe informacje o różnych polach.

Patrz

- Strona ustawień ATM, Strona 151
- strona Interfejs do ATM/POS Bridge firmy Bosch, Strona 150
- Strona ustawień urządzenia DTP, Strona 151

13.11.4**Strona ustawień urządzenia DTP**

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > 

Umożliwia skonfigurowanie urządzenia DTP z maksymalnie 4 podłączonymi do niego ATM.

Port szeregowy

Zaznacz odpowiedni port na liście.

Patrz

- Strona ustawień ATM, Strona 151
- Konfiguracja urządzenia peryferyjnego, Strona 151

13.11.5**Strona ustawień ATM**

Okno główne > **Urządzenia** > rozwinąć  > rozwinąć  >  > 

Umożliwia skonfigurowanie urządzenia ATM, które jest podłączone do DTP.

Numer wejściowy urządzenia DTP

Wybierz żądany numer wejścia. Jeśli dany numer jest już używany przez inne urządzenie ATM, można zamienić miejscami numery wejściowe.

Limit czasu połączenia [w godzinach]

Wprowadź żadaną liczbę godzin. Gdy w tym okresie urządzenie ATM nie wysłało żadnych danych transakcyjnych, BVMS przyjmuje, że połączenie jest rozłączone. Zostanie wywołane odpowiednie zdarzenie. Jest dostępne zdarzenie **Nieuwierzytelnione** dla urządzenia ATM, ale nie jest istotne.

Wpisanie **0** oznacza, że sprawdzanie połączenia nie będzie wykonywane.

Wejścia danych

Kliknij, aby włączyć żądane wejścia i wprowadzić odpowiednią nazwę dla tych wejść.

Patrz

- Konfiguracja urządzenia peryferyjnego, Strona 151

13.11.6

strona Wejścia

Okno główne > **Urządzenia** > rozwinąć  > rozwinąć  > karta **Wejścia**
Umożliwia skonfigurowanie wejść urządzenia ATM/POS Bridge firmy Bosch.

Patrz

- Konfiguracja urządzenia peryferyjnego, Strona 151
- Dodawanie interfejsu do ATM/POS-Bridge firmy Bosch, Strona 97

13.12

Czytniki kart

Okno główne > **Urządzenia** > rozwinąć  >  > karta **Ustawienia globalne czytników kart**
Można skonfigurować ustawienia, które będą poprawne dla wszystkich czytników kart w systemie.

Port szeregowy

Wybierz port szeregowy, do którego jest podłączony czytnik kart.

Odblokowane

Umożliwia wprowadzenie kodu banku w celu zablokowania. To znaczy, że wprowadzone tu karty spełniające parametry blokady nie uzyskują autoryzacji. Czytnik kart odmawia dostępu. Dla domyślnego trybu zwalniania elektrycznej blokady drzwi czytnika kart musi być wybrane ustawienie **Auto**.

Lista może zawierać wpisy z symbolami wieloznacznymi:

?: oznacza dowolny znak lub brak znaku na tej pozycji.

*: oznacza ciąg (jednego lub więcej) dowolnych znaków lub brak znaków (wyjątek: symbol * jako jedyny oznacza, że wszystkie kody banków są zablokowane).

Ignoruj kod kraju na kartach EC

Kliknij, aby włączyć opcję powodującą, że system BVMS nie analizuje danych karty używanych do identyfikacji kraju jej wystawienia. Dostęp będzie możliwy dla kart z różnymi kodami krajów.

13.12.1

Okno dialogowe Dodaj czytnik kart

Okno główne > **Urządzenia** > rozwinąć  > kliknij prawym przyciskiem myszy  > polecenie

Dodaj czytnik kart

Można teraz dodać czytnik kart.

Nazwa

Wprowadź nazwę urządzenia.

Identyfikator urządzenia

Wybierz unikatowy numer urządzenia. Jeśli nie ma dostępnych numerów, oznacza to, że do systemu dodano już maksymalną liczbę czytników kart.

13.12.2

Strona ustawień czytnika kart

Okno główne > **Urządzenia** > rozwiń  >  >  > karta **Ustawienia czytnika kart**
Można teraz skonfigurować czytnik kart.

Identyfikator urządzenia

Wyświetla unikatowy numer urządzenia.

Włącz ochronę przed skimmingiem

Kliknij, aby włączyć opcję powodującą, że system BVMS wyzwala zdarzenie, gdy do czytnika kart zostanie zamocowany jako nakładka fałszywy czytnik (skimming). Nie wszystkie czytniki kart obsługują tę funkcję.

Domyślny tryb zwalniania blokady drzwi elektrycznych

Otwórz: Drzwi są otwarte i wszyscy mają dostęp bez karty.

Zamkn.: Drzwi pozostają zamknięte, niezależnie od tego, jaka karta została włożona.

Auto: Drzwi otwierają się tylko po włożeniu do czytnika karty z autoryzowanym dostępem.

Włącz sterowanie na podstawie harmonogramu

Kliknij, aby umożliwić przypisanie harmonogramu terminów wyboru trybów zwalniania blokady drzwi. Po uaktywnieniu harmonogramu system BVMS przełącza czytnik kart do odpowiedniego trybu zwalniania.

Jeśli wybrane terminy się pokrywają, wynikowy tryb zwalniania drzwi jest określany na podstawie priorytetu trybów: 1. **Otwórz** 2. **Zamkn.** 3. **Auto**

13.13

strona Wirtualne wejścia

Okno główne > **Urządzenia** > rozwinąć  > 
Wyświetla wirtualne wejścia skonfigurowane w systemie.
Umożliwia dodawanie nowych wirtualnych wejść i usuwanie istniejących.

Dodaj wejścia

Kliknij, aby wyświetlić okno dialogowe dodawania nowych wirtualnych wejść.

Usuń wejścia

Kliknij, aby usunąć zaznaczone wirtualne wejścia.

Numer

Wyświetla numer wirtualnego wejścia.

Nazwa

Kliknij komórkę, aby zmodyfikować nazwę wirtualnego wejścia.

13.13.1

Ręczne dodawanie wirtualnych wejść

Okno główne > **Urządzenia** > Rozwiń  > Przycisk **Dodaj wejścia**
Umożliwia dodanie nowych wirtualnych wejść.

Aby dodać wirtualne wejście:

1. Rozwiń , a następnie kliknij .
Zostanie wyświetlona odpowiednia strona.
2. Kliknij **Dodaj wejścia**.
Do tabeli zostanie dodany nowy wiersz.
3. Wprowadź odpowiednie ustawienia.

4. Kliknij **Dodaj**.

Wejście wirtualne zostanie dodane do systemu użytkownika.

Okno dialogowe Dodaj wejścia**Uruchom:**

Zaznaczyć pierwszy numer nowych wirtualnych wejść.

Zakończ:

Zaznaczyć ostatni numer nowych wirtualnych wejść.

Nazwa:

Wprowadzić nazwę wszystkich nowych wirtualnych wejść. Kolejny numer jest dołączany.

Dodaj

Kliknij, aby dodać nowe wirtualne wejścia.

13.14

strona SNMP

Okno główne > **Urządzenia** > Rozwiń



Umożliwia dodanie lub skonfigurowanie pomiaru SNMP służącego do kontroli jakości połączeń sieciowych.

Patrz

- Konfigurowanie odbiornika komunikatów trap SNMP (strona odbiornika komunikatów trap SNMP), Strona 154

13.14.1

Ręczne dodawanie SNMP

Okno główne > **Urządzenia** > Rozwiń



>



>

Dodaj SNMP

Umożliwia dodanie do systemu BVMS rozwiązania z zakresu monitoringu sieci.

Aby dodać urządzenie do monitoringu sieci:

1. Rozwiń , prawym przyciskiem myszy kliknij , a następnie kliknij polecenie **Dodaj SNMP**.

Zostanie wyświetlone okno dialogowe **Dodaj SNMP**.

2. Wprowadź nazwę urządzenia SNMP.

Urządzenie do monitoringu sieci zostanie dodane do systemu.

Okno dialogowe Dodaj SNMP**Nazwa:**

Wpisać nazwę urządzenia monitorowania sieci.

Patrz

- Konfigurowanie odbiornika komunikatów trap SNMP (strona odbiornika komunikatów trap SNMP), Strona 154

13.14.2

Konfigurowanie odbiornika komunikatów trap SNMP (strona odbiornika komunikatów trap SNMP)

Okno główne > **Urządzenia** > rozwiń



Aby skonfigurować SNMP trap receiver, należy:

1. Kliknąć , aby wyświetlić stronę **Odbiornik komunikatów Trap SNMP**.
2. Wprowadzić żądane zmiany.

Więcej informacji o różnych polach znajduje się w Pomocy ekranowej wybranego okna programu.

Strona Odbiornik komunikatów Trap SNMP.

Okno główne > **Urządzenia** > rozwinąć  > rozwinąć 

Umożliwia wybranie urządzeń, które mają być monitorowane, oraz identyfikatorów OID komunikatów trap SNMP inicjujących zdarzenie w określonym urządzeniu, do którego są przesyłane.



Uwaga!

Wymagane jest wpisanie adresu IP komputera typu Management Server wchodzącego w skład systemu Bosch Video Management System, który ma otrzymywać komunikaty typu trap dotyczące monitorowanych urządzeń.

Urządzenia wysyłające komunikaty Trap SNMP

Umożliwia określenie zakresu adresów IP dla monitorowanych urządzeń sieciowych. Jeśli monitorowane ma być tylko jedno urządzenie, należy wprowadzić odpowiadający mu adres IP w komórce **Zakres od**.

Adresy należy zmieniać ostrożnie. Wprowadzenie nieprawidłowego adresu spowoduje zatrzymanie sieciowego monitoringu danego urządzenia.

Reguły filtrowania komunikatów Trap SNMP

Umożliwia wprowadzenie identyfikatorów OID i powiązanych z nimi wartości. Aby rozszerzyć zakres filtrowania, można użyć symboli wieloznacznych * i ?. W przypadku wprowadzenia identyfikatorów OID i wartości w więcej niż jednym wierszu reguły dotyczące filtrowania muszą być ze sobą zgodne, aby możliwe było wyzwolenie zdarzenia. W obu kolumnach można wprowadzić wyrażenie regularne, używając nawiasów klamrowych „{” i „}”. Jeśli jakiegokolwiek znaki zostaną wpisane poza tymi nawiasami, wyrażenie zostanie uznane za niepoprawne.

Pokaż narzędzie do rejestrowania komunikatów Trap

Kliknij, aby wyświetlić okno dialogowe **Narzędzie do rejestrowania komunikatów Trap SNMP** służące do śledzenia identyfikatorów OID komunikatów trap SNMP.

13.14.3

Okno dialogowe Narzędzie do rejestrowania komunikatów Trap SNMP

Okno główne > **Urządzenia** > rozwinąć  > rozwinąć  > wybierz odbiornik ogólnych komunikatów trap SNMP > kliknij **Pokaż narzędzie do rejestrowania komunikatów Trap**

Umożliwia śledzenie identyfikatorów OID komunikatów trap SNMP. Można otrzymywać komunikaty trap ze wszystkich urządzeń w sieci lub tylko z wybranych. Komunikaty trap można filtrować; można także dodać identyfikatory OID i odpowiednie wartości dotyczące komunikatów do tabeli **Reguły filtrowania komunikatów Trap SNMP**.

Uruchom/Pauza

Kliknij, aby rozpocząć lub przerwać śledzenie.

Tylko komunikaty Trap od nadawcy

Wprowadź adres IP lub nazwę DNS urządzenia. Śledzone będą jedynie komunikaty trap dotyczące tego urządzenia.

Tylko komunikaty Trap zawierające

Wprowadź ciąg, który powinien znajdować się w komunikacie trap. Dopuszczalne jest użycie symboli wieloznacznych * i ?. Ciągi ujęte w nawiasy klamrowe „{” i „}” są traktowane jak wyrażenia regularne. Śledzone będą tylko komunikaty trap zawierające taki ciąg.

Otrzymane komunikaty Trap

Wyświetla komunikaty trap odbierane w procesie śledzenia.



Kliknij, aby usunąć wszystkie wpisy w polu **Otrzymane komunikaty Trap**.

Szczegóły komunikatu Trap

Wyświetla szczegółowe informacje o komunikacie trap. Identyfikator OID i wartość można skopiować do tabeli **Reguły filtrowania komunikatów Trap SNMP**.

Patrz

- Konfigurowanie odbiornika komunikatów trap SNMP (strona odbiornika komunikatów trap SNMP), Strona 154

13.15

Strona Przypisz klawiaturę

Okno główne > **Urządzenia** > rozwinąć  > 

Umożliwia dodanie klawiatury KBD-Universal XF (podłączonej do stacji roboczej BVMS) lub klawiatury Bosch IntuiKey (podłączonej do stacji roboczej BVMS lub do odbiornika).

Aby dodać klawiaturę CCTV:

Uwaga: Aby dodać klawiaturę, należy w pierwszej kolejności dodać stację roboczą.

1. Rozwiń , a następnie kliknij pozycję  .
Pojawi się odpowiednia strona.
2. Kliknij **Dodaj klawiaturę**.
Do tabeli zostanie dodany nowy wiersz.
3. W odpowiednim polu kolumny **Typ klawiatury** wybierz właściwy typ klawiatury:
Klawiatura IntuiKey
Klawiatura KBD-Universal XF.
4. W odpowiednim polu kolumny **Połączenie** wybierz stację roboczą, do której jest podłączona klawiatura.
5. Wprowadź odpowiednie ustawienia.
Klawiatura zostanie dodana do systemu.

Dodaj klawiaturę

Kliknij, aby dodać wiersz w tabeli do skonfigurowania klawiatury.

Usuń klawiaturę

Kliknij, aby usunąć zaznaczony wiersz.

Typ klawiatury

Podaje typ klawiatury dołączonej do stacji roboczej lub dekodera.

Kliknij komórkę w celu wybrania odpowiedniego typu klawiatury.

- **IntuiKey**
Ten typ należy wybrać, jeśli podłączona jest klawiatura IntuiKey firmy Bosch.
- **Klawiatura KBD-Universal XF**
Ten typ należy wybrać, jeśli podłączona jest klawiatura KBD-Universal XF.

Połączenie

W komórce wybrać urządzenie, do którego podłączona jest klawiatura. W przypadku wybrania stacji roboczej klawiatura zostanie dodana także w lokalizacji  -> strona .

Port

W komórce zaznacz żądany port COM.

Szybkość transmisji

Wybierz maksymalną prędkość w bitach na sekundę (b/s), z którą mają być przesyłane dane przez port. Zwykle jest to maksymalna prędkość obsługiwana przez komputer lub urządzenie, z którym jest nawiązywana komunikacja.

Bity danych

Wyświetla liczbę bitów danych dla każdego znaku, który jest odbierany i transmitowany.

Bity stopu

Wyświetla czas pomiędzy każdym transmitowanym ciągiem znaków (czas jest podawany w bitach).

Parzystość

Wyświetla rodzaj sprawdzania błędów używany dla wybranego portu.

Typ portu

Wyświetla typ połączenia używanego do połączenia klawiatury Bosch IntuiKey ze stacją roboczą.

Patrz

- Konfigurowanie odbiornika podłączonego do klawiatury Bosch IntuiKey, Strona 145
- Konfigurowanie klawiatury Bosch IntuiKey (strona Ustawienia) (stacja robocza), Strona 137
- Konfigurowanie klawiatury Bosch IntuiKey (odbiornik), Strona 145

13.16

strona Moduły wejścia / wyjścia

Okno główne > **Urządzenia** > Rozwiń  > 

Umożliwia dodanie lub skonfigurowanie modułu wejścia-wyjścia.

Obecnie obsługiwane są tylko urządzenia ADAM.

Patrz

- Konfiguracja modułu wejścia / wyjścia, Strona 158

13.16.1

Ręczne dodawanie modułu wejścia-wyjścia

Aby dodać moduł wejść / wyjść:

1. Rozwiń węzeł , kliknąć prawym przyciskiem myszy , a następnie kliknąć **Dodaj nowe urządzenie ADAM**.
Zostanie wyświetlone okno dialogowe **Dodaj urządzenie ADAM**.
2. Wpisać adres IP urządzenia.
3. Wybierz typ urządzenia.
Zostanie wyświetlona odpowiednia strona.
4. Kliknąć kartę **ADAM**, aby zmienić wyświetlane nazwy wejść, jeśli jest to wymagane.
5. Kliknąć kartę **Nazwa**, aby zmienić wyświetlane nazwy przekaźników, jeśli jest to wymagane.

**Uwaga!**

Można także wykonać skanowanie w poszukiwaniu urządzeń ADAM (**Skanuj w poszukiwaniu urządzeń ADAM**). Adresy IP urządzeń zostaną wykryte. Typ urządzenia zostanie zaznaczony, jeśli jest dostępny. Użytkownik musi potwierdzić wybór.

13.16.2**Konfiguracja modułu wejścia / wyjścia**

Okno główne > **Urządzenia** > rozwinąć



> rozwinąć



>



Aby skonfigurować moduł wejścia/wyjścia:

**Uwaga!**

Należy unikać zmieniania typu urządzenia.

Po zmniejszeniu liczby wejść lub przekaźników wszystkie dane konfiguracyjne usuniętych wejść lub przekaźników są kasowane.

1. Kliknąć kartę **ADAM**.
2. Z listy **Typ Adam:** wybrać odpowiedni typ urządzenia.
3. Kliknąć kartę **Wejścia**.
4. W kolumnie **Nazwa** zmienić nazwę wejścia, jeśli jest to wymagane.
5. Kliknąć kartę **Przekaźniki**.
6. W kolumnie **Przekaźniki** zmienić nazwę przekaźnika, jeśli jest to wymagane.

Aby zmienić adres IP, należy:

1. Na drzewie urządzeń kliknąć prawym przyciskiem myszy urządzenie ADAM.
 2. Wybrać pozycję **Zmień adres sieciowy**.
 3. Wprowadzić nowy adres IP i kliknąć przycisk **OK**.
 4. Uaktywnić konfigurację.
- ⇒ Nowy adres IP służy do uzyskiwania dostępu do urządzenia.

Patrz

– strona Moduły wejścia / wyjścia, Strona 157

13.16.3**strona ADAM**

Okno główne > **Urządzenia** > rozwinąć



>



>



>

karta **ADAM**

Wyświetla informacje o wybranym urządzeniu ADAM.

Umożliwia zmianę wyświetlanej nazwy urządzenia ADAM.

Typ Adam:

Wybrać odpowiedni typ urządzenia.

Łączna liczba wejść:

Wyświetla całkowitą liczbę wejść dostępnych dla tego typu urządzenia.

Łączna liczba przekaźników/wyjść:

Wyświetla całkowitą liczbę przekaźników/wyjść dostępnych dla tego typu urządzenia.

13.16.4**strona Wejścia**

Okno główne > **Urządzenia** > rozwinąć



>



>



>

karta **Wejścia**

Umożliwia zmianę nazw wejść wybranego urządzenia ADAM.

Numer

Wyświetla logiczny numer wejścia.

Nazwa

Kliknij komórkę, aby zmienić nazwę wejścia.

13.16.5**strona Przekazniki**

Okno główne > **Urządzenia** > rozwinąć  >  >  > karta **Przekazniki**
Umożliwia zmianę nazw przekazników wybranego urządzenia ADAM.

Numer

Kliknij komórkę, aby zmienić numer logiczny przekaznika.

Nazwa

Wprowadź nazwę przekaznika.

13.17**Strona Emulacja komend CCL krosownicy Allegiant**

Okno główne > **Urządzenia** > rozwiń  > 
Umożliwia uaktywnienie usługi emulacji poleceń CCL urządzenia Allegiant.
Polecenia CCL systemu Allegiant obsługiwane w systemie BVMS, Strona 63 – zawiera listę poleceń CCL obsługiwanych w systemie Bosch Video Management System.

Uwaga:

Emulacji komend CCL krosownicy Allegiant oraz urządzenia Allegiant nie należy konfigurować na tym samym porcie COM. W przypadku ustawienia tego samego portu COM będzie z niego korzystać urządzenie Allegiant. Urządzenie emulujące polecenia CCL urządzenia Allegiant nie uzyska dostępu i pojawi się odpowiedni komunikat.

Aby uniknąć tego problemu, Management Serwer musi mieć dwa różne porty COM lub urządzenie Allegiant musi zostać podłączone do innego komputera.

Enable Allegiant CCL Emulation

Zaznacz to pole wyboru, aby włączyć emulację.

Prędkość transmisji

Określ żądaną prędkość transmisji w b/s.

Bity stopu

Określ liczbę bitów stopu przypadających na każdy znak.

Kontrola parzystości

Wybierz rodzaj kontroli parzystości.

Uzgadnianie

Wybierz żądaną metodę sterowania przepływem.

Model

Wybierz model urządzenia Allegiant, które ma być emulowane.

Patrz

– Konfigurowanie usługi emulacji poleceń CCL urządzenia Allegiant, Strona 160

13.17.1 Ręczne dodawanie emulacji poleceń CCL krosownicy Allegiant

Aby uaktywnić usługę emulacji poleceń CCL urządzenia Allegiant:

1. Rozwiń , a następnie kliknij .
Zostanie wyświetlona karta **Emulacja komend CCL krosownicy Allegiant**.
2. Kliknij, aby zaznaczyć opcję **Włącz emulację poleceń CCL krosownicy Allegiant**.
3. Wprowadź żądane zmiany.
Na komputerze typu Management Server zostanie uruchomiona emulacja poleceń CCL urządzenia Allegiant.

13.17.2 Polecenia CCL krosownicy Allegiant

Do przełączania kamer IP lub nadajników na dekodery IP (wszystkie skonfigurowane w systemie BVMS) używa się poleceń CCL. Poleceń CCL nie można używać do bezpośredniego sterowania kamerami analogowymi ani krosownicą Allegiant.

Emulowanie poleceń CCL dla krosownicy Allegiant uruchamia wewnętrzną usługę systemu BVMS, która przekształca polecenia CCL krosownicy wizyjnej do postaci zrozumiałej dla systemu BVMS. Aby nasłuchiwanie poleceń CCL było możliwe, należy odpowiednio skonfigurować port COM komputera typu Management Server. Usługa emulacji poleceń CCL pomaga zastępować istniejące urządzenia Allegiant modułami wchodzącymi w skład systemu Bosch Video Management System i umożliwia współpracę systemu Bosch Video Management System z aplikacjami obsługującymi polecenia CCL używane przez urządzenia Allegiant. Za pomocą tych poleceń nie da się sterować starymi krosownicami Allegiant skonfigurowanymi w systemie BVMS.

13.17.3 Konfigurowanie usługi emulacji poleceń CCL urządzenia Allegiant

Okno główne > **Urządzenia** > Rozwiń  > 

W celu korzystania z poleceń CCL należy zapoznać się z instrukcją użytkownika poleceń CCL. Jest ona dostępna w Internetowym katalogu produktów, w sekcji dokumentacji poszczególnych krosownic LTC Allegiant.

W sekcji **Polecenia CCL systemu Allegiant obsługiwane w systemie BVMS**, Strona 63 wymieniono polecenia CCL obsługiwane przez system Bosch Video Management System.

Aby skonfigurować usługę emulacji poleceń CCL urządzenia Allegiant:

1. Kliknij polecenie **Enable Allegiant CCL Emulation**.
2. Skonfiguruj odpowiednio ustawienia komunikacji.

Więcej informacji o różnych polach znajduje się w Pomocy ekranowej wybranego okna programu.

Patrz

– Strona *Emulacja komend CCL krosownicy Allegiant*, Strona 159

13.18 Strona Centrale alarmowe

Okno główne > **Urządzenia** > rozwiń  > 

Umożliwia dodawanie i konfigurowanie central alarmowych firmy Bosch. Urządzenie musi być połączone i dostępne.

Po dodaniu centrali alarmowej obszary, punkty, drzwi i przekaźniki są wyświetlane w sposób hierarchiczny w drzewie urządzeń.

Można przenosić centrale, obszary, punkty, drzwi i przekaźniki oraz zmieniać ich nazwy.

Po zmianie konfiguracji centrali alarmowej należy ponownie przeskanować to urządzenie, aby wprowadzone modyfikacje zostały uwzględnione w systemie BVMS.

**Uwaga!**

Wszystkie zdarzenia alarmowe, które mogą wystąpić w danym punkcie, są skonfigurowane automatycznie jako alarmy systemu BVMS.

Przykład: alarm pożarowy

**Uwaga!**

Jeśli dane drzwi nie są przypisane do punktu w konfiguracji centrali alarmowej dodanej do systemu BVMS, alarm sygnalizowany przez te drzwi nie wywoła zdarzenia systemu BVMS, więc w konsekwencji nie wywoła też alarmu systemu BVMS.

13.18.1

Ręczne dodawanie centrali alarmowej

Okno główne > **Urządzenia** > rozwinąć  > kliknąć prawym przyciskiem myszy  > polecenie **Dodaj centralę**

Umożliwia dodanie centrali alarmowej firmy Bosch.

Aby dodać centralę alarmową:

1. Rozwinąć , prawym przyciskiem myszy kliknij , a następnie kliknij polecenie **Dodaj centralę**.
Zostanie wyświetlone okno dialogowe **Dodaj centralę alarmową**.
2. Wpisz odpowiednie wartości.
3. Kliknij **OK**.
Centrala alarmowa zostanie dodana do systemu.

Okno dialogowe Dodaj centralę alarmową

Adres sieciowy

Wpisz adres IP urządzenia.

Port sieciowy

Wybierz numer portu ustawiony w urządzeniu.

Hasło automatyzacji

Wpisz hasło, które umożliwia zalogowanie się do urządzenia.

13.18.2

Strona Ustawienia

Okno główne > **Urządzenia** > rozwinąć  > rozwinąć  >  > karta **Ustawienia**
Umożliwia zmianę ustawień połączenia centrali alarmowej.

13.19

Strona systemów kontroli dostępu

Okno główne > **Urządzenia** > Rozwinąć  > 

Umożliwia dodawanie i konfigurowanie systemów kontroli dostępu firmy Bosch. Urządzenie musi być podłączone i dostępne. Po dodaniu systemu kontroli dostępu kontroler, wejścia, czytniki i drzwi są wyświetlane w oknie Drzewo urządzeń w sposób hierarchiczny.

Na stronie **Mapy i struktura** można usunąć kontroler, wejścia, czytniki i drzwi lub zmienić ich nazwę. Po zmianie konfiguracji lub hierarchii kontrolerów, czytników lub drzwi objętych systemem kontroli dostępu należy ponownie przeskanować urządzenie, aby wyświetlić zmiany w systemie BVMS.

Certyfikat HTTPS dla klienta

Aby zapewnić bezpieczne połączenie między systemem kontroli dostępu i systemem BVMS, należy wyeksportować certyfikat klienta z systemu kontroli dostępu i zaimportować go do systemu BVMS. Procedura ta została opisana w sekcji **Certyfikat HTTPS dla klienta** dokumentacji systemu kontroli dostępu.

**Uwaga!**

Jeśli certyfikat nie zostanie dodany, systemy nie będą w stanie wymieniać między sobą informacji.

13.19.1**Dodawanie systemu kontroli dostępu**

Okno główne > **Urządzenia** > rozwinąć  > 

Aby dodać system kontroli dostępu:

1. Prawym przyciskiem myszy kliknij ikonę .
2. Kliknij **Dodaj system kontroli dostępu**.

Zostanie wyświetlone okno dialogowe **Dodaj system kontroli dostępu**.

Uwaga: w przypadku dodawania systemu kontroli dostępu, drzwi skonfigurowane, czytniki, wejścia i przekaźniki są wymienione na liście znajdującej się na stronie **Mapy i struktura**.

Okno dialogowe Dodaj system kontroli dostępu**Adres sieciowy/port HTTPS**

Wprowadzić nazwę hosta urządzenia. Jeśli jest to wymagane, zmień numer portu.

Nazwa użytkownika

Wyświetla nazwę użytkownika używaną w celu uwierzytelniania w urządzeniu.

Hasło

Wprowadź poprawne hasło używane do uwierzytelniania w urządzeniu.

Aby przetestować połączenie:

1. Kliknij przycisk **Połącz**.
Program BVMS Configuration Client spróbuje nawiązać połączenie z systemem kontroli dostępu i pobrać odpowiednie informacje.
2. Kliknij **OK**.
System kontroli dostępu zostanie dodany do systemu w oparciu o wyświetlone informacje.

13.19.2**Edycja systemu kontroli dostępu**

Okno główne > **Urządzenia** > Rozwiń  >  > 

Aby dokonać edycji systemu kontroli dostępu:

1. Prawym przyciskiem myszy kliknij ikonę .
2. Kliknij **Edytuj system kontroli dostępu**.

Zostanie wyświetlone okno dialogowe **Edytuj system kontroli dostępu**.

13.19.3 Strona Ustawienia

Okno główne > **Urządzenia** > Rozwiń  >  >  > Karta **Ustawienia**
Umożliwia zmianę ustawień połączenia z systemem kontroli dostępu.

13.20 Strona analizy obrazu

Okno główne > > **Urządzenia** > rozwiń  > 
Umożliwia dodawanie analizy obrazu, urządzeń Person Identification (PID) i urządzeń Tattile LPR.

13.20.1 Strona ustawień Video Analytics

Okno główne > > **Urządzenia** > rozwiń  > rozwiń  >  > **Video Analytics** > strona **Ustawienia Video Analytics**

Można dodać oparte na serwerze urządzenie analizy sygnału wizyjnego.

Muszą być dostępne dane uwierzytelniające i ścieżka instalacji aplikacji do przeglądu danych analizy używanej w przypadku urządzenia do analizy sygnału wizyjnego.

Adres sieciowy

Należy wpisać adres IP urządzenia analizy sygnału wizyjnego. Nazwa DNS jest niedozwolona.

Nazwa użytkownika

Należy wprowadzić nazwę użytkownika, zgodnie z konfiguracją w urządzeniu analizy sygnału wizyjnego.

Hasło

Wpisać hasło zgodnie z konfiguracją urządzenia analizy opartej na serwerze.

Ścieżka przeglądarki analiz

Wprowadź ścieżkę względną ścieżki instalacji aplikacji do przeglądu danych analizy. Ścieżka jest względna w stosunku do katalogu `C:\Program Files (x86)\` na komputerze, na którym jest używana aplikacja do przeglądu danych analizy.

Przykład — aplikacja do przeglądu danych analizy (*AnalyticsViewer.exe*) jest zainstalowana w katalogu:

```
C:\Program Files (x86)\VideoAnalytics\
```

Należy skonfigurować następującą ścieżkę w polu **Ścieżka przeglądarki analiz**:

```
VideoAnalytics\AnalyticsViewer.exe
```

13.20.2 Dodawanie urządzenia analizy sygnału wizyjnego

Okno główne > > **Urządzenia** > kliknij prawym przyciskiem myszy  polecenie **Dodaj urządzenie Video Analytics** > okno dialogowe **Dodaj urządzenie Video Analytics**
Podczas dodawania urządzenia analizy opartej na serwerze należy wprowadzić poświadczenia dla nowego urządzenia.

Aby dodać analizy oparte na serwerze, należy:

1. Rozwinąć element , kliknąć prawym przyciskiem , a następnie kliknąć **Dodaj urządzenie Video Analytics**.
Zostanie wyświetlone okno dialogowe **Dodaj urządzenie Video Analytics**.
2. Wpisać odpowiednie wartości.

3. Kliknąć **OK**.
Urządzenie zostanie dodane do systemu.

Okno dialogowe Dodaj urządzenie Video Analytics

Adres sieciowy

Należy wpisać adres IP urządzenia analizy sygnału wizyjnego. Nazwa DNS jest niedozwolona.

Nazwa użytkownika

Należy wprowadzić nazwę użytkownika, zgodnie z konfiguracją w urządzeniu analizy sygnału wizyjnego.

Hasło

Wpisać hasło zgodnie z konfiguracją urządzenia analizy opartej na serwerze.

13.20.3

Strona urządzeń Person Identification Device

Okno główne > > **Urządzenia** > Rozwinąć  > Rozwinąć  > strona urządzeń  Person Identification

Umożliwia dodanie urządzenia Person Identification. Urządzenie musi być połączone i dostępne. Można dodać kamery do urządzenia Person Identification i konfigurować zdarzenia i alarmy Person Identification.

Grupy osób

Na karcie **Grupy osób** można dodawać i konfigurować grupy osób.

Kamery

Na karcie **Kamery** można dodać kamery do urządzenia Person Identification. Dodane kamery pojawiają się na liście.

Uwaga: w pierwszej kolejności należy dodać odpowiednie kamery do drzewa logicznego.

13.20.4

Dodawanie urządzenie PID (Person Identification Device)



Uwaga!

W przypadku awarii Management Server należy przywrócić konfigurację BVMS i certyfikat Bosch VMS CA. W przeciwnym wypadku nie można użyć istniejącego PID bez resetowania, co spowoduje usunięcie wszystkich zapisanych osób.

Zaleca się utworzenie kopii zapasowej konfiguracji BVMS i certyfikatu Bosch VMS CA.

Podczas dodawania urządzenia Person Identification upewnij się, że certyfikat wyświetlany w oknie dialogowym **Dodaj urządzenie Person Identification Device** odpowiada urządzeniu PID, które ma zostać dodane.

Począwszy od BVMS w wersji 10.1 można dodawać wiele urządzeń PID.

Pierwsze dodane urządzenie PID to główne urządzenie połączone do systemu BVMS. Pierwsze urządzenie PID ustanawia połączenie z innymi urządzeniami PID i przechowuje bazę danych osób.

Uwaga: zanim usuniesz pierwsze urządzenie PID, musisz usunąć wszystkie pozostałe skonfigurowane urządzenia PID.

Aby dodać urządzenie Person Identification, należy:

1. Rozwinąć węzeł .
2. Prawym przyciskiem myszy kliknij ikonę .

3. Kliknij **Dodaj urządzenie Person Identification Device**.
Pojawi się okno dialogowe **Dodaj urządzenie Person Identification Device**.
4. Wpisać odpowiednie wartości.
5. Kliknąć **Wyświetl certyfikat...**, aby sprawdzić, czy certyfikat odpowiada urządzeniu PID.
6. Aby potwierdzić, kliknij przycisk **OK**.
7. Kliknij **OK**.
Urządzenie zostanie dodane do systemu.

Okno dialogowe Dodaj urządzenie Person Identification Device

Adres sieciowy

Wpisz adres IP urządzenia.

Numer portu

Wpisać numer portu urządzenia.

Patrz

- Przywracanie dostępu do PID po awarii serwera BVMS Management Server., Strona 165
- Aby eksportować dane konfiguracyjne, należy:, Strona 94

13.20.5

Strona PID

Okno główne > **Urządzenia** > Rozwinąć  > Rozwinąć  >  urządzenia Person Identification > strona  PID

Połączenie

Na karcie **Połączenie** wyświetlany jest adres sieciowy i numer portu urządzenia Person Identification. Ustawienia połączenia z urządzeniem Person Identification są tylko do odczytu.

13.20.6

Przywracanie dostępu do PID po awarii serwera BVMS Management Server.



Uwaga!

W przypadku awarii Management Server należy przywrócić konfigurację BVMS i certyfikat Bosch VMS CA. W przeciwnym wypadku nie można użyć istniejącego PID bez resetowania, co spowoduje usunięcie wszystkich zapisanych osób.

Zaleca się utworzenie kopii zapasowej konfiguracji BVMS i certyfikatu Bosch VMS CA.

Aby uzyskać więcej informacji o zapisywaniu konfiguracji BVMS, patrz *Aby eksportować dane konfiguracyjne, należy:, Strona 77*. Certyfikaty są zarządzane poza systemem BVMS w aplikacji **Manage Computer Certificates** systemu Windows.



Uwaga!

Certyfikaty zawierają informacje poufne. Aby je chronić, należy postępować następująco:

- Ustawić silne hasło.
- Zapisać certyfikat w obszarze zastrzeżonym, np. na niepublicznym serwerze.
- Upewnić się, że do certyfikatu mają dostęp tylko uprawnieni pracownicy.

Aby utworzyć kopię zapasową certyfikatu Bosch VMS CA, należy:

1. Otworzyć aplikację **Manage Computer Certificates** w systemie Windows.

2. W folderze **Trusted Root Certification Authorities** wybrać certyfikat Bosch VMS CA.
3. Wyeksportować certyfikat za pomocą klucza prywatnego, wybierając opcję **Tak, eksportuj prywatny klucz**.
4. Użyć formatu wymiany informacji osobistych (Personal Information Exchange).
5. Ustawić silne hasło.
6. Zapisać certyfikat jako plik PFX.

Aby przywrócić dostęp do PID z nowo zainstalowanego BVMS Management Server należy:

1. Otworzyć aplikację **Manage Computer Certificates** w systemie Windows.
2. Zaimportować plik PFX zawierający certyfikat Bosch VMS CA do folderu **Trusted Root Certification Authorities** w nowym Management Server. Dołączyć wszystkie właściwości rozszerzone.
3. Zaimportować kopię zapasową konfiguracji BVMS.

Patrz

– Eksportowanie danych konfiguracyjnych, Strona 94

13.20.7

Dodawanie kamer do urządzenia PID (Person Identification Device)

Można dodawać kamery do urządzenia Person Identification, jeśli zostały one już dodane do drzewa logicznego.

Aby dodać kamery do urządzenia Person Identification, należy:

1. Rozwinąć węzeł .
2. Rozwinąć węzeł .
3. Kliknąć .
4. Kliknąć kartę **Kamery**.
5. Przeciągnąć odpowiednie kamery z okna **Drzewo logiczne** do okna **Kamery**.

LUB

Kliknąć dwukrotnie odpowiednie kamery w oknie **Drzewo logiczne**.

Kamery zostaną dodane do urządzenia Person Identification i są wyświetlane na liście **Kamery**.

13.20.8

Konfigurowanie parametrów kamery do obsługi alarmów Person Identification.

Dla każdej dostępnej kamery można skonfigurować parametry kamery dotyczące alarmów Person Identification, aby zmniejszyć fałszywe alarmy.

Parametr kamery

Nazwa	Informacje o wartości	Opis
Prawdopodobieństwo progu (%)	Domyślnie: 55 % Min.: 0 % Maks.: 100 %	Minimalne prawdopodobieństwo pozytywnej identyfikacji twarzy w celu wygenerowania zdarzenia Person Identification.
Wielkość twarzy (%)	Domyślnie: 7,5 % Min.: 5 % Maks.: 100 %	Minimalna wielkość twarzy do wykrycia w porównaniu do wielkością całej klatki wideo.

Nazwa	Informacje o wartości	Opis
Min. liczba klatek	Domyślnie: 4 Min.: 1	Minimalna liczba kolejnych klatek wideo, na których musi być widoczna twarz, aby została wykryta.
Klatki do analizy (%)	Domyślnie: 100 % Min.: 10 % Maks.: 100 %	Procent klatek analizowanych w celu identyfikacji osób. Wartość 50% oznacza, że analizowana jest co druga klatka.

13.20.9

Konfigurowanie grup osób

Okno główne > > **Urządzenia** > rozwiń  > 

Aby skonfigurować grupy osób:

- Wybrać kartę **Grupy osób**.
- Kliknąć ikonę , aby dodać nową grupę osób.
- Wpisać odpowiednie wartości.
- Kliknąć ikonę , aby usunąć grupę osób.

**Uwaga!**

Nie można usuwać ani zmieniać wartości grupy domyślnej.

Tabela grup osób

Grupa osób	Wprowadzić nazwę grupy osób.
Kolor alarmu	Kliknąć dwukrotnie, aby wybrać kolor alarmu.
Tytuł alarmu	Wprowadzić nazwę alarmu, która będzie wyświetlana w aplikacji Operator Client.

Aby zmienić wartości w tabeli grup osób, należy:

- Kliknąć dwukrotnie odpowiednie pole tabeli.
- Zmienić wartość.

Priorytet alarmu

Można ustawiać priorytety alarmów Person Identification na stronie **Alarmy**.

**Uwaga!**

Priorytet alarmów mogą być różne dla poszczególnych kamer w odpowiedniej grupie osób. Można także zmienić priorytet alarmu domyślnej grupy osób.

Patrz

– strona Alarmy, Strona 310

13.20.10**Dodawanie urządzenia Tattile LPR**

Okno główne > **Urządzenia**  > rozwiń  > 

Urządzenia Tattile LPR identyfikują i wykrywają numery tablic rejestracyjnych. Można odpowiednio skonfigurować zdarzenia i alarmy LPR.

Aby urządzenie Tattile LPR wykrywało określone numery tablic rejestracyjnych, najpierw trzeba skonfigurować listę odpowiednich tablic rejestracyjnych bezpośrednio w urządzeniu Tattile LPR. Szczegółowe informacje można znaleźć w dokumentacji użytkownika urządzenia.

**Uwaga!**

Urządzenie musi być podłączone i dostępne.

BVMS łączy się tylko wtedy, gdy w urządzeniu Tattile LPR jest włączone uwierzytelnianie i zostały określone nazwa użytkownika oraz hasło. Nazwa użytkownika i hasło nie mogą być puste.

Aby dodać urządzenie Tattile LPR, należy:

1. Prawym przyciskiem myszy kliknąć 
2. Kliknąć **Dodaj urządzenie Tattile LPR**.
Zostanie wyświetlone okno dialogowe **Dodaj urządzenie Tattile LPR**.
3. Wpisać odpowiednie wartości.
4. Kliknąć **Uwierzytelnij**.
5. Kliknij **OK**.
Urządzenie zostanie dodane do systemu.

**Uwaga!**

Należy określić adres IP urządzenia BVMSManagement Server w konfiguracji urządzenia LPR. W przeciwnym razie system BVMS nie pobiera zdarzeń z tego urządzenia LPR.

Okno dialogowe Dodaj urządzenie Tattile LPR**Adres sieciowy**

Wpisz adres IP urządzenia.

Numer portu

Wpisać numer portu urządzenia.

Nazwa użytkownika

Należy wprowadzić poprawną użytkownika używaną do uwierzytelniania w urządzeniu.

Hasło

Wprowadź poprawne hasło używane do uwierzytelniania w urządzeniu.

Uwierzytelnij

Kliknąć, aby uwierzytelnić w urządzeniu z wykorzystaniem wprowadzonych powyżej poświadczeń.

13.21**strona Urządzenia VRM**

Okno główne > **Urządzenia** > rozwinąć  > 

Umożliwia dodanie i skonfigurowanie urządzeń VRM. Do urządzenia VRM należy przypisać co najmniej jeden nadajnik, jedno urządzenie iSCSI i jeden numer LUN powiązany z urządzeniem iSCSI oraz pulę pamięci masowej. Zapoznać się z uwagami i kartą katalogową dla bieżących wersji oprogramowania układowego.

**Uwaga!**

Po dodaniu do systemu BVMS urządzenia iSCSI wraz z odpowiednimi nadajnikami należy dodać do urządzenia iSCSI nazwę IQN każdego nadajnika (dotyczy niektórych typów urządzeń iSCSI).

Aby uzyskać więcej informacji, patrz *Konfiguracja urządzenia iSCSI, Strona 192*.

**Uwaga!**

Należy się upewnić, że czas komputera z systemem VRM jest zsynchronizowany z serwerem Management Server. W przeciwnym razie może dojść do utraty zapisów.

Na komputerze typu Management Server należy odpowiednio skonfigurować oprogramowanie serwera czasu. Z kolei na komputerze z zainstalowaną usługą VRM należy ustawić adres IP komputera typu Management Server taki, jak adres serwera czasu. W tym celu należy posłużyć się standardowymi procedurami obsługi systemu Windows.

Patrz

- Konfigurowanie trybu Multicast, Strona 234
- Synchronizowanie konfiguracji systemu BVMS, Strona 178
- strona Ustawienia VRM, Strona 172
- Strona puli, Strona 179
- Strona urządzenia iSCSI, Strona 188
- Zmiana hasła urządzenia VRM, Strona 175

13.21.1

Dodawanie urządzeń VRM poprzez skanowanie:



Okno główne > **Urządzenia** >

W sieci musi znajdować się urządzenie iSCSI, a ponadto musi działać usługa VRM uruchomiona na jednym z przyłączonych komputerów.

**Uwaga!**

W przypadku dodania urządzenia iSCSI bez skonfigurowanych lokalizacji docelowych i numerów LUN należy uruchomić konfigurację domyślną i dodać do tego urządzenia iSCSI nazwę IQN każdego nadajnika.

W przypadku dodawania urządzenia iSCSI ze wstępnie skonfigurowanymi lokalizacjami docelowymi i numerami LUN należy dodać do tego urządzenia iSCSI nazwę IQN każdego nadajnika.

Aby uzyskać więcej informacji, patrz *Konfiguracja urządzenia iSCSI, Strona 192*.

Aby poprzez skanowanie dodać urządzenia VRM:

1. Kliknij prawym przyciskiem myszy , a następnie kliknij **Skanuj w poszukiwaniu urządzeń VRM**.

Zostanie wyświetlone okno dialogowe **BVMS Scan Wizard**.

2. Zaznacz pola wyboru odpowiadające urządzeniom, które mają zostać dodane.
3. Na liście **Rola** zaznacz pożądaną rolę.
Role, które można wybrać, zależą od rodzaju bieżącego urządzenia VRM.
Po wybraniu opcji **Nadmiarowy** lub **Tryb awaryjny** należy wykonać kolejny etap konfiguracji.
4. Na liście **Rola** zaznacz pożądaną rolę.
Role, które można wybrać, zależą od rodzaju bieżącego urządzenia VRM.

5. Kliknij **Dalej >>**
6. Wybierz z listy **Główny VRM** główne urządzenie VRM dla wybranego nadmiarowego lub awaryjnego urządzenia VRM.
7. Kliknij **Dalej >>**.
Zostanie wyświetlone okno dialogowe kreatora **Uwierzytelnianie urządzeń**.
8. Wpisać hasło w przypadku każdego urządzenia, które jest nim chronione.
Jeśli przez kilka sekund nie wprowadzisz żadnego znaku w polu hasła lub klikniesz poza tym polem, sprawdzenie hasła następuje automatycznie.
Jeśli hasło do wszystkich urządzeń jest identyczne, można wpisać je w pierwszym polu **Hasło**.
Następnie kliknąć to pole prawym przyciskiem myszy i wybrać opcję **Kopiuj komórkę do kolumny**.



Udane logowanie jest oznaczane w kolumnie **Stan** ikoną



Nieudane próby logowania są oznaczane ikoną

9. Kliknąć **Zakończ**.
Urządzenie zostanie dodane do drzewa urządzeń.

Uwaga: wszystkie urządzenia VRM są domyślnie dodawane z bezpiecznym połączeniem.

Aby zmienić bezpieczne/niebezpieczne połączenie, należy:



1. Prawym przyciskiem myszy kliknąć ikonę
2. Kliknąć **Edytuj urządzenie VRM**.
Zostanie wyświetlone okno dialogowe **Edytuj urządzenie VRM**.
3. Zaznaczyć pole wyboru **Zabezpiecz połączenie**.
Używany port zmienia się automatycznie na port HTTPS.
LUB
Usunąć zaznaczenie pole wyboru **Zabezpiecz połączenie**.
Używany port zmienia się automatycznie na port rcpp.

Patrz

- Dodawanie urządzenia, Strona 125
- strona Urządzenia VRM, Strona 168
- Konfiguracja urządzenia iSCSI, Strona 192
- Zapis podwójny / awaryjny, Strona 30

13.21.2

Ręczne dodawanie podstawowego lub pomocniczego urządzenia VRM



Okno główne > **Urządzenia** > kliknij prawym przyciskiem myszy > kliknij **Dodaj system VRM** > okno dialogowe **Dodaj system VRM**

Umożliwia dodanie urządzenia VRM. Można wybrać typ urządzenia i wprowadzić poświadczenia. Skutecznie przypisać awaryjny VRM do głównego VRM można tylko wtedy, gdy oba są online i zostały prawidłowo uwierzytelnione. W takim wypadku hasła są zsynchronizowane. Podstawowy VRM można dodać ręcznie, jeśli zna się jego adres IP i hasło.

Aby dodać podstawowy VRM:

1. Wpisz wymagane ustawienia w urządzeniu VRM.
2. Zaznacz na liście **Typ** pozycję **Główny**.
3. Kliknij **OK**.

Urządzenie VRM zostanie dodane.

Pomocniczy VRM można dodać ręcznie, jeśli zna się jego adres IP i hasło.

**Uwaga!**

Aby skonfigurować pomocniczy VRM, należy najpierw zainstalować na komputerze odpowiednie oprogramowanie. Uruchom program Setup.exe i wybierz **Pomocniczy VRM**.

Aby dodać pomocniczy VRM:

1. Wpisz wymagane ustawienia w urządzeniu VRM.
2. Zaznacz na liście **Typ** pozycję **Pomocniczy**.
3. Kliknij **OK**.

Urządzenie VRM zostanie dodane.

Teraz można skonfigurować pomocniczy VRM podobnie jak podstawowy.

Okno dialogowe Dodaj system VRM**Nazwa**

Wpisz wyświetlaną nazwę urządzenia.

Adres/port sieciowy

Wprowadź adres IP urządzenia.

Jeśli pole wyboru **Zabezpiecz połączenie** jest zaznaczone, port zmienia się automatycznie na HTTPS.

Numer portu można zmienić, jeśli nie są używane żadne porty domyślne.

Typ

Wybierz żądany typ urządzenia.

Nazwa użytkownika

Wprowadź nazwę użytkownika w celu uwierzytelnienia.

Hasło

Wprowadź hasło w celu uwierzytelnienia.

Pokaż hasło

Kliknąć, aby włączyć opcję wyświetlania wprowadzonego hasła.

Bezpieczeństwo

Pole wyboru **Zabezpiecz połączenie** jest zaznaczone domyślnie, jeśli protokół HTTPS jest obsługiwany.

**Uwaga!**

W przypadku przejścia na system BVMS w wersji 10.0 lub nowszej, pole wyboru **Zabezpiecz połączenie** nie jest domyślnie zaznaczone i połączenie jest niezabezpieczone (rcpp).

Aby zmienić połączenie bezpieczne lub niezabezpieczone, należy użyć polecenia **Edytuj urządzenie VRM** i zaznaczyć pole wyboru **Zabezpiecz połączenie** lub usunąć zaznaczenie.

Test

Kliknij, aby sprawdzić, czy urządzenie jest podłączone i uwierzytelnianie zostało wykonane pomyślnie.

Właściwości

W razie potrzeby zmień numery portu dla protokołu HTTP i HTTPS. Jest to możliwe tylko w przypadku dodawania lub edytowania urządzenia VRM, które nie jest podłączone. Jeśli urządzenie VRM jest podłączone, te wartości są pobierane i nie można ich zmienić.

Wiersz tabeli **Główny VRM** przedstawia wybrane urządzenie (jeśli dotyczy).

Patrz

- Edytowanie urządzenia VRM, Strona 172
- Dodawanie nadmiarowego urządzenia VRM, Strona 176
- Ręczne dodawanie awaryjnego VRM, Strona 175

13.21.3**Edytowanie urządzenia VRM**

Okno główne > **Urządzenia**

Umożliwia edytowanie urządzenia VRM.

Aby zmienić bezpieczne/niebezpieczne połączenie, należy:

1. Prawym przyciskiem myszy kliknąć ikonę .
2. Kliknąć **Edytuj urządzenie VRM**.
Zostanie wyświetlone okno dialogowe **Edytuj urządzenie VRM**.
3. Zaznaczyć pole wyboru **Zabezpiecz połączenie**.
Używany port zmienia się automatycznie na port HTTPS.
LUB
Usunąć zaznaczenie pole wyboru **Zabezpiecz połączenie**.
Używany port zmienia się automatycznie na port rcpp.

**Uwaga!**

Po zaktualizowaniu do nowszej wersji zalecamy zmianę połączenia na bezpieczne.

Aby uzyskać szczegółowe informacje o oknie dialogowym **Edytuj urządzenie VRM**, patrz rozdział Ręczne dodawanie podstawowego lub pomocniczego urządzenia VRM.

Patrz

- Ręczne dodawanie podstawowego lub pomocniczego urządzenia VRM, Strona 170

13.21.4**strona Ustawienia VRM**

Główne okno > **Urządzenia** > rozwiń  >  > **Ustawienia główne** > **Ustawienia VRM**

Nazwa początkowa serwera

Wyświetla nazwę węzła inicjującego połączenie iSCSI z modułem VRM Server.

13.21.5**strona SNMP**

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > **Sieć** > **SNMP**

1. Adres SNMP hosta 2. Adres SNMP hosta

VRM obsługuje protokół SNMP (Simple Network Management Protocol) do zarządzania i monitorowania elementów sieci i ma możliwość wysyłania komunikatów SNMP do adresów IP. Urządzenie obsługuje SNMP MIB II w kodzie zunifikowanym. Aby wysyłać pułapki SNMP, należy wprowadzić w tym polu adres IP jednego lub dwóch wybranych urządzeń docelowych. Część zdarzeń jest wysyłana tylko jako komunikaty SNMP. Opisy można znaleźć w pliku MIB.

13.21.6**Strona Konta**

Aby skonfigurować przesyłanie obrazów oraz eksportować filmy w formacie MP4, należy utworzyć konto, za pomocą którego będzie można zapisywać te filmy i obrazy oraz uzyskiwać do nich dostęp. Można utworzyć maksymalnie cztery (4) konta.

Typ

W tym obszarze należy wybrać typ konta (**FTP** lub **Dropbox**).

Adres IP

W tym polu należy wprowadzić adres IP serwera, na którym będą zapisywane obrazy.

Nazwa użytkownika

W tym polu należy wprowadzić nazwę użytkownika serwera.

Hasło

W tym obszarze należy wprowadzić hasło dostępu do serwera. Aby zweryfikować hasło, należy kliknąć przycisk **Sprawdź** po prawej stronie.

Sprawdź

Kliknięcie tego przycisku powoduje weryfikację hasła.

Ścieżka

W tym polu należy wprowadzić pełną ścieżkę do katalogu, w którym na serwerze będą zapisywane obrazy i filmy.

13.21.7**strona Zaawansowane**

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > **Serwis** > **Zaawansowane**

Logowanie RCP+ / Logowanie debugera / Logowanie powtórek / Logowanie VDP / Logowanie wydajności

Należy uaktywnić różne rejestry dla modułów VRM Server i Configuration Manager.

Pliki rejestrów modułu VRM Server są przechowywane na komputerze, na którym są uruchomione, i można je przeglądać oraz pobierać za pomocą programu VRM Monitor.

Pliki dziennika programu Configuration Manager są przechowywane lokalnie w katalogu:

%USERPROFILE%\My Documents\Bosch\Video Recording Manager\Log

Czas przechowywania (dni)

Należy określić czas przechowywania plików rejestrów (w dniach).

Kompletny zrzut pamięci

Należy zaznaczyć to pole wyboru tylko w razie konieczności – gdy na przykład dział pomocy technicznej poprosi o zestawienie zawartości pamięci głównej.

Obsługa Telnet

To pole wyboru należy zaznaczyć, jeśli ma być obsługiwany dostęp za pośrednictwem protokołu Telnet. Należy zaznaczyć tylko w razie konieczności.

**Uwaga!**

Rejestrowanie na dużą skalę wymaga znacznej mocy procesora i pojemności dysku twardego. Nie należy korzystać z tej opcji w codziennej eksploatacji.

13.21.8**Zapis szyfrowany na urządzeniach VRM**

Zapis szyfrowany na nadajnikach VRM nie jest włączony domyślnie.

Trzeba osobno włączyć zapis szyfrowany na głównych i podrzędnych nadajnikach VRM.

**Uwaga!**

Przed włączeniem zapisu szyfrowanego po raz pierwszy, należy utworzyć klucz redundancji (kopię zapasową certyfikatu). Dla każdego urządzenia VRM wystarczy jednokrotnie utworzyć klucz redundancji.

W przypadku utraty zwykłego klucza szyfrowania można odszyfrować nagrania za pomocą klucza redundancji.

Zaleca się przechowywanie kopii klucza redundancji w bezpiecznym miejscu (np. w sejfie).

Aby utworzyć klucz redundancji:

1. Wybrać odpowiednie urządzenie VRM.
2. Wybrać kartę **Serwis**.
3. Wybrać kartę **Szyfrowanie nagrań**.
4. Kliknąć **Klucz redundancji**.
5. Wybrać lokalizację magazynu certyfikacji.
6. Wpisać hasło, które spełnia wymagania złożoności hasła, i potwierdzić je.
7. Kliknąć **Utwórz**.

Nastąpi utworzenie klucza redundancji (kopii zapasowej certyfikatu).

Aby włączyć/wyłączyć zapis szyfrowany, należy:

1. Wybrać odpowiednie urządzenie VRM.
2. Wybrać kartę **Serwis**.
3. Wybrać kartę **Szyfrowanie nagrań**.
4. Zaznaczyć pole wyboru **Włącz zapis szyfrowany** lub usunąć zaznaczenie tego pola.

5. Kliknąć .

Uwaga: szyfrowanie zostanie włączone po następnej zmianie blokowej. Może to chwilę potrwać.

Należy upewnić się, że nadajniki szyfrują dane.

Aby sprawdzić, czy nadajniki VRM szyfrują dane:

1. Wybrać odpowiednie urządzenie VRM.
2. Wybrać kartę **Serwis**.
3. Wybrać kartę **Szyfrowanie nagrań**.

Uwaga: można także zajrzeć na kartę **Monitoring** w narzędziu VRM Monitor.

**Uwaga!**

Wszystkie nadajniki VRM obsługujące szyfrowanie automatycznie szyfrują zapis, jeśli szyfrowanie jest włączone w VRM.

Szyfrowanie można wyłączać w poszczególnych nadajnikach.

Nadajniki VSG są zawsze szyfrowane, jeśli szyfrowanie jest włączone w VRM.

Aby włączyć/wyłączyć szyfrowanie zapisu w jednym nadajniku VRM, należy:

1. Wybrać odpowiedni nadajnik VRM.
2. Wybrać kartę **Zapis**.
3. Wybrać kartę **Zarządzanie zapisami**.
4. Zaznaczyć pole wyboru **Szyfrowanie** lub usunąć zaznaczenie tego pola.

5. Kliknąć .

13.21.9 Zmiana hasła urządzenia VRM

Okno główne > **Urządzenia** > rozwiń  > 

Aby zmienić hasło:

1. Kliknąć prawym przyciskiem myszy  i wybrać **Zmień hasło systemu VRM**.
Zostanie wyświetlone okno dialogowe **Zmień hasło**.
2. W polu **Stare hasło** wpisać odpowiednie hasło.
3. W polu **Nowe hasło** wpisać nowe hasło, a następnie kliknąć i wpisać ponownie to samo hasło w drugim polu **Nowe hasło**.

Kliknąć **OK**.

- ▶ Potwierdź następne okno dialogowe.
- ⇒ Hasło na urządzeniu zostanie natychmiast zmienione.

13.21.10 Dodawanie puli VRM

Okno główne > **Urządzenia** > rozwiń 

Aby dodać pulę VRM:

- ▶ Kliknij prawym przyciskiem myszy ikonę  lub , a następnie kliknij polecenie **Dodaj pulę**.
Do systemu zostanie dodana nowa pula.

Patrz

– Pula pamięci iSCSI, Strona 188

13.21.11 Ręczne dodawanie awaryjnego VRM

Okno główne > **Urządzenia** > rozwiń  > kliknij prawym przyciskiem myszy  > kliknij **Dodaj awaryjny VRM** > okno dialogowe **Dodaj awaryjny VRM**



Uwaga!

Aby skonfigurować pomocniczy VRM, należy najpierw zainstalować na komputerze odpowiednie oprogramowanie. Uruchom program Setup.exe i wybierz **Pomocniczy VRM**.

Podstawowy VRM albo pomocniczy VRM mogą pełnić rolę awaryjnego VRM. Podstawowy awaryjny VRM dodaje się do podstawowego VRM lub pomocniczy awaryjny VRM dodaje się do pomocniczego VRM.

Można dodać ręcznie urządzenie nadmiarowego VRM, jeśli jest znany jego adres IP i hasło. Wybrany początkowo VRM jest głównym VRM dla nadmiarowego.

Można dodać awaryjny VRM. Można to zrobić ręcznie albo wyszukać urządzenie na liście skanowanych urządzeń VRM.

Skutecznie przypisać awaryjny VRM do głównego VRM można tylko wtedy, gdy oba są online i zostały prawidłowo uwierzytelnione. W takim wypadku hasła są zsynchronizowane.

Aby dodać awaryjny VRM:

1. Wprowadzić wymagane ustawienia w urządzeniu VRM.
2. Upewnić się, że został prawidłowo wybrany główny VRM. Jeśli nie został, anulować tę procedurę.
3. Kliknąć **OK**.

⇒ Awaryjne urządzenie VRM zostanie dodane do wybranego głównego VRM.

Okno dialogowe Dodaj awaryjny VRM

Adres sieciowy

Wpisz adres IP urządzenia lub zaznacz adres sieciowy na liście **Przeskanowane urządzenia VRM**.

Przeskanowane urządzenia VRM

Wyświetla listę zeskanowanych komputerów VRM. Aby powtórzyć skanowanie, należy zamknąć to okno dialogowe i otworzyć je ponownie.



Uwaga!

Awaryjne urządzenie VRM przejmuje ustawienia skonfigurowane w głównym urządzeniu VRM. Jeżeli ustawienia głównego urządzenia VRM zmienią się, ustawienia awaryjnego urządzenia VRM również odpowiednio ulegną zmianie.

Patrz

– Zapis podwójny / awaryjny, Strona 30

13.21.12

Dodawanie nadmiarowego urządzenia VRM

Okno główne > **Urządzenia** > rozwiń  > kliknij prawym przyciskiem myszy  > kliknij **Dodaj nadmiarowe urządzenie VRM** > okno dialogowe **Dodaj system VRM**



Uwaga!

Aby skonfigurować pomocniczy VRM, należy najpierw zainstalować na komputerze odpowiednie oprogramowanie. Uruchom program Setup.exe i wybierz **Pomocniczy VRM**.

Tylko pomocniczy VRM może pełnić rolę nadmiarowego VRM. Nadmiarowy VRM dodaje się do podstawowego VRM.

Nadmiarowy VRM można dodać ręcznie, o ile zna się jego adres IP i hasło. Wybrany początkowo VRM jest głównym VRM dla nadmiarowego VRM.

Aby dodać nadmiarowe urządzenie VRM:

1. Wpisz wymagane ustawienia w urządzeniu VRM.
2. Upewnij się, że został prawidłowo wybrany główny VRM. Jeśli nie został, anuluj tę procedurę.
3. Kliknij **OK**.

Nadmiarowe urządzenie VRM zostanie dodane do wybranego podstawowego VRM.

Okno dialogowe Dodaj system VRM

Nazwa

Wpisz wyświetlaną nazwę urządzenia.

Adres/port sieciowy

Wprowadź adres IP urządzenia.

Jeśli pole wyboru **Zabezpiecz połączenie** jest zaznaczone, port zmienia się automatycznie na HTTPS. Numer portu można zmienić, jeśli nie są używane żadne porty domyślne.

Typ

Wybierz żądany typ urządzenia.

Nazwa użytkownika

Wprowadź nazwę użytkownika w celu uwierzytelnienia.

Pokaż hasło

Kliknąć, aby włączyć opcję wyświetlania wprowadzonego hasła.

Hasło

Wprowadź hasło w celu uwierzytelnienia.

Bezpieczeństwo

Pole wyboru **Zabezpiecz połączenie** jest zaznaczone domyślnie, jeśli protokół HTTPS jest obsługiwany.

**Uwaga!**

W przypadku przejścia na system BVMS w wersji 10.0 lub nowszej, pole wyboru **Zabezpiecz połączenie** nie jest domyślnie zaznaczone i połączenie jest niezabezpieczone (rcpp).

Aby zmienić połączenie bezpieczne lub niezabezpieczone, należy użyć polecenia **Edytuj urządzenie VRM** i zaznaczyć pole wyboru **Zabezpiecz połączenie** lub usunąć zaznaczenie.

Test

Kliknij, aby sprawdzić, czy urządzenie jest podłączone i uwierzytelnianie zostało wykonane pomyślnie.

Właściwości

W razie potrzeby zmień numery portu dla protokołu HTTP i HTTPS. Jest to możliwe tylko w przypadku dodawania lub edytowania urządzenia VRM, które nie jest podłączone. Jeśli urządzenie VRM jest podłączone, te wartości są pobierane i nie można ich zmienić.

Wiersz tabeli **Główny VRM** przedstawia wybrane urządzenie (jeśli dotyczy).

Patrz

- Ręczne dodawanie podstawowego lub pomocniczego urządzenia VRM, Strona 170
- Zapis podwójny / awaryjny, Strona 30

13.21.13**Dodawanie nadajników poprzez skanowanie**

Aby dodać nadajniki poprzez skanowanie:

1. Kliknij prawym przyciskiem myszy , a następnie kliknij **Skanuj w poszukiwaniu nadajników**.
Zostanie wyświetlone okno dialogowe **BVMS Scan Wizard**.
2. Wybierz wymagane nadajniki oraz żądaną pulę VRM, a następnie kliknij **Przypisz**, aby przypisać nadajniki do puli VRM.
3. Kliknij **Dalej >>**.
Zostanie wyświetlone okno dialogowe kreatora **Uwierzytelnianie urządzeń**.
4. Wpisać hasło w przypadku każdego urządzenia, które jest nim chronione.
Jeśli przez kilka sekund nie wprowadzisz żadnego znaku w polu hasła lub klikniesz poza tym polem, sprawdzenie hasła następuje automatycznie.
Jeśli hasło do wszystkich urządzeń jest identyczne, można wpisać je w pierwszym polu **Hasło**.
Następnie kliknij to pole prawym przyciskiem myszy i kliknij polecenie **Kopiuj komórkę do kolumny**.
5. Kliknąć **Zakończ**.
Urządzenie zostanie dodane do drzewa urządzeń.

Ikona  oznacza błąd, którym należy się zająć. Więcej informacji o charakterze błędu uzyskasz z etykietyki narzędzia.

13.21.14

Dodawanie urządzeń VSG poprzez skanowanie

Aby poprzez skanowanie dodać urządzenia VSG:

1. Kliknij prawym przyciskiem myszy , a następnie kliknij **Skanuj w poszukiwaniu bram Video Streaming Gateway**.

Zostanie wyświetlone okno dialogowe **BVMS Scan Wizard**.

2. Wybierz wymagane urządzenia VSG i żądaną pulę VRM, a następnie kliknij **Przypisz**, aby przypisać nadajniki do puli VRM.
3. Kliknij **Dalej >>**.

Zostanie wyświetlone okno dialogowe kreatora **Uwierzytelnianie urządzeń**.

4. Wpisać hasło w przypadku każdego urządzenia, które jest nim chronione.

Jeśli przez kilka sekund nie wprowadzisz żadnego znaku w polu hasła lub klikniesz poza tym polem, sprawdzenie hasła następuje automatycznie.

Jeśli hasło do wszystkich urządzeń jest identyczne, można wpisać je w pierwszym polu **Hasło**.

Następnie kliknąć to pole prawym przyciskiem myszy i wybrać opcję **Kopiuj komórkę do kolumny**.

Udane logowanie jest oznaczane w kolumnie **Stan** ikoną .

Nieudane próby logowania są oznaczane ikoną .

5. Kliknąć **Zakończ**.

Urządzenie zostanie dodane do drzewa urządzeń.

13.21.15

Synchronizowanie konfiguracji systemu BVMS

Okno główne > **Urządzenia** > rozwiń  > kliknij prawym przyciskiem myszy ikonę  > wybierz polecenie **Synchronizuj konfigurację systemu BVMS**

Podobnie jak w przypadku systemu BVMS w wersji 6.0, obsługiwane jest oprogramowanie VRM w wersji 3.50. Jeśli w trakcie uaktualniania do systemu BVMS 6.0 nie wykona się aktualizacji oprogramowania VRM do wersji 3.50, zapis będzie kontynuowany, ale nie można zmieniać konfiguracji starego oprogramowania VRM.

W przypadku uaktualnienia oprogramowania VRM do wersji 3.50 konieczne jest ręczne zsynchronizowanie konfiguracji systemu BVMS.

13.21.16

Importowanie konfiguracji z VRM

Okno główne > **Urządzenia** > rozwinąć  > 

W przypadku konieczności wymiany głównego urządzenia VRM, można zaimportować konfigurację poprzedniego głównego urządzenia VRM.

Uwaga: jest to możliwe tylko w przypadku głównych urządzeń VRM.

Wymagania wstępne: wykonano kopię zapasową pliku konfiguracji poprzedniego urządzenia VRM (config.xml). Aby dowiedzieć się, jak wykonać kopię zapasową, patrz *Utrzymanie systemu BVMS*, Strona 77.

Aby zaimportować konfigurację z urządzenia VRM:

1. Skopiować kopię zapasową pliku konfiguracji VRM (config.xml) do ścieżki C:
 \ProgramData\Bosch\VRM\primary.

2. Prawym przyciskiem myszy kliknąć ikonę .
3. Wybrać **Importuj konfigurację z VRM**.
Konfiguracja poprzedniego urządzenia VRM jest importowana.

**Uwaga!**

Importowane są tylko konfiguracje nadajnika, VSG i iSCSI.

Należy ponownie wykonać wszystkie inne czynności konfiguracyjne, na przykład dodać wymagane urządzenia do **Drzewo logiczne**, skonfigurować alarmy lub ustawienia nagrywania.

13.22

Strona puli

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > 

Umożliwia skonfigurowanie ustawień zapisu ważnych dla wszystkich urządzeń, które są zgromadzone w tej puli pamięci.

Identyfikacja puli

Wyświetlany jest tu numer puli.

Tryb preferencji zapisu

- **Przełączenie awaryjne**
Nagrania są zapisywane tylko w lokalizacji podstawowej. Jeśli zapis w tej lokalizacji nie będzie możliwy, nagranie zostanie zapisane w lokalizacji drugorzędnej.
Do sytuacji awaryjnej dochodzi, gdy lokalizacja podstawowa nie dostarcza bloków pamięci, np. wskutek awarii systemu, błędu sieci czy braku wolnych zasobów.
Lista lokalizacji drugorzędnej może pozostać pusta. W takim przypadku nie jest możliwy zapis awaryjny, ale liczba wymaganych sesji iSCSI jest mniejsza i lokalizacji drugorzędnej nie jest przydzielona żadna przestrzeń dyskowa. To zmniejsza obciążenie systemu i wydłuża czas przechowywania danych w systemie.
Uwaga: W przypadku każdej kamery i nadajnika należy skonfigurować lokalizację podstawową i drugorzędną.
- **Automatyczny**
Równoważenie obciążenia jest konfigurowane automatycznie. Tryb **automatyczny** automatycznie podejmuje próbę optymalizacji czasu pod przechowywania dostępnych lokalizacji iSCSI. Aby przydzielić bloki drugiego lokalizacji pomocniczej iSCSI, należy wybrać opcję **On (Wł.)** na liście **Użycie lokalizacji drugorzędnej**.

Okres testu poprawności działania (w dniach)

Wprowadź wymagany okres. Po upływie tego czasu program Video Recording Manager przeanalizuje, czy podział magazynu w trybie **automatycznym** jest nadal optymalny. Jeśli nie, program Video Recording Manager wprowadzi zmiany.

Wykorzystanie lokalizacji drugorzędnej

Umożliwia określenie, czy bloki są rozmieszczone z drugiej lokalizacji docelowej.

Wybrać **Wł.** lub **Wył.** w celu włączenia lub wyłączenia użycia dodatkowej lokalizacji docelowej.

- **Wł.:** Wybrać **Wł.**, aby używać dodatkowej lokalizacji docelowej w celu skrócenia przerwy w zapisie w przypadku awarii w lokalizacji podstawowej. Jeśli dostępna jest lokalizacja podstawowa, bloki w lokalizacji drugorzędnej nie są używane, ale przestrzeń dyskowa jest przydzielona. Ta nadmiarowość skraca czas pod przechowywania systemu.

- **Wył.:** Wybrać **Wył.**, jeśli użytkownik nie chce używać lokalizacji drugorzędnej. W przypadku niepowodzenia w realizacji celu głównego program Video Recording Manager będzie potrzebować więcej czasu na reorganizację. Oznacza to, że przerwa w zapisie będzie większa.

Rezerwacja bloku na czas przestoju

Wprowadzić liczbę dni, w ciągu których informacje z przypisanych nadajników mają być zapisywane mimo awarii VRM Server.

Przykład: w przypadku wpisania 4, informacje z nadajników będą zapisywane przez około 4 dni od czasu awarii VRM Server.

Jeśli system korzysta z nadajników o małej przepływności, możliwe jest znaczne ograniczenie ilości wstępnie przydzielonej przestrzeni na dysku. Zapewnia to odpowiednie rozdzielenie pojemności pamięci i wydłuża czas przechowywania.

Zezwalaj na jednostki LUN o rozmiarze przekraczającym 2 TB

Kliknij, aby umożliwić korzystanie z jednostek LUN większych niż 2 TB.

Jednostki LUN większe niż 2 TB („duże jednostki LUN”) nie są obsługiwane przez następujące urządzenia:

- Urządzenia VRM z oprogramowaniem układowym w wersji starszej niż 3.60
- Urządzenia VSG z oprogramowaniem układowym w wersji starszej niż 6.30
- Nadajniki z oprogramowaniem układowym w wersji starszej niż 6.30

System BVMS zapobiega wykonywaniu następujących czynności:

- Dodawanie lub przenoszenie urządzeń z oprogramowaniem układowym w wersji starszej niż 6.30 do puli, która umożliwia stosowanie dużych jednostek LUN.
- Dodawanie lub przenoszenie urządzeń, które nie mają obecnie połączenia z siecią, do puli, która umożliwia stosowanie dużych jednostek LUN.
- Dodawanie lub przenoszenie urządzenia iSCSI, które zawierają duże jednostki LUN, do puli, która nie umożliwia stosowania dużych jednostek LUN.
- Zezwalanie na użycie dużych jednostek LUN w puli, która zawiera urządzenia z oprogramowaniem układowym w wersji starszej niż 6.30.
- Wyłączanie dużych jednostek LUN w puli z urządzeniem iSCSI, które zawiera duże jednostki LUN.

Urządzenia z oprogramowaniem układowym w wersji starszej niż 6.30 należy przenieść do puli, która nie zezwala na użycie dużych jednostek LUN.

Patrz

- Dodawanie jednostki LUN, Strona 196
- Dodawanie puli VRM, Strona 175

13.22.1

Konfigurowanie automatycznego trybu zapisu dla puli

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > 

Uwaga:

Jeżeli wcześniej skonfigurowano tryb zapisu awaryjnego, ta konfiguracja zostanie nadpisana.

Aby przeprowadzić konfigurację:

- ▶ Na liście **Tryb preferencji nagrywania** wybierz pozycję **Auto**.
Po uaktywnieniu konfiguracji włączony będzie tryb zapisu **Auto**. Na stronie **Preferencje zapisu** nadajnika lista lokalizacji podstawowej i pomocniczej jest wyłączona.

Tematy pokrewne

- Konfigurowanie trybu zapisu awaryjnego w nadajniku, Strona 232

13.22.2

Ręczne dodawanie nadajnika

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > kliknij prawym przyciskiem myszy

 > kliknij **Dodaj nadajnik** > okno dialogowe **Dodaj nadajnik**

lub

Okno główne > **Urządzenia** > kliknij prawym przyciskiem myszy  > kliknij **Dodaj nadajnik** > okno dialogowe **Dodaj nadajnik**

lub

Okno główne > **Urządzenia** > kliknij prawym przyciskiem myszy  > kliknij **Dodaj nadajnik** > okno dialogowe **Dodaj nadajnik**

lub

Okno główne > **Urządzenia** > rozwiń  > kliknij prawym przyciskiem myszy  > kliknij **Dodaj odbiornik** > okno dialogowe **Dodaj nadajnik**

Umożliwia ręczne dodanie nadajnika. Jest to szczególnie użyteczne, gdy chce się dodać sieciowe urządzenie wizyjne firmy Bosch (tylko dla VRM).

Uwaga:

W przypadku dodawania nadajnika strumienia wideo firmy Bosch za pomocą funkcji <**Automatyczne wykrywanie**> to urządzenie musi być dostępne w sieci.

Aby dodać sieciowe urządzenie wizyjne firmy Bosch:

1. Rozwiń , rozwiń , kliknąć prawym przyciskiem myszy .

lub
Kliknąć prawym przyciskiem myszy .

lub
Kliknąć prawym przyciskiem myszy .

2. Kliknąć **Dodaj nadajnik**.
Zostanie wyświetlone okno dialogowe **Dodaj nadajnik**.
3. Wprowadzić prawidłowy adres IP.
4. Na liście zaznaczyć pozycję <**Automatyczne wykrywanie**>, wprowadź hasło dostępu do urządzenia i kliknij przycisk **Uwierzytelnij**.
Lub
Na liście zaznaczyć określony typ nadajnika lub <**Symbol zastępczy jednej kamery**>.
5. Kliknij **OK**.
Urządzenie zostanie dodane do systemu.

Ikona  oznacza błąd, którym należy się zająć. Więcej informacji o charakterze błędu uzyskasz z etykiety narzędzia.

Okno dialogowe Dodaj nadajnik**Adres sieciowy**

Wpisz poprawny adres IP.

Numer portu

Wpisać numer portu urządzenia.

Typ nadajnika

W przypadku urządzeń, których typ jest znany, wybierz odpowiednią pozycję. Urządzenie nie musi być dostępne w sieci.

Dodając sieciowe urządzenie wizyjne firmy Bosch, zaznacz opcję **<Automatyczne wykrywanie>**.

Urządzenie musi być dostępne w sieci.

Aby dodać kamerę w konfiguracji offline, wybierz opcję **<Symbol zastępczy jednej kamery>**.

Nazwa użytkownika

Wyświetla nazwę użytkownika używaną w celu uwierzytelniania w urządzeniu.

Hasło

Wprowadź poprawne hasło używane do uwierzytelniania w urządzeniu.

Pokaż hasło

Kliknij, aby włączyć opcję wyświetlania wprowadzonego hasła. Uważaj, aby osoby postronne nie poznały tego hasła.

Uwierzytelnij

Kliknąć, aby uwierzytelnić w urządzeniu z wykorzystaniem wprowadzonych powyżej poświadczeń.

13.22.3**Ręczne dodawanie urządzenia iSCSI**

Okno główne > **Urządzenia** >  > Rozwiń  > Kliknij prawym przyciskiem myszy  >

Dodaj urządzenie iSCSI > Okno dialogowe **Dodaj urządzenie iSCSI**

Umożliwia dodawanie urządzeń iSCSI do VRM.

Aby dodać urządzenie iSCSI:

1. Kliknij prawym przyciskiem myszy  i wybierz **Dodaj urządzenie iSCSI**.
Zostanie wyświetlone okno dialogowe **Dodaj urządzenie iSCSI**.
2. Wpisz nazwę żadanego wyświetlacza, adres sieciowy urządzenia iSCSI i typ urządzenia, a następnie kliknij **OK**.
Urządzenie iSCSI jest dodawane do wybranej puli VRM.
W razie potrzeby dodaj cele i jednostki LUN.

Okno dialogowe Dodaj urządzenie iSCSI**Nazwa**

Wpisać wyświetlaną nazwę urządzenia.

Adres sieciowy

Wpisać poprawny adres sieciowy urządzenia.

Typ urządzenia iSCSI

Wybrać odpowiedni typ urządzenia.

Nazwa użytkownika

Wprowadź nazwę użytkownika w celu uwierzytelnienia.

Hasło

Wprowadź hasło w celu uwierzytelnienia.

Włącz monitorowanie

Jeśli urządzenie DIVAR IP jest wybrane jako typ urządzenia iSCSI i jakiegokolwiek monitoring SNMP (Simple Network Management Protocol) jest obsługiwany w odniesieniu do typu urządzenia DIVAR IP, pole wyboru **Włącz monitorowanie** jest zaznaczone.

Zaznaczyć pole wyboru, aby włączyć monitorowanie stanu urządzenia DIVAR IP. System BVMS automatycznie odbiera i analizuje komunikaty SNMP z urządzenia DIVAR IP i aktywuje zdarzenia i alarmy monitorowania stanu (np. CPU, pamięć masowa, wiatrak itd.). Domyślnie wyzwalane są tylko alarmy krytyczne.

Uwaga: należy najpierw skonfigurować SNMP na urządzeniu DIVAR IP.

Uwaga: to ustawienie jest dostępne tylko na obsługiwanych urządzeniach.

Aby uzyskać więcej informacji na temat konfigurowania SNMP na urządzeniu DIVAR IP, należy odwołać się do odpowiedniej dokumentacji DIVAR IP.

Tematy pokrewne

- Dodawanie urządzeń VRM poprzez skanowanie; Strona 169

Patrz

- strona SNMP, Strona 154
- Konfigurowanie monitorowania SNMP, Strona 95

13.22.4

Ręczne dodawanie urządzenia Video Streaming Gateway

Okno główne > **Urządzenia** > rozwiń  > 

Do puli VRM można dodawać urządzenia VSG.

Aby dodać ręcznie urządzenie VSG:

1. Kliknąć prawym przyciskiem myszy , a następnie kliknąć polecenie **Dodaj komponent Video Streaming Gateway**.
Pojawi się okno dialogowe **Dodaj komponent Video Streaming Gateway**.
 2. Wpisać wymagane ustawienia w urządzeniu VSG.
 3. Kliknąć **Dodaj**.
- ⇒ Urządzenie VSG zostanie dodane do systemu. Zostaną zapisane kamery przypisane do tego urządzenia VSG.

Okno dialogowe Dodaj komponent Video Streaming Gateway

Kliknij  prawym przyciskiem myszy > **Dodaj komponent Video Streaming Gateway** > okno dialogowe **Dodaj komponent Video Streaming Gateway**

Numer portu

Wpisać numer portu urządzenia.

Nazwa użytkownika

Wprowadź nazwę użytkownika używaną do uwierzytelniania w urządzeniu. Zwykle: service.

Adres/port sieciowy

Wprowadzić adres IP urządzenia.

Jeśli pole wyboru **Zabezpiecz połączenie** jest zaznaczone, port zmienia się automatycznie na HTTPS.

Numer portu można zmienić, jeśli nie jest wykorzystywany port domyślny, lub instancje VSG są skonfigurowane w innej kolejności.

Domyślne porty

Instancja VSG	port rcpp	Port HTTPS
1	8756	8443
2	8757	8444
3	8758	8445
4	8759	8446
5	8760	8447
6	8761	8448
7	8762	8449

Hasło

Wprowadź poprawne hasło używane do uwierzytelniania w urządzeniu.

Show password

Kliknąć, aby włączyć opcję wyświetlania wprowadzonego hasła. Uważaj, aby osoby postronne nie poznały tego hasła.

Bezpieczeństwo

Pole wyboru **Zabezpiecz połączenie** jest zaznaczone domyślnie, jeśli protokół HTTPS jest obsługiwany.

Z wersji VSG 7.0, VSG obsługuje bezpieczne połączenie.

**Uwaga!**

W przypadku przejścia na system BVMS w wersji 10.0 lub nowszej, pole wyboru **Zabezpiecz połączenie** nie jest domyślnie zaznaczone i połączenie jest niezabezpieczone (rcpp).

Aby zmienić połączenie bezpieczne lub niezabezpieczone, należy użyć polecenia **Edytuj komponent Video Streaming Gateway** i zaznaczyć pole wyboru **Zabezpiecz połączenie** lub usunąć zaznaczenie.

Uwierzytelnij

Kliknąć, aby uwierzytelnić w urządzeniu z wykorzystaniem wprowadzonych powyżej poświadczeń.

Patrz

– Edytowanie komponentu Video Streaming Gateway, Strona 200

13.22.5**Ręczne dodawanie urządzenia iSCSI DSA E-Series**

Okno główne > **Urządzenia** > > rozwiń węzeł

Można dodać albo urządzenie iSCSI E-Series, które jest już zainicjowane, albo urządzenie iSCSI E-Series, które jeszcze nie jest zainicjowane.

Można dodawać jednostki LUN większe niż 2 TB, jeśli włączono w puli stosowanie dużych jednostek LUN.

Jednostki LUN większe niż 2 TB („duże jednostki LUN”) nie są obsługiwane przez następujące urządzenia:

- Urządzenia VRM z oprogramowaniem układowym w wersji starszej niż 3.60
- Urządzenia VSG z oprogramowaniem układowym w wersji starszej niż 6.30
- Nadajniki z oprogramowaniem układowym w wersji starszej niż 6.30

System BVMS zapobiega wykonywaniu następujących czynności:

- Dodawanie lub przenoszenie urządzeń z oprogramowaniem układowym w wersji starszej niż 6.30 do puli, która umożliwia stosowanie dużych jednostek LUN.
- Dodawanie lub przenoszenie urządzeń, które nie mają obecnie połączenia z siecią, do puli, która umożliwia stosowanie dużych jednostek LUN.
- Dodawanie lub przenoszenie urządzenia iSCSI, które zawierają duże jednostki LUN, do puli, która nie umożliwia stosowania dużych jednostek LUN.
- Zezwalanie na użycie dużych jednostek LUN w puli, która zawiera urządzenia z oprogramowaniem układowym w wersji starszej niż 6.30.
- Wyłączanie dużych jednostek LUN w puli z urządzeniem iSCSI, które zawiera duże jednostki LUN.

Urządzenia z oprogramowaniem układowym w wersji starszej niż 6.30 należy przenieść do puli, która nie zezwala na użycie dużych jednostek LUN.

Aby dodać zainicjowane urządzenie iSCSI:



1. Kliknij prawym przyciskiem myszy ikonę , a następnie wybierz polecenie **Dodaj urządzenie DSA E-Series**.
Zostanie wyświetlone okno dialogowe **Dodaj urządzenie DSA E-Series**.
2. Wpisz adres IP do zarządzania i hasło.
3. Kliknij przycisk **Połącz**.
Po nawiązaniu połączenia zostaną wypełnione pola w grupie **Kontroler** i/lub **2. kontroler**.
4. Kliknąć **OK**.
Urządzenie zostanie dodane do systemu.
Dostępne lokalizacje docelowe są automatycznie skanowane, czego efektem jest wyświetlenie jednostek LUN.
Można użyć urządzenia iSCSI.
Jeśli w puli włączone jest użycie dużych jednostek LUN, a urządzenie iSCSI ma skonfigurowane duże jednostki LUN, w kolumnie **Duża jednostka LUN** wyświetlany jest znacznik wyboru w przypadku odpowiednich jednostek LUN.

Aby dodać niezainicjowane urządzenie iSCSI:



1. Kliknij prawym przyciskiem myszy ikonę , a następnie wybierz polecenie **Dodaj urządzenie DSA E-Series**.
Zostanie wyświetlone okno dialogowe **Dodaj urządzenie DSA E-Series**.
2. Wpisz adres IP do zarządzania i hasło.
3. Kliknij przycisk **Połącz**.
Po nawiązaniu połączenia zostaną wypełnione pola w grupie **Kontroler** i/lub **2. kontroler**.
4. Kliknąć **OK**.
Urządzenie zostanie dodane do systemu.
5. Kliknąć , a następnie kliknąć .
6. Kliknij kartę **Konfiguracja podstawowa**.
7. Wpisz odpowiednią pojemność jednostki LUN.
Po wpisaniu wartości przekraczającej 2 TB należy włączyć w puli opcję stosowania jednostek LUN większych niż 2 TB.
8. Kliknij przycisk **Inicjalizacja**.
Nastąpi utworzenie jednostek LUN.
9. Kliknij **Zamknij**.

10. Kliknij urządzenie iSCSI prawym przyciskiem myszy, a następnie wybierz polecenie **Cel skanowania**.
Jednostki LUN są wyświetlane z nieznanym stanem.
11. Zapisz i uaktywnij konfigurację.
12. Sformatuj wszystkie jednostki LUN.
13. Jeśli zostało dodane urządzenie iSCSI z podwójnym kontrolerem, usuń odpowiednie jednostki LUN z pierwszego kontrolera, kliknij prawym przyciskiem myszy drugi kontroler, a następnie wybierz polecenie **Cel skanowania**, aby dodać te jednostki LUN.

Okno dialogowe Dodaj urządzenie DSA E-Series

Okno główne > **Urządzenia** >  > Rozwiń  > Kliknij prawym przyciskiem myszy  >

Dodaj urządzenie DSA E-Series > Okno dialogowe **Dodaj urządzenie DSA E-Series**

Umożliwia dodanie urządzenia iSCSI DSA E-Series. Adres IP do zarządzania w urządzeniach tego typu jest inny niż adres IP pamięci masowej iSCSI. Za pośrednictwem tego adresu IP do zarządzania odbywa się automatyczne wykrywanie i konfigurowanie urządzenia.

Nazwa

Wpisz wyświetlaną nazwę urządzenia.

Adres do zarządzania

Wpisz adres IP potrzebny do automatycznej konfiguracji urządzenia.

Hasło:

Wpisać hasło danego urządzenia.

Typ DSA E-Series

Wyświetla typ urządzenia.

Adres sieciowy kanału iSCSI

Wyświetla adres IP urządzenia iSCSI. Można wybrać inny adres IP, o ile jest dostępny.

Adres do zarządzania

Wyświetla adres IP do automatycznej konfiguracji drugiego sterownika, o ile jest dostępny. Można wybrać inny adres IP, o ile jest dostępny.

Adres sieciowy kanału iSCSI

Wyświetla adres IP portu iSCSI drugiego sterownika, o ile jest dostępny. Można wybrać inny adres IP, o ile jest dostępny.

Połącz

Kliknij w celu wykrycia ustawień danego urządzenia.

W przypadku nawiązania połączenia pola w grupach **Sterownik** i **2 Sterownik** zostaną wypełnione.

Patrz

- Strona Konfiguracja podstawowa, Strona 194
- Formatowanie urządzenia o określonym numerze LUN, Strona 198

13.22.6

Dodawanie nadajników poprzez skanowanie

Aby dodać nadajniki poprzez skanowanie:

1. Kliknij prawym przyciskiem myszy , a następnie kliknij **Skanuj w poszukiwaniu nadajników**.
Zostanie wyświetlone okno dialogowe **BVMS Scan Wizard**.

- Wybierz wymagane nadajniki oraz żadaną pulę VRM, a następnie kliknij **Przypisz**, aby przypisać nadajniki do puli VRM.
- Kliknij **Dalej >>**.
Zostanie wyświetlone okno dialogowe kreatora **Uwierzytelnianie urządzeń**.
- Wpisać hasło w przypadku każdego urządzenia, które jest nim chronione.
Jeśli przez kilka sekund nie wprowadzisz żadnego znaku w polu hasła lub klikniesz poza tym polem, sprawdzenie hasła następuje automatycznie.
Jeśli hasło do wszystkich urządzeń jest identyczne, można wpisać je w pierwszym polu **Hasło**.
Następnie kliknij to pole prawym przyciskiem myszy i kliknij polecenie **Kopiuj komórkę do kolumny**.



Udane logowanie jest oznaczane w kolumnie **Stan** ikoną .



Nieudane próby logowania są oznaczane ikoną .

- Kliknąć **Zakończ**.
Urządzenie zostanie dodane do drzewa urządzeń.

Ikona  oznacza błąd, którym należy się zająć. Więcej informacji o charakterze błędu uzyskasz z etykiety narzędzia.

13.22.7

Dodawanie urządzeń VSG poprzez skanowanie

Aby poprzez skanowanie dodać urządzenia VSG:



- Kliknij prawym przyciskiem myszy , a następnie kliknij **Skanuj w poszukiwaniu bram Video Streaming Gateway**.
Zostanie wyświetlone okno dialogowe **BVMS Scan Wizard**.
- Wybierz wymagane urządzenia VSG i żadaną pulę VRM, a następnie kliknij **Przypisz**, aby przypisać nadajniki do puli VRM.
- Kliknij **Dalej >>**.
Zostanie wyświetlone okno dialogowe kreatora **Uwierzytelnianie urządzeń**.
- Wpisać hasło w przypadku każdego urządzenia, które jest nim chronione.
Jeśli przez kilka sekund nie wprowadzisz żadnego znaku w polu hasła lub klikniesz poza tym polem, sprawdzenie hasła następuje automatycznie.
Jeśli hasło do wszystkich urządzeń jest identyczne, można wpisać je w pierwszym polu **Hasło**.
Następnie kliknąć to pole prawym przyciskiem myszy i wybrać opcję **Kopiuj komórkę do kolumny**.



Udane logowanie jest oznaczane w kolumnie **Stan** ikoną .



Nieudane próby logowania są oznaczane ikoną .

- Kliknąć **Zakończ**.
Urządzenie zostanie dodane do drzewa urządzeń.

13.22.8

Konfigurowanie podwójnego zapisu w drzewie urządzeń



Okno główne > **Urządzenia** > rozwinięte > podwójny zapis
Aby móc skonfigurować podwójny zapis, należy wyłączyć funkcję ANR.

Jeśli zostanie skonfigurowany podwójny zapis dla jednej kamery wielokanałowego nadajnika, system zapewni to samo miejsce docelowe zapisu dla wszystkich kamer tego nadajnika.

Podwójny zapis można skonfigurować, przypisując nadajniki związane z podstawowym VRM do pomocniczego VRM. Jest to użyteczne na przykład wtedy, gdy chce się przypisać tylko część nadajników zapisywanych przez podstawowy VRM.

Pomocniczy VRM musi być już dodany.

Aby przeprowadzić konfigurację:

1. Kliknąć prawym przyciskiem myszy  i wybrać **Dodaj nadajnik z głównego urządzenia VRM**.
Wyświetlone zostanie okno dialogowe **Dodaj nadajniki**.
2. Kliknąć przycisk, aby wybrać żądane nadajniki.
Po wybraniu puli lub VRM, automatycznie wybierane są wszystkie elementy podrzędne.
3. Kliknąć **OK**.
Zaznaczone nadajniki są dodawane do pomocniczego VRM.

Patrz

- Konfigurowanie podwójnego zapisu w tabeli kamery, Strona 303
- Konfigurowanie funkcji ANR, Strona 302
- Zapis podwójny / awaryjny, Strona 30

13.23

Strona Bosch Encoder / Decoder (Nadajnik/odbiornik firmy Bosch)

Aby skonfigurować nadajnik/odbiornik firmy Bosch, patrz Strona Bosch Encoder / Decoder / Camera (Nadajnik/odbiornik/kamera firmy Bosch), Strona 215.

13.24

Strona urządzenia iSCSI

Okno główne > **Urządzenia** > rozwiń opcję  > rozwiń opcję  > rozwiń opcję  >
rozwiń opcję 

Można dodać urządzenie iSCSI z serii E lub inne obsługiwane urządzenie iSCSI.

Patrz

- Ręczne dodawanie urządzenia iSCSI, Strona 189
- Ręczne dodawanie urządzenia iSCSI DSA E-Series, Strona 190
- Konfiguracja urządzenia iSCSI, Strona 192
- Dodawanie jednostki LUN, Strona 196
- Formatowanie urządzenia o określonym numerze LUN, Strona 198

13.24.1

Pula pamięci iSCSI

Pula pamięci może służyć do logicznego odwzorowywania topologii sieci w systemie Video Recording Manager. Na przykład: gdy mamy dwa budynki, oba wyposażone w pamięć oraz urządzenia, i chcemy uniknąć trasowania ruchu w sieci z jednego budynku do drugiego.

Pule pamięci mogą też być używane w celu grupowania kamer i systemów pamięci masowej zależnie od ważnego aspektu wyświetlania. Na przykład, gdy system zawiera bardzo ważne kamery i dużo kamer o mniejszym znaczeniu. W tym przypadku możliwe jest przydzielenie ich do dwóch osobnych pul pamięci, z których jedna cechuje się dużą, a druga mniejszą nadmiarowością.

Dla puli pamięci można skonfigurować następujące właściwości równoważenia obciążenia:

- Preferencje zapisu (**Automatyczny** lub **Przełączenie awaryjne**)

- Użycie lokalizacji drugorzędnej

Lokalizacja drugorzędna jest używana w przypadku trybu **Przełączenie awaryjne** w razie awarii lokalizacji podstawowej. Jeśli ta opcja jest wyłączona, zapis zostaje wyłączony na wszystkich urządzeniach przypisanych do uszkodzonej lokalizacji podstawowej.

W przypadku trybu **Automatyczny**: jeśli jedna lokalizacja ulegnie awarii, moduł VRM Server wykonuje automatyczne ponowne przypisanie powiązanych urządzeń do innych pamięci. Jeśli moduł VRM Server nie będzie działał, gdy lokalizacja docelowa ulegnie awarii, zapis z urządzeń, które aktualnie dokonują zapisu w uszkodzonej lokalizacji docelowej, zostanie zatrzymany.

- Rezerwacja bloku na czas przestoju
- Okres sprawdzania sprawności systemu

W przypadku każdej puli można skonfigurować zezwalanie na użycie jednostek LUN większych niż 2 TB.

Jednostki LUN większe niż 2 TB („duże jednostki LUN”) nie są obsługiwane przez następujące urządzenia:

- Urządzenia VRM z oprogramowaniem układowym w wersji starszej niż 3.60
- Urządzenia VSG z oprogramowaniem układowym w wersji starszej niż 6.30
- Nadajniki z oprogramowaniem układowym w wersji starszej niż 6.30

System BVMS zapobiega wykonywaniu następujących czynności:

- Dodawanie lub przenoszenie urządzeń z oprogramowaniem układowym w wersji starszej niż 6.30 do puli, która umożliwia stosowanie dużych jednostek LUN.
- Dodawanie lub przenoszenie urządzeń, które nie mają obecnie połączenia z siecią, do puli, która umożliwia stosowanie dużych jednostek LUN.
- Dodawanie lub przenoszenie urządzenia iSCSI, które zawierają duże jednostki LUN, do puli, która nie umożliwia stosowania dużych jednostek LUN.
- Zezwalanie na użycie dużych jednostek LUN w puli, która zawiera urządzenia z oprogramowaniem układowym w wersji starszej niż 6.30.
- Wyłączanie dużych jednostek LUN w puli z urządzeniem iSCSI, które zawiera duże jednostki LUN.

Urządzenia z oprogramowaniem układowym w wersji starszej niż 6.30 należy przenieść do puli, która nie zezwala na użycie dużych jednostek LUN.

Jeśli główny rejestrator VRM zawiera pulę, która umożliwia stosowanie dużych jednostek LUN, odpowiedni nadmiarowy rejestrator VRM przejmuje to ustawienie i nie można zaznaczyć ani usunąć zaznaczenia pola wyboru **Zezwalaj na jednostki LUN o rozmiarze przekraczającym 2 TB** związanego z odpowiednią pulą nadmiarowego rejestratora VRM. Po dodaniu do nadmiarowego rejestratora VRM urządzenia iSCSI zawierającego duże jednostki LUN nie można usunąć zaznaczenia pola wyboru **Zezwalaj na jednostki LUN o rozmiarze przekraczającym 2 TB** związanego z odpowiednią pulą głównego rejestratora VRM.

Patrz

- Strona puli, Strona 179

13.24.2

Ręczne dodawanie urządzenia iSCSI

Okno główne > **Urządzenia** >  > Rozwiń  > Kliknij prawym przyciskiem myszy  > **Dodaj urządzenie iSCSI** > Okno dialogowe **Dodaj urządzenie iSCSI**

Umożliwia dodawanie urządzeń iSCSI do VRM.

Aby dodać urządzenie iSCSI:

1. Kliknij prawym przyciskiem myszy  i wybierz **Dodaj urządzenie iSCSI**.
Zostanie wyświetlone okno dialogowe **Dodaj urządzenie iSCSI**.
2. Wpisz nazwę żadanego wyświetlacza, adres sieciowy urządzenia iSCSI i typ urządzenia, a następnie kliknij **OK**.
Urządzenie iSCSI jest dodawane do wybranej puli VRM.
W razie potrzeby dodaj cele i jednostki LUN.

Okno dialogowe Dodaj urządzenie iSCSI**Nazwa**

Wpisać wyświetlaną nazwę urządzenia.

Adres sieciowy

Wpisać poprawny adres sieciowy urządzenia.

Typ urządzenia iSCSI

Wybrać odpowiedni typ urządzenia.

Nazwa użytkownika

Wprowadź nazwę użytkownika w celu uwierzytelnienia.

Hasło

Wprowadź hasło w celu uwierzytelnienia.

Włącz monitorowanie

Jeśli urządzenie DIVAR IP jest wybrane jako typ urządzenia iSCSI i jakiegokolwiek monitoring SNMP (Simple Network Management Protocol) jest obsługiwany w odniesieniu do typu urządzenia DIVAR IP, pole wyboru **Włącz monitorowanie** jest zaznaczone.

Zaznaczyć pole wyboru, aby włączyć monitorowanie stanu urządzenia DIVAR IP. System BVMS automatycznie odbiera i analizuje komunikaty SNMP z urządzenia DIVAR IP i aktywuje zdarzenia i alarmy monitorowania stanu (np. CPU, pamięć masowa, wiatrak itd.). Domyślnie wyzwalane są tylko alarmy krytyczne.

Uwaga: należy najpierw skonfigurować SNMP na urządzeniu DIVAR IP.

Uwaga: to ustawienie jest dostępne tylko na obsługiwanych urządzeniach.

Aby uzyskać więcej informacji na temat konfigurowania SNMP na urządzeniu DIVAR IP, należy odwołać się do odpowiedniej dokumentacji DIVAR IP.

Tematy pokrewne

- Dodawanie urządzeń VRM poprzez skanowanie:, Strona 169

Patrz

- strona SNMP, Strona 154
- Konfigurowanie monitorowania SNMP, Strona 95

13.24.3**Ręczne dodawanie urządzenia iSCSI DSA E-Series**

Okno główne > **Urządzenia** >  > rozwiń węzeł  > 

Można dodać albo urządzenie iSCSI E-Series, które jest już zainicjowane, albo urządzenie iSCSI E-Series, które jeszcze nie jest zainicjowane.

Można dodawać jednostki LUN większe niż 2 TB, jeśli włączono w puli stosowanie dużych jednostek LUN.

Jednostki LUN większe niż 2 TB („duże jednostki LUN”) nie są obsługiwane przez następujące urządzenia:

- Urządzenia VRM z oprogramowaniem układowym w wersji starszej niż 3.60

- Urządzenia VSG z oprogramowaniem układowym w wersji starszej niż 6.30
- Nadajniki z oprogramowaniem układowym w wersji starszej niż 6.30

System BVMS zapobiega wykonywaniu następujących czynności:

- Dodawanie lub przenoszenie urządzeń z oprogramowaniem układowym w wersji starszej niż 6.30 do puli, która umożliwia stosowanie dużych jednostek LUN.
- Dodawanie lub przenoszenie urządzeń, które nie mają obecnie połączenia z siecią, do puli, która umożliwia stosowanie dużych jednostek LUN.
- Dodawanie lub przenoszenie urządzenia iSCSI, które zawierają duże jednostki LUN, do puli, która nie umożliwia stosowania dużych jednostek LUN.
- Zezwalanie na użycie dużych jednostek LUN w puli, która zawiera urządzenia z oprogramowaniem układowym w wersji starszej niż 6.30.
- Wyłączanie dużych jednostek LUN w puli z urządzeniem iSCSI, które zawiera duże jednostki LUN.

Urządzenia z oprogramowaniem układowym w wersji starszej niż 6.30 należy przenieść do puli, która nie zezwala na użycie dużych jednostek LUN.

Aby dodać zainicjowane urządzenie iSCSI:



1. Kliknij prawym przyciskiem myszy ikonę , a następnie wybierz polecenie **Dodaj urządzenie DSA E-Series**.

Zostanie wyświetlone okno dialogowe **Dodaj urządzenie DSA E-Series**.

2. Wpisz adres IP do zarządzania i hasło.

3. Kliknij przycisk **Połącz**

Po nawiązaniu połączenia zostaną wypełnione pola w grupie **Kontroler** i/lub **2. kontroler**.

4. Kliknąć **OK**.

Urządzenie zostanie dodane do systemu.

Dostępne lokalizacje docelowe są automatycznie skanowane, czego efektem jest wyświetlenie jednostek LUN.

Można użyć urządzenia iSCSI.

Jeśli w puli włączone jest użycie dużych jednostek LUN, a urządzenie iSCSI ma skonfigurowane duże jednostki LUN, w kolumnie **Duża jednostka LUN** wyświetlany jest znacznik wyboru w przypadku odpowiednich jednostek LUN.

Aby dodać niezainicjowane urządzenie iSCSI:



1. Kliknij prawym przyciskiem myszy ikonę , a następnie wybierz polecenie **Dodaj urządzenie DSA E-Series**.

Zostanie wyświetlone okno dialogowe **Dodaj urządzenie DSA E-Series**.

2. Wpisz adres IP do zarządzania i hasło.

3. Kliknij przycisk **Połącz**

Po nawiązaniu połączenia zostaną wypełnione pola w grupie **Kontroler** i/lub **2. kontroler**.

4. Kliknąć **OK**.

Urządzenie zostanie dodane do systemu.



5. Kliknąć , a następnie kliknąć .

6. Kliknij kartę **Konfiguracja podstawowa**.

7. Wpisz odpowiednią pojemność jednostki LUN.

Po wpisaniu wartości przekraczającej 2 TB należy włączyć w puli opcję stosowania jednostek LUN większych niż 2 TB.

8. Kliknij przycisk **Inicjalizacja**.

Nastąpi utworzenie jednostek LUN.

9. Kliknij **Zamknij**.
10. Kliknij urządzenie iSCSI prawym przyciskiem myszy, a następnie wybierz polecenie **Cel skanowania**.
Jednostki LUN są wyświetlane z nieznanym stanem.
11. Zapisz i uaktywnij konfigurację.
12. Sformatuj wszystkie jednostki LUN.
13. Jeśli zostało dodane urządzenie iSCSI z podwójnym kontrolerem, usuń odpowiednie jednostki LUN z pierwszego kontrolera, kliknij prawym przyciskiem myszy drugi kontroler, a następnie wybierz polecenie **Cel skanowania**, aby dodać te jednostki LUN.

Okno dialogowe Dodaj urządzenie DSA E-Series

Okno główne > **Urządzenia** >  > Rozwiń  > Kliknij prawym przyciskiem myszy  > **Dodaj urządzenie DSA E-Series** > Okno dialogowe **Dodaj urządzenie DSA E-Series**
Umożliwia dodanie urządzenia iSCSI DSA E-Series. Adres IP do zarządzania w urządzeniach tego typu jest inny niż adres IP pamięci masowej iSCSI. Za pośrednictwem tego adresu IP do zarządzania odbywa się automatyczne wykrywanie i konfigurowanie urządzenia.

Nazwa

Wpisz wyświetlaną nazwę urządzenia.

Adres do zarządzania

Wpisz adres IP potrzebny do automatycznej konfiguracji urządzenia.

Hasło:

Wpisać hasło danego urządzenia.

Typ DSA E-Series

Wyświetla typ urządzenia.

Adres sieciowy kanału iSCSI

Wyświetla adres IP urządzenia iSCSI. Można wybrać inny adres IP, o ile jest dostępny.

Adres do zarządzania

Wyświetla adres IP do automatycznej konfiguracji drugiego sterownika, o ile jest dostępny. Można wybrać inny adres IP, o ile jest dostępny.

Adres sieciowy kanału iSCSI

Wyświetla adres IP portu iSCSI drugiego sterownika, o ile jest dostępny. Można wybrać inny adres IP, o ile jest dostępny.

Połącz

Kliknij w celu wykrycia ustawień danego urządzenia.

W przypadku nawiązania połączenia pola w grupach **Sterownik** i **2 Sterownik** zostaną wypełnione.

Patrz

- Strona Konfiguracja podstawowa, Strona 194
- Formatowanie urządzenia o określonym numerze LUN, Strona 198

13.24.4

Konfiguracja urządzenia iSCSI

Okno główne > **Urządzenia** > rozwiń węzeł  > rozwiń węzeł  > 

Po dodaniu urządzeń VRM, urządzeń iSCSI i nadajników należy wykonać poniższe czynności, aby upewnić się, że dane wizyjne z nadajników są przechowywane w urządzeniach iSCSI lub mogą być z tych urządzeń odtwarzane:

- Przeprowadź konfigurację domyślną, aby utworzyć numery LUN dla każdej lokalizacji docelowej urządzenia iSCSI.
Ten krok jest opcjonalny. Nie trzeba go wykonywać w przypadku urządzenia iSCSI ze wstępnie skonfigurowanymi numerami LUN.
- Uruchom funkcję skanowania urządzenia iSCSI, aby dodać lokalizacje docelowe i numery LUN do Drzewa urządzeń po wykonanej konfiguracji domyślnej.

Uwaga:

Nie wszystkie urządzenia iSCSI obsługują funkcje konfiguracji domyślnej oraz automatycznego mapowania nazw IQN.

Wymagania:

Urządzenie iSCSI musi być skonfigurowane z użyciem prawidłowych adresów IP.

Aby przeprowadzić podstawową konfigurację urządzenia iSCSI DSA E-Series:

- Rozwiń węzeł odpowiedniego urządzenia VRM  i , a następnie kliknij ikonę  właściwego urządzenia iSCSI.
1. Kliknij kartę **Konfiguracja podstawowa**.
 2. Wpisz odpowiednią pojemność jednostki LUN.
Po wpisaniu wartości przekraczającej 2 TB należy włączyć w puli opcję stosowania jednostek LUN większych niż 2 TB.
 3. Kliknij przycisk **Inicjalizacja**.
Nastąpi utworzenie jednostek LUN.
 4. Kliknij **Zamknij**.
 5. Kliknij urządzenie iSCSI prawym przyciskiem myszy, a następnie wybierz polecenie **Cel skanowania**.
Jednostki LUN są wyświetlane z nieznanym stanem.
 6. Zapisz i uaktywnij konfigurację.
 7. Sformatuj wszystkie jednostki LUN.
 8. Jeśli zostało dodane urządzenie iSCSI z podwójnym kontrolerem, usuń odpowiednie jednostki LUN z pierwszego kontrolera, kliknij prawym przyciskiem myszy drugi kontroler, a następnie wybierz polecenie **Cel skanowania**, aby dodać te jednostki LUN.

Aby przeprowadzić podstawową konfigurację innych urządzeń iSCSI:

1. Kliknij kartę **Konfiguracja podstawowa**.
2. Wpisz odpowiednią liczbę jednostek LUN.
3. Kliknij przycisk **Ustaw**.
Nastąpi utworzenie jednostek LUN.
4. Kliknij przycisk **Zamknij**.
5. Kliknij urządzenie iSCSI prawym przyciskiem myszy, a następnie wybierz polecenie **Cel skanowania**.
Jednostki LUN są wyświetlane z nieznanym stanem.
6. Zapisz i uaktywnij konfigurację.
7. Sformatuj wszystkie jednostki LUN.

Aby przeprowadzić odwzorowanie nazw IQN w przypadku innych urządzeń iSCSI:

1. Rozwiń węzeł odpowiedniego urządzenia VRM  i , a następnie kliknij ikonę właściwego urządzenia iSCSI .
2. Kliknij ikonę  prawym przyciskiem myszy i wybierz polecenie **Mapuj IQN**. Zostanie otwarte okno dialogowe iqn-Mapper i rozpocznie się cały proces. Nadajniki przypisane do wybranego urządzenia VRM są analizowane, a ich nazwy IQN dodawane do danego urządzenia iSCSI.
3. Kliknij ikonę , aby zapisać ustawienia.
4. Kliknij ikonę , aby uaktywnić konfigurację.

Patrz

- Strona Konfiguracja podstawowa, Strona 194
- Okno dialogowe Balans obciążenia, Strona 195
- Okno dialogowe iqn-Mapper, Strona 198
- Formatowanie urządzenia o określonym numerze LUN, Strona 198

13.24.5

Strona Konfiguracja podstawowa

Okno główne > **Urządzenia** > rozwinąć  > rozwinąć  > rozwinąć  > kliknąć  > karta **Konfiguracja podstawowa**

Wyświetlane opcje mogą różnić się w zależności od typu używanego systemu pamięci masowej iSCSI.

Umożliwia przeprowadzenie podstawowej konfiguracji urządzenia iSCSI. Należy utworzyć numery LUN na dysku twardym urządzenia iSCSI i sformatować te numery.

Wyświetlana tylko jeżeli urządzenie jest jednym z systemów zapisu iSCSI obsługiwanych przez Bosch, na przykład DSA lub DLS 1x00.



Uwaga!

Po zakończeniu podstawowej konfiguracji macierzy dyskowych E-Series inicjalizacja systemu może potrwać wiele godzin (lub nawet dni). Na tym etapie nie jest dostępna pełna wydajność i w fazie 1.5 formatowanie może zakończyć się niepowodzeniem.

Pojemność fizyczna [GB]

Informacje dotyczące całkowitej pojemności systemu pamięci masowej.

Liczba jednostek LUN

Istnieje możliwość zmiany liczby jednostek LUN.



Uwaga!

Zmiana liczby jednostek LUN spowoduje, że cały system iSCSI zostanie zreorganizowany i zapisane w nim sekwencje zostaną utracone.

Dlatego przed wprowadzeniem zmian należy sprawdzić nagrania i ewentualnie wykonać kopie zapasowe ważnych sekwencji.

Pojemność nowych jednostek LUN [GB]

Ponieważ liczba 256 jest maksymalną liczbą jednostek LUN macierzy dyskowej, rozmiar LUN-ów nie powinien być ustawiony na zbyt małą wartość. W przeciwnym razie, jeśli zainstalowana zostanie dodatkowa półka, nie będzie można utworzyć więcej LUN-ów.

Dyski rezerwowej lokalizacji docelowej

Liczba dysków rezerwowych, które mają znajdować się w systemie.

Rzeczywiste dyski rezerwowe

Liczba dysków rezerwowych, które aktualnie znajdują się w systemie. Ta liczba może się różnić od powyższej, np. jeśli system pamięci masowej zostanie ponownie skonfigurowany ręcznie lub jeśli dyski są uszkodzone.

Status inicjalizacji (%)

W trakcie inicjowania wyświetlane są dodatkowe informacje. Po ukończeniu inicjowania (100%) można usunąć wszystkie jednostki LUN.

RAID-DP (niezawodność)

Należy uaktywnić tę opcję, jeśli zamiast wyznaczonej macierzy RAID typu RAID-4 ma zostać użyta bardziej niezawodna odmiana RAID-DP.

RAID 6 (niezawodność)

Należy wybrać tę opcję, jeśli zamiast wyznaczonej macierzy RAID typu RAID 5 ma zostać użyta bardziej niezawodna odmiana RAID 6.

Dodatkowe informacje

Wyświetla dodatkowe informacje, np. o tym, że system pamięci masowej jest nieprawidłowo skonfigurowany i uruchomienie go jest niemożliwe.

Patrz

– Ręczne dodawanie urządzenia iSCSI DSA E-Series, Strona 190

13.24.6**Okno dialogowe Balans obciążenia**

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > rozwiń  > kliknij prawym przyciskiem myszy  > polecenie **Równoważenie obciążenia...** > okno dialogowe **Balans obciążenia**

Wymagania: należy skonfigurować tryb zapisu **Automatyczny**.

Należy ustawić górne limity dozwolonej przepływności oraz liczbę jednoczesnych połączeń iSCSI dla każdego systemu iSCSI. W przypadku przekroczenia limitów dane przestaną być zapisywane w systemie iSCSI i nastąpi ich utrata.

W przypadku obsługiwanych systemów (na przykład Bosch RAID, NetApp, DLA) należy użyć wartości domyślnych. W przypadku innych urządzeń należy postępować zgodnie z ich dokumentacją. Testowanie należy rozpocząć od małych wartości.

13.24.7**Przenoszenie systemu iSCSI do innej puli (Zmień pulę...)**

Okno główne > **Urządzenia** > rozwiń węzeł  > rozwiń węzeł  > rozwiń węzeł  > 

W ramach jednego urządzenia VRM można przenosić urządzenia między pulami bez utraty zapisanych materiałów.

Aby przenieść urządzenie:

1. Kliknąć prawym przyciskiem myszy  /  / , a następnie kliknąć **Zmień pulę**
Zostanie wyświetlone okno dialogowe **Zmień pulę**.
2. Wybrać odpowiednią pulę z listy **Nowa pula:**.
3. Kliknąć przycisk **OK**.
Urządzenie zostanie przeniesione do wybranej puli.

13.24.8**Strona Jednostki LUN**

Okno główne > **Urządzenia** > rozwiń węzeł  > rozwiń węzeł  > rozwiń węzeł  >
rozwiń węzeł  > 

Umożliwia dodawanie, usuwanie i formatowanie jednostek LUN oraz wyświetlanie informacji o nich.

Dodaj

Kliknij, aby wyświetlić okno dialogowe **Dodaj numer LUN**.

Usuń

Kliknij, aby usunąć zaznaczone wiersze. Aby zaznaczyć wiersz, kliknij jego nagłówek po lewej stronie.

Każdy wiersz odpowiada jednostce LUN.

Pojawi się okno komunikatu.

Formatuj numer LUN

Kliknij, aby sformatować zaznaczoną jednostkę LUN. Pojawi się okno komunikatu.

Format

Kliknij pole wyboru, aby wybrać jednostkę LUN, i kliknij polecenie **Formatuj numer LUN**.

LUN

Wyświetlana jest tu nazwa jednostki LUN.

Rozmiar [GB]

Wyświetlana jest tu maksymalna pojemność jednostki LUN.

Duża jednostka LUN

W każdej komórce podane jest, czy dana jednostka LUN jest większa niż 2 TB, czy też nie.

Stan

Wyświetlany jest tu stan jednostki LUN.

Postęp

Wyświetlany jest tu postęp procesu formatowania.

Patrz

- Strona puli, Strona 179
- Dodawanie jednostki LUN, Strona 196
- Dodawanie urządzeń VRM poprzez skanowanie:, Strona 169

13.24.9**Dodawanie jednostki LUN**

Okno główne > **Urządzenia** > rozwiń węzeł  > rozwiń węzeł  > 

Funkcja skanowania sieci zazwyczaj dodaje wskazane urządzenia iSCSI wraz z automatycznie skonfigurowanymi urządzeniami docelowymi i numerami LUN. Jeśli tak się nie stało lub przed zintegrowaniem urządzenia iSCSI z siecią wymagane jest ręczne wybranie jego ustawień konfiguracyjnych, należy skonfigurować w module iSCSI urządzenie docelowe, a w tym urządzeniu docelowym – skonfigurować co najmniej jeden numer LUN.

Można dodawać jednostki LUN większe niż 2 TB, jeśli włączono w puli stosowanie dużych jednostek LUN.

Jednostki LUN większe niż 2 TB („duże jednostki LUN”) nie są obsługiwane przez następujące urządzenia:

- Urządzenia VRM z oprogramowaniem układowym w wersji starszej niż 3.60
- Urządzenia VSG z oprogramowaniem układowym w wersji starszej niż 6.30
- Nadajniki z oprogramowaniem układowym w wersji starszej niż 6.30

System BVMS zapobiega wykonywaniu następujących czynności:

- Dodawanie lub przenoszenie urządzeń z oprogramowaniem układowym w wersji starszej niż 6.30 do puli, która umożliwia stosowanie dużych jednostek LUN.
- Dodawanie lub przenoszenie urządzeń, które nie mają obecnie połączenia z siecią, do puli, która umożliwia stosowanie dużych jednostek LUN.
- Dodawanie lub przenoszenie urządzenia iSCSI, które zawierają duże jednostki LUN, do puli, która nie umożliwia stosowania dużych jednostek LUN.
- Zezwalanie na użycie dużych jednostek LUN w puli, która zawiera urządzenia z oprogramowaniem układowym w wersji starszej niż 6.30.
- Wyłączanie dużych jednostek LUN w puli z urządzeniem iSCSI, które zawiera duże jednostki LUN.

Urządzenia z oprogramowaniem układowym w wersji starszej niż 6.30 należy przenieść do puli, która nie zezwala na użycie dużych jednostek LUN.

Aby dodać:

1. W razie potrzeby zaznacz pole wyboru **Zezwalaj na jednostki LUN o rozmiarze przekraczającym 2 TB**.



2. Kliknij prawym przyciskiem myszy , a następnie kliknij **Cel skanowania**.



Zostanie dodany element docelowy.

3. Kliknij element docelowy.

Zostanie wyświetlona strona **jednostek LUN**.

4. Kliknij **Dodaj**.

Zostanie wyświetlone okno dialogowe **Dodaj numer LUN**.

5. Wpisz odpowiedni numer jednostki LUN i kliknij **OK**.

Jednostka LUN zostanie dodana do tabeli w postaci jej nowego wiersza.

Powtórz tę czynność dla każdej żądanej jednostki LUN.

Uwagi:

- Aby usunąć numer LUN, kliknij **Usuń**.
Nie spowoduje to skasowania danych wizyjnych z urządzenia o danym numerze LUN.
- Aby sformatować urządzenie o danym numerze LUN, kliknij **Formatuj numer LUN**.
Wszystkie dane zapisane w urządzeniu o tym numerze LUN zostaną usunięte!

Okno dialogowe Dodaj numer LUN



Umożliwia dodanie jednostki LUN.

Id

Wprowadź identyfikator żądanej jednostki LUN.

Patrz

- Strona puli, Strona 179
- Strona Jednostki LUN, Strona 196

13.24.10

Formatowanie urządzenia o określonym numerze LUN

Okno główne > **Urządzenia** > rozwinąć węzeł



> rozwinąć węzeł



> rozwinąć węzeł



> rozwinąć węzeł



>



Formatowanie urządzenia o określonym numerze LUN ma na celu przygotowanie go do pierwszego użycia.



Uwaga!

W wyniku tej operacji wszystkie dane znajdujące się w tym urządzeniu zostaną skasowane.

Aby skonfigurować:

1. Wybierz żądany numer LUN, a następnie w kolumnie **Format** kliknij, aby zaznaczyć.
2. Kliknij **Formatuj numer LUN**.
3. Dokładnie zapoznaj się z wyświetlonymi komunikatami i potwierdź komunikat w razie potrzeby. Wybrany LUN zostaje sformatowany. Wszystkie dane zapisane w tym LUN zostaną usunięte.

Patrz

- Strona Jednostki LUN, Strona 196

13.24.11

Okno dialogowe iqn-Mapper

Okno główne > **Urządzenia** > rozwinąć



> rozwinąć



> rozwinąć



> kliknąć prawym

przyciskiem



> **Mapuj IQN**

Umożliwia rozpoczęcie procesu mapowania nazw IQN.

Patrz

- Dodawanie urządzeń VRM poprzez skanowanie:, Strona 169
- Konfiguracja urządzenia iSCSI, Strona 192

13.25

Strona Urządzenie Video Streaming Gateway

Okno główne > **Urządzenia** > rozwinąć



> rozwinąć



> rozwinąć



>

Niniejszy rozdział zawiera informacje o sposobie konfigurowania urządzeń VSG w tym systemie. Pozwala dodawać i konfigurować następujące typy nadajników:

- Nadajnik firmy Bosch
- Nadajniki ONVIF
- Nadajniki JPEG

- Nadajniki RTSP

Aby poprzez skanowanie dodać urządzenia VSG:

1. Kliknąć prawym przyciskiem myszy  i kliknąć **Skanuj w poszukiwaniu bram Video Streaming Gateway**.
Zostanie wyświetlone okno dialogowe **BVMS Scan Wizard**.
2. Wybrać wymagane urządzenia VSG i żadaną pulę VRM, a następnie kliknąć **Przypisz**, aby przypisać nadajniki do puli VRM.
3. Kliknij **Dalej >>**.
Zostanie wyświetlone okno dialogowe kreatora **Uwierzytelnianie urządzeń**.
4. Wpisać hasło w przypadku każdego urządzenia, które jest nim chronione.
Jeśli przez kilka sekund nie wprowadzisz żadnego znaku w polu hasła lub klikniesz poza tym polem, sprawdzenie hasła następuje automatycznie.
Jeśli hasło do wszystkich urządzeń jest identyczne, można wpisać je w pierwszym polu **Hasło**.
Następnie kliknąć to pole prawym przyciskiem myszy i wybrać opcję **Kopiuj komórkę do kolumny**.

Udane logowanie jest oznaczane w kolumnie **Stan** ikoną .

Nieudane próby logowania są oznaczane ikoną .

5. Kliknąć **Zakończ**.

Urządzenie zostanie dodane do drzewa urządzeń.

Jeśli dodasz nową wersję VSG 7.0 lub wyższą, pole wyboru **Zabezpiecz połączenie** jest domyślnie zaznaczone.

Aby zmienić połączenie bezpieczne lub niezabezpieczone, należy użyć polecenia **Edytuj komponent Video Streaming Gateway** i zaznaczyć pole wyboru **Zabezpiecz połączenie** lub usunąć zaznaczenie.

Patrz

- Edytowanie komponentu Video Streaming Gateway, Strona 200
- Strona ONVIF, Strona 236

13.25.1

Ręczne dodawanie urządzenia Video Streaming Gateway

Okno główne > **Urządzenia** > rozwiń  > 
Do puli VRM można dodawać urządzenia VSG.

Aby dodać ręcznie urządzenie VSG:

1. Kliknąć prawym przyciskiem myszy , a następnie kliknąć polecenie **Dodaj komponent Video Streaming Gateway**.
Pojawi się okno dialogowe **Dodaj komponent Video Streaming Gateway**.
2. Wpisać wymagane ustawienia w urządzeniu VSG.
3. Kliknąć **Dodaj**.
⇒ Urządzenie VSG zostanie dodane do systemu. Zostaną zapisane kamery przypisane do tego urządzenia VSG.

Okno dialogowe Dodaj komponent Video Streaming Gateway

Kliknij  prawym przyciskiem myszy > **Dodaj komponent Video Streaming Gateway** > okno dialogowe **Dodaj komponent Video Streaming Gateway**

Numer portu

Wpisać numer portu urządzenia.

Nazwa użytkownika

Wprowadź nazwę użytkownika używaną do uwierzytelniania w urządzeniu. Zwykle: service.

Adres/port sieciowy

Wprowadzić adres IP urządzenia.

Jeśli pole wyboru **Zabezpiecz połączenie** jest zaznaczone, port zmienia się automatycznie na HTTPS.

Numer portu można zmienić, jeśli nie jest wykorzystywany port domyślny, lub instancje VSG są skonfigurowane w innej kolejności.

Domyślne porty

Instancja VSG	port rcpp	Port HTTPS
1	8756	8443
2	8757	8444
3	8758	8445
4	8759	8446
5	8760	8447
6	8761	8448
7	8762	8449

Hasło

Wprowadź poprawne hasło używane do uwierzytelniania w urządzeniu.

Show password

Kliknąć, aby włączyć opcję wyświetlania wprowadzonego hasła. Uważaj, aby osoby postronne nie poznały tego hasła.

Bezpieczeństwo

Pole wyboru **Zabezpiecz połączenie** jest zaznaczone domyślnie, jeśli protokół HTTPS jest obsługiwany.

Z wersji VSG 7.0, VSG obsługuje bezpieczne połączenie.

**Uwaga!**

W przypadku przejścia na system BVMS w wersji 10.0 lub nowszej, pole wyboru **Zabezpiecz połączenie** nie jest domyślnie zaznaczone i połączenie jest niezabezpieczone (rcpp).

Aby zmienić połączenie bezpieczne lub niezabezpieczone, należy użyć polecenia **Edytuj komponent Video Streaming Gateway** i zaznaczyć pole wyboru **Zabezpiecz połączenie** lub usunąć zaznaczenie.

Uwierzytelnij

Kliknąć, aby uwierzytelnić w urządzeniu z wykorzystaniem wprowadzonych powyżej poświadczeń.

Patrz

– Edytowanie komponentu Video Streaming Gateway, Strona 200

13.25.2**Edytowanie komponentu Video Streaming Gateway**

Okno główne > **Urządzenia** > rozwinąć



> rozwinąć



> rozwinąć



>



Aby zmienić bezpieczne/niebezpieczne połączenie, należy:

1. Prawym przyciskiem myszy kliknąć ikonę .
2. Kliknąć **Edytuj komponent Video Streaming Gateway**.
Zostanie wyświetlone okno dialogowe **Edytuj komponent Video Streaming Gateway**.
3. Zaznaczyć pole wyboru **Zabezpiecz połączenie**.
Używany port zmienia się automatycznie na port HTTPS.
LUB
Usunąć zaznaczenie pole wyboru **Zabezpiecz połączenie**.
Używany port zmienia się automatycznie na port rcpp.



Uwaga!

Po zaktualizowaniu do nowszej wersji zalecamy zmianę połączenia na bezpieczne.

Patrz

- Ręczne dodawanie urządzenia Video Streaming Gateway, Strona 199

13.25.3

Dodawanie kamery do urządzenia VSG

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > rozwiń  > 

Do VSG można dodać następujące urządzenia:

- Nadajniki firmy Bosch
- Kamery ONVIF
- Kamery JPEG
- Nadajniki RTSP

Jeśli nadajniki VSG zostały dodane w trybie offline, można odświeżyć ich stan.

Aby dodać urządzenie:

1. Kliknij prawym przyciskiem myszy ikonę , wskaż opcję **Dodaj nadajnik/kamerę** i kliknij żądane polecenie.
2. W oknie dialogowym wykonaj żądane ustawienia dla dodawanego urządzenia.
3. Kliknij **OK**.

Urządzenie zostanie dodane.

Aby odświeżyć:

- ▶ Kliknij odpowiedni nadajnik prawym przyciskiem myszy, a następnie kliknij polecenie **Odśwież stan**.
Nastąpi pobranie właściwości tego urządzenia.

Patrz

- Okno dialogowe *Dodaj / Edytuj nadajnik Bosch*, Strona 202
- Okno dialogowe *Dodaj / Edytuj nadajnik ONVIF*, Strona 203
- Okno dialogowe *Dodaj / Edytuj kamerę JPEG*, Strona 205
- Okno dialogowe *Dodaj / Edytuj nadajnik RTSP*, Strona 206

13.25.4

Okno dialogowe Dodaj / Edytuj nadajnik Bosch

Okno główne > **Urządzenia** > rozwinąć  > rozwinąć  > rozwinąć  > kliknąć prawym

przyciskiem myszy  > **Dodaj nadajnik/kamerę** > polecenie **Nadajnik firmy Bosch**
LUB

Okno główne > **Urządzenia** > rozwinąć  > rozwinąć  > rozwinąć  > rozwinąć  > kliknąć prawym przyciskiem myszy  > kliknąć **Edytuj nadajnik** > okno dialogowe **Edytuj nadajnik Bosch**

Do urządzenia VSG można dodać nadajnik firmy Bosch.

Adres sieciowy

Wpisz adres sieciowy urządzenia.

Numer portu

Wpisać numer portu urządzenia.

Zabezpiecz połączenie

Można włączyć bezpieczne połączenie bieżącego obrazu wizyjnego przesyłanego z nadajnika ONVIF do urządzenia VSG.

Uwaga:

Po włączeniu szyfrowania użytkownik programu Operator Client nie może przełączyć strumienia na protokół UDP ani UDP multicast.

Po włączeniu szyfrowania tryb ANR nie działa w przypadku urządzenia, do którego trafia zaszyfrowany przekaz.

Po uaktywnieniu odtwarzanie nadajnika nie działa w nadajnikach z oprogramowaniem układowym starszym niż wersja 6.30.

Typ nadajnika

W przypadku urządzeń, których typ jest znany, wybierz odpowiednią pozycję. Urządzenie nie musi być dostępne w sieci.

Dodając sieciowe urządzenie wizyjne firmy Bosch, zaznacz opcję **<Automatyczne wykrywanie>**.

Urządzenie musi być dostępne w sieci.

Aby dodać kamerę w konfiguracji offline, wybierz opcję **<Symbol zastępczy jednej kamery>**.

Nazwa użytkownika

Wprowadź nazwę użytkownika używaną do uwierzytelniania w urządzeniu. Zwykle: service.

Hasło

Wprowadź poprawne hasło używane do uwierzytelniania w urządzeniu.

Show password

Kliknąć, aby włączyć opcję wyświetlania wprowadzonego hasła. Uważaj, aby osoby postronne nie poznały tego hasła.

Uwierzytelnij

Kliknąć, aby uwierzytelnić w urządzeniu z wykorzystaniem wprowadzonych powyżej poświadczeń.

Protokół kamery

Kliknąć, aby włączyć żądany protokół urządzenia.

TCP

Służy do przesyłania informacji przez Internet i do bezstratnej transmisji danych. Zapewnia możliwość przesłania wszystkich pakietów danych. Wymagania dotyczące szerokości pasma mogą być wysokie. Należy użyć, jeśli urządzenie jest chronione zaporą sieciową. Nie obsługuje trybu Multicast.

UDP

Służy do bezpołączeniowej transmisji niewielkiej ilości danych w sieciach prywatnych. Może nastąpić utrata pakietów danych. Wymagania dotyczące szerokości pasma mogą być niewielkie.

Obsługuje tryb Multicast.

Użyj wejść wizyjnych

Kliknij, aby wybrać wejścia wideo w przypadku konfigurowania urządzenia wielokanałowego.

Używane wejścia wideo

Zaznaczyć pole wyboru, aby użyć odpowiedniego wejścia wizyjnego.

Patrz

– Dodawanie kamery do urządzenia VSG, Strona 201

13.25.5

Okno dialogowe Dodaj / Edytuj nadajnik ONVIF

Okno główne > **Urządzenia** > rozwinąć  > rozwinąć  > rozwinąć  > kliknąć prawym

przyciskiem myszy  > **Dodaj nadajnik/kamerę** > polecenie **Dodaj nadajnik ONVIF**
lub

Okno główne > **Urządzenia** > kliknąć prawym przyciskiem myszy  > polecenie **Dodaj nadajnik ONVIF**

LUB

Okno główne > **Urządzenia** > rozwinąć  > rozwinąć  > rozwinąć  > rozwinąć 

> kliknąć prawym przyciskiem myszy  > kliknąć **Edytuj nadajnik ONVIF** > okno dialogowe **Edytuj nadajnik ONVIF**

LUB

Okno główne > **Urządzenia** > kliknąć prawym przyciskiem myszy  > kliknąć prawym

przyciskiem myszy  > kliknąć **Edytuj nadajnik ONVIF** > okno dialogowe **Edytuj nadajnik ONVIF**

Nadajnik ONVIF można dodać do urządzenia VSG lub jako nadajnik udostępniający tylko podgląd na żywo.

W tabeli kamery należy skonfigurować używany profil na zapisywanie i obraz na żywo.

Z systemu BVMS w wersji 10.0 wydarzenia nadajnika ONVIF mogą być pobierane bezpośrednio z VSG lub nadajnika ONVIF. Po dodaniu nowego nadajnika ONVIF pole wyboru **zdarzenia pobrania ONVIF z VSG (Profil S, T)** jest domyślnie zaznaczone, a profil T jest obsługiwany.

Następujące funkcje są obsługiwane tylko w przypadku, gdy nadajnik ONVIF został dodany do systemu za pośrednictwem urządzenia VSG:

- Jeśli zdarzenia nadajnika ONIV są pobierane z VSG, domyślne zdarzenia ONVIF są już odwzorowane.
- Operator może włączać lub wyłączać przełączniki w aplikacji Operator Client

**Uwaga!**

Pobieranie zdarzeń ONVIF z VSG jest obsługiwane tylko w wersji VSG 7.0. Po przeprowadzeniu migracji do systemu BVMS w wersji 10.0 istniejące zdarzenia nadajnika ONVIF są pobierane bezpośrednio z nadajnika ONVIF. Należy zaktualizować VSG do wersji 7.0.

Nazwa

Wpisać wyświetlaną nazwę urządzenia.

Adres sieciowy

Wpisz adres sieciowy urządzenia.

Numer portu

Wpisać numer portu urządzenia.

Zabezpiecz połączenie

Można włączyć bezpieczne połączenie bieżącego obrazu wizyjnego przesyłanego z nadajnika ONVIF do urządzenia VSG.

Uwaga:

Po włączeniu szyfrowania użytkownik programu Operator Client nie może przełączyć strumienia na protokół UDP ani UDP multicast.

Po włączeniu szyfrowania tryb ANR nie działa w przypadku urządzenia, do którego trafia zaszyfrowany przekaz.

Po uaktywnieniu odtwarzanie nadajnika nie działa w nadajnikach z oprogramowaniem układowym starszym niż wersja 6.30.

**Uwaga!**

Port 443 jest ustawiany domyślnie. Można edytować numer portu, aby dopasować go do portu HTTPS ustawionego w nadajniku.

Ustawiony numer portu nie jest zapamiętywany.

Nazwa użytkownika

Wprowadź nazwę użytkownika używaną do uwierzytelniania w urządzeniu. Zwykle: service.

Hasło

Wprowadź poprawne hasło używane do uwierzytelniania w urządzeniu.

Show password

Kliknąć, aby włączyć opcję wyświetlania wprowadzonego hasła. Uważaj, aby osoby postronne nie poznały tego hasła.

Uwierzytelnij

Kliknąć, aby uwierzytelnić w urządzeniu z wykorzystaniem wprowadzonych powyżej poświadczeń.

Protokół kamery

Wybrać odpowiedni protokół kamery.

Profil ONVIF

Jeśli jest obsługiwane, wybierz profil, który chcesz skonfigurować.

Profil ONVIF G

Jeśli koder ONVIF obsługuje profil G i planowane jest lokalne nagrywanie, należy skonfigurować ustawienia lokalnego nagrywania w narzędziu konfiguracyjnym dostarczonej przez producenta oraz zaznaczyć pole wyboru **Aktywowano nagrywanie lokalne**.

Jeśli pole nie zostanie zaznaczone, koder ONVIF z profilem G będzie działać jako standardowy koder ONVIF.

Kamera panoramiczna

W razie potrzeby zaznaczyć pole wyboru.

Położenie montażowe

Wybrać pozycję montażu.

Liczba kanałów wejściowych sygnału wizyjnego

Wpisać odpowiednią liczbę wejść wizyjnych.

Użyj wejścia wizyjnego {0}

Zaznaczyć pole wyboru, aby użyć odpowiedniego wejścia wizyjnego.

Liczba kanałów wejściowych audio

Wpisać odpowiednią liczbę wejść fonicznych.

Liczba wejść alarmowych

Wpisać odpowiednią liczbę wejść alarmowych.

Liczba przekaźników

Wpisać odpowiednią liczbę przekaźników.

**Uwaga!**

Opcje **Ustawienia bramy Video Streaming Gateway** nie są dostępne dla nadajnika ONVIF, który jest dodawany jako nadajnik podglądu bieżącego.

Patrz

– Dodawanie kamery do urządzenia VSG, Strona 201

13.25.6**Okno dialogowe Dodaj / Edytuj kamerę JPEG**

Okno główne > **Urządzenia** > rozwinąć  > rozwinąć  > rozwinąć  > kliknąć prawym

przyciskiem myszy  > **Dodaj nadajnik/kamerę** > polecenie **Kamera JPEG**
LUB

Okno główne > **Urządzenia** > rozwinąć  > rozwinąć  > rozwinąć  > rozwinąć 
> kliknąć prawym przyciskiem myszy  > kliknąć **Edytuj kamerę JPEG** > okno dialogowe **Edytuj JPEG**

Do urządzenia VSG można dodać kamerę JPEG.

Nazwa

Wpisać wyświetlaną nazwę urządzenia.

URL

Wprowadź adres URL kamery JPEG/RTSP.

W przypadku kamery JPEG firmy Bosch wprowadź następujący ciąg:

`http://<ip-address>/snap.jpg?jpegCam=<channel_no.>`

W przypadku kamery RTSP firmy Bosch wprowadź następujący ciąg:

`rtsp://<ip-address>/rtsp_tunnel`

Nazwa użytkownika

Wprowadź nazwę użytkownika używaną do uwierzytelniania w urządzeniu. Zwykle: service.

Hasło

Wprowadź poprawne hasło używane do uwierzytelniania w urządzeniu.

Show password

Kliknąć, aby włączyć opcję wyświetlania wprowadzonego hasła. Uważaj, aby osoby postronne nie poznały tego hasła.

Częstotliwość odświeżania [obrazów/s]

Wprowadź odpowiednią częstotliwość odświeżania.

Patrz

– Dodawanie kamery do urządzenia VSG, Strona 201

13.25.7**Okno dialogowe Dodaj / Edytuj nadajnik RTSP**

Okno główne > **Urządzenia** > rozwinąć  > rozwinąć  > rozwinąć  > kliknąć prawym

przyciskiem myszy  > **Dodaj nadajnik/kamerę** > polecenie **Kamera RTSP**
LUB

Okno główne > **Urządzenia** > rozwinąć  > rozwinąć  > rozwinąć  > rozwinąć 
> kliknąć prawym przyciskiem myszy  > kliknąć **Edytuj kamerę RTSP** > okno dialogowe **Edytuj RTSP**

Do urządzenia VSG można dodać nadajnik RTSP.

Nazwa

Wpisać wyświetlaną nazwę urządzenia.

URL

Wprowadź adres URL kamery JPEG/RTSP.

W przypadku kamery JPEG firmy Bosch wprowadź następujący ciąg:

`http://<ip-address>/snap.jpg?jpegCam=<channel_no.>`

W przypadku kamery RTSP firmy Bosch wprowadź następujący ciąg:

`rtsp://<ip-address>/rtsp_tunnel`

Uwaga: Jeśli VSG obsługuje dwa strumienie, wpisz odpowiedni adres URL dla strumienia wysokiej i niskiej jakości.

Nazwa użytkownika

Wprowadź nazwę użytkownika używaną do uwierzytelniania w urządzeniu. Zwykle: service.

Hasło

Wprowadź poprawne hasło używane do uwierzytelniania w urządzeniu.

Show password

Kliknąć, aby włączyć opcję wyświetlania wprowadzonego hasła. Uważaj, aby osoby postronne nie poznały tego hasła.

Patrz

– Dodawanie kamery do urządzenia VSG, Strona 201

13.25.8

Przenoszenie bramy VSG do innej puli (Zmień pulę)

Okno główne > **Urządzenia** > rozwiń  > rozwiń  >  > 

W ramach jednego urządzenia VRM można przenosić urządzenia między pulami bez utraty zapisanych materiałów.

Aby przenieść urządzenie:

1. Kliknąć prawym przyciskiem myszy  /  / , a następnie kliknąć **Zmień pulę ...**.
Zostanie wyświetlone okno dialogowe **Zmień pulę**.
2. Wybrać odpowiednią pulę z listy **Nowa pula:**.
3. Kliknąć przycisk **OK**.
Urządzenie zostanie przeniesione do wybranej puli.

13.25.9

Konfigurowanie multicastingu (karta trybu Multicast)

Okno główne > **Urządzenia** > rozwinąć  > rozwinąć  > rozwinąć  > 

Dla każdej kamery przypisanej do urządzenia Video Streaming Gateway można skonfigurować adres i port trybu multicast.

Aby skonfigurować tryb Multicast:

1. Zaznaczyć żądane pole wyboru, aby włączyć tryb Multicast.
2. Wprowadzić prawidłowy adres Multicast i numer portu.
3. W razie potrzeby skonfigurować ciągłą transmisję strumieniową pod adres Multicast.

Karta Multicast

Okno główne > **Urządzenia** > Rozwiń  > Rozwiń  > Rozwiń  >  > Karta Sieć >

Karta Multicast

Umożliwia skonfigurowanie trybu Multicast dla przydzielonych kamer.

Włącz

Kliknąć, aby włączyć tryb Multicast dla tej kamery.

Adres multicastingu

Wprowadzić prawidłowy adres Multicast (w zakresie od 224.0.0.0 do 239.255.255.255).

Wprowadzić 1.0.0.0 Niepowtarzalny adres Multicast jest wstawiany automatycznie na podstawie adresu MAC urządzenia.

Port

Jeśli używana jest zapora sieciowa, należy wpisać numer portu, który nie jest przez nią blokowany.

Przes. strum

Kliknąć, aby włączyć w przełączniku tryb ciągłego strumieniowania Multicast. Oznacza to, że połączenie w trybie Multicast nie jest poprzedzone rejestracją RCP+. Nadajnik zawsze przesyła wszystkie dane do przełącznika. Natomiast przełącznik (jeśli filtrowanie trybu Multicast IGMP nie jest obsługiwane lub nie zostało skonfigurowane) wysyła te dane do wszystkich portów. W rezultacie przełącznik zostaje przepełniony.

Przesyłanie strumieniowe jest konieczne w przypadku odbierania strumienia Multicast za pomocą urządzeń innych producentów.

13.25.10

Konfigurowanie rejestrowania (karta Zaawansowane)

Okno główne > **Urządzenia** > rozwinąć  > rozwinąć  > rozwinąć  > karta **Serwis** > karta **Zaawansowane**

Umożliwia uaktywnienie logowania do urządzenia Video Streaming Gateway.

Pliki rejestru są zwykle zapisywane w następującej lokalizacji:

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

Od wersji 7.0 VSG pliki rejestru są zwykle zapisywane w następującej lokalizacji:

```
C:\ProgramData\Bosch\VSG\log
```

Uwaga: po uaktualnieniu VSG do wersji 7.0 lub nowszej wcześniejsze pliki rejestru są automatycznie przenoszone do tej lokalizacji.

Pliki rejestru ze starszych wersji VSG są zwykle przechowywane w następujących lokalizacjach:

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

Karta Zaawansowane

Logowanie RCP+

Kliknij, aby włączyć rejestrowanie RCP+.

Logowanie debugera

Kliknij, aby włączyć rejestrowanie debugowania.

Logowanie RTP

Kliknij, aby włączyć rejestrowanie RTP.

Czas przechowywania (dni)

Wybierz żadaną liczbę dni.

Kompletny zrzut pamięci

Należy zaznaczyć to pole wyboru tylko w razie konieczności – gdy na przykład dział pomocy technicznej poprosi o zestawienie zawartości pamięci głównej.

Obsługa Telnet

To pole wyboru należy zaznaczyć, jeśli ma być obsługiwany dostęp za pośrednictwem protokołu Telnet. Należy zaznaczyć tylko w razie konieczności.



Uwaga!

Rejestrowanie na dużą skalę wymaga znacznej mocy procesora i pojemności dysku twardego. Nie należy korzystać z tej opcji w codziennej eksploatacji.

13.25.11

Uruchamianie narzędzia ONVIF Camera Event Driver Tool za pomocą Configuration Client

Okno główne > **Urządzenia** > rozwinąć  > rozwinąć  > rozwinąć  >

Możesz uruchomić narzędzie ONVIF Camera Event Driver Tool bezpośrednio z Configuration Client odnośnie do wybranego VSG.

Uwaga: można również uruchomić to narzędzie z menu Start systemu Windows.

Narzędzie ONVIF Camera Event Driver Tool pozwala mapować zdarzenia ONVIF na zdarzenia BVIP VSG. Można nawiązać połączenie z kamerami ONVIF i pobrać zdarzenia ONVIF do mapowania.

Aby uruchomić narzędzie ONVIF Camera Event Driver Tool z poziomu Configuration Client:

1. Kliknąć prawym przyciskiem myszy odpowiedni VSG
2. Kliknąć narzędzie **Uruchom narzędzie ONVIF Camera Event Driver Tool**.

Wyświetla się ONVIF Camera Event Driver Tool.

**Uwaga!**

Narzędzie ONVIF Camera Event Driver Tool obsługuje tylko bezpieczne połączenie z VSG.

Aby włączyć ONVIF Camera Event Driver Tool:

Patrz [Film instruktażowy](#).

13.26**strona Tylko podgląd bieżący i lokalna pamięć masowa**

Okno główne > **Urządzenia** > Rozwiń > >

Umożliwia dodawanie i konfigurowanie nadajników używanych wyłącznie do podglądu bieżącego. Można dodawać nadajniki firmy Bosch i sieciowe nadajniki wizyjne zgodne ze standardem ONVIF.

Aby dodać, edytować i skonfigurować nadajnik ONVIF tylko do podglądu bieżącego, patrz Strona ONVIF, Strona 236.

Patrz

- Dodawanie nadajnika udostępniającego tylko podgląd bieżący, Strona 218
- Skanowanie w poszukiwaniu urządzeń, Strona 74
- Strona Bosch Encoder / Decoder / Camera (Nadajnik/odbiornik/kamera firmy Bosch), Strona 215
- Strona ONVIF, Strona 236
- Konfigurowanie trybu Multicast, Strona 234

13.26.1**Dodawanie urządzeń podglądu bieżącego poprzez skanowanie**

Aby poprzez skanowanie dodać urządzenia Bosch tylko z podglądem bieżącym:

1. Kliknij prawym przyciskiem myszy , a następnie kliknij **Skanuj w poszukiwaniu nadajników tylko podglądu bieżącego**.
Zostanie wyświetlone okno dialogowe **BVMS Scan Wizard**.
2. Zaznacz pola wyboru odpowiadające urządzeniom, które mają zostać dodane.
3. Kliknij **Dalej >>**.
Zostanie wyświetlone okno dialogowe kreatora **Uwierzytelnianie urządzeń**.
4. Wpisać hasło w przypadku każdego urządzenia, które jest nim chronione.
Jeśli przez kilka sekund nie wprowadzisz żadnego znaku w polu hasła lub klikniesz poza tym polem, sprawdzenie hasła następuje automatycznie.
Jeśli hasło do wszystkich urządzeń jest identyczne, można wpisać je w pierwszym polu **Hasło**.
Następnie kliknij to pole prawym przyciskiem myszy i kliknij polecenie **Kopiuj komórkę do kolumny**.

Udane logowanie jest oznaczane w kolumnie **Stan** ikoną .

Nieudane próby logowania są oznaczane ikoną .

5. Kliknąć **Zakończ**.
Urządzenie zostanie dodane do drzewa urządzeń.

Ikona oznacza błąd, którym należy się zająć. Więcej informacji o charakterze błędu uzyskasz z etykiety narzędzia.

13.26.2

Ręczne dodawanie nadajnika

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > kliknij prawym przyciskiem myszy



> kliknij **Dodaj nadajnik** > okno dialogowe **Dodaj nadajnik**

lub

Okno główne > **Urządzenia** > kliknij prawym przyciskiem myszy  > kliknij **Dodaj nadajnik** > okno dialogowe **Dodaj nadajnik**

lub

Okno główne > **Urządzenia** > kliknij prawym przyciskiem myszy  > kliknij **Dodaj nadajnik** > okno dialogowe **Dodaj nadajnik**

lub

Okno główne > **Urządzenia** > rozwiń  > kliknij prawym przyciskiem myszy  > kliknij **Dodaj odbiornik** > okno dialogowe **Dodaj nadajnik**

Umożliwia ręczne dodanie nadajnika. Jest to szczególnie użyteczne, gdy chce się dodać sieciowe urządzenie wizyjne firmy Bosch (tylko dla VRM).

Uwaga:

W przypadku dodawania nadajnika strumienia wideo firmy Bosch za pomocą funkcji <**Automatyczne wykrywanie**> to urządzenie musi być dostępne w sieci.

Aby dodać sieciowe urządzenie wizyjne firmy Bosch:

1. Rozwiń  , rozwiń  , kliknąć prawym przyciskiem myszy  .
lub

Kliknąć prawym przyciskiem myszy  .
lub

Kliknąć prawym przyciskiem myszy  .

2. Kliknąć **Dodaj nadajnik**.
Zostanie wyświetlone okno dialogowe **Dodaj nadajnik**.
3. Wprowadzić prawidłowy adres IP.
4. Na liście zaznaczyć pozycję <**Automatyczne wykrywanie**>, wprowadź hasło dostępu do urządzenia i kliknij przycisk **Uwierzytelnij**.
Lub
Na liście zaznaczyć określony typ nadajnika lub <**Symbol zastępczy jednej kamery**>.
5. Kliknij **OK**.
Urządzenie zostanie dodane do systemu.

Ikona  oznacza błąd, którym należy się zająć. Więcej informacji o charakterze błędu uzyskasz z etykiety narzędzia.

Okno dialogowe Dodaj nadajnik**Adres sieciowy**

Wpisz poprawny adres IP.

Numer portu

Wpisać numer portu urządzenia.

Typ nadajnika

W przypadku urządzeń, których typ jest znany, wybierz odpowiednią pozycję. Urządzenie nie musi być dostępne w sieci.

Dodając sieciowe urządzenie wizyjne firmy Bosch, zaznacz opcję **<Automatyczne wykrywanie>**.

Urządzenie musi być dostępne w sieci.

Aby dodać kamerę w konfiguracji offline, wybierz opcję **<Symbol zastępczy jednej kamery>**.

Nazwa użytkownika

Wyświetla nazwę użytkownika używaną w celu uwierzytelniania w urządzeniu.

Hasło

Wprowadź poprawne hasło używane do uwierzytelniania w urządzeniu.

Pokaż hasło

Kliknij, aby włączyć opcję wyświetlania wprowadzonego hasła. Uważaj, aby osoby postronne nie poznały tego hasła.

Uwierzytelnij

Kliknąć, aby uwierzytelnić w urządzeniu z wykorzystaniem wprowadzonych powyżej poświadczeń.

13.26.3**Dostarczanie hasła docelowego dla dekodera (Uwierzytelnij...)**

Okno główne > **Urządzenia** > Rozwiń  > Rozwiń  > Kliknij prawym przyciskiem myszy



> Kliknij **Uwierzytelnij...** > Okno dialogowe **Wprowadź hasło**

Aby umożliwić dostęp chronionego hasłem nadajnika do dekodera, należy wprowadzić w dekodерze hasło poziomu autoryzacji użytkownika nadajnika jako hasło docelowe.

Aby wprowadzić hasło:

1. Na liście **Wprowadź nazwę użytkownika** wybierz pozycję destination password.
 2. W polu **Wprowadź hasło dla użytkownika** wpisz nowe hasło.
 3. Kliknąć **OK**.
- ⇒ Hasło na urządzeniu zostanie natychmiast zmienione.

Patrz

– Zmiana hasła nadajnika/dekodera (Zmień hasło / Wprowadź hasło), Strona 143

13.27**strona Lokalne urządzenia pamięci masowej**

Okno główne > **Urządzenia** > rozwinąć  > 

Umożliwia dodawanie i konfigurowanie nadajników służących do nagrywania na lokalnych urządzeniach pamięci masowej.

Aby poprzez skanowanie dodać nadajniki z obsługą lokalnego urządzenia pamięci masowej:

1. W oknie Drzewo urządzeń kliknij prawym przyciskiem myszy , a następnie kliknij **Skanuj w poszukiwaniu nadajników z pamięcią lokalną**.
Zostanie wyświetlone okno dialogowe **BVMS Scan Wizard**.
2. Zaznacz pola wyboru odpowiadające urządzeniom, które mają zostać dodane.

3. Kliknij **Dalej >>**.
Zostanie wyświetlone okno dialogowe kreatora **Uwierzytelnianie urządzeń**.
4. Wpisać hasło w przypadku każdego urządzenia, które jest nim chronione.
Jeśli przez kilka sekund nie wprowadzisz żadnego znaku w polu hasła lub klikniesz poza tym polem, sprawdzenie hasła następuje automatycznie.
Jeśli hasło do wszystkich urządzeń jest identyczne, można wpisać je w pierwszym polu **Hasło**.
Następnie kliknij to pole prawym przyciskiem myszy i kliknij polecenie **Kopiuj komórkę do kolumny**.



Udane logowanie jest oznaczane w kolumnie **Stan** ikoną .



Nieudane próby logowania są oznaczane ikoną .

5. Kliknąć **Zakończ**.
Urządzenie zostanie dodane do drzewa urządzeń.

Ikona  oznacza błąd, którym należy się zająć. Więcej informacji o charakterze błędu uzyskasz z etykiety narzędzia.

Patrz

- Konfigurowanie trybu Multicast, Strona 234
- Dodawanie nadajnika z pamięcią lokalną, Strona 218
- Strona Bosch Encoder / Decoder / Camera (Nadajnik/odbiornik/kamera firmy Bosch), Strona 215
- Skanowanie w poszukiwaniu urządzeń, Strona 74

13.28

Strona Unmanaged Site



Okno główne > **Urządzenia** > rozwiń węzeł



Można dodać urządzenie sieciowe wideo do pozycji **Unmanaged Sites** drzewa urządzeń.

Zakłada się, że wszystkie niezarządzane urządzenia sieciowe należące do unmanaged site znajdują się w tej samej strefie czasowej.

Nazwa witryny

Wyświetlana jest tu nazwa lokalizacji wprowadzona podczas jej tworzenia.

Opis

Wprowadź opis dla site.

Strefa czasowa

Należy wybrać odpowiednią strefę czasową danej unmanaged site.

Patrz

- Unmanaged site, Strona 28
- Ręczne dodawanie lokalizacji unmanaged site, Strona 212
- Importowanie niezarządzanych lokalizacji, Strona 213
- Konfigurowanie strefy czasowej, Strona 214

13.28.1

Ręczne dodawanie lokalizacji unmanaged site



Okno główne > **Urządzenia** >

Aby utworzyć:

1. Kliknij prawym przyciskiem myszy ikonę  , a następnie wybierz polecenie **Dodaj Unmanaged Site**.
Zostanie wyświetlone okno dialogowe **Dodaj Unmanaged Site**.
2. Wpisz nazwę i opis lokalizacji.
3. Wybrać odpowiednią pozycję na liście **Strefa czasowa**.
4. Kliknąć **OK**.
Do systemu zostanie dodana nowa pozycja unmanaged site.

Patrz

- *Unmanaged site*, Strona 28
- *Strona Unmanaged Site*, Strona 212

13.28.2**Importowanie niezarządzanych lokalizacji**

Okno główne > **Urządzenia** > 

Można zaimportować plik CSV zawierający konfigurację urządzenia DVR lub innego urządzenia BVMS, które użytkownik chce zaimportować w systemie BVMS jako unmanaged site.

Aby zaimportować dane:

1. Kliknij prawym przyciskiem myszy ikonę  , a następnie kliknij opcję **Zaimportuj Unmanaged Sites**.
2. Otwórz żądany plik i kliknij przycisk **Otwórz**.
Do systemu zostanie dodana jedna lub więcej unmanaged site.
Te unmanaged sites można teraz dodać do drzewa logicznego.
Uwaga: jeśli wystąpi błąd uniemożliwiający zaimportowanie pliku, pojawi się odpowiedni komunikat z informacjami o tym.

13.28.3**Strona Unmanaged Site****Nazwa witryny**

Wyświetlana jest tu nazwa lokalizacji wprowadzona podczas jej tworzenia.

Opis

Wprowadź opis dla site.

Strefa czasowa

Należy wybrać odpowiednią strefę czasową danej unmanaged site.

13.28.4**Dodawanie niezarządzanego urządzenia sieciowego**

Okno główne > **Urządzenia** >  > 

1. Kliknąć ten element prawym przyciskiem myszy, a następnie wybrać polecenie **Dodaj urządzenie sieciowe Unmanaged**.
Pojawi się okno dialogowe **Dodaj urządzenie sieciowe Unmanaged**.
2. Wybierz żądany typ urządzenia.
3. Wpisz prawidłowy adres IP lub nazwę hosta oraz dane uwierzytelniające odpowiednie dla tego urządzenia.
4. Kliknąć **OK**.
Do systemu zostanie dodana nowa pozycja **Urządzenie sieciowe Unmanaged**.

Można teraz dodać lokalizację unmanaged site do drzewa logicznego.

Należy zwrócić uwagę, że w oknie drzewa logicznego jest widoczna tylko dana lokalizacja, ale nie urządzenia sieciowe należące do tej lokalizacji.

5. Wpisz prawidłową nazwę użytkownika tego urządzenia sieciowego, o ile jest dostępna.
6. Wpisz prawidłowe hasło, o ile jest dostępne.

Okno dialogowe Dodaj urządzenie sieciowe Unmanaged

Okno główne > **Urządzenia** > Rozwiń  > Kliknij prawym przyciskiem myszy  > Kliknij **Dodaj urządzenie sieciowe Unmanaged**

Typ urządzenia:

Wybrać pozycję odpowiednią w przypadku tego urządzenia.

Dostępne pozycje:

- **DIVAR AN / DVR**
- **DIVAR IP (AiO) w systemie BVMS**
- **+Kamera IP firmy Bosch / nadajnik**

Adres sieciowy:

Wpisz adres IP lub nazwę hosta. Jeśli jest to wymagane, zmień numer portu.

Uwaga: używając połączenia SSH, należy wprowadzić adres w następującym formacie:

SSH://IP lub nazwa_serwera:5322

Bezpieczeństwo

Pole wyboru **Bezpieczne połączenie** jest domyślnie zaznaczone.



Uwaga!

W przypadku dodawania DVR przy zaznaczonym polu wyboru **Bezpieczne połączenie** połączenia związane z poleceniami i sterowaniem są bezpieczne. Strumieniowe przesyłanie danych wideo nie jest zabezpieczone.

Nazwa użytkownika:

Wpisz prawidłową nazwę użytkownika tego urządzenia sieciowego, o ile jest dostępna. Aby uzyskać więcej informacji, patrz *Unmanaged site*, Strona 28.

Hasło:

Wpisz prawidłowe hasło, o ile jest dostępne. Więcej informacji na temat poświadczeń użytkownika znajduje się w rozdziale *Unmanaged site*, Strona 28.

Patrz

- *Unmanaged site*, Strona 28

13.28.5

Konfigurowanie strefy czasowej

Okno główne > **Urządzenia** > rozwiń węzeł  > 

Można skonfigurować strefę czasową unmanaged site. Jest to przydatne, gdy użytkownik Operator Client chce uzyskać dostęp do unmanaged site za pomocą komputera z programem Operator Client znajdującego się w innej strefie czasowej niż ta unmanaged site.

Aby skonfigurować strefę czasową:

- ▶ Wybierz odpowiednią pozycję na liście **Strefa czasowa**.

Patrz

- *Strona Unmanaged Site*, Strona 212

14

Strona Bosch Encoder / Decoder / Camera (Nadajnik/odbiornik/kamera firmy Bosch)

Niniejszy rozdział zawiera informacje o sposobie konfigurowania nadajników i dekodów w tym systemie.



Uwaga!

Program BVMS Viewer nie obsługuje odbiorników.

Szczegółowe informacje na temat ustawień nadajnika, dekodera lub kamery, na przykład Video Content Analysis (VCA) lub ustawień sieci można znaleźć w instrukcji obsługi odpowiedniego urządzenia.

Liczba elementów poniżej pozycji jest wyświetlana w nawiasach kwadratowych.

Aby skonfigurować nadajnik:

Okno główne > **Urządzenia** > rozwinąć  > rozwinąć  >  > 

Okno główne > **Urządzenia** > rozwinąć  > rozwinąć  > rozwinąć  > 

Okno główne > **Urządzenia** >  > 

Okno główne > **Urządzenia** >  > 

Aby skonfigurować odbiornik:

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > 

Szczegółowe informacje zawiera Pomoc ekranowa dla stron  .

Aby skonfigurować kamerę:

Okno główne > **Urządzenia** > rozwinąć  > rozwinąć  >  > 

Okno główne > **Urządzenia** > rozwiń  > rozwiń  >  >  > 

Okno główne > **Urządzenia** > rozwinąć  > rozwinąć  > rozwinąć  >  > 

Okno główne > **Urządzenia** >  >  > 

Okno główne > **Urządzenia** >  >  > 

– Kliknij  , aby zapisać ustawienia.

- Kliknij  , aby cofnąć ostatnią zmianę.

- Kliknij  , aby uaktywnić konfigurację.

Większość ustawień na stronach nadajnika/odbiornika/kamery jest aktywnych zaraz po kliknięciu

przycisku  . Jeśli użytkownik wybierze inną kartę bez kliknięcia przycisku  , a nastąpiły zmiany w ustawieniach, pojawią się dwa okna komunikatów. Aby zapisać zmiany, należy potwierdzić oba komunikaty.

Aby zmienić hasła nadajnika, należy kliknąć prawym przyciskiem myszy ikonę urządzenia, a następnie kliknąć przycisk **Zmień hasło...**

Aby wyświetlić urządzenie w sieci Web, należy kliknąć prawym przyciskiem myszy ikonę urządzenia, a następnie przycisk **Pokaż stronę sieciową w przeglądarce**.

Uwaga:

W zależności od wybranego nadajnika lub kamery nie wszystkie opisane tutaj strony są dostępne dla każdego urządzenia. Słowa użyte tutaj do opisu nazw pól mogą różnić się od oprogramowania użytkownika.

- ▶ Kliknąć kartę, aby wyświetlić odpowiednią stronę właściwości.

Aby dodać nadajniki poprzez skanowanie:

1. Kliknąć prawym przyciskiem myszy  i kliknąć **Skanuj w poszukiwaniu nadajników**.
Zostanie wyświetlone okno dialogowe **BVMS Scan Wizard**.
2. Wybrać wymagane nadajniki oraz żadaną pulę VRM, a następnie kliknąć **Przypisz**, aby przypisać nadajniki do puli VRM.
3. Kliknij **Dalej >>**.
Zostanie wyświetlone okno dialogowe kreatora **Uwierzytelnianie urządzeń**.
4. Wpisać hasło w przypadku każdego urządzenia, które jest nim chronione.
Jeśli przez kilka sekund nie wprowadzisz żadnego znaku w polu hasła lub klikniesz poza tym polem, sprawdzenie hasła następuje automatycznie.
Jeśli hasło do wszystkich urządzeń jest identyczne, można wpisać je w pierwszym polu **Hasło**.
Następnie kliknij to pole prawym przyciskiem myszy i kliknij polecenie **Kopiuj komórkę do kolumny**.

Udane logowanie jest oznaczane w kolumnie **Stan** ikoną  .

Nieudane próby logowania są oznaczane ikoną  .

5. Kliknąć **Zakończ**.
Urządzenie zostanie dodane do drzewa urządzeń.

Ikona  oznacza błąd, którym należy się zająć. Więcej informacji o charakterze błędu uzyskasz z etykiety narzędzia.

Patrz

- Skanowanie w poszukiwaniu urządzeń, Strona 74

14.1 Ręczne dodawanie nadajnika

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > kliknij prawym przyciskiem myszy



> kliknij **Dodaj nadajnik** > okno dialogowe **Dodaj nadajnik**

lub

Okno główne > **Urządzenia** > kliknij prawym przyciskiem myszy  > kliknij **Dodaj nadajnik** > okno dialogowe **Dodaj nadajnik**

lub

Okno główne > **Urządzenia** > kliknij prawym przyciskiem myszy  > kliknij **Dodaj nadajnik** > okno dialogowe **Dodaj nadajnik**

lub

Okno główne > **Urządzenia** > rozwiń  > kliknij prawym przyciskiem myszy  > kliknij **Dodaj odbiornik** > okno dialogowe **Dodaj nadajnik**

Umożliwia ręczne dodanie nadajnika. Jest to szczególnie użyteczne, gdy chce się dodać sieciowe urządzenie wizyjne firmy Bosch (tylko dla VRM).

Uwaga:

W przypadku dodawania nadajnika strumienia wideo firmy Bosch za pomocą funkcji **<Automatyczne wykrywanie>** to urządzenie musi być dostępne w sieci.

Aby dodać sieciowe urządzenie wizyjne firmy Bosch:

1. Rozwiń , rozwiń , kliknąć prawym przyciskiem myszy .
lub

Kliknąć prawym przyciskiem myszy .
lub

Kliknąć prawym przyciskiem myszy .

2. Kliknąć **Dodaj nadajnik**.
Zostanie wyświetlone okno dialogowe **Dodaj nadajnik**.
3. Wprowadzić prawidłowy adres IP.
4. Na liście zaznaczyć pozycję **<Automatyczne wykrywanie>**, wprowadź hasło dostępu do urządzenia i kliknij przycisk **Uwierzytnij**.
Lub
Na liście zaznaczyć określony typ nadajnika lub **<Symbol zastępczy jednej kamery>**.
5. Kliknij **OK**.
Urządzenie zostanie dodane do systemu.

Ikona  oznacza błąd, którym należy się zająć. Więcej informacji o charakterze błędu uzyskasz z etykiety narzędzia.

Okno dialogowe Dodaj nadajnik

Adres sieciowy

Wpisz poprawny adres IP.

Numer portu

Wpisać numer portu urządzenia.

Typ nadajnika

W przypadku urządzeń, których typ jest znany, wybierz odpowiednią pozycję. Urządzenie nie musi być dostępne w sieci.

Dodając sieciowe urządzenie wizyjne firmy Bosch, zaznacz opcję **<Automatyczne wykrywanie>**.

Urządzenie musi być dostępne w sieci.

Aby dodać kamerę w konfiguracji offline, wybierz opcję **<Symbol zastępczy jednej kamery>**.

Nazwa użytkownika

Wyświetla nazwę użytkownika używaną w celu uwierzytelniania w urządzeniu.

Hasło

Wprowadź poprawne hasło używane do uwierzytelniania w urządzeniu.

Pokaż hasło

Kliknij, aby włączyć opcję wyświetlania wprowadzonego hasła. Uważaj, aby osoby postronne nie poznały tego hasła.

Uwierzytelnij

Kliknąć, aby uwierzytelnić w urządzeniu z wykorzystaniem wprowadzonych powyżej poświadczeń.

14.2

Dodawanie nadajnika do puli VRM

Aby dodać nadajniki do puli VRM, patrz *Dodawanie nadajników poprzez skanowanie*, Strona 177.

Patrz

- *Dodawanie urządzenia*, Strona 125

14.3

Dodawanie nadajnika udostępniającego tylko podgląd bieżący

Aby dodać nadajnik udostępniający tylko podgląd bieżący poprzez skanowanie, patrz *Dodawanie urządzeń podglądu bieżącego poprzez skanowanie*, Strona 209.

Patrz

- *Dodawanie urządzenia*, Strona 125
- *strona Tylko podgląd bieżący i lokalna pamięć masowa*, Strona 209

14.4

Dodawanie nadajnika z pamięcią lokalną

Aby dodać nadajniki z obsługą lokalnego urządzenia pamięci masowej poprzez skanowanie, patrz *strona Lokalne urządzenia pamięci masowej*, Strona 211.

Patrz

- *Dodawanie urządzenia*, Strona 125
- *strona Lokalne urządzenia pamięci masowej*, Strona 211

14.5

Dodawanie pojedynczej kamery zastępczej

Aby dodać i skonfigurować kamerę, która jest aktualnie w trybie offline, można wprowadzić pojedynczą kamerę zastępczą. Kamerę taką można dodać do drzewa logicznego i map, a następnie skonfigurować dla niej zdarzenia i alarmy.

Aby dodać pojedynczą kamerę zastępczą

1. Kliknij prawym przyciskiem myszy element drzewa urządzeń, w którym chcesz dodać nową kamerę.
2. Kliknij **Dodaj nadajnik**.
Zostanie wyświetlone okno dialogowe **Dodaj nadajnik**.
3. Wpisz adres IP urządzenia, który jest obecnie w trybie offline.
4. Wybierz typ nadajnika <**Symbol zastępczy jednej kamery**>.
5. Skonfiguruj wszystkie odpowiednie ustawienia zastępczej kamery.

Aby zamienić pojedynczą kamerę zastępczą

1. Kliknij prawym przyciskiem myszy odpowiednią kamerę zastępczą.
2. Kliknij **Edytuj nadajnik**.
Zostanie wyświetlone okno dialogowe **Edytuj nadajnik**.
3. Wpisz adres sieciowy kamery, która ma zastąpić dotychczasową.
4. Wpisać prawidłowe hasło nowej kamery.
5. Kliknij przycisk **OK**.
Zostanie wyświetlone okno dialogowe **Aktualizacja nazw urządzeń**.
6. Kliknij **OK**.

Uwaga: Po zaktualizowaniu funkcji nowej kamery trzeba sprawdzić ustawienia wprowadzone w kamerach i tabeli zapisów.

14.6

Importowanie kamer z pliku CSV

Okno główne > **Urządzenia** > rozwinąć  > rozwinąć 

Z pliku CSV można importować większą liczbę kamer. Można określić nazwy nadajników lub kamer, węzły drzewa logicznego oraz grupy użytkowników, które będą miały dostęp do nowo dodanych kamer.

Szablon pliku CSV

Można użyć szablonu MassConfigurationTemplate.csv znajdującego się tutaj: C:\Program Files\Bosch\VMS\Samples.

Uwaga: Do rozgraniczania kolumn w pliku CSV należy używać przecinków.

Kolumna	Informacje
NetworkAddress	Adres IP nadajnika. Pole nie może być puste, a jego wartość musi być unikatowa.
EncoderName	Nazwa nadajnika. Pole nie może być puste.
CameraNames	Nazwa kamer powiązanych z obecnym nadajnikiem. Pole nie może być puste. Poszczególne nazwy należy rozdzielać średnikami.
UserName	Nazwa użytkownika, którą się należy uwierzytelnić w nadajniku. Pole nie może być puste.
Password	Hasło, którym się należy uwierzytelnić w nadajniku. Pole nie może być puste.

Kolumna	Informacje
LogicalTree	Ścieżki drzewa logicznego, w którym mają zostać dodane kamery. Poszczególne ścieżki należy rozdzielać średnikami. Jeśli pole jest puste, kamery nie zostaną dodane do drzewa logicznego i nie można przypisać żadnych grup użytkowników. Ścieżki w drzewie logicznym zaczynają się znakiem „/”. Znak „/” jest wymagany tylko dla węzła głównego. Przy pozostałych folderach można go nie wstawiać. W ścieżce folderu nie trzeba dodawać nazwy węzła głównego. Jeśli ścieżka nie istnieje, zostanie utworzona.
Permissions	Dozwolone grupy użytkowników. Poszczególne grupy użytkowników należy rozdzielać średnikami. Jeśli pole jest puste, kamery będą dostępne dla wszystkich grup. Grupa administratorów ma uprawnienie dostępu do wszystkich kamer. Nawet jeśli dostęp nie ma być przyznawany żadnej grupie, trzeba dodać grupę administratorów. Jeśli grupa użytkowników nie istnieje, kamera nie zostanie zaimportowana. Uwaga: Enterprise User Groups nie są obsługiwane, działają tylko Enterprise Accounts.

Przykłady:

NetworkAddress,EncoderName,CameraNames,UserName>Password,LogicalTree,Permissions

1.1.1.1,Encoder1,Camera1,service,pwd,/Folder1/Folder2/Folder3,Admin Group

2.2.2.2,Multichannel2,Camera21;Camera22,service,pwd,/Folder1/Folder2,Admin Group;Operator

Przed rozpoczęciem importowania trzeba uzyskać trzy poniższe uprawnienia:

- **Zmień właściwości urządzenia**
- **Zmień drzewo logiczne**
- **Konfiguruj grupy użytkowników/Enterprise Accounts**

Uwaga: Administrator zawsze może importować dane.

Aby zaimportować kamery z pliku CSV:

1. Prawym przyciskiem myszy kliknąć ikonę  i wybrać polecenie **Import kamer z pliku CSV...**. Zostanie otwarty Eksplorator plików.
2. Zaznaczyć odpowiedni plik CSV i kliknąć przycisk **Otwórz**.
Uwaga: Przetwarzanie pliku CSV może nieco potrwać. Maksymalna liczba importowanych kamer wynosi 250.
3. W oknie dialogowym **Import kamer z pliku CSV** zostaną wyświetlone wszystkie odnośne informacje o udanym lub nieudanym zaimportowaniu kamer. Kliknięcie przycisku **Wyświetl tylko usterki** spowoduje wyświetlenie listy kamer, których import się nie powiódł.
4. Kliknąć przycisk **Zamknij**, aby zamknąć okno dialogowe, lub przycisk **Dziennik eksportu**, aby wyeksportować i zapisać plik dziennika.

Aby wyświetlić zaimportowaną kamerę na mapie:

1. Okno główne > **Mapy i struktura** > Drzewo logiczne

2. Kliknij prawym przyciskiem myszy żądaną kamerę, a następnie wybierz **Widoczny na mapie**. Kamera zostanie wyświetlona na mapie.

14.7

Dodawanie nadajnika Bosch ze wstępnie skonfigurowaną geolokalizacją

Po dodaniu nadajnika Bosch ze wstępnie skonfigurowaną geolokalizacją (długość i szerokość geograficzna, azymut) ustawienia te zostaną zapisane w systemie BVMS, a miejsce aktywne kamery zostanie automatycznie dodane w odpowiedniej pozycji na mapie globalnej.

W przypadku zmiany położenia kamery na mapie lub jej kierunku i stożka widzenia, wystąpi niezgodność między konfiguracją geolokalizacji w systemie BVMS a tą w kamerze.

- ▶ Aby zsynchronizować konfigurację kamery z ustawieniami w BVMS, zapisz i aktywuj konfigurację BVMS.

Jeśli w ustawienia geolokalizacji kamery zostaną później zmienione, to po aktywacji konfiguracji w systemie BVMS, ustawienia w kamerze wrócą do tych zapisanych w systemie BVMS.

Patrz

- Konfigurowanie kamer na mapie globalnej, Strona 272

14.8

Edytowanie nadajnika

14.8.1

Szyfrowanie obrazu wizyjnego na żywo (Edytuj nadajnik)

Okno główne > **Urządzenia** > Rozwiń  > Rozwiń  > Rozwiń  > Kliknij  > Okno dialogowe **Edytuj nadajnik**

Okno główne > **Urządzenia** > Rozwiń  > Kliknij prawym przyciskiem myszy  > Okno dialogowe **Edytuj nadajnik**

Okno główne > **Urządzenia** > Rozwiń  > Kliknij  > Okno dialogowe **Edytuj nadajnik**

Jeśli w nadajniku skonfigurowany jest port 443 protokołu HTTPS, można włączyć bezpieczne połączenie obrazu na żywo przekazywanego przez nadajnik do następujących urządzeń:

- Komputer z programem Operator Client
- Komputer z oprogramowaniem Management Server
- Komputer z programem Configuration Client
- Komputer z usługą VRM
- Odbiornik

Uwaga:

Po włączeniu szyfrowania tryb ANR nie działa w przypadku urządzenia, do którego trafia zaszyfrowany przekaz.

Po uaktywnieniu odtwarzanie nadajnika nie działa w nadajnikach z oprogramowaniem układowym starszym niż wersja 6.30.

Tylko nadajnik z oprogramowaniem układowym w wersji 7.0 lub nowszej obsługuje bezpieczne UDP. Jeśli w takim przypadku zostanie włączone bezpieczne połączenie, użytkownik Operator Client może również przełączyć strumień na UDP i na UDP multicast.

Aby uaktywnić:

1. Zaznaczyć pole wyboru **Zabezpiecz połączenie**.
2. Kliknąć **OK**.
Bezpieczne połączenie jest włączone dla tego nadajnika.

Patrz

- Konfigurowanie trybu Multicast, Strona 234
- Okno dialogowe Edytuj nadajnik/odbiornik, Strona 222

14.8.2**Aktualizacja informacji o funkcjach urządzenia (Edytuj nadajnik)**

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > rozwiń  > kliknij prawym

przyciskiem myszy  > kliknij okno dialogowe **Edytuj nadajnik** > okno dialogowe **Edytuj nadajnik** lub

Okno główne > **Urządzenia** > Rozwiń  > Kliknij prawym przyciskiem myszy  > Kliknij **Edytuj nadajnik** > Okno dialogowe **Edytuj nadajnik** lub

Okno główne > **Urządzenia** > Rozwiń  > Kliknij prawym przyciskiem myszy  > Kliknij **Edytuj nadajnik** > Okno dialogowe **Edytuj nadajnik** lub

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > kliknij prawym przyciskiem myszy 

 > kliknij **Edytuj odbiornik** > okno dialogowe **Edytuj odbiornik**

Po zakończeniu rozbudowy urządzenia można zaktualizować informacje dotyczące jego wydajności. Tekst komunikatu informuje, czy pobrane dane o wydajności urządzenia są zgodne z informacjami zapisanymi w BVMS.

Aby zaktualizować program:

1. Kliknij **OK**.
Zostanie wyświetlone okno komunikatu zawierające wiadomość:
Jeśli zatwierdzisz informacje dotyczące wydajności urządzenia, ustawienia zapisu i ustawienia zdarzeń tego urządzenia mogą ulec zmianie. Sprawdź ustawienia tego urządzenia.
2. Kliknij **OK**.
Informacje o wydajności urządzenia zostały zaktualizowane.

Patrz

- Okno dialogowe Edytuj nadajnik/odbiornik, Strona 222

14.8.3**Okno dialogowe Edytuj nadajnik/odbiornik**

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > rozwiń  > kliknij prawym

przyciskiem myszy  > kliknij okno dialogowe **Edytuj nadajnik** > okno dialogowe **Edytuj nadajnik** lub

Okno główne > **Urządzenia** > Rozwiń  > Kliknij prawym przyciskiem myszy  > Kliknij **Edytuj nadajnik** > Okno dialogowe **Edytuj nadajnik** lub

Okno główne > **Urządzenia** > Rozwiń  > Kliknij prawym przyciskiem myszy  > Kliknij **Edytuj nadajnik** > Okno dialogowe **Edytuj nadajnik**
lub

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > kliknij prawym przyciskiem myszy  > kliknij **Edytuj odbiornik** > okno dialogowe **Edytuj odbiornik**

Umożliwia sprawdzanie i aktualizowanie możliwości urządzenia. Po otwarciu tego okna nawiązywane jest połączenie z urządzeniem. Po weryfikacji hasła dane dotyczące wydajności urządzenia są porównywane z informacjami zapisanymi w BVMS.

Nazwa

Wyświetla nazwę urządzenia. Podczas dodawania sieciowego urządzenia wizyjnego firmy Bosch wygenerowana zostaje nazwa urządzenia. Jeśli jest to wymagane, należy zmienić wprowadzone dane.

Adres/port sieciowy

Wprowadź adres sieciowy urządzenia. Jeśli jest to wymagane, zmień numer portu.

Nazwa użytkownika

Wyświetla nazwę użytkownika używaną w celu uwierzytelniania w urządzeniu.

Hasło

Wprowadź poprawne hasło używane do uwierzytelniania w urządzeniu.

Pokaż hasło

Kliknij, aby włączyć opcję wyświetlania wprowadzonego hasła. Uważaj, aby osoby postronne nie poznały tego hasła.

Uwierzytelnij

Kliknąć, aby uwierzytelnić w urządzeniu z wykorzystaniem wprowadzonych powyżej poświadczeń.

Bezpieczeństwo

Pole wyboru **Zabezpiecz połączenie** jest domyślnie zaznaczone.

Jeśli połączenie bezpieczne jest niemożliwe, zostanie wyświetlony odpowiedni komunikat. Kliknąć, aby usunąć zaznaczenie.

Następujące odbiorniki obsługują bezpieczne połączenie:

- VJD 7000
- VJD 8000
- VIP XD HD



Uwaga!

Połączenie pomiędzy odbiornikiem i nadajnikiem jest bezpieczne, jeśli oba urządzenia zostały skonfigurowane z obsługą bezpiecznego połączenia.

Strumień wizyjny

UDP: umożliwia szyfrowany streaming multicast do obsługiwanych odbiorników.

TCP: umożliwia szyfrowany sstreaming unicast do obsługiwanych odbiorników.

Uwaga: Jeśli w nadajniku nie zostanie skonfigurowany adres multicast, odbiornik będzie przyjmował strumień w formie unicast.

**Uwaga!**

Oprogramowanie BVMS nie obsługuje kamer Bosch podłączonych do bramy VSG.
BVMS obsługuje szyfrowanie protokołem UDP tylko dla platform starszych niż CPP13.

Wydajność urządzenia

Wyświetlone informacje o wydajności urządzenia można sortować według kategorii lub alfabetycznie. Tekst komunikatu informuje, czy wykryte dane o wydajności urządzenia są zgodne z bieżącymi informacjami.

Kliknij przycisk **OK**, aby wprowadzić zmiany dotyczące wydajności urządzenia po jego rozbudowie.

Patrz

- Szyfrowanie obrazu wizyjnego na żywo (Edytuj nadajnik), Strona 221
- Aktualizacja informacji o funkcjach urządzenia (Edytuj nadajnik), Strona 222

14.9

Zarządzanie sprawdzaniem autentyczności

Aby uaktywnić sprawdzanie autentyczności w nadajniku, należy wykonać następujące czynności:

- Skonfigurować uwierzytelnianie w nadajniku.
- Pobrać certyfikat z nadajnika.
- Zainstalować ten certyfikat nadajnika na stacji roboczej służącej do sprawdzania autentyczności.

Patrz

- Sprawdzanie autentyczności , Strona 224

14.9.1

Sprawdzanie autentyczności

Użytkownik programu Operator Client może sprawdzać autentyczność nagrań. Autentyczność eksportów jest sprawdzana automatycznie.

Administrator musi wykonać poniższe czynności, aby zapewnić nieprzerwany łańcuch certyfikatów.

W przypadku rozbudowanych instalacji (> 30 kamer) zaleca się następującą procedurę:

- Należy uzyskać certyfikat urzędu certyfikacji (CA) dla każdego nadajnika.
- W bezpieczny sposób należy przesłać wydany certyfikat (w tym klucz prywatny) do każdego nadajnika.
- Należy zainstalować certyfikat CA na stacjach roboczych Operator Client, na których będzie sprawdzana autentyczność lub na innych komputerach, na których będzie wykonywany eksport danych.

W przypadku małych instalacji (< 30 kamer) zaleca się następującą procedurę:

- Należy pobrać z każdego nadajnika certyfikat *HTTPS Server*.
- Zainstalować te certyfikaty na stacjach roboczych z programem Operator Client, na których ma być sprawdzane uwierzytelnianie.

Szczegółowe informacje na ten temat można uzyskać od zespołu pomocy technicznej działu informatycznego swojej firmy.

Aby uaktywnić bezpieczne sprawdzanie autentyczności, administrator musi wykonać następujące działania:

- Włącz uwierzytelnianie w każdej kamerze objętej sprawdzaniem autentyczności.
- W przypadku rozbudowanych instalacji: przesłać i przypisać odpowiedni certyfikat do każdej kamery objętej sprawdzaniem autentyczności.
- W przypadku małych instalacji: pobierz certyfikat z każdego nadajnika. Zainstaluj na stacji roboczej certyfikaty umożliwiające sprawdzanie autentyczności.

Ograniczenia

Wymagane jest oprogramowanie układowe w wersji 6.30 lub nowszej.

Zaleca się sprawdzanie autentyczności maksymalnie 4 kamer jednocześnie.

Użytkownik programu Operator Client nie może sprawdzać autentyczności obrazu na żywo.

Uwaga: nie należy zmieniać certyfikatu, gdy trwa zapisywanie obrazu. Aby zmienić certyfikat, należy najpierw zatrzymać zapisywanie, zmienić certyfikat i wznowić zapisywanie.

W celu sprawdzenia autentyczności zapisu jest on odtwarzany w tle z maksymalną prędkością. W przypadku sieci o małej szerokości pasma odtwarzanie może być powolne. Proces sprawdzania może więc wtedy potrwać tak długo, jak przedział czasowy wybrany do sprawdzania. Przykład: wybrano przedział czasowy o długości 1 godziny. Proces sprawdzania może trwać maksymalnie 1 godzinę. Użytkownik może sprawdzać tylko autentyczność zapisu. Jeśli proces sprawdzania się nie powiedzie, nie oznacza to automatycznie, że obraz został zmanipulowany. Niepowodzenie może mieć wiele przyczyn, np. ręczne usuwanie fragmentów zapisu. Użytkownik programu Operator Client nie ma możliwości rozróżnienia między zamierzoną zmianą a manipulacją w celu oszustwa.

Uwierzytelnianie materiału wizyjnego dotyczy wyłącznie metod sprawdzania autentyczności obrazu.

Uwierzytelnianie materiału wizyjnego nie dotyczy w żaden sposób jego przesyłania ani samych danych.

Funkcja znaku wodnego służąca do sprawdzania autentyczności w starszych wersjach systemu BVMS została zastąpiona. Nowy sposób sprawdzania autentyczności staje się automatycznie dostępny po uaktualnieniu do najnowszej wersji systemu BVMS. Nie można obecnie zweryfikować kontroli autentyczności, które zakończyły się kiedyś pomyślnie, ponieważ takie nagrania nie zawierają wymaganych informacji dodatkowych.

Sprawdzanie autentyczności nie jest obsługiwane w następujących przypadkach:

- Transkodowanie
- Zapis lokalny
- Urządzenie VSG
- Cyfrowy rejestrator wizyjny
- Bosch Recording Station
- ANR

Patrz

- Konfigurowanie uwierzytelniania, Strona 225
- Przesyłanie certyfikatu, Strona 226
- Pobieranie certyfikatu, Strona 226
- Instalowanie certyfikatu na stacji roboczej, Strona 226

14.9.2

Konfigurowanie uwierzytelniania

Okno główne > **Urządzenia** > rozwiń węzeł  > rozwiń węzeł  > rozwiń węzeł  >

lub

Okno główne > **Urządzenia** > rozwiń węzeł  > 

Można włączyć w nadajniku sprawdzanie autentyczności.

Aby przeprowadzić konfigurację:

1. Kliknij kolejno przyciski: **Kamera** i **Wejście wizyjne**.
2. Na liście **Uwierzytelnianie wideo** wybierz pozycję **SHA-256**.
3. Na liście **Interwały podpisywania** wybierz odpowiednią wartość.

Mała wartość zapewnia wzrost bezpieczeństwa, a duża — zmniejsza obciążenie nadajnika.

4. Kliknij przycisk .

14.9.3

Przesyłanie certyfikatu

Okno główne > **Urządzenia** > rozwiń węzeł  > rozwiń węzeł  > rozwiń węzeł  > 

lub

Okno główne > **Urządzenia** > rozwiń węzeł  > 

Certyfikat pochodny można przesłać do nadajnika.

Aby przesłać:

1. Kliknij kolejno przyciski: **Serwis** i **Certyfikaty**.
2. Kliknij przycisk **Prześlij certyfikat**.
3. Wybierz odpowiedni plik zawierający certyfikat przeznaczony do danego nadajnika. W pliku tym musi się znajdować klucz prywatny, np. *.pem.
Zadbaj o bezpieczne przesłanie danych.
4. Kliknij przycisk **Otwórz**.
5. Na liście **Wykorzystanie** wybierz pozycję **Serwer HTTPS**, aby przypisać do niej przesłany certyfikat.

6. Kliknij ikonę .

14.9.4

Pobieranie certyfikatu

Okno główne > **Urządzenia** > rozwiń węzeł  > rozwiń węzeł  > rozwiń węzeł  > 

lub

Okno główne > **Urządzenia** > rozwiń węzeł  > 

Certyfikat można pobrać z nadajnika.

Aby pobrać:

1. Kliknąć kolejno przyciski: **Serwis** i **Certyfikaty**.
2. Wybrać odpowiedni certyfikat, a następnie kliknąć ikonę *Save*.
3. Wybrać odpowiedni katalog, aby zapisać w nim plik certyfikatu.
4. Zmienić nazwę rozszerzenia pliku certyfikatu na *.cer.

Można teraz zainstalować ten certyfikat na stacji roboczej, na której ma być sprawdzana autentyczność.

14.9.5

Instalowanie certyfikatu na stacji roboczej

Certyfikat pobrany z nadajnika można zainstalować na stacji roboczej, na której ma być sprawdzana autentyczność.

1. Na stacji roboczej uruchom program *Microsoft Management Console*.
2. Dodaj na tym komputerze przystawkę *Certificates* z zaznaczoną opcją *Computer account*.

3. Rozwiń kolejno węzły: *Certificates (Local computer)* i *Trusted Root Certification Authorities*.
4. Kliknij pozycję *Certificates* prawym przyciskiem myszy, wskaż pozycję *All Tasks*, a następnie kliknij przycisk *Import...*
Pojawi się *Certificate Import Wizard*.
Opcja *Local Machine* jest domyślnie zaznaczona i nie można tego zmienić.
5. Kliknij przycisk *Next*.
6. Wybierz plik certyfikatu pobrany z nadajnika.
7. Kliknij przycisk *Next*.
8. Pozostaw ustawienia bez zmian i kliknij przycisk *Next*.
9. Pozostaw ustawienia bez zmian i kliknij przycisk *Finish*.

14.10

Dostarczanie hasła docelowego dla dekodera (Uwierzytelnij...)

Okno główne > **Urządzenia** > Rozwiń  > Rozwiń  > Kliknij prawym przyciskiem myszy

 > Kliknij **Uwierzytelnij...** > Okno dialogowe **Wprowadź hasło**

Aby umożliwić dostęp chronionego hasłem nadajnika do dekodera, należy wprowadzić w dekodерze hasło poziomu autoryzacji użytkownika nadajnika jako hasło docelowe.

Aby wprowadzić hasło:

1. Na liście **Wprowadź nazwę użytkownika** wybierz pozycję *destination password*.
 2. W polu **Wprowadź hasło dla użytkownika** wpisz nowe hasło.
 3. Kliknąć **OK**.
- ⇒ Hasło na urządzeniu zostanie natychmiast zmienione.

Patrz

– Zmiana hasła nadajnika/dekodera (*Zmień hasło / Wprowadź hasło*), Strona 227

14.11

Zmiana hasła nadajnika/dekodera (Zmień hasło / Wprowadź hasło)

Okno główne > **Urządzenia** > rozwinąć  > rozwinąć  >  > 
lub

Okno główne > **Urządzenia** >  > 
lub

Okno główne > **Urządzenia** >  > 
lub

Okno główne > **Urządzenia** > Rozwiń  > Rozwiń  > 
Określ i zmień hasła osobno dla każdego z poziomów. Wpisz hasło (maks. 19 znaków bez znaków specjalnych) dla wybranego poziomu.

Aby zmienić hasło:

1. Kliknij prawym przyciskiem myszy , a następnie kliknij polecenie **Zmień hasło...**
Pojawi się okno dialogowe **Wprowadź hasło**.
2. Na liście **Wprowadź nazwę użytkownika** zaznacz żądanego użytkownika, dla którego chcesz zmienić hasło.

3. W polu **Wprowadź hasło dla użytkownika** wpisz nowe hasło.
 4. Kliknij **OK**.
- ⇒ Hasło na urządzeniu zostanie natychmiast zmienione.

Hasło uniemożliwia dostęp do urządzenia osobom nieuprawnionym. Do kontroli dostępu można używać różnych poziomów autoryzacji.

Właściwa ochrona hasłem jest zagwarantowana tylko wówczas, gdy wszystkie wyższe poziomy autoryzacji są także chronione hasłem. Przydzielając hasła, należy zawsze zaczynać od najwyższego poziomu autoryzacji.

Można zdefiniować i zmienić hasło dla każdego z poziomów autoryzacji, jeśli użytkownik jest zalogowany do konta użytkownika „service”.

Urządzenie obsługuje trzy poziomy autoryzacji: service, user i live.

- Poziom service jest najwyższym poziomem autoryzacji. Po wprowadzeniu prawidłowego hasła użytkownik uzyskuje dostęp do wszystkich funkcji i może zmieniać wszystkie ustawienia konfiguracyjne.
- Poziom user jest średnim poziomem autoryzacji. Umożliwia on na przykład obsługę urządzenia, odtwarzanie nagrań oraz sterowanie kamerami, ale nie pozwala zmieniać ustawień konfiguracyjnych.
- Poziom live jest najniższym poziomem autoryzacji. Umożliwia on tylko podgląd obrazu wideo na żywo i przełączanie pomiędzy różnymi obrazami na żywo.

Dla dekodera następujący poziom autoryzacji zastępuje poziom autoryzacji live:

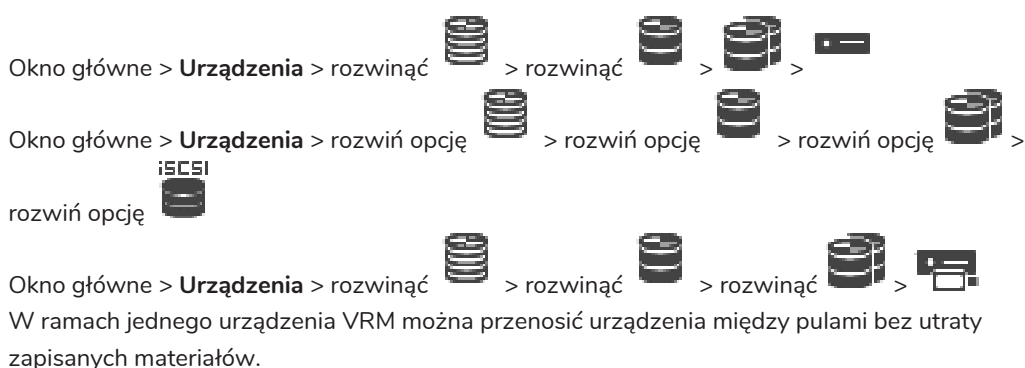
- destination password (dostępne tylko dla dekodów)
- Używane do dostępu do nadajnika.

Patrz

- Dostarczanie hasła docelowego dla dekodera (Uwierzytelnij...), Strona 227

14.12

Przenoszenie nadajnika do innej puli (Zmień pulę)



Aby przenieść urządzenie:

1. Kliknąć prawym przyciskiem myszy  /  / , a następnie kliknąć **Zmień pulę**
Zostanie wyświetlone okno dialogowe **Zmień pulę**.
 2. Wybrać odpowiednią pulę z listy **Nowa pula:**.
 3. Kliknąć przycisk **OK**.
- Urządzenie zostanie przeniesione do wybranej puli.

Okno dialogowe Zmień pulę

Umożliwia zmianę puli, do której przypisane jest urządzenie.

Obecna pula:

Wyświetla numer puli, do której jest obecnie przypisane wybrane urządzenie.

Nowa pula:

Wybierz żądany numer puli.

14.13**Odzyskiwanie zapisów z wymienianego nadajnika (Tworzenie powiązań z zapisami poprzednika)**

Okno główne > **Urządzenia** > rozwiń  > rozwiń  >  > 

W przypadku wymiany uszkodzonego nadajnika nagrania wymienianego nadajnika będą dostępne dla nowego nadajnika w przypadku wybrania nowego nadajnika w programie Operator Client.

**Uwaga!**

Nadajnik można wymienić wyłącznie na nadajnik o takiej samej liczbie kanałów.

Aby odzyskać nagrania z wymienianego nadajnika**Uwaga!**

Nie używaj polecenia **Edytuj nadajnik**.

1. Kliknij prawym przyciskiem myszy polecenie  > **Powiąż z zapisami poprzednika....**
2. Zostanie wyświetlone okno dialogowe **Powiąż z zapisami poprzednika....**
3. Wprowadź adres sieci i prawidłowe hasło dla nowego urządzenia.
4. Kliknij **OK**.

5. Kliknij , aby zapisać ustawienia.

6. Kliknij , aby uaktywnić konfigurację.

Okno dialogowe Powiąż z zapisami poprzednika...

Umożliwia odzyskanie zapisów z wymienianego nadajnika. Po skonfigurowaniu ustawień w oknie dialogowym zapisy z wymienianego nadajnika będą dostępne dla nowego nadajnika po wybraniu nowego nadajnika w programie Operator Client.

Adres/port sieciowy

Wprowadź adres sieciowy urządzenia.

Nazwa użytkownika

Wyświetla nazwę użytkownika używaną w celu uwierzytelniania w urządzeniu.

Hasło

Wprowadź poprawne hasło używane do uwierzytelniania w urządzeniu.

Uwierzytelnij

Kliknij, aby uwierzytelnić się na urządzeniu z wykorzystaniem wprowadzonych powyżej danych uwierzytelniających.

14.14 Konfigurowanie nadajników/odbiorników

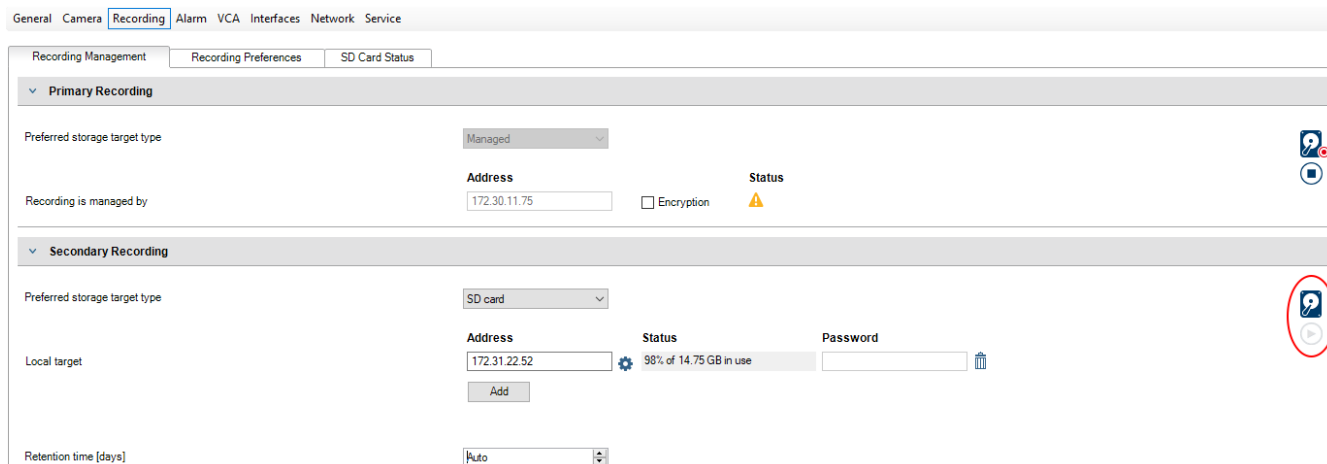
14.14.1 Konfigurowanie nośnika zapisu nadajnika

Okno główne > **Urządzenia** > rozwiń  > rozwiń  >  >  > **Ustawienia zaawansowane** > **Zarządzanie zapisem**

Uwaga: Należy się upewnić, że żądane kamery tego nadajnika są dodane do drzewa logicznego.

Nośnik zapisu nadajnika należy skonfigurować pod kątem użycia funkcji ANR.

Uwaga: aby skonfigurować nośnik zapisu nadajnika, który został już dodany do systemu i jest zapisany przez usługę VRM, należy upewnić się, że zapis pomocniczy jest zatrzymany:



Funkcja ANR działa tylko na nadajnikach z oprogramowaniem układowym w wersji 5.90 lub wyższej. Nie wszystkie typy nadajników obsługują funkcję ANR, nawet jeśli mają zainstalowaną prawidłową wersję oprogramowania układowego.

Aby skonfigurować nośnik zapisu nadajnika, należy:

1. W obszarze **Zapis pomocniczy** na liście **Preferowany typ miejsca docelowego zapisu** wybrać nośnik zapisu. W zależności od typu urządzenia dostępne będą różne nośniki.
2. W razie potrzeby kliknąć przycisk ..., aby sformatować nośnik zapisu. Po udanym zakończeniu formatowania nośnik zapisu jest gotowy do użycia za pomocą funkcji ANR.
3. Skonfiguruj funkcję ANR pod kątem tego nadajnika na stronie **Kamery i zapis**.

Patrz

- Strona Zarządzanie zapisem, Strona 233
- Konfigurowanie funkcji ANR, Strona 302

14.14.2 Konfiguracja wielu nadajników / odbiorników

okno główne

Użytkownik może jednocześnie modyfikować następujące właściwości wielu nadajników i odbiorników:

- Hasła urządzeń
- Adresy IP
- Wyświetlanie nazw
- Maska podsieci
- Identyfikator bramy
- Wersje oprogramowania układowego

Aby wybrać wiele urządzeń:

- ▶ Wybrać wymagane urządzenia za pomocą klawiszy CTRL lub SHIFT.

Aby wybrać wszystkie dostępne urządzenia:

- ▶ Kliknąć polecenie  **Zaznacz wszystkie.**

Aby zmienić hasło dla wielu urządzeń:

1. W oknie głównym **Urządzenia** kliknąć polecenie  **Zmień hasła urządzenia.**
Lub
w menu **Urządzenie** kliknąć **Zmień hasła urządzenia...**
Zostanie wyświetlone okno dialogowe **Zmień hasła urządzenia.**
2. Zaznaczyć żądane urządzenia.
3. Kliknąć prawym przyciskiem myszy zaznaczone urządzenia.
4. Kliknąć **Edytuj hasło....** Zostanie wyświetlone okno dialogowe **Zmianie hasel.**
5. Wprowadzić odpowiednie ustawienia.

**Uwaga!**

Można wybrać tylko te typy haseł, które są dostępne dla wszystkich wybranych urządzeń.

Aby skonfigurować wyświetlanie wielu nazw:

1. W menu **Urządzenie** kliknij pozycję **Zmień adres IP urządzenia i ustawienia sieciowe...**
Zostanie wyświetlone okno dialogowe **Zmień adres IP urządzenia i ustawienia sieciowe.**
2. Zaznaczyć żądane urządzenia.
3. Kliknąć prawym przyciskiem myszy zaznaczone urządzenia.
4. Kliknąć **Ustaw wyświetlanie nazw....**
Zostanie wyświetlone okno dialogowe **Ustaw wyświetlanie nazw.**
5. Wprowadzić odpowiednie ustawienia.

Aby skonfigurować wiele adresów IP:**Uwaga!**

Zmiana adresu IP urządzenia sieciowego może spowodować, że nie będzie ono dostępne.

1. W menu **Urządzenie** kliknij pozycję **Zmień adres IP urządzenia i ustawienia sieciowe...**
Zostanie wyświetlone okno dialogowe **Zmień adres IP urządzenia i ustawienia sieciowe.**
2. Zaznaczyć żądane urządzenia.
3. Kliknąć prawym przyciskiem myszy zaznaczone urządzenia.
4. Kliknąć **Ustaw adresy IP....**
Zostanie wyświetlone okno dialogowe **Ustaw adresy IP.**
5. Wprowadzić odpowiednie ustawienia.

Aby zmienić maskę podsieci/identyfikator bramy dla wielu urządzeń:

1. Kliknąć w polu wymaganym jednego z urządzeń, dla którego ma być zmieniona wartość.

2. Wprowadzić odpowiednią wartość.
3. Zaznaczyć wszystkie żądane urządzenia.
4. Kliknąć prawym przyciskiem myszy żądane pole w urządzeniu, którego wartość została już zmieniona.
5. Kliknąć polecenie **Kopiuj komórkę do** i polecenie **Zaznaczenie w kolumnie** .
Lub kliknąć polecenie **Uzupełnij kolumnę** , jeśli jest to wymagane.

**Uwaga!**

Można także kopiować kompletne wiersze, aby zmieniać adresy IP, nazwy wyświetlane, maski podsieci i identyfikatory bram dla wielu urządzeń.

Aby uaktualnić oprogramowanie układowe dla wielu urządzeń:

1. W menu **Urządzenie** kliknąć pozycję **Aktualizuj oprogramowanie układowe urządzenia....**
Zostanie wyświetlone okno dialogowe **Aktualizuj oprogramowanie układowe urządzenia.**
2. Zaznaczyć żądane urządzenia.
3. Kliknąć polecenie **Aktualizuj oprogramowanie układowe.**
4. Wybrać plik zawierający aktualizację.
5. Kliknąć **OK**.

Wynik działania

Wyświetla odpowiedni stan odpowiednich urządzeń.

14.14.3**Konfigurowanie trybu zapisu awaryjnego w nadajniku**

Okno główne > **Urządzenia** > rozwinąć  > rozwinąć  >  > 

Warunki wstępne: na stronie **Pula** należy z listy **Tryb preferencji nagrywania** wybrać pozycję **Przełączenie awaryjne**. Jeśli wybrano opcję **Auto**, ustawienia są wprowadzane automatycznie i nie można ich konfigurować.

Aby korzystać z lokalizacji pomocniczej w przypadku trybu automatycznego i awaryjnego, należy: na stronie **Pula** wybrać z listy **Użycie lokalizacji drugorzędnej** pozycję **Wł.**

Zaleca się skonfigurowanie trybu awaryjnego w przypadku co najmniej 2 urządzeń iSCSI.

Aby przeprowadzić konfigurację, należy:

1. Kliknąć **Ustawienia zaawansowane**.
2. Kliknąć **Preferencje zapisu**.
3. W pozycji **Cel podstawowy** należy wybrać wpis odpowiadający żądanej lokalizacji docelowej. Wszystkie systemy pamięci masowej zostaną wyświetlone na liście w sekcji **Systemy zapisu**.
4. W pozycji **Lokalizacja drugorzędnej** należy wybrać wpis odpowiadający żądanej lokalizacji docelowej. Na liście wyświetlane są wszystkie systemy pamięci masowej wprowadzone w pozycji **Systemy zapisu**.

Zmiany są wprowadzane natychmiast. Aktywacja nie jest wymagana.

Tematy pokrewne

- Konfigurowanie automatycznego trybu zapisu dla puli, Strona 180

14.14.4 Strona Zarządzanie zapisem



Aktywne nagrania są oznaczone ikoną . Najedź kursorem na tę ikonę. Pojawią się szczegółowe informacje o aktywnych zapisach.

Zapisy zarządzane ręcznie

Zarządzanie nagraniami odbywa się lokalnie w tym nadajniku. Wszelkie niezbędne ustawienia należy wprowadzać ręcznie. Nadajnik/kamera IP działa jako urządzenie udostępniające tylko podgląd bieżący. Urządzenie to nie jest automatycznie usuwane z systemu VRM.

Zapis 1 zarządzany przez VRM

Nagraniami tego nadajnika zarządza system VRM.

Podwójny VRM

Nagraniami 2 tego nadajnika zarządza zapasowy program VRM.

Karta Nośniki iSCSI

Kliknij, aby wyświetlić dostępne pamięci masowe iSCSI połączone do danego nadajnika.

Karta Nośniki lokalne

Kliknij, aby wyświetlić dostępne pamięci masowe w tym nadajniku.

Dodaj

Kliknij, aby dodać urządzenie pamięci masowej do listy zarządzanych nośników pamięci.

Usuń

Kliknij, aby usunąć urządzenie pamięci masowej z listy zarządzanych nośników pamięci.

Patrz

– Konfigurowanie nośnika zapisu nadajnika, Strona 230

14.14.5 Strona Preferencje zapisu

Strona **Preferencje zapisu** zapisu jest wyświetlana dla każdego nadajnika. Ta strona jest wyświetlana tylko w przypadku przypisania urządzenia do systemu VRM.

Cel podstawowy

Jest wyświetlana tylko wtedy, gdy dla listy **Tryb preferencji zapisu** na stronie **Pula** wybrane jest ustawienie **Przełączenie awaryjne**.

Należy wybrać wpis odpowiadający właściwej lokalizacji docelowej.

Lokalizacja drugorzędnej

Jest wyświetlana tylko wtedy, gdy dla listy **Tryb preferencji zapisu** na stronie **Pula** jest wybrane ustawienie **Przełączenie awaryjne**, a dla listy **Wykorzystanie lokalizacji drugorzędnej** ustawienie **Wł..**

Należy wybrać wpis odpowiadający właściwej lokalizacji docelowej w celu skonfigurowania trybu awaryjnego.

Patrz

– Strona puli, Strona 179

14.14.6 Konfiguracja dekoderek do wyświetlania OSD

Aby włączyć wyświetlanie OSD (OSD) dla dekoderek, należy skonfigurować odpowiednie ustawienia dekodera.

Konfiguracja technologii VIDEOJET decoder 8000

Okno główne > **Urządzenia** > Rozwiń  > Rozwiń  >  > **Zaawansowane** > **Wyświetlanie**

W sekcji **Display stamping (Wyświetlanie informacji na obrazie)** skonfiguruj następujące ustawienia:

- **Alarm mode stamping (Wyświetlanie informacji i alarmach):** wybierz **Custom (Niestandardowe)**
- Wprowadź współrzędne **X** i **Y**, aby wskazać położenie etykiety OSD.
- Ustaw żadaną wysokość tekstu alarmu, jego kolor oraz kolor tła.

Konfigurowanie VIDEOJET decoder 7513, VIDEOJET decoder 7523

Okno menu > **Urządzenia** > Rozwiń  > Rozwiń  >  > **Advanced (Zaawansowane)** > **Wyświetlanie**

W sekcji **Display stamping (Wyświetlanie informacji na obrazie)** skonfiguruj następujące ustawienia:

- **Alarm mode stamping (Wyświetlanie informacji i alarmach):** wybierz **Custom (Niestandardowe)**
- Wprowadź współrzędne **X** i **Y**, aby wskazać położenie etykiety OSD.
- Ustaw żadaną wysokość tekstu alarmu, jego kolor oraz kolor tła.

W sekcji **Overlay mode (Tryb nakładki)** skonfiguruj następujące ustawienia:

- **Overlay mode (Tryb nakładki):** wybierz **Text (Tekst)**

14.15**Konfigurowanie trybu Multicast**

Dla każdej przypisanej kamery można skonfigurować adres i port trybu Multicast.

Aby skonfigurować tryb Multicast:

1. Zaznacz żądane pole wyboru, aby włączyć tryb Multicast.
2. Wprowadź prawidłowy adres Multicast i numer portu.
3. W razie potrzeby skonfiguruj ciągłą transmisję strumieniową pod adres Multicast.

Karta Multicast

Okno główne > **Urządzenia** >  > 
LUB

Okno główne > **Urządzenia** >  > 
LUB

Okno główne > **Urządzenia** > rozwinąć  > rozwinąć  >  > 
> karta **Sieć** > karta **Multicast**

Umożliwia skonfigurowanie trybu Multicast dla przydzielonych kamer.

Włącz

Kliknąć, aby włączyć tryb Multicast dla tej kamery.

Adres multicastingu

Wprowadzić prawidłowy adres Multicast (w zakresie od 224.0.0.0 do 239.255.255.255).

Wprowadzić 1.0.0.0 Niepowtarzalny adres Multicast jest wstawiany automatycznie na podstawie adresu MAC urządzenia.

Port

Jeśli używana jest zaporą sieciowa, należy wpisać numer portu, który nie jest przez nią blokowany.

Przes. strum

Kliknąć, aby włączyć w przełączniku tryb ciągłego strumieniowania Multicast. Oznacza to, że połączenie w trybie Multicast nie jest poprzedzone rejestracją RCP+. Nadajnik zawsze przesyła wszystkie dane do przełącznika. Natomiast przełącznik (jeśli filtrowanie trybu Multicast IGMP nie jest obsługiwane lub nie zostało skonfigurowane) wysyła te dane do wszystkich portów. W rezultacie przełącznik zostaje przepełniony.

Przesyłanie strumieniowe jest konieczne w przypadku odbierania strumienia Multicast za pomocą urządzeń innych producentów.

**Uwaga!**

Strumienie Multicast są bezpieczne tylko wtedy, gdy nadajnik ma oprogramowanie układowe w wersji 7.0 lub nowszej i zaznaczone jest pole wyboru **Zabezpiecz połączenie**.

Patrz

- Szyfrowanie obrazu wizyjnego na żywo (Edytuj nadajnik), Strona 221

15 Strona ONVIF

Okno główne > **Urządzenia** > rozwiń  > 

lub

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > rozwiń  > rozwiń  > 

Patrz

- Strona Urządzenie Video Streaming Gateway, Strona 198
- strona Tylko podgląd bieżący i lokalna pamięć masowa, Strona 209

15.1 Dodawanie urządzenia ONVIF tylko do podglądu bieżącego za pomocą skanowania

Aby poprzez skanowanie dodać urządzenia ONVIF tylko z podglądem bieżącym:

1. Kliknąć prawym przyciskiem myszy  i wybrać **Skanuj w poszukiwaniu nadajników ONVIF tylko podglądu bieżącego**.
Zostanie wyświetlone okno dialogowe **BVMS Scan Wizard**.
2. Zaznaczyć pola wyboru odpowiadające urządzeniom, które mają zostać dodane.
3. Kliknij **Dalej >>**.
Zostanie wyświetlone okno dialogowe kreatora **Uwierzytelnianie urządzeń**.
4. Wpisać hasło w przypadku każdego urządzenia, które jest nim chronione.
Jeśli przez kilka sekund nie wprowadzisz żadnego znaku w polu hasła lub klikniesz poza tym polem, sprawdzenie hasła następuje automatycznie.
Jeśli hasło do wszystkich urządzeń jest identyczne, można wpisać je w pierwszym polu **Hasło**.
Następnie kliknąć to pole prawym przyciskiem myszy i wybrać opcję **Kopiuj komórkę do kolumny**.

Udane logowanie jest oznaczane w kolumnie **Stan** ikoną .

Nieudane próby logowania są oznaczane ikoną .

5. Kliknąć **Zakończ**.
Urządzenie zostanie dodane do drzewa urządzeń.

15.2 Strona Nadajnik zgodny ze standardem ONVIF

Okno główne > **Urządzenia** > Rozwiń  > Rozwiń  > Rozwiń  > Rozwiń  >

 > karta **Nadajnik ONVIF**

lub

Okno główne > **Urządzenia** > Rozwiń  >  > karta **Nadajnik ONVIF**

Umożliwia wyświetlanie informacji o dodanym do systemu BVMS nadajniku ONVIF, który udostępnia tylko podgląd na żywo.

Nazwa

Wyświetla nazwę urządzenia ONVIF. Nazwę urządzenia można zmienić bezpośrednio w oknie Drzewo urządzeń.

Adres sieciowy

Wyświetla adres IP urządzenia.

Producent

Umożliwia wyświetlanie nazwy producenta.

Model

Umożliwia wyświetlanie nazwy modelu.

Oprogramowanie układowe

Wyświetla wersję oprogramowania układowego.

Profil ONVIF

Umożliwia wyświetlenie skonfigurowanego profilu.

Profil ONVIF G

Wyświetla, czy koder ONVIF obsługuje profil G i czy aktywne jest lokalne nagrywanie.

Liczba wejść wideo

Wyświetla liczbę kamer podłączonych do tego nadajnika.

Liczba wejść audio

Wyświetla liczbę wejść fonicznych podłączonych do tego nadajnika.

Liczba wejść alarmowych

Wyświetla liczbę wejść alarmowych podłączonych do tego nadajnika.

Liczba przekaźników

Wyświetla liczbę przekaźników podłączonych do tego nadajnika.

Patrz

- Strona ONVIF Encoder Events (Zdarzenia nadajników ONVIF), Strona 237
- Dodawanie nadajnika udostępniającego tylko podgląd bieżący, Strona 218
- Konfigurowanie tabeli odwzorowań ONVIF, Strona 241

15.3

Strona ONVIF Encoder Events (Zdarzenia nadajników ONVIF)

Z systemu BVMS w wersji 10.0 wydarzenia nadajnika ONVIF mogą być pobierane bezpośrednio z VSG lub nadajnika ONVIF. Po dodaniu nowego nadajnika ONVIF pole wyboru **zdarzenia pobrania ONVIF z VSG (Profil S, T)** jest domyślnie zaznaczone, a profil T jest obsługiwany.

Następujące funkcje są obsługiwane tylko w przypadku, gdy nadajnik ONVIF został dodany do systemu za pośrednictwem urządzenia VSG:

- Jeśli zdarzenia nadajnika ONIV są pobierane z VSG, domyślne zdarzenia ONVIF są już odwzorowane.
- Operator może włączać lub wyłączać przekaźniki w aplikacji Operator Client

**Uwaga!**

Pobieranie zdarzeń ONVIF z VSG jest obsługiwane tylko w wersji VSG 7.0. Po przeprowadzeniu migracji do systemu BVMS w wersji 10.0 istniejące zdarzenia nadajnika ONVIF są pobierane bezpośrednio z nadajnika ONVIF. Należy zaktualizować VSG do wersji 7.0.

Okno główne > **Urządzenia** > Rozwiń  > Rozwiń  > Rozwiń  > Rozwiń  >
 > karta **Zdarzenia nadajników ONVIF**
 lub

Okno główne > **Urządzenia** > Rozwiń  >  > karta **Zdarzenia nadajników ONVIF**

Jeśli zdarzenia nadajnika ONVIF są pobierane bezpośrednio z niego, należy odwzorowywać zdarzenia ONVIF na zdarzeniach BVMS. Umożliwia to późniejsze konfigurowanie zdarzeń ONVIF jako alarmów systemu BVMS.



Uwaga!

Jeśli zdarzenia nadajnika ONIV są pobierane z VSG, domyślne zdarzenia ONVIF są już odwzorowane.

Tablica odwzorowań

Można tworzyć i edytować tablice odwzorowań.



Kliknąć , aby wyświetlić okno dialogowe **Dodaj tablicę odwzorowań**.

Kliknąć , aby wyświetlić okno dialogowe **Zmień nazwę tablicy odwzorowań**.

Kliknąć przycisk , aby usunąć tablicę odwzorowań ze wszystkimi wierszami.

Kliknąć  lub , aby zaimportować lub wyeksportować tablicę odwzorowań ONVIF.

Zdarzenia i alarmy

Wybrać zdarzenie systemu BVMS do odwzorowania za pomocą zdarzenia ONVIF.

Dodaj wiersz

Kliknięcie tego przycisku powoduje dodanie wiersza do tablicy odwzorowań.

Jeśli występuje wiele wierszy, zdarzenie zachodzi, gdy spełniony jest warunek w co najmniej jednym wierszu.

Usuń wiersz

Kliknięcie tego przycisku powoduje usunięcie wybranego wiersza z tablicy odwzorowań.

Temat ONVIF

Należy tu wpisać lub wybrać ciąg, np.:

tnsl:VideoAnalytics/tnsaxis:MotionDetection

Nazwa danych zdarzenia ONVIF

Należy tu wpisać lub wybrać ciąg.

Rodzaj danych zdarzenia ONVIF

Należy tu wpisać lub wybrać ciąg.

Wartość danych zdarzenia ONVIF

Należy tu wpisać lub wybrać ciąg bądź liczbę.

Jeśli zdarzenia ONVIF są pobierane z VSG, następujące zdarzenia są domyślnie odwzorowane na VSG:

- **Zmiana globalna — wykryto**
- **Zmiana globalna — nie wykryto**
- **Detekcja ruchu - Wykryto ruch**
- **Detekcja ruchu - Ruch zatrzymany**
- **Sprawdzanie obrazu odniesienia - Rozregulowany**

- Sprawdzanie obrazu odniesienia - Wyregulowany
- Zanik sygnału wizyjnego - Zanik sygnału wizyjnego
- Zanik sygnału wizyjnego - Sygnał wizyjny OK
- Zanik sygnału wizyjnego - Stan sygnału wizyjnego nieznan
- Sygnał wizyjny zbyt zamazany — sygnał wizyjny OK
- Sygnał wizyjny zbyt zamazany — sygnał wizyjny nie OK
- Sygnał wizyjny zbyt jaskrawy - Sygnał wizyjny OK
- Sygnał wizyjny zbyt jaskrawy - Problem z sygnałem wizyjnym
- Sygnał wizyjny zbyt ciemny - Sygnał wizyjny OK
- Sygnał wizyjny zbyt ciemny - Problem z sygnałem wizyjnym
- Sygnał wizyjny zbyt zaszumiony - Sygnał wizyjny OK Problem z sygnałem wizyjnym
- Stan przekaźnika - Przekaźnik otwarty
- Stan przekaźnika - Przekaźnik zamknięty
- Stan przekaźnika - Błąd przekaźnika
- Stan wejścia - Wejście otwarte
- Stan wejścia - Wejście zamknięte
- Stan wejścia - Błąd wejścia

Patrz

- Uruchamianie narzędzia ONVIF Camera Event Driver Tool za pomocą Configuration Client, Strona 208
- Mapowanie zdarzeń ONVIF, Strona 42
- Konfigurowanie tabeli odwzorowań ONVIF, Strona 241

15.3.1

Dodawanie i usuwanie profilu ONVIF

Okno główne > **Urządzenia** > Rozwiń  > Rozwiń  > Rozwiń  > Rozwiń  >
 > karta **Zdarzenia nadajników ONVIF**
 lub

Okno główne > **Urządzenia** > Rozwiń  >  > karta **Zdarzenia nadajników ONVIF**
 Można dodawać, usuwać i zmieniać profile ONVIF wybranego nadajnika.

Aby dodać profil:

1. Kliknij przycisk **Dodaj...**
2. W oknie dialogowym **Dodaj profil** wpisz nazwę profilu.
3. Kliknij przycisk **Dalej** >.
4. W następnym oknie dialogowym wybierz odpowiednią kamerę.
5. Kliknij przycisk **Dalej** >.
6. W następnym oknie dialogowym wybierz odpowiedni profil nadajnika bez zapisu.
7. Kliknij przycisk **Zapisz**.
 Nowy profil zostanie zapisany.
 Ustawienia tego profilu są wypełniane wartościami z wybranego profilu nadajnika. W razie potrzeby można zmienić te wartości.

Aby usunąć profil:

- Wybierz profil na liście i kliknij przycisk **Usuń**.

Aby zmienić profil:

1. Wybierz profil na liście.
2. Zmień odpowiednio jego ustawienia.

15.3.2

Eksportowanie pliku tablicy odwzorowań ONVIF

Okno główne > **Urządzenia** > Rozwiń  > Rozwiń  > Rozwiń  > Rozwiń  >

 > karta **Zdarzenia nadajników ONVIF**

lub

Okno główne > **Urządzenia** > Rozwiń  >  > karta **Zdarzenia nadajników ONVIF**

Tablicę odwzorowań ONVIF można eksportować do pliku OMF. Tablica odwzorowań jest zapisywana z uwzględnieniem wybranego modelu nadajnika.

Aby wyeksportować tablicę:

1. Kliknij przycisk .
2. Wpisz nazwę pliku i kliknij przycisk **Zapisz**.
Tablica odwzorowań ONVIF zostanie wyeksportowana do pliku OMF z uwzględnieniem wybranego modelu nadajnika.

Patrz

- Strona ONVIF Encoder Events (Zdarzenia nadajników ONVIF), Strona 237

15.3.3

Importowanie pliku tablicy odwzorowań ONVIF

Okno główne > **Urządzenia** > Rozwiń  > Rozwiń  > Rozwiń  > Rozwiń  >

 > karta **Zdarzenia nadajników ONVIF**

lub

Okno główne > **Urządzenia** > Rozwiń  >  > karta **Zdarzenia nadajników ONVIF**

Można importować tablicę odwzorowań ONVIF dostępną w formie pliku OMF.

Udostępnione pliki odwzorowań ONVIF są przechowywane w następującym katalogu programu Configuration Client:

- `%programdata%\Bosch\VMS\ONVIF`

Jeśli jest już zaimportowana tablica odwzorowań o tej samej nazwie, pojawi się komunikat o błędzie.

Jeśli importowana jest nowsza wersja pliku to pojawi się ostrzeżenie. Aby zaimportować ten plik, kliknij przycisk **OK**. W przeciwnym razie kliknij przycisk **Anuluj**.

Aby zaimportować dane:

1. Kliknij .
2. Wybierz odpowiedni plik i kliknij przycisk **Otwórz**.
Pojawi się okno dialogowe **Importuj tablicę odwzorowań**.
3. Wprowadź odpowiednie ustawienia.
4. Kliknij **OK**.

Okno dialogowe Importuj tablicę odwzorowań

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > rozwiń  > rozwiń  >  >

> karta **Zdarzenia nadajników ONVIF** > 

lub

Okno główne > **Urządzenia** > rozwiń  >  > karta **Zdarzenia nadajników ONVIF** > 

Producent

Podaje nazwę producenta urządzeń, do których przeznaczona jest dana tablica odwzorowań.

Model

Podaje nazwę modelu, do którego przeznaczona jest dana tablica odwzorowań.

Opis

Zawiera dodatkowe informacje, np. o przetestowanych modelach kamer.

Nazwa tablicy odwzorowań

Podaje nazwę tablicy odwzorowań. Można ją zmienić, jeśli znajduje się już w użyciu w systemie BVMS.

Można wybrać jedną z poniższych opcji, aby określić, do których nadajników ONVIF ma mieć zastosowanie tablica odwzorowań.

Zastosuj tylko do wybranego koderów ONVIF

Zastosuj do wszystkich koderów ONVIF modeli na liście

Zastosuj do wszystkich koderów ONVIF producenta

Dotychczasowe odwzorowywanie zdarzeń ONVIF jest kontynuowane. Nie można importować plików OMT ze starszych wersji systemu BVMS.

15.3.4

Konfigurowanie tabeli odwzorowań ONVIF

Okno główne > **Urządzenia** > Rozwiń  > Rozwiń  > Rozwiń  > Rozwiń  >  > karta **Zdarzenia nadajników ONVIF**

lub

Okno główne > **Urządzenia** > Rozwiń  >  > karta **Zdarzenia nadajników ONVIF**

Konfigurowanie tablic odwzorowań zdarzeń ONVIF na zdarzenia BVMS.

Dotyczy to wszystkich nadajników ONVIF tego samego modelu lub wszystkich nadajników ONVIF tego samego producenta.

Kliknij przycisk , aby zaktualizować odwzorowanie zdarzeń w nadajnikach ONVIF, które zostały dodane w trybie offline, korzystając z dodanego już nadajnika ONVIF tego samego producenta i (lub) modelu.

W przypadku nadajników wielokanałowych można skonfigurować źródła zdarzeń, np. konkretną kamerę lub określony przekaznik.

Aby utworzyć tablicę odwzorowań:

1. Kliknij .
Zostanie wyświetlone okno dialogowe **Dodaj tablicę odwzorowań**.
2. Wpisz nazwę tablicy odwzorowań.
3. W razie potrzeby wybierz odpowiednie pozycje na listach **Producent** i **Model**.
Jeżeli wybierzesz **<brak>** na obu listach, odwzorowanie zdarzeń będzie obowiązywać tylko w przypadku bieżącego urządzenia.
Jeżeli wybierzesz **<brak>** na liście **Model** oraz nazwę producenta na liście **Producent**, odwzorowanie zdarzeń będzie obowiązywać w przypadku wszystkich urządzeń tego samego

producenta.

Po wybraniu odpowiednich pozycji na obu listach odwzorowanie zdarzeń będzie obowiązywać w przypadku wszystkich urządzeń tego samego producenta i modelu.

4. Kliknij przycisk **OK**.

Można teraz edytować tablicę odwzorowań, np. dodać wiersz do zdarzenia **Wykryto ruch**.

Aby edytować tablicę odwzorowań:

1. Kliknij  .
Zostanie wyświetlone okno dialogowe **Zmień nazwę tablicy odwzorowań**.
2. Zmień odpowiednie pozycje.

Aby dodać lub usunąć odwzorowania zdarzeń:

1. Na liście **Tablica odwzorowań** zaznacz żądaną nazwę.
2. Aby dodać wiersz: kliknij przycisk **Dodaj wiersz**.
3. Wybierz żądane pozycje w wierszu.
Jeśli występuje wiele wierszy, zdarzenie jest wyzwalane, gdy spełniony jest warunek w co najmniej jednym wierszu.
4. Aby usunąć wiersz, kliknij przycisk **Usuń wiersz**.

Aby usunąć tablicę odwzorowań:

1. Kliknij na liście **Tablica odwzorowań** kliknij nazwę odwzorowania zdarzeń, które chcesz usunąć.
2. Kliknij  .

Aby skonfigurować źródło zdarzeń:

1. Rozwiń węzeł  i kliknij przycisk  ,  lub  .
2. Kliknij kartę **Źródło zdarzeń ONVIF**.
3. W kolumnie **Wyzwól zdarzenie** uaktywnij zdarzenie skonfigurowane w danym wierszu.
4. Wybierz odpowiednie definicje zdarzeń.

Okno dialogowe Add/Rename ONVIF Mapping Table (Dodawanie/zmiana nazwy tablicy odwzorowań zdarzeń ONVIF)

Okno główne > **Urządzenia** > Rozwiń  > Rozwiń  > Rozwiń  > Rozwiń  >  > karta **Zdarzenia nadajników ONVIF** >  lub  .

lub

Okno główne > **Urządzenia** > Rozwiń  >  > karta **Zdarzenia nadajników ONVIF** >  .

lub 

Umożliwia dodanie tablicy odwzorowań. Jeśli ta tablica odwzorowań ma służyć za szablon do konfigurowania przyszłych nadajników ONVIF tego samego producenta i modelu, należy wybrać prawidłowe pozycje.

Nazwa tablicy odwzorowań

Wpisz nazwę w celu ułatwienia późniejszej identyfikacji.

Producent

W razie potrzeby wybierz odpowiednią pozycję.

Model

W razie potrzeby wybierz odpowiednią pozycję.

Patrz

- Włączanie rejestrowania zdarzeń ONVIF, Strona 379
- Mapowanie zdarzeń ONVIF, Strona 42
- Strona ONVIF Encoder Events (Zdarzenia nadajników ONVIF), Strona 237
- Strona ONVIF Event Source (Źródło zdarzeń ONVIF), Strona 255

15.4**Strona Konfiguracja ONVIF**

Okno główne > **Urządzenia** > rozwinąć  > rozwinąć  > rozwinąć  > rozwinąć 
 >  > karta **Konfiguracja ONVIF**
 lub

Okno główne > **Urządzenia** > rozwinąć  >  > karta **Konfiguracja ONVIF**

Można wybrać wiele nadajników ONVIF i zmieniać ich ustawienia na stronie **Profil nadajnika wizyjnego**. Zmienione ustawienia mają zastosowanie do wszystkich wybranych urządzeń.
 Ta strona jest dostępna tylko w przypadku nadajników ONVIF.

**Uwaga!**

Ograniczenia konfiguracji ONVIF

Ustawienia, których można dokonać na tych stronach, prawdopodobnie nie są wykonywane prawidłowo, ponieważ nie są obsługiwane przez kamerę. Obsługiwane kamery ONVIF zostały przetestowane tylko z ustawieniami domyślnymi.

15.4.1**Dostęp do urządzenia**

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > rozwiń  > rozwiń  >
 > karta **Konfiguracja ONVIF** > karta **Ustawienia główne** > karta **Dostęp do urządzenia**
 lub

Okno główne > **Urządzenia** > rozwiń  > karta  > **Konfiguracja ONVIF** > karta **Ustawienia główne** > karta **Dostęp do urządzenia**

Producent

Podaje nazwę producenta wybranego nadajnika.

Model

Podaje nazwę modelu wybranego nadajnika.

Uwaga: jeśli wszelkie odwzorowania zdarzeń mają być eksportowane do ONVIF, plik odwzorowań wybiera ten model jako nazwę pliku.

Identyfikator sprzętu

Podaje identyfikator sprzętu wybranego nadajnika.

Wersja opr. układowego

Podaje wersję oprogramowania układowego wybranego nadajnika.

Uwaga: na podstawie listy zgodności BVMS upewnić się, że wersja oprogramowania układowego jest prawidłowa.

Numer seryjny

Podaje numer seryjny wybranego nadajnika.

Adres MAC

Podaje adres MAC wybranego nadajnika.

Wersja ONVIF

Podaje wersję standardu ONVIF, z którą zgodny jest wybrany nadajnik.

W przypadku BVMS wymagana jest wersja ONVIF 2.0.

15.4.2

Data/godzina

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > rozwiń  > rozwiń  > karta **Konfiguracja ONVIF** > karta **Ustawienia główne** > karta **Data / godzina**

lub

Okno główne > **Urządzenia** > rozwiń  > karta  > **Konfiguracja ONVIF** > karta **Ustawienia główne** > karta **Data / godzina**

Strefa czasowa

Wybrać strefę czasową, w której pracuje system.

Jeśli w systemie lub sieci pracuje wiele urządzeń, ważne jest właściwe zsynchronizowanie ich zegarów wewnętrznych. Na przykład prawidłowa identyfikacja i ocena jednocześnie wykonanych nagrań jest możliwa tylko wówczas, gdy wszystkie urządzenia pracują według tego samego czasu.

1. Wprowadź aktualną datę. Czas urządzenia jest kontrolowany przez zegar wewnętrzny, dlatego nie jest konieczne wprowadzanie dnia tygodnia – jest on dodawany automatycznie.
2. Wpisz bieżący czas lub kliknij przycisk **Synchr. PC**, aby zastosować w kamerze czas z komputera.

Uwaga:

Prawidłowe ustawienie daty i godziny jest ważne dla zapisu. Niepoprawne ustawienie daty i godziny mogłoby wpłynąć na jego prawidłowość.

15.4.3

Zarządzanie użytkownikami

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > rozwiń  > rozwiń  > karta **Konfiguracja ONVIF** > karta **Ustawienia główne** > karta **Zarządzanie przez użytkownika**

lub

Okno główne > **Urządzenia** > rozwiń  > karta  > **Konfiguracja ONVIF** > karta **Ustawienia główne** > karta **Zarządzanie przez użytkownika**

Te ustawienia użytkownika są używane do aplikacji trzecich stron, takich jak bezpośredni dostęp aplikacji Web Client do nadajników.

Obsługiwane są następujące role użytkownika dla dostępu do aplikacji trzeciej strony:

- **Anonimowy**: ta rola ma nieograniczony dostęp tylko do tych urządzeń w których nie zarejestrowano użytkowników o innych rolach (**Użytkownik**, **Operator**, **Administrator**). W urządzeniach z co najmniej jednym powyżej opisanym użytkownikiem użytkownik anonimowy ma w prawo tylko do oglądania ustawień czasowych.
- **Administrator** (nie jest obsługiwana przez Configuration Client): ta rola ma dostęp do wszystkich sekcji aplikacji i funkcji, uprawnienia do ponownego uruchamiania urządzenia, resetowania ustawień i aktualizacji oprogramowania układowego oraz tworzenia innych użytkowników z różnymi prawami dostępu.

Rolą pierwszego użytkownika utworzonego na urządzeniu musi być **Administrator**.

Różnice pomiędzy domyślnymi prawami dostępu na poziomie Operatora i Użytkownika (rola **Operator** i rola **Użytkownik**) można znaleźć w poniższej tabeli.

Sekcja konfiguracji ONVIF lub funkcji	Operator	Użytkownik
Identyfikacja	PODGLĄD	BRAK PODGLĄDU
Ustawienia czasu	PODGLĄD	PODGLĄD
Ustawienia sieci	PODGLĄD	PODGLĄD
Użytkownicy	BRAK PODGLĄDU	BRAK PODGLĄDU
Ustawienia przekaźników	EDYCJA	PODGLĄD
Obraz bieżący (w tym rtsp-link)	EDYCJA	EDYCJA
Strumieniowe przesyłanie obrazu	EDYCJA	PODGLĄD
Profile	EDYCJA	PODGLĄD

EDYCJA – zmiana bieżących ustawień i utworzenie nowych.

PODGLĄD – ustawienia nie są ukryte, ale nie jest dozwolona ich zmiana i tworzenia nowych.

BRAK PODGLĄDU — niektóre ustawienia lub całe części są ukryte.

Użytkownicy

Zawiera listę dostępnych użytkowników urządzenia.

Hasło

Należy tu wpisać hasło.

Potwierdź hasło

Należy tu potwierdzić wpisane hasło.

Rola

Należy wskazać odpowiednią rolę wybranego użytkownika. Spowoduje to właściwe dopasowanie jego uprawnień dostępu.

15.4.4

Strona Profil nadajnika wizyjnego

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > rozwiń  > rozwiń  > karta **Konfiguracja ONVIF** > karta **Kamera** > karta **Profil nadajnika wizyjnego**

lub

Okno główne > **Urządzenia** > rozwiń  >  > karta **Konfiguracja ONVIF** > karta **Kamera** > karta **Profil nadajnika wizyjnego**

Zaleca się korzystanie z profili wstępnie zdefiniowanych, ponieważ profile są dość złożone i obejmują dużą liczbą wzajemnie powiązanych parametrów. Użytkownik powinien dokonywać zmian profilu tylko wtedy, gdy jest całkowicie zaznajomiony z wszystkimi opcjami konfiguracji.

Profile

Należy kliknąć żądaną nazwę.

**Uwaga!**

Skonfigurowane tu profile można wybrać w kliencie konfiguracji.

W oknie głównym kliknij przycisk **Kamery i zapis**, a następnie  lub  .
Ustawienie domyślne „<Automatycznie>” może zostać zmienione na jeden ze skonfigurowanych profili wymienionych na liście.

Uwaga: należy pamiętać, że przy aktywnym użyciu więcej niż 1 profilu na pojedynczym urządzeniu występują pewne ograniczenia wydajności i w sytuacjach przeciążenia kamera może automatycznie ograniczyć jakość strumienia.

Nazwa

W tym polu można wprowadzić nową nazwę profilu. Nazwa ta jest wyświetlana na liście dostępnych profili w polu Aktywny profil.

Kodowanie

Należy wybrać żądany kodek.

Rozdzielczość obrazu

Należy wybrać wymaganą rozdzielczość obrazu wideo.

Jakość

Ten parametr umożliwia zmniejszenie obciążenia w kanale za pomocą redukcji definicji obrazu.

Wartość parametru jest ustawiana za pomocą suwaka: skrajna lewa pozycja odpowiada najwyższej rozdzielczości obrazu, skrajna prawa – najmniejsze obciążenie kanału wizyjnego.

Limit częstotliwości odświeżania

Częstotliwość odświeżania (w klatkach na sekundę) wskazuje, ile klatek na sekundę jest wychwytywanych za pomocą kamery wideo podłączonej do urządzenia. Ten parametr jest wyświetlany tylko informacyjnie.

Jeśli podano interwał kodowania wynikowa częstotliwość odświeżania jest ograniczana przez podany współczynnik.

Limit prędkości transmisji

Im mniejsza prędkość transmisji, tym mniejszy ostateczny rozmiar pliku wideo. Jednak gdy prędkość transmisji jest znacząco zredukowana, program będzie musiał wykorzystać silniejsze algorytmy kompresji, które również zmniejszają jakość obrazu.

Należy wybrać maksymalną wyjściową prędkość transmisji w kb/s. Maksymalna przepływność danych nigdy nie jest przekraczana. W zależności od ustawień jakości obrazu dla ramek typu I oraz P fakt ten może powodować pomijanie pojedynczych obrazów.

Wprowadzona wartość powinna być co najmniej o 10% większa od typowej docelowej szybkości transmisji danych.

Interwał kodowania

Interwał kodowania (liczba ramek) oznacza, przy jakiej częstotliwości odświeżania ramki pochodzące z kamery będą kodowane. Na przykład jeżeli interwał kodowania wynosi 25, oznacza to, że 1 z 25 ramek uchwyconych w ciągu sekundy jest kodowana i transmitowana do użytkownika. Wartość maksymalna redukuje obciążenie kanału, ale może powodować pomijanie informacji z ramek, które nie zostały zakodowane. Zmniejszenie interwału kodowania zwiększa częstotliwość aktualizacji obrazu, a także obciążenie kanału.

Długość GOP

Długość GOP można edytować tylko w przypadku nadajnika H.264 lub H.265. Ten parametr określa długość grupy obrazów pomiędzy dwoma kluczowymi ramkami. Im ta wartość jest wyższa, tym mniejsze jest obciążenie sieci, ale ma to wpływ na jakość obrazu.

Wartość 1 oznacza, że I-ramki są generowane w sposób ciągły. Wartość 2 oznacza, że co drugi obraz jest generowany jako I-ramka, a 3 — że tylko co trzecia ramka itd. Pozostałe ramki są kodowane jako ramki typu P lub typu B.

Limit czasu sesji

Limit czasu sesji RTSP dla powiązanego strumienia wideo.

Limit czasu sesji służy jako wskazówka w celu utrzymania sesji RTSP przez urządzenie.

Multicast - Adres IP

Wprowadzić prawidłowy adres Multicast, który ma być wykorzystywany w trybie Multicast (duplikacja strumieni danych w sieci).

Przy ustawieniu 0.0.0.0 nadajnik wysyłający strumień pracuje w trybie Multi-unicast (kopiowania strumienia danych w urządzeniu). Kamera obsługuje połączenia w trybie Multi-unicast dla maks. pięciu jednocześnie dołączonych odbiorników.

Duplikacja danych znacznie obciąża urządzenie i może prowadzić do pogorszenia jakości obrazu w określonych warunkach.

Multicast - Port

Wybrać port docelowy dla trybu RTP multicast. Urządzenie może obsługiwać RTCP. W takim przypadku numer portu powinien umożliwiać odpowiedniemu strumieniowi RTCP mapowanie do następnego wyższego (nietypowego) numeru docelowego portu w sposób zdefiniowany w specyfikacji RTSP.

Multicast — TTL

W polu można wprowadzić wartość określającą jak długo pakiety danych multicastingu pozostają aktywne w sieci. Jeśli transmisja w trybie Multicast będzie prowadzona przez router, to wartość ta musi być większa niż 1.



Uwaga!

Tryb Multicast działa tylko z protokołem UDP. Protokół TCP nie obsługuje połączeń Multicast. Jeśli urządzenie pracuje za zaporą sieciową, jako protokół transmisji należy wybrać TCP (port HTTP). W przypadku pracy w sieci lokalnej, należy wybrać UDP.

15.4.5

Profil nadajnika fonicznego

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > rozwiń  > rozwiń  > karta



> **Konfiguracja ONVIF** > karta **Kamera** > karta **Profil nadajnika fonicznego**

lub

Okno główne > **Urządzenia** > rozwiń  >  > karta **Konfiguracja ONVIF** > karta **Kamera** > karta **Profil nadajnika fonicznego**

Zaleca się korzystanie z profili wstępnie zdefiniowanych, ponieważ profile są dość złożone i obejmują dużą liczbę wzajemnie powiązanych parametrów. Użytkownik powinien dokonywać zmian profilu tylko wtedy, gdy jest całkowicie zaznajomiony z wszystkimi opcjami konfiguracji.

Kodowanie

Należy tu wybrać odpowiednie kodowanie źródłowego sygnału fonicznego, o ile jest dostępny:

- **G.711 [ITU-T G.711]**
- **G.726 [ITU-T G.726]**
- **AAC [ISO 14493-3]**

Szybkość transmisji

Należy tu wybrać odpowiednią przepływność nadawanego sygnału akustycznego, na przykład 64 kb/s.

Częstotliwość próbkowania

Wprowadź wyjściową częstotliwość próbkowania w kHz, na przykład 8 kb/s.

Limit czasu sesji

Limit czasu sesji RTSP dla powiązanego strumienia audio.

Limit czasu sesji służy jako wskazówka w celu utrzymania sesji RTSP przez urządzenie.

15.4.6**Przetw. obrazów - ogólne**

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > rozwiń  > rozwiń  > karta **Konfiguracja ONVIF** > karta **Kamera** > karta **Przetw. obrazów - ogólne**
lub

Okno główne > **Urządzenia** > rozwiń  >  > karta **Konfiguracja ONVIF** > karta **Kamera** > karta **Przetw. obrazów - ogólne**

Jaskrawość

Dostosuj jasność obrazu do środowiska pracy.

Nasycenie kolorów

Dostosuj wartość nasycenia kolorów w obrazie tak, aby odwzorowanie kolorów na monitorze było jak najbardziej realistyczne.

Kontrast

Można dostosować kontrast obrazu do środowiska pracy.

Ostrość

Dostosuj ostrość obrazu.

Niska wartość sprawia, że obraz jest mniej ostry. Zwiększenie ostrości uwydatnia więcej szczegółów. Większa ostrość może poprawić widok szczegółów tablic rejestracyjnych, rysów twarzy oraz krawędzi niektórych powierzchni, ale jednocześnie może zwiększyć wymaganą szerokość pasma.

Filtr podczerwieni

Należy wybrać stan filtra odcinającego podczerwieni.

Stan AUTO umożliwia algorytmowi ekspozycji obsługę po przełączeniu filtra odcinającego podczerwień.

15.4.7**Kompensacja tła**

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > rozwiń  > rozwiń  > karta **Konfiguracja ONVIF** > karta **Ustawienia główne** > karta **Kompensacja tła**
lub

Okno główne > **Urządzenia** > rozwiń  >  > karta **Konfiguracja ONVIF** > karta **Ustawienia główne** > karta **Kompensacja tła**

W zależności od modelu urządzenia można tu konfigurować parametry kompensacji tła.

Tryb

Wybrać opcję **Wył.**, aby wyłączyć kompensację tła.

Wybrać ustawienie **Wł.**, aby zapewnić rejestrowanie szczegółów przy wysokim kontraście i w warunkach bardzo silnego lub słabego oświetlenia.

Poziom

Należy tu wprowadzić lub wybrać odpowiednią wartość.

15.4.8

Ekspozycja

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > rozwiń  > rozwiń  > karta **Konfiguracja ONVIF** > karta **Ustawienia główne** > karta **Ekspozycja**
lub

Okno główne > **Urządzenia** > rozwiń  >  > karta **Konfiguracja ONVIF** > karta **Ustawienia główne** > karta **Ekspozycja**

W zależności od modelu urządzenia można tu konfigurować parametry ekspozycji.

Tryb

Należy wybrać **Auto**, aby uruchomić algorytm ekspozycji w urządzeniu. Algorytm używa wartości z następujących pól:

- **Priorytet**
- **Okno**
- **Min. czas ekspozycji**
- **Maks. czas ekspozycji**
- **Min. poziom wzmocnienia**
- **Maks. poziom wzmocnienia**
- **Min. ustawienie przysłony**

Wybrać opcję **instrukcja**, aby wyłączyć algorytm ekspozycji w urządzeniu. Algorytm używa wartości z następujących pól:

- **Czas ekspozycji**
- **Wzmocnienie**
- **Przysłona**

Priorytet

Skonfigurować tryb priorytetu ekspozycji (niski poziom/częstotliwość odświeżania).

Okno

Zdefiniować prostokątną maskę ekspozycji.

Min. czas ekspozycji

Skonfigurować minimalny czas ekspozycji [μs].

Maks. czas ekspozycji

Skonfigurować maksymalny czas ekspozycji [μs].

Min. poziom wzmocnienia

Skonfigurować minimalny zakres wzmocnienia czujnika [dB].

Maks. poziom wzmocnienia

Skonfigurować maksymalny zakres wzmocnienia czujnika [dB].

Min. ustawienie przysłony

Skonfigurować minimalne tłumienie światła wejściowego pod wpływem przysłony [dB]. 0 dB mapuje do maksymalnie otwartej przysłony.

Maks. ustawienie przysłony

Skonfigurować maksymalne tłumienie światła wejściowego pod wpływem przysłony [dB]. 0 dB mapuje do maksymalnie otwartej przysłony.

Czas ekspozycji

Ustawić czas stałej ekspozycji [μs].

Wzmocnienie

Skonfigurować stałe wzmocnienie [dB].

Przystona

Skonfigurować stałe tłumienie światła wejściowego pod wpływem przystony [dB]. 0 dB mapuje do maksymalnie otwartej przystony.

15.4.9**Ogniskowanie**

Okno główne > **Urządzenia** > rozwiń 

> rozwiń 

> rozwiń 

> rozwiń 



> karta **Konfiguracja ONVIF** > karta **Ustawienia główne** > karta **Ogniskowanie**

lub

Okno główne > **Urządzenia** > rozwiń 

> 

> karta **Konfiguracja ONVIF** > karta **Ustawienia główne** > karta **Ogniskowanie**

W zależności od modelu urządzenia można tu konfigurować parametry ogniskowania.

Ta strona umożliwia przesuwanie obiektywów w sposób bezwzględny, względny lub ciągły.

Ustawianie ostrości za pomocą tego działania spowoduje wyłączenie automatycznej regulacji ostrości.

Urządzenia z obsługą zdalnego sterowania ostrością zwykle umożliwiają sterowanie za pomocą tej operacji przesuwania. Położenie ogniskowania jest przedstawiane za pomocą wartości

numerycznych. Możliwe stany ogniskowania to:

PRZESUWANIE**OK****NIEZNANY**

Mogą być wyświetlane dodatkowe informacje o błędzie, takim jak błąd pozycjonowania wskazywany przez sprzęt.

Tryb

Wybranie opcji **Auto** umożliwi automatyczną regulację ostrości obiektywu w dowolnym momencie w zależności od obiektów na scenie. Algorytm używa wartości z następujących pól:

- **Limit bliższy**
- **Limit dalszy**

Wybrać opcję **RĘCZNY**, aby ręcznie dostosować ostrość. Algorytm używa wartości z następujących pól:

- **Prędkość domyślna**

Prędkość domyślna

Skonfigurować domyślne ustawienie szybkości dla operacji przenoszenia ogniskowania (jeśli parametr szybkości nie jest obecny).

Limit dalszy

Skonfigurować limit bliskiej ostrości [m].

Limit dalszy

Skonfigurować limit dalekiej ostrości [m].

15.4.10**Szeroki zakres dynamiki**

Okno główne > **Urządzenia** > rozwiń 

> rozwiń 

> rozwiń 

> rozwiń 



> karta **Konfiguracja ONVIF** > karta **Ustawienia główne** > karta **Szeroki zakres dynamiczny**

lub

Okno główne > **Urządzenia** > rozwiń  >  > karta **Konfiguracja ONVIF** > karta **Ustawienia główne** > karta **Szeroki zakres dynamiczny**

W zależności od modelu urządzenia można tu konfigurować parametry szerokiego zakresu dynamiki.

Tryb

Należy tu wprowadzić lub wybrać odpowiednią wartość.

Poziom

Należy tu wprowadzić lub wybrać odpowiednią wartość.

15.4.11

Balans bieli

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > rozwiń  > rozwiń  > karta **Konfiguracja ONVIF** > karta **Ustawienia główne** > karta **Balans bieli**

lub

Okno główne > **Urządzenia** > rozwiń  >  > karta **Konfiguracja ONVIF** > karta **Ustawienia główne** > karta **Balans bieli**

W zależności od modelu urządzenia można tu konfigurować parametry balansu bieli.

Tryb

Tryb Auto umożliwia kamerze ciągłą regulację w celu uzyskania optymalnego odwzorowania kolorów za pomocą metody średniej refleksyjności lub w przypadku otoczenia z naturalnymi źródłami światła.

W trybie Ręcznym wzmocnienie sygnału składowej czerwonej, zielonej i niebieskiej można zmieniać ręcznie w celu uzyskania żądanych ustawień.

Regulacja punktu bieli jest konieczna tylko w specjalnych warunkach sceny:

- przy oświetleniu wewnętrznym i kolorowym oświetleniu diodami LED;
- przy oświetleniu lampami sodowymi (oświetlenie uliczne);
- w przypadku dominującego koloru na obrazie, na przykład zielonego na boisku piłkarskim lub stole bilardowym.

Wzm. skład. czerwonej

W Ręcznym trybie balansu bieli należy wyregulować położenie suwaka wzmocnienia składowej czerwonej, aby przesunąć fabrycznie ustawiony punkt bieli (osłabienie składowej czerwonej wzmacnia składową niebiesko-zieloną).

Wzm. skład. niebieskiej

W Ręcznym trybie balansu bieli należy wyregulować położenie suwaka wzmocnienia składowej niebieskiej, aby przesunąć fabrycznie ustawiony punkt bieli (osłabienie składowej niebieskiej wzmacnia składową żółtą).

15.4.12

Dostęp do sieci

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > rozwiń  > rozwiń  > karta **Konfiguracja ONVIF** > karta **Sieć** > karta **Dostęp do sieci**

lub

Okno główne > **Urządzenia** > rozwiń  >  > karta **Konfiguracja ONVIF** > karta **Sieć** > karta **Dostęp do sieci**

Można tu konfigurować różne ustawienia sieci.

Ethernet IPv4

DHCP

Jeśli w sieci zastosowano serwer DHCP do dynamicznego przydzielania adresów IP, można włączyć akceptowanie adresów IP automatycznie przydzielanych nadajnikowi.

BVMS używa adresu IP do unikalnego przypisania nadajnika. Serwer DHCP musi obsługiwać stałe przypisanie pomiędzy adresem IP i adresem MAC oraz musi być odpowiednio skonfigurowany, tak aby przypisany adres IP, pozostał taki sam po każdym ponownym uruchomieniu systemu.

Maska podsieci

Wprowadzić odpowiednią maskę podsieci dla wybranego adresu IP.

Jeśli serwer DHCP jest włączony, maska podsieci jest przypisywana automatycznie.

Brama domyślna

Jeśli moduł ma nawiązywać połączenie ze zdalną lokalizacją w innej podsieci, należy wprowadzić adres IP bramy. W innym przypadku pole należy pozostawić puste (0.0.0.0).

Ethernet IPv6

DHCP

Należy tu wprowadzić lub wybrać odpowiednią wartość.

Adres IP

Wyświetla adres IPv6 urządzenia, dostarczany przez serwer DHCP.

Długość prefiksu

Wyświetla długość prefiksu urządzenia, dostarczaną przez serwer DHCP.

Brama domyślna

Wyświetla bramę domyślną urządzenia, dostarczaną przez serwer DHCP.

Nazwa hosta

Należy tu wprowadzić lub wybrać odpowiednią wartość.

DNS

Korzystając z serwera DNS, urządzenie może odczytać adres oznaczony jako nazwa. Wprowadzić w polu adres IP żądanego serwera DNS.

Serwery NTP

Wpisać adres IP serwera czasu lub wybrać opcję konfiguracji tego ustawienia przez serwer DHCP. Nadajnik może odbierać sygnał czasu z serwera czasu przy użyciu różnych protokołów serwera czasu. Na podstawie odebranych informacji ustawiany jest zegar wewnętrzny urządzenia. Moduł sprawdza sygnał czasu automatycznie co minutę. Wprowadzić w polu adres IP serwera czasu. Zapewnia on dużą dokładność i jest wymagany do obsługi zastosowań specjalnych.

Porty HTTP

Jeśli jest to wymagane, wybrać z listy inny port HTTP przeglądarki. Domyślny port HTTP to 80. Jeśli dozwolone mają być tylko bezpieczne połączenia HTTPS, należy wyłączyć port HTTP.

Uwaga: nieobsługiwane przez BVMS.

Porty HTTPS

Uwaga: nieobsługiwane przez BVMS.

Jeśli dostęp do sieci ma być przyznawany za pomocą bezpiecznego połączenia, należy w razie potrzeby wybrać port HTTPS. Domyślny port HTTPS to 443. W celu dezaktywowania portów HTTPS należy wybrać opcję **Wył.** – odtąd obsługiwane będą jedynie połączenia niezabezpieczone.

Brama domyślna

Należy tu wprowadzić lub wybrać odpowiednią wartość.

Porty RTSP

W razie potrzeby wybrać inny port w celu wymiany danych RTSP. Standardowy port RTSP to port 554. Wybrać **Wył.** w celu dezaktywowania funkcji RTSP.

Adres konfiguracji zerowej

Włączanie lub wyłączanie wykrywania konfiguracji zerowej z wybranej kamery.

Konfiguracja zerowa jest alternatywą w stosunku do DHCP i DNS metodą przypisywania adresów IP do kamer. Automatycznie tworzy użyteczny adres sieciowy IP bez konfiguracji lub specjalnych serwerów.

Uwaga: w standardzie ONVIF używane jest tylko wykrywanie usługi konfiguracji zerowej.

Alternatywnie, bez konfiguracji zerowej, sieć musi świadczyć usługi takie jak DHCP lub DNS.

W przeciwnym wypadku należy ręcznie skonfigurować ustawienia sieciowe każdej kamery IP.

Tryb wykrywania ONVIF

Jeśli opcja jest włączona, kamera może być wykryta w sieci. Obejmuje to funkcje kamery.

Jeśli opcja jest wyłączona, kamera nie będzie wysyłać komunikatów wykrywania, aby uniknąć ataków typu odmowa usługi.

Zaleca się wyłączenie wykrywania po dodaniu kamery do konfiguracji.

Należy tu wprowadzić lub wybrać odpowiednią wartość.

Włącz DynDNS

Umożliwia włączenie DynDNS.

Usługa Domain Name Service (DNS) umożliwia wybór urządzenia przez Internet za pomocą nazwy hosta, bez koniecznej znajomości bieżącego adresu IP tego urządzenia. W celu skorzystania z tej usługi należy posiadać konto u jednego z dostawców dynamicznych usług DNS. Konieczne jest również zarejestrowanie w tej witrynie wymaganej nazwy hosta dla jednostki.

Uwaga:

Informacje na temat usługi, procesu rejestracji i dostępnych nazw hosta można uzyskać u dostawcy usług DynDNS w witrynie dyndns.org.

Typ

Należy tu wprowadzić lub wybrać odpowiednią wartość.

Nazwa

Wprowadzić nazwę konta użytkownika DynDNS.

TTL

Należy tu wprowadzić lub wybrać odpowiednią wartość.

15.4.13

Zakresy

Okno główne > **Urządzenia** > rozwiń węzeł  > rozwiń węzeł  > rozwiń  > rozwiń

węzeł  > karta  > **Konfiguracja ONVIF** > karta **Sieć** > karta **Zakresy**
lub

Okno główne > **Urządzenia** > rozwiń węzeł  >  > karta **Konfiguracja ONVIF** > karta **Sieć**
> karta **Zakresy**

Użytkownik może dodawać i usuwać zakresy urządzenia ONVIF z identyfikatorami URI w następującym formacie:

`onvif://www.onvif.org/<path>`

Poniższy przykład ilustruje użycie zakresu wartości. To tylko przykład, a nie wskazanie rodzaju zakresu parametru, który ma być częścią konfiguracji nadajnika. W tym przykładzie przyjmujemy, że nadajnik jest skonfigurowany w następujących zakresach:

```
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
```

Można nadać urządzeniu szczegółową lokalizację i nazwę w celu identyfikacji na liście urządzeń.

W tabeli przedstawiono podstawowe funkcje i inne właściwości urządzenia, które są standardowe:

Kategoria	Zdefiniowane wartości	Opis
typ	nadajnik sygnału wizyjnego	To urządzenie jest nadajnikiem sygnału wizyjnego.
	Ptz	Urządzenie jest urządzeniem PTZ.
	audio_encoder	Urządzenie obsługuje nadajnik sygnału fonicznego.
	video_analytics	Urządzenie obsługuje analizę sygnału wizyjnego.
	Network_Video_Transmitter	To urządzenie jest sieciowym nadajnikiem wizyjnym.
	Network_Video_Decoder	To urządzenie jest sieciowym dekoderym wizyjnym.
	Network_Video_Storage	Urządzenie jest urządzeniem sieciowego zapisu danych wizyjnych.
	Network_Video_Analytic	Urządzenie jest urządzeniem sieciowym analizy sygnału wizyjnego.
lokalizacja	Dowolny ciąg znaków lub wartość ścieżki.	Nieobsługiwane przez BVMS.
sprzęt	Dowolny ciąg znaków lub wartość ścieżki.	Ciąg lub wartość ścieżki opisująca sprzęt urządzenia. Urządzenie powinno zawierać na liście zakresu co najmniej jeden wpis sprzętu.
nazwa	Dowolny ciąg znaków lub wartość ścieżki.	Nazwa urządzenia, którą można wyszukiwać. Nazwa ta jest wyświetlana w urządzeniu oraz w drzewie logicznym.

Nazwa zakresu, model i producent wpływają na to, jak urządzenie jest wyświetlane w drzewie urządzeń, identyfikacji nadajnika ONVIF i w ustawieniach głównych.

15.4.14

Przełączniki

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > rozwiń  > rozwiń  > karta **Konfiguracja ONVIF** > karta **Interfejsy** > karta **Przełącznik**

Okno główne > **Urządzenia** > rozwiń  >  > karta **Konfiguracja ONVIF** > karta **Interfejsy** > karta **Przełącznik**

Fizyczny stan bezczynności wyjścia przełącznikowego można skonfigurować przez wybranie ustawienia stanu bezczynności **otwarte** lub **zamknięte** (odwrócenie zachowania przełącznika).

Dostępne wyjścia cyfrowego urządzenia są oznaczone nazwami, np.:

- **AlarmOut_0**
- **AlarmOut_1**

Do mapowania zdarzeń przekaźników w systemie BVMS należy użyć nazw wymienionych w tym miejscu.

Tryb

Przekaźnik może działać w dwóch trybach:

- **Bistabilny**: po ustawieniu stanu przekaźnik pozostaje w tym stanie.
- **Monostabilny**: po ustawieniu stanu przekaźnik powraca do stanu bezczynności po upływie określonego czasu opóźnienia.

Stan bezczynności

Jeśli przekaźnik ma działać jako styk normalnie otwarty, należy wybrać opcję **Otwarty**. Z kolei w przypadku, gdy ma działać jako styk normalnie zamknięty, należy wybrać opcję **Zamknięty**.

Czas opóźnienia

Ustawić czas opóźnienia. Po tym okresie przekaźnik przechodzi ponownie w stan bezczynności, jeśli skonfigurowano tryb **Monostabilny**.

Aby przetestować dowolną z konfiguracji powiązanych ze zmianą stanu przekaźnika, należy kliknąć przycisk **Uaktywnij** lub **Wyłącz** w celu przełączenia przekaźnika. Można sprawdzić prawidłowe działanie skonfigurowanych zdarzeń przekaźników kamery: wyświetlacz stanu ikony przekaźnika w drzewie logicznym, zdarzeniach na liście alarmów lub w dzienniku zdarzeń.

Uaktywnij

Kliknąć, aby przełączyć przekaźnik skonfigurowanego stanu bezczynności.

Wyłącz

Kliknij, aby przełączyć przekaźnik w skonfigurowany stan aktywny.

15.5

Strona ONVIF Event Source (Źródło zdarzeń ONVIF)

Okno główne > **Urządzenia** > Rozwiń  > Rozwiń  > Rozwiń  > Rozwiń  >

Rozwiń  >  > karta **Źródło zdarzeń ONVIF**
lub

Okno główne > **Urządzenia** > Rozwiń  > Rozwiń  >  > karta **Źródło zdarzeń ONVIF**
lub

Okno główne > **Urządzenia** > Rozwiń  > Rozwiń  > Rozwiń  > Rozwiń  >
Rozwiń  >  > karta **Źródło zdarzeń ONVIF**
lub

Okno główne > **Urządzenia** > Rozwiń  > Rozwiń  >  > karta **Źródło zdarzeń ONVIF**
lub

Okno główne > **Urządzenia** > Rozwiń  > Rozwiń  > Rozwiń  > Rozwiń  >
Rozwiń  >  > karta **Źródło zdarzeń ONVIF**
lub

Okno główne > **Urządzenia** > Rozwiń  > Rozwiń  >  > karta **Źródło zdarzeń ONVIF**

Zdarzenia ONVIF można skonfigurować jako źródło (kanał wizyjny, wejście lub przekaźnik). Definicja uaktywnionego zdarzenia zostaje dodana do tablicy odwzorowań nadajnika.

Na przykład w przypadku nadajnika wielokanałowego można określić, dla której kamery wyzwalane jest zdarzenie **Wykryto ruch**.

Wyzwól zdarzenie

Uaktywnianie tego zdarzenia.

Temat ONVIF

Należy wpisać lub wybrać ciąg.

Nazwa źródłowa ONVIF

Należy wpisać lub wybrać ciąg.

Typ źródła ONVIF

Należy wpisać lub wybrać ciąg.

Wartość źródłowa ONVIF

Należy wpisać lub wybrać ciąg.

Patrz

- Mapowanie zdarzeń ONVIF, Strona 42
- Konfigurowanie tabeli odwzorowań ONVIF, Strona 241

15.6

Przypisywanie profilu ONVIF



Okno główne > **Kamery i zapis** >

Do kamery ONVIF można przypisać profil nośnika ONVIF.

Można go przypisać albo dla obrazu wideo na żywo, albo dla zapisywanego.

Aby przypisać token dla obrazu wideo na żywo:

- ▶ W kolumnie **Obraz bieżący** – **Profil** zaznacz żądany wpis.

Aby przypisać token dla obrazu rejestrowanego:

- ▶ W kolumnie **Zapis** – **Profil** zaznacz żądany wpis.

Patrz

- strona Kamery, Strona 285

16

Strona rozpoznawania tablic rejestracyjnych

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > rozwiń  > karta **VCA** > karta **Rozpoznawanie tablic rejestracyjnych**
lub

Okno główne > **Urządzenia** > rozwiń  > rozwiń  > rozwiń  > karta **VCA** > karta **Rozpoznawanie tablic rejestracyjnych**
lub

Okno główne > **Urządzenia** >  > karta **VCA** > karta **Rozpoznawanie tablic rejestracyjnych**
lub

Okno główne > **Urządzenia** >  > karta **VCA** > karta **Rozpoznawanie tablic rejestracyjnych**

Na stronie **Rozpoznawanie tablic rejestracyjnych** wyświetlane są następujące informacje:

- data i czas zeskanowania tablicy rejestracyjnej,
- obraz tablicy rejestracyjnej,
- ciąg znaków z tablicy rejestracyjnej,
- kraj pochodzenia tablicy rejestracyjnej.

► Aby zobaczyć więcej, kliknij **Pokaż więcej**.

► Aby dodać dodatkowy pas ruchu, kliknij **Dodaj pas ruchu**.

**Uwaga!**

Aby skonfigurować ustawienia LPR, przejdź do strony internetowej kamery.

17

Karta Mapy i struktura

**Uwaga!**

Program BVMS Viewer zapewnia tylko podstawowe funkcje. Funkcje zaawansowane udostępnia program BVMS Professional. Aby uzyskać szczegółowe informacje na temat różnych wersji systemu BVMS, należy odwiedzić witrynę www.boschsecurity.com i zobaczyć skrócony poradnik wyboru systemu BVMS: [Skrócony poradnik wyboru systemu BVMS](#).

Liczba elementów poniżej pozycji jest wyświetlana w nawiasach kwadratowych.

Okno główne > **Mapy i struktura**

Uprawnienia mogą zostać utracone. Jeśli grupa urządzeń zostanie przesunięta, urządzenia te tracą swoje ustawienia uprawnień. Należy wówczas ponownie ustawić uprawnienia na stronie **Grupy użytkowników**.

Wyświetla obszary Drzewo urządzeń i Drzewo logiczne oraz okno **Mapa globalna**.

Umożliwia utworzenie struktury dla wszystkich urządzeń w systemie BVMS. Struktura użytkownika jest wyświetlana w oknie Drzewo logiczne.

Umożliwia wykonywanie następujących zadań:

- Konfigurowanie pełnego drzewa logicznego
- Zarządzanie zasobami
- Tworzenie skryptów poleceń
- Tworzenie sekwencji
- Tworzenie okien roboczych mapy
- Tworzenie przekaźników awaryjnych
- Dodawanie map obszaru i tworzenie aktywnych miejsc

Aktywnymi miejscami na mapach mogą być:

- Kamery
- Wejścia
- Przekaźniki
- Skrypty poleceń
- Sekwencje
- Dokumenty
- Łączy do innych map obszaru
- VRM
- iSCSI
- Czytniki systemu kontroli dostępu
- Centrale alarmowe
- Serwer zarządzający systemami Enterprise System

Plikami zasobów mogą być:

- Pliki map
- Pliki dokumentów
- Łączy do zewnętrznych adresów URL
- Pliki dźwiękowe
- Łączy do aplikacji zewnętrznych

Ikony

	Wyświetla okno dialogowe zarządzania plikami zasobów.
	Wyświetla okno dialogowe, w którym można dodawać skrypty poleceń do drzewa logicznego oraz nimi zarządzać.

	Wyświetla okno dialogowe dodawania i edytowania pliku sekwencji kamer.
	Umożliwia tworzenie folderów w drzewie logicznym.
	Wyświetla okno dialogowe dodawania plików zasobów map.
	Tworzy okno robocze mapy w drzewie logicznym.
	Wyświetla okno dialogowe dodawania pliku dokumentu.
	Wyświetla okno dialogowe dodawania łącza do aplikacji zewnętrznej.
	Umożliwia wyświetlanie okna dialogowego dodawania przekaźnika awaryjnego.

Symbole

	Urządzenie zostało dodane do okna Drzewo logiczne.

Aby wyszukać elementy:

- ▶ W polu wyszukiwania  wpisz ciąg znaków i naciśnij przycisk ENTER aby przefiltrować wyświetlone elementy.
Pojawią się tylko elementy zawierające łańcuch i odpowiadające im elementy nadrzędne (tylko w drzewach). Zostanie podana liczba odfiltrowanych elementów oraz całkowita liczba elementów.

Uwaga: ciąg znaków należy otoczyć cudzysłowem, aby znaleźć go precyzyjnie. Na przykład wpisanie "Camera 1" odfiltruje kamery o tej nazwie, a nie camera 201.

18

Konfiguracja map i drzewa logicznego

Niniejszy rozdział zawiera informacje o sposobie konfiguracji drzewa logicznego i sposobie zarządzania plikami zasobów takimi jak mapy.



Uwaga!

Jeśli nastąpi przeniesienie grupy urządzeń w drzewie logicznym, urządzenia te tracą swoje ustawienia uprawnień. Należy wówczas ponownie ustawić uprawnienia w oknie **Grupy użytkowników**.

- Kliknij , aby zapisać ustawienia.
- Kliknij , aby cofnąć ostatnią zmianę.
- Kliknij , aby uaktywnić konfigurację.

Patrz

- Okno dialogowe Manager zasobów, Strona 263
- Okno dialogowe Wybierz zasób, Strona 264
- Okno dialogowe Budowa sekwencji, Strona 266
- Okno dialogowe Dodaj sekwencję, Strona 268
- Okno dialogowe Dodaj krok sekwencji, Strona 268
- Okno dialogowe Dodaj adres URL, Strona 264
- Okno dialogowe Wybierz mapę dla łącza, Strona 269
- Okno dialogowe Przekaznik awaryjny, Strona 276
- Okno dialogowe Łącze do aplikacji zewnętrznej, Strona 265

18.1

Konfigurowanie okna Drzewo logiczne

Okno główne > **Mapy i struktura** > karta **Drzewo logiczne**

Można dodawać urządzenia, pliki zasobów, okna robocze map, sekwencje, skrypty poleceń klienta i foldery do drzewa logicznego. Drzewo urządzeń zawiera listę urządzeń. Do drzewa logicznego można przeciągnąć dowolny poziom drzewa urządzeń.

Plikami zasobów może być przykładowo mapa obszaru, dokument, plik internetowy, plik audio lub skrypt poleceń.

- Mapa obszaru jest plikiem, który można dodać do drzewa logicznego. Dodanie mapy obszaru do drzewa logicznego umożliwia utworzenie folderu mapy, w którym można porządkować urządzenia logiczne związane z daną mapą.
- Okno robocze mapy to obszar mapy globalnej z określonym środkiem i poziomem zoomu.
- Folder umożliwia dodatkowo porządkowanie urządzeń w obrębie drzewa logicznego.

Podczas uruchamiania systemu Configuration Client po raz pierwszy, drzewo logiczne jest puste.

Jeśli grupa użytkowników nie posiada uprawnień dostępu do urządzenia (np. kamery), urządzenie nie zostanie wyświetlone na mapie obszaru, w oknie roboczym mapy lub w drzewie logicznym.

Do mapy obszaru można dodać jako aktywne miejsca następujące pozycje okna drzewo urządzeń lub drzewo logiczne:

- Kamery
- Wejścia
- Przekazniki
- Skrypty poleceń
- Sekwencje

- Dokumenty
- Łączy do innych map obszaru
- VRM
- iSCSI
- Czytniki systemu kontroli dostępu
- Centrale alarmowe
- Serwer zarządzający systemami Enterprise System

Dodanie pozycji do mapy obszaru tworzy na tej mapie miejsce aktywne.

Jeśli następuje dodanie pozycji do folderu mapy w drzewie logicznym, zostaje ona również wyświetlona w lewym górnym rogu mapy. Dodanie pozycji do folderu mapy powoduje również umieszczenie jej poniżej odpowiedniego węzła mapy w drzewie logicznym systemu Operator Client.

Do mapy globalnej można dodać następujące pozycje z drzewa urządzeń:

- Kamery

W celu skonfigurowania drzewa logicznego należy wielokrotnie wykonać niektóre lub wszystkie z poniższych czynności.

Aby zmienić nazwę drzewa logicznego:

1. Wybierz element główny drzewa logicznego.

2. Kliknij  .

3. Wpisz nową nazwę.

Nazwa będzie widoczna dla wszystkich użytkowników drzewa logicznego aplikacji Operator Client.

Patrz

- Karta Mapy i struktura , Strona 258

18.2

Dodawanie urządzenia do okna Drzewo logiczne

Okno główne > **Mapy i struktura** > karta **Drzewo logiczne**

Aby dodać urządzenie:

- ▶ Przeciągnąć element z okna Drzewo urządzeń do wybranej lokalizacji w oknie Drzewo logiczne. Użytkownik może przeciągnąć cały węzeł ze wszystkimi elementami podrzędnymi z okna Drzewo urządzeń do okna Drzewo logiczne. Za pomocą klawiszy CTRL lub SHIFT można wybrać wiele urządzeń równocześnie.

Patrz

- Karta Mapy i struktura , Strona 258

18.3

Usuwanie elementu drzewa

Okno główne > **Mapy i struktura** > karta **Drzewo logiczne**

Aby usunąć element drzewa z okna Drzewo logiczne, należy:

- ▶ Kliknąć prawym przyciskiem myszy element w oknie Drzewo logiczne, a następnie kliknąć polecenie **Usuń**. Jeśli wybrany element zawiera elementy składowe, pojawi się odpowiednie okno komunikatu. Aby potwierdzić, kliknąć przycisk **OK**. Element zostanie usunięty. Kiedy element zostanie usunięty z folderu mapy okna Drzewo logiczne, jest także usuwany z mapy.

Patrz

- Karta Mapy i struktura , Strona 258

18.4 Zarządzanie plikami zasobów

Okno główne > **Mapy i struktura** > karta **Drzewo logiczne** > 
LUB

Okno główne > **Alarmy** > 

Pliki zasobów można importować w następujących formatach:

- pliki DWF (2D, pliki zasobów mapy)
- PDF
- JPG
- PNG
- pliki HTML
- pliki MP3 (pliki dźwiękowe)
- pliki TXT (skrypty poleceń lub sekwencje kamer)
- pliki MHT (archiwa sieciowe)
- pliki URL (łącza do stron sieciowych)
- pliki URL HTTPS (łącza do widżetów Intelligent Insights)
- pliki WAV (pliki dźwiękowe)

Importowane pliki zasobów są dodawane do bazy danych. Nie są połączone z plikami oryginalnymi.



Uwaga!

Po każdym z poniższych zadań:

Kliknąć , aby zapisać ustawienia.

Aby zaimportować plik zasobów:

1. Kliknąć .
Zostanie wyświetlone okno dialogowe **Importuj zasób**.
2. Zaznaczyć jeden lub więcej plików.
3. Kliknąć **Otwórz**.
Wybrane pliki zostaną dodane do listy.
Jeżeli plik został już wcześniej zaimportowany, zostanie wyświetlone okno komunikatu.
W razie ponownego importowania już zaimportowanego pliku nowa pozycja zostanie dodana do listy.

Aby usunąć plik zasobów:

1. Zaznaczyć plik zasobów.
2. Kliknąć .
Zaznaczony plik zasobów jest usuwany z listy.

Aby zmienić nazwę pliku zasobów:

1. Zaznaczyć plik zasobów.
2. Kliknąć .
3. Wpisać nową nazwę.
Oryginalna nazwa pliku i data utworzenia pozostanie.

Aby zastąpić zawartość pliku zasobów:

1. Zaznaczyć plik zasobów.

2. Kliknąć  .
Zostanie wyświetlone okno dialogowe **Zastąp zasób**.
3. Wybierz plik o żądanej zawartości i kliknąć **Otwórz**.
Nazwa zasobu pozostanie, oryginalna nazwa pliku zostanie zamieniona na nową nazwę.

Aby wyeksportować plik zasobów:

1. Zaznaczyć plik zasobów.
2. Kliknąć  .
Zostanie wyświetlone okno dialogowe wyboru katalogu.
3. Wybrać odpowiedni katalog i kliknąć **OK**.
Oryginalny plik zostanie wyeksportowany.

Patrz

- Okno dialogowe Wybierz zasób, Strona 264

18.4.1

Okno dialogowe Manager zasobów

Okno główne > **Mapy i struktura** >  > okno dialogowe **Manager zasobów**

Umożliwia zarządzanie plikami zasobów.

Użytkownik może zarządzać następującymi formatami plików:

- pliki DWF (pliki zasobów mapy)
Aby można było używać tych plików w programie Operator Client, są one przekształcane do formatu mapy bitowej.
- PDF
- JPG
- PNG
- pliki HTML (dokumenty HTML, np. plany działań)
- pliki MP3 (pliki dźwiękowe)
- pliki TXT (pliki tekstowe)
- Pliki URL (zawierają łącza do stron www lub widżetów Intelligent Insights)
- pliki MHT (archiwa sieciowe)
- pliki WAV (pliki dźwiękowe)
- pliki EXE



Kliknąć, aby wyświetlić okno dialogowe importowania pliku zasobów.

Kliknąć, aby wyświetlić okno dialogowe  **Dodaj adres URL**.



Kliknąć, aby wyświetlić okno dialogowe **Łącze do aplikacji zewnętrznej**.



Kliknąć, aby usunąć zaznaczony plik zasobów.



Kliknąć, aby zmienić nazwę zaznaczonego pliku zasobów.



Kliknąć, aby wyświetlić okno dialogowe zamiany zaznaczonego pliku zasobów na inny plik.



Kliknąć, aby wyświetlić okno dialogowe eksportowania wybranego pliku zasobów.

18.4.2 Okno dialogowe Wybierz zasób



Okno główne > **Mapy i struktura** >

Umożliwia dodanie pliku mapy w formacie DWF, PDF, JPG lub PNG do drzewa logicznego.

Wybierz plik zasobów:

Kliknąć nazwę pliku w celu wybrania pliku mapy. W okienku podglądu ukaże się zawartość wybranego pliku.

Zarządzaj...

Kliknąć w celu wyświetlenia okna dialogowego **Manager zasobów**.

Patrz

- Dodawanie mapy, Strona 269
- Przypisywanie mapy do folderu, Strona 270
- Dodawanie dokumentu, Strona 264

18.5 Dodawanie dokumentu

Okno główne > **Mapy i struktura** > karta **Drzewo logiczne**

Można dodawać pliki tekstowe, pliki HTML (w tym pliki MHT), pliki URL (zawierające adres internetowy) lub pliki URL HTTPS (na przykład zawierające widżet Intelligent Insights) jako dokumenty. Użytkownik może też dodawać łącza do innych aplikacji.

Przed dodaniem dokumentu należy zaimportować pliki dokumentów.

Aby zaimportować pliki dokumentów, zapoznać się z informacjami w **Zarządzanie plikami zasobów**, Strona 262.

Aby dodać plik dokumentu mapy / widżet Intelligent Insights:

1. Upewnić się, że plik dokumentu, który ma być dodany, został już zaimportowany.
2. Zaznaczyć folder, do którego ma być dodany nowy dokument.
3. Kliknąć . Pojawi się okno dialogowe **Wybierz zasób**.
4. Zaznaczyć plik na liście. Jeśli wymagane pliki nie są dostępne na liście, kliknąć **Zarządzaj...**, aby wyświetlić okno dialogowe **Manager zasobów** w celu importowania plików.
5. Kliknąć **OK**. Nowy dokument zostanie dodany do wybranego folderu.

Patrz

- Okno dialogowe Wybierz zasób, Strona 264
- Zarządzanie plikami zasobów, Strona 262

18.5.1 Okno dialogowe Dodaj adres URL



Okno główne > **Mapy i struktura** >

Umożliwia to dodanie do systemu adresu internetowego HTTP (URL) lub adresu internetowego HTTPS, np. widżetów Intelligent Insights. Adres URL można dodać do okna Drzewo logiczne w postaci dokumentu. Użytkownik może wyświetlić stronę sieciową lub widżet Intelligent Insights w aplikacji Operator Client.

Nazwa

Wprowadzić nazwę dla adresu URL.

URL

Wprowadzić adres URL.

Tylko do połączeń bezpiecznych**Użytkownik**

Wprowadzić nazwę użytkownika adresu URL HTTPS.

Hasło:

Wprowadzić hasło adresu URL HTTPS.

Pokaż hasło

Kliknij, aby włączyć opcję wyświetlania wprowadzonego hasła. Uważaj, aby osoby postronne nie poznały tego hasła.

Patrz

– Dodawanie dokumentu, Strona 264

18.6

Okno dialogowe Łącze do aplikacji zewnętrznej

Okno główne > **Mapy i struktura** > karta **Drzewo logiczne** >  > okno dialogowe **Manager**

zasobów >  > okno dialogowe **Łącze do aplikacji zewnętrznej**

Umożliwia dodanie łącza do aplikacji zewnętrznej. Łącze musi być prawidłowe na stacji roboczej, na której jest używane.

**Uwaga!**

Aplikacja zewnętrzna, która przy uruchamianiu wyświetla ekran powitalny, nie będzie działać zgodnie z oczekiwaniami.

Aplikacja zewnętrzna, która współdzieli funkcje z programem Operator Client, nie będzie działać zgodnie z oczekiwaniami i w rzadkich przypadkach może nawet doprowadzić awarii Operator Client.

Nazwa

Należy tu wprowadzić nazwę łącza, która jest wyświetlana w drzewie logicznym.

Ścieżka

Należy tu wpisać lub wskazać ścieżkę dostępu do aplikacji zewnętrznej. Ścieżka ta musi być prawidłowa na stacji roboczej, na której użytkownik programu Operator Client będzie korzystać z tego łącza.

Argumenty

W razie potrzeby należy wprowadzić argumenty polecenia, które służą do uruchamiania aplikacji zewnętrznej.

18.7

Dodawanie skryptu poleceń

Okno główne > **Mapy i struktura** > karta **Drzewo logiczne**

Przed dodaniem skryptu poleceń, należy zaimportować lub utworzyć pliki skryptów poleceń.

Aby uzyskać więcej informacji na ten temat, patrz *Konfiguracja skryptów poleceń*, Strona 89.

Aby dodać plik skryptu poleceń:

1. Wybierz folder, do którego ma być dodany nowy skrypt poleceń.

2. Kliknąć . Zostanie wyświetlone okno dialogowe **Wybierz skrypt klienta**.

3. Zaznacz plik na liście.

4. Kliknąć **OK**.

W wybranym folderze zostanie dodany nowy skrypt poleceń.

Patrz

– Okno dialogowe Wybierz zasób, Strona 264

18.8**Dodawanie sekwencji kamer**

Okno główne > **Mapy i struktura** > karta **Drzewo logiczne**

Sekwencja kamer jest dodawana do katalogu głównego lub do folderu okna Drzewo logiczne.

Aby dodać sekwencję kamer, należy:

1. W oknie Drzewo logiczne zaznaczyć folder, w którym ma zostać dodana nowa sekwencja kamer.
2. Kliknąć . Pojawi się okno dialogowe **Kreator sekwencji**.
3. Na liście zaznaczyć sekwencję kamer.
4. Kliknąć **Dodaj do Drzewa logicznego**. Nowa  zostanie dodana do wybranego folderu.

Patrz

– Okno dialogowe Budowa sekwencji, Strona 266

18.8.1**Okno dialogowe Budowa sekwencji**

Okno główne > **Mapy i struktura** > 

Umożliwia zarządzanie sekwencjami kamer.

Ikony

	Kliknij, aby wyświetlić okno dialogowe Dodaj sekwencję .
	Kliknij, aby zmienić nazwę sekwencji kamer.
	Kliknij, aby usunąć zaznaczoną sekwencję kamer.

Dodaj krok

Kliknij, aby wyświetlić okno dialogowe **Dodaj krok sekwencji**.

Usuń krok

Kliknij, aby usunąć zaznaczone kroki.

Krok

Wyświetla numer kroku. Wszystkie kamery określonego kroku mają taki sam czas przełączania.

Przełączanie

Umożliwia zmianę czasu prezentowania sekwencji (sekundy).

Numer kamery

Kliknij komórkę, aby wybrać kamerę na podstawie jej numeru logicznego.

Kamera

Kliknij komórkę, aby wybrać kamerę na podstawie jej nazwy.

Funkcja kamery

Kliknij, aby zmienić funkcję kamery w tym wierszu.

Dane

Wprowadź czas działania wybranej funkcji kamery. Aby móc skonfigurować jednostkę czasu, w kolumnach **Kamera** i **Funkcja kamery** muszą być zaznaczone pozycje.

Jednostka danych

Wybierz jednostkę czasu dla ustawionego czasu, np. sekundy. Aby móc skonfigurować jednostkę czasu, w kolumnach **Kamera** i **Funkcja kamery** muszą być zaznaczone pozycje.

Dodaj do Drzewa logicznego

Kliknij, aby dodać wybraną sekwencję kamery do drzewa logicznego i zamknąć okno dialogowe.

Patrz

- Zarządzanie wstępnie zaprogramowanymi sekwencjami kamer, Strona 267

18.9**Zarządzanie wstępnie zaprogramowanymi sekwencjami kamer**

Okno główne > **Mapy i struktura** > karta **Drzewo logiczne**

Aby zarządzać sekwencjami kamer, należy wykonać następujące czynności:

- Utworzyć sekwencję kamer
- Dodać krok z nowym czasem prezentowania sekwencji do istniejącej sekwencji kamer
- Usunąć krok z sekwencji kamer
- Usunąć sekwencję kamer

**Uwaga!**

Po zmianie i aktywacji konfiguracji sekwencja kamery (wstępnie skonfigurowana lub automatyczna) jest zazwyczaj kontynuowana po ponownym uruchomieniu programu Operator Client.

Seqwencja nie będzie jednak kontynuowana w następujących przypadkach:

Po usunięciu monitora, na którym zgodnie z konfiguracją miała być wyświetlana sekwencja. W przypadku zmiany trybu monitora (widok pojedynczy / poczwórny), na którym zgodnie z konfiguracją miała być wyświetlana sekwencja.

W przypadku zmiany numeru logicznego monitora, na którym zgodnie z konfiguracją miała być wyświetlana sekwencja.

**Uwaga!**

Po każdym z poniższych zadań:

Kliknąć  , aby zapisać ustawienia.

Aby utworzyć sekwencję kamer, należy:

1. W oknie Drzewo logiczne zaznaczyć folder, w którym ma zostać utworzona sekwencja kamer.

2. Kliknąć .

Zostanie wyświetlone okno dialogowe **Kreator sekwencji**.

3. W oknie dialogowym **Kreator sekwencji** kliknąć .

Zostanie wyświetlone okno dialogowe **Dodaj sekwencję**.

4. Wpisz odpowiednie wartości.
5. Kliknąć **OK**.

Zostanie dodana nowa sekwencja kamer .

Więcej informacji o różnych polach znajduje się w Pomocy ekranowej wybranego okna programu.

Aby dodać krok z nowym czasem prezentowania sekwencji do istniejącej sekwencji kamer:

1. Zaznacz żądaną sekwencję kamer.
2. Kliknąć **Dodaj krok**.
Zostanie wyświetlone okno dialogowe **Dodaj krok sekwencji**.
3. Wprowadzić odpowiednie ustawienia.
4. Kliknąć **OK**.
Nowy krok zostanie dodany do sekwencji kamer.

Aby usunąć krok z sekwencji kamer:

- ▶ Kliknąć prawym przyciskiem myszy na wybraną sekwencję kamer i kliknąć **Usuń krok**.
Krok z najwyższym numerem zostanie usunięty.

Aby usunąć sekwencję kamer:

1. Zazaczyć żądaną sekwencję kamer.
2. Kliknąć . Wybrana sekwencja kamer zostanie usunięta.

Patrz

- Okno dialogowe Budowa sekwencji, Strona 266

18.9.1

Okno dialogowe Dodaj sekwencję

Okno główne > **Mapy i struktura** >  > Okno dialogowe **Kreator sekwencji** > 
Umożliwia skonfigurowanie właściwości sekwencji kamer.

Nazwa sekwencji:

Wprowadź odpowiednią nazwę nowej sekwencji kamer.

Numer logiczny:

Aby używać w połączeniu z klawiaturą Bosch IntuiKey, wpisz numer logiczny dla sekwencji.

Czas przełączania:

Wprowadź odpowiedni czas prezentowania sekwencji.

Kamery w jednym kroku:

Wprowadź liczbę kamer w każdym kroku.

Kroki:

Wprowadź liczbę kroków.

18.9.2

Okno dialogowe Dodaj krok sekwencji

Okno główne > **Mapy i struktura** >  > przycisk **Dodaj krok**
Umożliwia dodanie kroku z nowym czasem prezentowania sekwencji do istniejącej sekwencji kamer.

Czas przełączania:

Wprowadź odpowiedni czas prezentowania sekwencji.

18.10

Dodawanie folderu

Okno główne > **Mapy i struktura** > karta **Drzewo logiczne**

Aby dodać folder, należy:

1. Zazaczyć folder, do którego ma być dodany nowy folder.
2. Kliknąć przycisk . Nowy folder zostanie dodany do wybranego folderu.

3. Kliknąć przycisk , aby zmienić nazwę folderu.
4. Wprowadzić nową nazwę i nacisnąć klawisz ENTER.

Patrz

- Karta Mapy i struktura , Strona 258

18.11

Dodawanie mapy

Okno główne > **Mapy i struktura** > karta **Drzewo logiczne**

Przed dodaniem mapy należy zaimportować pliki zasobów mapy.

Aby zaimportować plik zasobów mapy zapoznaj się ze szczegółowymi informacjami w Zarządzanie plikami zasobów, Strona 262.

Aby dodać mapę:

1. Upewnij się, że plik zasobów mapy, który ma być dodany, został już zaimportowany.
2. Zaznacz folder, do którego ma być dodana nowa mapa.

3. Kliknij . Zostanie wyświetlone okno dialogowe **Wybierz zasób**.
4. Zaznacz plik na liście.

Jeśli wymagane pliki nie są dostępne na liście, kliknij **Zarządzaj...**, aby wyświetlić okno dialogowe **Manager zasobów** w celu importowania plików.

5. Kliknąć **OK**.

Nowa mapa  zostanie dodana w wybranym folderze.

Mapy jest wyświetlana.

Wszystkie urządzenia znajdujące się w tym folderze są wyświetlane w lewym górnym rogu mapy.

Patrz

- Okno dialogowe Wybierz zasób, Strona 264

18.12

Dodawanie łącza do innej mapy

Okno główne > **Mapy i struktura** > karta **Drzewo logiczne**

Po dodaniu co najmniej dwóch map, można na jednej mapie dodać łącze do drugiej mapy, aby użytkownik miał możliwość przejścia z jednej mapy do drugiej przez kliknięcie łącza.

Aby dodać łącze, należy:

1. Kliknąć folder mapy  w drzewie logicznym.
2. Kliknąć prawym przyciskiem myszy mapę i kliknąć **Utwórz łącze**.
Zostanie wyświetlone okno dialogowe **Wybierz mapę dla łącza**.

3. W oknie dialogowym kliknąć mapę .
4. Kliknąć **Wybierz**.
5. Przeciągnąć element na odpowiednie miejsce na mapie.

18.12.1

Okno dialogowe Wybierz mapę dla łącza

Okno główne > **Mapy i struktura** > wybrać folder mapy  w drzewie logicznym > kliknąć prawym przyciskiem myszy na mapie i kliknąć opcję **Utwórz łącze**

Umożliwia wybranie mapy do utworzenia łącza do innej mapy.



Kliknąć inną mapę, aby ją wybrać.

Wybierz

Kliknąć, aby wstawić łącze do wybranej mapy.

18.13

Przypisywanie mapy do folderu

Okno główne > **Mapy i struktura** > karta **Drzewo logiczne**

Przed przypisaniem map należy zaimportować pliki zasobów mapy.

Aby uzyskać więcej informacji na ten temat, patrz *Zarządzanie plikami zasobów*, Strona 262.

Aby przypisać plik zasobów mapy:

1. Kliknij folder prawym przyciskiem myszy, a następnie kliknij **Przypisz mapę**.
Zostanie wyświetlone okno dialogowe **Wybierz zasób**.
2. Zaznacz na liście plik zasobów mapy.
3. Kliknąć **OK**. Wybrany folder jest wyświetlany jako .
Mapa jest wyświetlana w oknie mapy.
Wszystkie elementy tego folderu są wyświetlane w lewym górnym rogu mapy.

Patrz

- Karta *Mapy i struktura*, Strona 258
- Okno dialogowe *Wybierz zasób*, Strona 264

18.14

Zarządzanie urządzeniami na mapie obszaru

Okno główne > **Mapy i struktura** > karta **Drzewo logiczne**

Przed rozpoczęciem zarządzania urządzeniami na mapie obszaru należy dodać lub przypisać mapę do folderu oraz dodać urządzenia do tego folderu.



Uwaga!

Po każdym z poniższych zadań:



Kliknąć, aby zapisać ustawienia.

Aby umieścić elementy na mapie obszaru:

1. Zaznaczyć folder mapy.
2. Przeciągnij urządzenia z drzewa logicznego do folderu mapy.
Urządzenia z folderu mapy są umieszczone w lewym górnym rogu mapy obszaru.
3. Przeciągnij elementy na odpowiednie miejsca na mapie obszaru.

Aby usunąć element w drzewie logicznym tylko z mapy obszaru:

1. Kliknąć prawym przyciskiem myszy element na mapie, a następnie kliknąć polecenie **Niewidoczny**.
Element zostanie usunięty z mapy obszaru.
Pozostanie on jednak w drzewie logicznym.
2. Aby element był ponownie widoczny, kliknąć prawym przyciskiem myszy urządzenie w drzewie logicznym i kliknąć **Widoczny na mapie**.

Aby usunąć element z mapy obszaru oraz z pełnego drzewa logicznego:

- ▶ Kliknąć prawym przyciskiem myszy element na drzewie logicznym i kliknąć **Usuń**.
Element zostanie usunięty z mapy obszaru oraz z drzewa logicznego.

Aby zmienić ikonę orientacji kamery:

- ▶ Kliknąć element prawym przyciskiem myszy, wybrać polecenie **Zmień obraz**, a następnie kliknąć właściwą ikonę.
Ikona ulegnie odpowiedniej zmianie.

Aby zmienić kolor elementu:

- ▶ Kliknąć prawym przyciskiem myszy element i wybrać **Zmień kolor**. Wybrać właściwy kolor.
Ikona ulegnie odpowiedniej zmianie.

Aby pominąć urządzenie lub anulować jego pominięcie na mapie obszaru:

1. Kliknąć prawym przyciskiem myszy konkretne urządzenie na mapie obszaru.
2. Kliknąć przycisk **Pomiń** / **Cofnij pominięcie**.

**Uwaga!**

Istnieje możliwość filtrowania pominiętych urządzeń w polu tekstowym wyszukiwania.

Patrz

- Konfigurowanie pomijania urządzeń, Strona 277
- Karta Mapy i struktura, Strona 258

18.15

Konfiguracja mapy globalnej i okna roboczego mapy

Okno główne > **Mapy i struktura** karta **Mapa globalna**

Aby korzystać z map online lub Map-based tracking assistant w Operator Client należy dodać i skonfigurować kamery na mapie globalnej.

Okna robocze mapy można skonfigurować z poziomu mapy globalnej. Okno robocze mapy to obszar mapy globalnej z określonym środkiem i poziomem zoomu. Okno robocze mapy może być wyświetlane w okienku obrazu Operator Client.

Aby utworzyć okno robocze mapy lub użyć Map-based tracking assistant w Operator Client, należy najpierw wykonać następujące czynności:

1. Wybrać typ mapy tła dla mapy globalnej.
2. Przeciągnąć kamery na mapę globalną.
3. Skonfigurować kierunek i stożek widzenia kamer na mapie globalnej.

Aby utworzyć okna robocze map lub użyć narzędzia Map-based tracking assistant w programie Operator Client **na wielu kondygnacjach**, należy wykonać następujące czynności:

1. Wybrać typ mapy tła dla mapy globalnej.
2. Dodaj mapę do mapy globalnej.
Uwaga:Pierwsza dodana mapa będzie parterem. W przypadku wybrania typu mapy tła offline **Brak** pierwsza dodana mapa stanie się mapą tła.
3. Dodaj kondygnacje do parteru lub mapy tła.
4. Zaznacz żądaną kondygnację.
5. Przeciągnij kamery na mapę kondygnacji.
6. Skonfiguruj kierunki i stożki widzenia kamer.

18.15.1

Konfigurowanie mapy globalnej

Można zdefiniować typy map tła dla mapy globalnej, a także wyszukiwać kamery, lokalizacje i adresy.

Aby zmienić typ mapy tła dla mapy globalnej:

1. Przejdź do okna głównego i wybrać menu **Ustawienia** > polecenie **Opcje**.
2. W sekcji **Funkcje systemowe** wybierz **Mapy**.

3. Na liście **Typ mapy tła** wybierz żadaną opcję.

Uwaga: Jeśli masz dostęp do Internetu, możesz wybrać typ mapy tła online (mapy **HERE**). Jeśli nie ma dostępu do Internetu, należy wybrać mapę tła **Brak** w trybie offline.

Aby korzystać z map online, należy wykupić licencję.

4. Kliknij **OK**.



Uwaga!

Jeśli zmienisz typ mapy tła z offline (**Brak**) na online (mapy **HERE**), sprawdź, czy położenie map podrzędnych i punktów aktywnych kamery jest wciąż prawidłowe.

Aby wyszukać kamery lub lokalizacje na mapie globalnej:

1. W polu wyszukiwania wpisać nazwę kamery, lokalizacji lub adresu.
Po rozpoczęciu wpisywania zostanie wyświetlone menu rozwijane z listą odpowiednich opcji.
2. Wybrać odpowiednią opcję z listy

Kamera, lokalizacja lub adres są wyświetlane i przez kilka sekund oznaczone symbolem .

Patrz

- Okno dialogowe *Opcje (menu Ustawienia)*, Strona 120

18.15.2

Konfigurowanie kamer na mapie globalnej

Aby skonfigurować kamerę na mapie globalnej:

Uwaga: Jeśli na mapach skonfigurowano wiele kondygnacji, uważaj, aby podczas konfigurowania kamer zaznaczyć odpowiednią.

1. Wybrać kartę **Mapa globalna**.
2. Aby przejść do pozycji, w której chce się umieścić kamerę, należy wpisać adres lub lokalizację w polu wyszukiwania.

Można także powiększać i pomniejszać obrazy za pomocą przycisków  lub pokrętła przewijania myszy.

3. Przeciągnąć kamerę z drzewa urządzeń do odpowiedniego obszaru mapy globalnej.
4. Kliknąć kamerę, aby ją zaznaczyć.
5. Skonfigurować kierunek i stożek widzenia kamery.

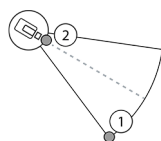
Uwaga: po wybraniu kamery kopułkowej widać dostępny i aktualny stożek widzenia kamery. Symbol ostrzeżenia informuje, że stożek widzenia kamery wymaga kalibracji w płaszczyźnie poziomej i pionowej. Aby skalibrować kamerę kopułkową, otworzyć podgląd obrazu na żywo.

6. Kliknąć , aby wyświetlić podgląd obrazu na żywo z wybranej kamery.
Podgląd wideo może pomóc w skonfigurowaniu kierunku i widoku stożka.

7. Kliknąć , aby ukryć podgląd wideo z wybranej kamery.

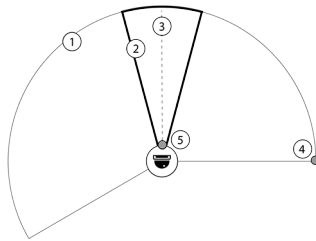
Uwaga: jeśli kamera zostanie dodana do mapy globalnej, a nie została jeszcze dodana do drzewa logicznego, zostanie ona umieszczona automatycznie na końcu drzewa logicznego.

Aby skonfigurować kierunek i stożek widzenia kamery:



1. Przeciągnąć, aby skonfigurować stożek widzenia.
2. Przeciągnąć, aby obrócić i skonfigurować kierunek.

Aby skonfigurować kierunek działania kamery PTZ w poziomie i stożek widzenia (platforma CPP4 lub nowsza wersja):



1. Dostępny stożek widzenia wskazuje teoretycznie dostępny obszar widzenia.
2. Rzeczywisty stożek widzenia wskazuje rzeczywiste położenie PTZ kamery PTZ
3. Kąt obrotu 0.
4. Przeciągnąć, aby skonfigurować stożek widzenia.
5. Przeciągnąć, aby obrócić i skonfigurować kierunek.



Uwaga!

Aby zapewnić optymalne wykorzystanie funkcji Map-based tracking assistant, należy także ustawić położenie pionowe kamery PTZ. Zaleca się ustawienie pozycji pionowej podglądu obrazu na żywo na podstawie dobrze znanej pozycji w tym obszarze, np. na podstawie wyraźnie widocznego ruchu. Później funkcja Map-based tracking assistant będzie zawsze używała tej skonfigurowanej pozycji pionowej.

Aby wyświetlać lub ukrywać podglądy obrazów z kamer:

1. Kliknąć , aby wyświetlić podgląd obrazu na żywo z wybranej kamery.
Lub
Kliknij kamerę prawym przyciskiem myszy i wybierz opcję **Pokaż podglądy**.
Podgląd obrazu może pomóc skonfigurować kierunek i stożek widzenia.
2. Kliknij przycisk , aby ukryć podgląd obrazu z wybranej kamery.
Lub
Kliknij kamerę prawym przyciskiem myszy i wybierz opcję **Ukryj podglądy**.

Aby usunąć kamerę z mapy globalnej:

- ▶ Kliknij kamerę prawym przyciskiem myszy i wybierz opcję **Usuń**.

Aby kamera była widoczna na wszystkich kondygnacjach:

- ▶ Kliknij prawym przyciskiem myszy miejsce aktywne kamery i wybierz opcję **Widoczne na wszystkich kondygnacjach**.
Odtąd kamera będzie zawsze widoczna po wybraniu innej kondygnacji.

Aby edytować geolokalizację kamery

1. Kliknij kamerę prawym przyciskiem myszy i wybierz **Edytuj geolokalizację**.
Zostanie wyświetlone okno dialogowe **Edytuj geolokalizację**.
2. Wprowadź długość i szerokość geograficzną i kliknij **OK**.

Uwaga: Nie musisz wpisywać wartości szerokości i długości geograficznej. Możesz skopiować je z zewnętrznego źródła. Po wklejeniu szerokości geograficznej, długość geograficzna zostanie wypełniona automatycznie.

Aby włączyć funkcję śledzenia obiektów dla kamery:

- ▶ Kliknąć prawym przyciskiem myszy kamerę i wybrać opcję **Śledzenie obiektów (jeśli dodane do drzewa logicznego)**.

Funkcja śledzenia obiektów zostanie włączona dla tej kamery.

Uwaga: Funkcja śledzenia obiektów jest dostępna tylko dla kamer z platformą CPP6 lub nowszą, które zostały dodane do drzewa logicznego.

Łączenie aktywnych miejsc w grupy

Jeśli na mapie globalnej jest już skonfigurowanych kilka kamer i użytkownik oddali widok, aktywne miejsca kamery są łączone w grupy. Wyświetlana jest liczba aktywnych miejsc w grupie. Wybrana kamera nie jest wyświetlana jako część grupy.

Patrz

– Dodawanie nadajnika Bosch ze wstępnie skonfigurowaną geolokalizacją, Strona 221

18.15.3

Dodawanie map na mapie globalnej

Na mapie globalnej można dodać własne pliki map budynku.

Operatorzy systemu BVMS mogą wtedy zobaczyć określone lokalizacje kamer.

Aby dodać mapę na mapie globalnej:

1. Wybrać kartę **Mapa globalna**.
2. Aby przejść do pozycji, w której chce się umieścić mapę, należy wpisać adres lub lokalizację w polu wyszukiwania.

Można także powiększać i pomniejszać obrazy za pomocą przycisków  i  lub pokrętką przewijania myszy.

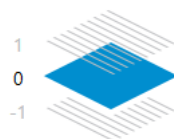
3. Kliknąć przycisk .
Zostanie wyświetlone okno **Wybierz zasób**.
4. Wybrać mapę i kliknąć przycisk **OK**.
5. Kliknąć i przeciągnąć , aby obrócić mapę.
6. Kliknąć i przeciągnąć , aby przenieść mapę.
7. Aby dopasować rozmiar mapy, należy użyć punktów przeciągania.
8. Kliknąć , aby usunąć mapę.

Uwaga: W przypadku dodawania wielu kondygnacji pierwsza dodana mapa będzie parterem. Parter

jest oznaczany cyfrą 0 w polu .

Aby dodać więcej kondygnacji do parteru:

1. Kliknąć liczbę 0 w polu .



Zostanie otwarte pole .

2. Wybrać kondygnację, na której ma zostać dodana mapa.
3. **Uwaga:** W celu dodania mapy można dodać tylko kondygnację bezpośrednio powyżej lub poniżej.

4. Kliknąć przycisk .
Zostanie wyświetlone okno **Wybierz zasób**.
5. Wybrać mapę i kliknąć przycisk **OK**.
6. Dopasować położenie dodanej mapy kondygnacji do położenia mapy parteru.

Aby kondygnacja była widoczna na wszystkich kondygnacjach:

1. Kliknąć prawym przyciskiem myszy dowolną ikonę regulacji na odpowiedniej mapie kondygnacji: ,  lub .

- Wybrać opcję **Widoczne na wszystkich kondygnacjach**.

Odtąd ta kondygnacja będzie zawsze widoczna po wybraniu innej kondygnacji.

Uwaga: Jeśli nie masz dostępu do Internetu oraz wybrano typu mapy tła offline **Brak**, można dodać mapę jako mapę tła. Zalecamy ustawienie widoczności tej mapy tła na wszystkich kondygnacjach.

Wtedy ta mapa będzie widoczna po wybraniu każdej innej kondygnacji.

Aby ustawić geolokalizację mapy

- Kliknij prawym przyciskiem myszy dowolną ikonę ustawień mapy odpowiedniego piętra, , ,  lub dowolny uchwyt wokół mapy, a następnie wybierz **Ustaw geolokalizację**.

Zostanie wyświetlone okno dialogowe **Ustaw geolokalizację**.

Uwaga: Aby lepiej widzieć, możesz zmaksymalizować okno dialogowe za pomocą przycisku maksymalizacji w prawym górnym rogu.

- Przeciągnij znaczniki  i  w żądane miejsca na mapie.
- Wprowadź dokładną szerokość i długość geograficzną dla każdego znacznika w odpowiednich polach, a następnie kliknij **OK**.

Uwaga: Nie musisz wpisywać szerokości i długości geograficznej. Możesz je skopiować z zewnętrznego źródła. Po wklejeniu szerokości geograficznej, długość geograficzna zostanie wypełniona automatycznie.

18.16

Dodawanie okna roboczego mapy

Okno główne > **Mapy i struktura** > karta **Drzewo logiczne**

Aby dodać okno robocze mapy:

- Kliknąć , aby dodać okno robocze.
- Wpisać nazwę okna roboczego mapy.
- Aby przejść do lokalizacji, w której chcesz utworzyć okno robocze mapy, należy wpisać adres lub lokalizację w polu wyszukiwania mapy globalnej.

Jeśli adres lub lokalizacja nie są dostępne, można powiększać i pomniejszać obrazy za pomocą

przycisków  i  lub kółka przewijania myszy.

- Kliknąć , aby zapisać konfigurację.



Uwaga!

Jeśli okno robocze mapy zawiera różne kondygnacje, podczas otwierania okna operator zobaczy w programie Operator Client kondygnację wybraną w momencie zapisywania konfiguracji. Następnie w okienku obrazu operator może zmienić kondygnację okna roboczego mapy.

18.17

Włączanie Map-based tracking assistant

Funkcja Map-based tracking assistant pomaga śledzić poruszające się obiekty z wielu kamer.

Odpowiednie kamery należy skonfigurować na mapie globalnej. Jeśli w okienku obrazu alarmowego, podglądu na żywo, odtwarzania lub w okienku obrazu alarmowego zostanie wyświetlony podejrzany ruchomy obiekt, operator może automatycznie uruchomić funkcję Map-based tracking assistant, która automatycznie wyświetli obraz z wszystkich kamer w pobliżu tego obiektu.

Aby włączyć funkcję Map-based tracking assistant:

- Przejdź do okna głównego i wybierz menu **Ustawienia** > polecenie **Opcje**.
- Zaznacz pole wyboru **Włącz funkcję systemową**.
- Kliknij **OK**.

18.18 Dodawanie przekaźnika awaryjnego



Okno główne > **Mapy i struktura** > karta **Drzewo logiczne** > okno dialogowe **Przekaźnik nieprawidłowego działania**

Użycie zgodne z przeznaczeniem

Zadaniem przekaźnika awaryjnego jest wyzwalanie zewnętrznego alarmu (sygnalizatora optycznego, syreny itd.) w przypadku wystąpienia jakiegokolwiek poważnego błędu systemu.

Przekaźnik musi być zresetowany ręcznie przez użytkownika.

Dopuszczalne przekaźniki awaryjne podano na poniższej liście:

- BVIP – przekaźnik nadajnika lub dekodera
- Przekaźnik ADAM
- Wyjście centrali alarmowej

Przykład

Przekaźnik aktywuje się w przypadku zdarzenia, które wpływa poważnie na działanie systemu (np. awaria dysku twardego), lub gdy wystąpi zagrożenie bezpieczeństwa lokalizacji (np. pogorszenie sprawdzania obrazu odniesienia). To może wyzwolić na przykład alarm dźwiękowy lub spowodować automatyczne zamknięcie drzwi.

Opis działania

Pojedynczy przekaźnik można skonfigurować do pracy jako przekaźnik awaryjny. Przekaźnik awaryjny zostanie aktywowany automatycznie, gdy wystąpi zdarzenie ze zbioru zdarzeń zdefiniowanych przez użytkownika. Aktywacja przekaźnika oznacza wystanie polecenia do zamknięcia się przekaźnika. Późniejsze zdarzenie „przekaźnik zamknięty” jest konsekwencją tego polecenia i jest generowane oraz otrzymywane tylko wtedy, gdy stan przekaźnika zmienia się fizycznie! Na przykład przekaźnik, który był już zamknięty wcześniej, nie wysyła tego zdarzenia.

Z wyjątkiem automatycznego wyzwalania przekaźnika w wyniku wystąpienia zdarzeń zdefiniowanych przez użytkownika, przekaźnik awaryjny jest traktowany jak każdy inny przekaźnik. Dlatego użytkownik może dezaktywować przekaźnik awaryjny w programie Operator Client. Program Web Client również może dezaktywować przekaźnik awaryjny. Ze względu na to, że zwykłe uprawnienia dostępu stosuje się również do przekaźnika awaryjnego, wszystkie programy klienckie powinny uwzględniać uprawnienia zalogowanych użytkowników.

Aby dodać przekaźnik:

1. Na liście **Przekaźnik nieprawidłowego działania** zaznacz żądany przekaźnik.
2. Kliknij **Zdarzenia...**
Pojawi się okno dialogowe **Wybór zdarzeń dla przekaźnika awaryjnego**.
3. Kliknij, aby zaznaczyć zdarzenia, które mogą wyzwać przekaźnik awaryjny.
4. Kliknij **OK**.
Przekaźnik awaryjny zostanie dodany do systemu.

18.18.1 Okno dialogowe Przekaźnik awaryjny



Okno główne > **Mapy i struktura** > karta **Drzewo logiczne** > okno dialogowe **Przekaźnik nieprawidłowego działania**

Do systemu można dodać przekaźnik awaryjny. Można określić przekaźnik, który będzie używany jako przekaźnik awaryjny, i skonfigurować zdarzenia, które będą go wyzwały.

Przekaźnik musi już być skonfigurowany w drzewie logicznym.

Przekaźnik nieprawidłowego działania

Na liście zaznacz żądany przekaźnik.

Zdarzenia...

Ten przycisk należy kliknąć, aby wyświetlić okno dialogowe **Wybór zdarzeń dla przekaźnika awaryjnego**.

18.19**Konfigurowanie pomijania urządzeń**

Okno główne > **Mapy i struktura** > karta **Drzewo logiczne**

Istnieje możliwość pominięcia niektórych nadajników, kamer, wejść i przekaźników, na przykład podczas prac budowlanych. W przypadku pominięcia nadajnika, kamery, wejścia lub przekaźnika zapis zostaje zatrzymany, a program BVMS Operator Client nie wyświetla żadnych zdarzeń ani alarmów, a alarmy nie są zapisywane w rejestrze.

W programie Operator Client nadal można wyświetlać obraz z pominiętych kamer na żywo, a operator ma dostęp do starych nagrań.

**Uwaga!**

W przypadku pominięcia nadajnika, dla kamer, przekaźników oraz wejść powiązanych w tym nadajnikiem nie będą generowane żadne zdarzenia ani alarmy. Jeśli konkretna kamera, przekaźnik lub wejście zostaną pominięte osobno i takie konkretne urządzenie zostanie odłączone od nadajnika, wówczas alarmy nadal będą generowane.

Aby pominąć urządzenie lub anulować jego pominięcie w drzewie logicznym lub drzewie urządzeń:

1. W drzewie logicznym lub drzewie urządzeń kliknij prawym przyciskiem myszy konkretne urządzenie.
2. Kliknij przycisk **Pomiń** / **Cofnij pominięcie**.

Aby pominąć urządzenie lub anulować jego pominięcie na mapie:

Patrz Zarządzanie urządzeniami na mapie obszaru, Strona 270

**Uwaga!**

Istnieje możliwość filtrowania pominiętych urządzeń w polu tekstowym wyszukiwania.

Patrz

- Zarządzanie urządzeniami na mapie obszaru, Strona 270

19

strona Harmonogramy

Okno główne > **Harmonogramy**

Umożliwia skonfigurowanie harmonogramów zapisu oraz harmonogramów zadań.



Kliknij, aby zmienić nazwę wybranego harmonogramu zapisu lub harmonogramu zadań.

Harmonogramy zapisu

Wyświetla drzewo harmonogramów zapisu. Zaznacz pozycję do skonfigurowania.

Harmonogramy zadań

Wyświetla drzewo harmonogramów zadań. Zaznacz pozycję do skonfigurowania.

Dodaj

Kliknij, aby dodać nowy harmonogram zadań.

Usuń

Kliknij, aby usunąć wybrany harmonogram zadań.

Patrz

– Konfigurowanie harmonogramów, Strona 280

19.1

strona Harmonogramy zapisu

Okno główne > > zaznaczyć żądany element drzewa Harmonogramy zapisu

Umożliwia skonfigurowanie harmonogramów zapisu.

Dni tygodnia

Kliknij, aby wyświetlić tabelę harmonogramów dla dni roboczych. Wyświetlone zostaną przedziały czasowe dla wszystkich skonfigurowanych harmonogramów zapisu.

Przeciągnij wskaźnik, aby zaznaczyć przedziały czasowe dla wybranego harmonogramu. Wszystkie zaznaczone komórki otrzymują kolor wybranego harmonogramu.

24 godziny dnia są wyświetlane poziomo. Każda godzina jest podzielona na 4 komórki. Jedna komórka odpowiada 15 minutom.

Święta

Kliknąć, aby wyświetlić tabelę harmonogramów dla świąt.

Dni wolne od pracy

Kliknąć, aby wyświetlić tabelę harmonogramów dla dni wolnych od pracy.

Dodaj

Kliknij, aby wyświetlić okno dialogowe dodawania wymaganych świąt i dni wolnych od pracy.

Usuń

Kliknąć, aby wyświetlić okno dialogowe usuwania świąt i dni wolnych od pracy.

Patrz

- Konfigurowanie harmonogramu zapisu, Strona 280
- Dodawanie świąt i dni wolnych od pracy, Strona 282
- Usuwanie świąt i dni wolnych od pracy, Strona 283
- Zmiana nazwy harmonogramu, Strona 283

19.2

strona Harmonogramy zadań

Okno główne > > zaznaczyć żądany element drzewa Harmonogramy zadań

Umożliwia skonfigurowanie dostępnych harmonogramów zadań. Użytkownik konfiguruje wzór standardowy lub powtarzający się.

Standardowo

Kliknąć, aby wyświetlić tabelę harmonogramów do konfigurowania standardowych harmonogramów zadań. Jeśli zostanie skonfigurowany model standardowy, dla wybranego harmonogramu nie będzie obowiązywał żaden model powtarzający się.

Cyklicznie

Kliknąć, aby wyświetlić tabelę harmonogramów do konfigurowania modelu powtarzającego się dla wybranego harmonogramu zadań. Na przykład użytkownik konfiguruje harmonogram dla co drugiego wtorku każdego miesiąca lub 4 lipca każdego roku. Jeśli zostanie skonfigurowany model powtarzający się, dla wybranego harmonogramu zadań nie będzie obowiązywał żaden model standardowy.

Dni tygodnia

Kliknij, aby wyświetlić tabelę harmonogramów dla dni roboczych.

Przeciągnij wskaźnik, aby zaznaczyć przedziały czasowe dla wybranego harmonogramu. Zaznaczone komórki są wyświetlane w kolorze wybranego harmonogramu.

24 godziny dnia są wyświetlane poziomo. Każda godzina jest podzielona na 4 komórki. Jedna komórka odpowiada 15 minutom.

Święta

Kliknąć, aby wyświetlić tabelę harmonogramów dla świąt.

Dni wolne od pracy

Kliknąć, aby wyświetlić tabelę harmonogramów dla dni wolnych od pracy.

Usunąć wszystko

Kliknąć, aby usunąć przedziały czasowe wszystkich dostępnych dni (dni tygodnia, święta, dni wolne od pracy).

Zaznacz wszystko

Kliknąć, aby zaznaczyć przedziały czasowe wszystkich dostępnych dni (dni tygodnia, święta, dni wolne od pracy).

Dodaj...

Kliknąć, aby wyświetlić okno dialogowe dodawania wymaganych świąt i dni wolnych od pracy.

Usuń...

Kliknąć, aby wyświetlić okno dialogowe usuwania świąt lub dni wolnych od pracy.

Wzór powtarzający się

Kliknąć częstotliwość, z jaką ma powtarzać się harmonogram zadań (Codziennie, Raz w tygodniu, Raz w miesiącu, Raz w roku), a następnie zaznaczyć odpowiednie opcje.

Wzór dzienny

Przeciągnąć wskaźnik, aby zaznaczyć przedziały czasowe dla modelu powtarzającego się.

Patrz

- Dodawanie harmonogramu zadań, Strona 281
- Konfigurowanie standardowego harmonogramu zadań, Strona 281
- Konfigurowanie powtarzającego się harmonogramu zadań, Strona 281
- Usuwanie harmonogramu zadań, Strona 282
- Dodawanie świąt i dni wolnych od pracy, Strona 282
- Usuwanie świąt i dni wolnych od pracy, Strona 283
- Zmiana nazwy harmonogramu, Strona 283

20 Konfigurowanie harmonogramów

Okno główne > **Harmonogramy**

Dostępne są dwa rodzaje harmonogramów:

- Harmonogramy zapisu
- Harmonogramy zadań

Istnieje możliwość skonfigurowania nawet 10 różnych harmonogramów zapisu w tabeli Tabela harmonogramów zapisu. W tych segmentach kamery mogą zachowywać się różnie. Mogą one, przykładowo, posiadać inne ustawienia częstotliwości odświeżania i rozdzielczości (konfigurowane na stronie **Kamery i zapis**). W każdym punkcie czasu obowiązuje dokładnie jeden harmonogram zapisu. Brak jest przerw oraz nie występuje wzajemne nakładanie.

Harmonogramy zadań umożliwiają skonfigurowanie harmonogramów dla różnych zdarzeń, które mogą wystąpić w systemie (konfigurowanych na stronie **Zdarzenia**).

Definicje harmonogramów zapisu oraz harmonogramów zadań można znaleźć w Słowniczku.

Harmonogramy są wykorzystywane w innych oknach systemu Configuration Client:

- strona **Kamery i zapis**
Służy do konfigurowania zapisu.
- strona **Zdarzenia**
Umożliwia określenie sytuacji, w których zdarzenia powodują uruchomienie rejestrowania alarmów lub wykonanie skryptów poleceń.
- strona **Grupy użytkowników**
Umożliwia określenie warunków, w których możliwe jest zalogowanie się członków grupy użytkowników.
- Kliknij , aby zapisać ustawienia.
- Kliknij , aby cofnąć ostatnią zmianę.
- Kliknij , aby uaktywnić konfigurację.

Patrz

- strona *Harmonogramy zapisu*, Strona 278
- strona *Harmonogramy zadań*, Strona 278

20.1 Konfigurowanie harmonogramu zapisu

Okno główne > **Harmonogramy**

Użytkownik może dodawać dni wolne od pracy oraz święta do każdego harmonogramu zapisu.

Ustawienia te mają wyższy priorytet niż ustawienia tygodniowe.

Pod względem rangi ustawień obowiązuje następująca kolejność: dni wolne od pracy, święta, dni robocze.

Maksymalna liczba harmonogramów zapisu to 10. Pierwsze trzy pozycje są skonfigurowane

domyślnie. Użytkownik może zmienić te ustawienia. Pozycje oznaczone szarą ikoną  nie mają skonfigurowanego przedziału czasowego.

Harmonogramy zapisu wykorzystują te same dni robocze.

Każdy standardowy harmonogram zadań ma własne wzory dni roboczych.

Aby skonfigurować harmonogram zapisu:

1. Wybierz harmonogram w drzewie **Harmonogramy zapisu**.
2. Kliknij kartę **Dni tygodnia**.

3. W polu **Tabela harmonogramów** przeciągnij wskaźnik, aby zaznaczyć przedziały czasowe dla wybranego harmonogramu. Zaznaczone komórki są wyświetlane w kolorze wybranego harmonogramu.

Uwagi:

- Można zaznaczyć przedział czasowy w danym dniu roboczym Harmonogramu zapisu używając koloru innego Harmonogramu zapisu.

Patrz

- strona Harmonogramy zapisu, Strona 278

20.2

Dodawanie harmonogramu zadań

Okno główne > **Harmonogramy**

Aby dodać harmonogram zadań, należy:

1. Kliknąć **Dodaj**.
Zostanie dodana nowa pozycja.
2. Wprowadzić odpowiednią nazwę.
3. Kliknąć opcję **Standardowo**, aby wybrać standardowy Harmonogram zadań lub opcję **Powtarzający się**, aby wybrać powtarzający się Harmonogram zadań.
Jeśli ustawienie zostanie zmienione, pojawi się komunikat. Kliknąć przycisk **OK**, jeśli typ harmonogramu ma zostać zmieniony.

Standardowy harmonogram zadań jest wyświetlany jako , natomiast powtarzający się harmonogram zadań jako .

4. Wprowadzić odpowiednie ustawienia dla wybranego harmonogramu.

Patrz

- strona Harmonogramy zadań, Strona 278

20.3

Konfigurowanie standardowego harmonogramu zadań

Okno główne > **Harmonogramy**

Każdy standardowy Harmonogram zadań ma własne wzory dni roboczych.

Aby skonfigurować standardowy harmonogram zadań:

1. W drzewie **Harmonogramy zadań** zaznacz standardowy Harmonogram zadań.
2. Kliknij kartę **Dni tygodnia**.
3. W polu **Tabela harmonogramów** przeciągnij wskaźnik, aby zaznaczyć przedziały czasowe dla wybranego harmonogramu.

Patrz

- strona Harmonogramy zadań, Strona 278

20.4

Konfigurowanie powtarzającego się harmonogramu zadań

Okno główne > **Harmonogramy**

Każdy powtarzający się Harmonogram zadań posiada swój własny wzór dzienny.

Aby skonfigurować powtarzający się harmonogram zadań, należy:

1. Na drzewie **Harmonogramy zadań** zaznaczyć powtarzający się Harmonogram zadań .

2. W polu **Wzór powtarzający się** kliknąć częstotliwość, z jaką ma powtarzać się harmonogram zadań (**Codziennie, Co tydzień, Co miesiąc,)Raz w roku**, a następnie wprowadzić odpowiednie ustawienia.
3. Na liście **Data rozpoczęcia**: zaznaczyć właściwą datę rozpoczęcia.
4. W polu **Wzór dzienny** przeciągnąć wskaźnik myszy, aby zaznaczyć odpowiedni przedział czasowy.

Patrz

– strona Harmonogramy zadań, Strona 278

20.5

Usuwanie harmonogramu zadań

Okno główne > > zaznaczyć żądany element drzewa **Harmonogramy zadań**

Aby usunąć harmonogram zadań, należy:

1. Na drzewie **Harmonogramy zadań** zaznaczyć żądany element.
2. Kliknąć przycisk **Usuń**.

Harmonogram zadań zostanie usunięty. Wszystkie elementy, które są przypisane do tego harmonogramu, nie są zaplanowane.

Patrz

– strona Harmonogramy zadań, Strona 278

20.6

Dodawanie świąt i dni wolnych od pracy

Okno główne > **Harmonogramy**

Uwaga!

Można skonfigurować puste dni wolne od pracy oraz święta. Dni wolne od pracy i święta zastępują harmonogram odpowiedniego dnia tygodnia.

Przykład:

Wcześniejsza konfiguracja:

Harmonogram dnia tygodnia jest skonfigurowany tak, aby był aktywny w godzinach od 9:00 do 10:00.

Harmonogram dni wolnych od pracy jest skonfigurowany tak, aby był aktywny w godzinach od 10:00 do 11:00.

Rezultat: aktywność w godzinach od 10:00 do 11:00.

Takie samo działanie obowiązuje dla świąt.



Do Harmonogramu zapisu lub Harmonogramu zadań można dodać święta oraz dni wolne od pracy.

Harmonogramy zapisu wykorzystują te same święta i dni wolne od pracy.

Każdy standardowy Harmonogram zadań posiada swoje własne wzory dni świątecznych i wolnych od pracy.

Aby dodać święta oraz dni wolne od pracy do harmonogramu, należy:

1. W drzewie **Harmonogramy zapisu** lub **Harmonogramy zadań** wybrać harmonogram.
2. Kliknąć kartę **Święta**.
3. Kliknąć **Dodaj**.
Zostanie wyświetlone okno dialogowe **Dodaj święta**.
4. Wybrać jeden lub więcej dni świątecznych i kliknąć przycisk **OK**.
Wybrane dni świąteczne zostaną dodane do Tabeli harmonogramu.
5. Przeciągnąć wskaźnik myszy, aby zaznaczyć odpowiedni przedział czasowy (nie jest to możliwe w przypadku Harmonogramów zapisu).
Zaznaczone komórki są resetowane i na odwrót.

6. Kliknąć kartę **Dni wolne od pracy**.
7. Kliknąć **Dodaj**.
Zostanie wyświetlone okno dialogowe **Dodaj dni wolne od pracy**.
8. Wybrać jeden lub więcej dni specjalnych i kliknąć przycisk **OK**.
Wybrane dni specjalne zostaną dodane do Tabeli harmonogramu.
9. Przeciągnąć wskaźnik myszy, aby zaznaczyć odpowiedni przedział czasowy (nie jest to możliwe w przypadku Harmonogramów zapisu).
Zaznaczone komórki są resetowane i na odwrót.
Dodane święta i dni wolne od pracy są uporządkowane w kolejności chronologicznej.

Uwagi:

- Można zaznaczyć przedział czasowy w czasie święta lub dnia wolnego od pracy Harmonogramu zapisu używając koloru innego Harmonogramu zapisu.

Patrz

- strona Harmonogramy zapisu, Strona 278
- strona Harmonogramy zadań, Strona 278

20.7

Usuwanie świąt i dni wolnych od pracy

Okno główne > **Harmonogramy**

Święta oraz dni wolne od pracy można usunąć z Harmonogramu zapisu lub Harmonogramu zadań.

Aby usunąć święta oraz dni wolne od pracy z harmonogramu, należy:

1. W drzewie **Harmonogramy zapisu** lub **Harmonogramy zadań** wybrać harmonogram.
2. Kliknąć kartę **Święta**.
3. Kliknąć **Usuń**.
Zostanie wyświetlone okno dialogowe **Zaznacz święta do usunięcia**.
4. Wybrać jeden lub więcej dni świątecznych i kliknąć przycisk **OK**.
Wybrane dni świąteczne zostaną usunięte z Tabeli harmonogramu.
5. Kliknąć kartę **Dni wolne od pracy**.
6. Kliknąć **Usuń**.
Zostanie wyświetlone okno dialogowe **Zaznacz dni wolne od pracy, które mają być usunięte..**
7. Wybrać jeden lub więcej dni wolnych od pracy i kliknąć przycisk **OK**.
Wybrane dni wolne od pracy zostaną usunięte z Tabeli harmonogramu.

Patrz

- strona Harmonogramy zapisu, Strona 278
- strona Harmonogramy zadań, Strona 278

20.8

Zmiana nazwy harmonogramu

Okno główne >

Aby zmienić nazwę harmonogramu, należy:

1. Na drzewie **Harmonogramy zapisu** lub **Harmonogramy zadań** wybrać żądany element.
2. Kliknąć przycisk  .
3. Wprowadzić nową nazwę i nacisnąć klawisz ENTER. Nazwa zostanie zmieniona.

Patrz

- strona Harmonogramy zapisu, Strona 278
- strona Harmonogramy zadań, Strona 278

21 strona Kamery i zapis



Uwaga!

Program BVMS Viewer zapewnia tylko podstawowe funkcje. Funkcje zaawansowane udostępnia program BVMS Professional. Aby uzyskać szczegółowe informacje na temat różnych wersji systemu BVMS, należy odwiedzić witrynę www.boschsecurity.com i zobaczyć skrócony poradnik wyboru systemu BVMS: [Skrócony poradnik wyboru systemu BVMS](#).

Okno główne > **Kamery i zapis**

Wyświetla stronę Tabela kamery lub Tabela zapisu.

Umożliwia skonfigurowanie właściwości kamery oraz ustawień zapisu.

Pozwala także użyć opcji filtrowania wyświetlanych kamer według ich typu.

Icons (Ikony)

	Kliknąć, aby skopiować ustawienia zapisu z jednego harmonogramu zapisu do innego.
	Kliknij, aby wyświetlić okno dialogowe Ustawienia jakości strumienia .
	Kliknij, aby wyświetlić okno dialogowe Ustawienia zaplanowanego zapisu .
	Kliknąć, aby wyświetlić okno dialogowe służące do konfiguracji ustawień wybranej kamery PTZ.
	Wyświetla wszystkie dostępne kamery, niezależnie od tego, z jakim urządzeniem pamięci masowej współpracują.
	Kliknij, aby zmienić tabelę kamery odpowiednio do wybranego urządzenia pamięci masowej.
	Wyświetla odpowiednią stronę Tabela kamery. Ustawienia zapisu nie są dostępne, ponieważ sygnał z tych kamer nie jest zapisywany w systemie BVMS.
	Kliknąć i zaznaczyć kolumny, które powinny być widoczne w tabeli Kamery .

Aby wyszukać elementy:

- W polu wyszukiwania wpisz ciąg znaków i naciśnij przycisk ENTER aby przefiltrować wyświetlone elementy.
Pojawią się tylko elementy zawierające łańcuch i odpowiadające im elementy nadrzędne (tylko w drzewach). Zostanie podana liczba odfiltrowanych elementów oraz całkowita liczba elementów.

Uwaga: ciąg znaków należy otoczyć cudzysłowem, aby znaleźć go precyzyjnie. Na przykład wpisanie "Camera 1" odfiltruje kamery o tej nazwie, a nie camera 201.

21.1

strona Kamery

Okno główne > **Kamery i zapis** > kliknij ikonę, aby zmienić stronę kamer odpowiednio do żadanego

urządzenia pamięci masowej, na przykład 

Wyświetla różnego rodzaju informacje o kamerach dostępnych w systemie BVMS.

Umożliwia zmianę następujących właściwości kamery:

- Nazwa kamery
- Przypisane źródło sygnału fonicznego
- Numer logiczny
- Sterowanie PTZ, jeśli jest dostępne
- Jakość podglądu bieżącego (dotyczy konfiguracji VRM i podgląd bieżący / lokalna pamięć masowa)
- Profil ustawień zapisu
- Minimalny i maksymalny czas przechowywania
- Obszar zainteresowania (ROI)
- Automated Network Replenishment
- Podwójny zapis

Aby dostosować tabelę Kamery, należy:

1. Kliknąć opcję  i zaznaczyć kolumny, które powinny być widoczne w tabeli **Kamery**.
2. Kliknąć nazwę kolumny, aby posortować tabelę według tej kolumny.

Kamera – Nadajnik

Wyświetla typ urządzenia.

Kamera – Kamera

Wyświetla nazwę kamery.

Kamera – Adres sieciowy

Wyświetla adres IP kamery.

Kamera - Lokalizacja

Umożliwia wyświetlanie lokalizacji kamery. Jeśli kamera nie jest jeszcze przypisana do drzewa logicznego, pojawia się okno **Nieprzypisana lokalizacja**.

Kamera – Seria urządzeń

Wyświetla nazwę serii urządzeń, do której należy wybrana kamera.

Kamera – Numer

Kliknij komórkę, aby edytować numer logiczny otrzymany automatycznie przez kamerę w momencie jej wykrycia. Jeśli zostanie wprowadzony już używany numer, pojawi się komunikat o błędzie.

Numer logiczny staje się dostępny po usunięciu kamery.

Dźwięk

Kliknij komórkę, aby przypisać źródło sygnału dźwiękowego do kamery.

Jeśli wystąpi alarm o niskim priorytecie dla kamery ze skonfigurowanym dźwiękiem, sygnał foniczny jest odtwarzany nawet wtedy, gdy aktualnie wyświetlany jest alarm o wyższym priorytecie. Reguła ta obowiązuje tylko wtedy, gdy alarm o wysokim priorytecie nie ma skonfigurowanego dźwięku.

Łączenie dźwięku między kamerami

Łączenie Audio podczas konfiguracji pozwala przypisać do każdej kamery wejścia i wyjścia audio innej kamery.

Ta funkcja jest korzystna w scenariuszach, takich jak przypisywanie wejścia/wyjścia audio innej kamery do kamery, która nie ma mikrofonu ani głośnika. Operator może wówczas komunikować się z kamerami w pobliżu, oglądając transmisję na żywo z dowolnej kamery.

Opcje łączenia dźwięku między urządzeniami są wyświetlane w następującej kolejności:

1. <Brak dźwięku>
2. Dźwięk z wybranego urządzenia
3. Dźwięk z urządzeń w tej samej lokalizacji na drzewie urządzeń
4. Dźwięk ze wszystkich innych dostępnych urządzeń

Strumienie / Limity strumieni

Ta kolumna jest tylko do odczytu i wskazuje limity strumieni z danej kamery.

Uwaga: Ograniczenia strumieni są wyświetlane tylko dla kamer CPP13, CPP14 i CPP16.



Uwaga!

Limitów strumieni nie można edytować w programie BVMS. Jest to możliwe w witrynie internetowej nadajnika oraz w programie Configuration Manager. Po zmodyfikowaniu ograniczeń strumieni w witrynie internetowej lub programie Configuration Manager należy zaktualizować funkcje urządzenia w programie BVMS. Jeśli nie zaktualizujesz funkcji, program BVMS zastąpi zaktualizowane ograniczenia strumieni starymi ustawieniami widocznymi przy ostatniej aktualizacji funkcji urządzenia.

Ustawienia Strumień 1 / Strumień 2 / Strumień 3



Uwaga!

Trzeci strumień obsługują tylko kamery CPP13, CPP14 i CPP16.



Uwaga!

Strumienia 3 można używać tylko do wyświetlania obrazu na żywo. Zapis nie jest możliwy.

Strumień 1 - Kodek / Strumień 2 - Kodek / Strumień 3 - Kodek (dostępne tylko w VRM, podglądzie na żywo i kamerach z zapisem na lokalnej pamięci masowej)

Kliknij komórkę, aby wybrać żądaną rozdzielczość obrazu.

Wartości rozdzielczości obrazu zostaną wczytane z nadajnika. Ich wyświetlenie może nieco potrwać.

Uwaga: Ta kolumna jest wyświetlana tylko wtedy, gdy skonfigurowano co najmniej jedną kamerę obsługującą trzeci strumień.

Strumień 1 - Jakość / Strumień 2 - Jakość / Strumień 3 - Jakość (dostępne tylko w VRM, podglądzie na żywo i kamerach z zapisem na lokalnej pamięci masowej)

Wybierz żądaną jakość strumienia dla transmisji na żywo lub zapisu. Do ustawiania jakości służy okno dialogowe **Ustawienia jakości strumienia**.

Uwaga: Ta kolumna jest wyświetlana tylko wtedy, gdy skonfigurowano co najmniej jedną kamerę obsługującą trzeci strumień.

Strumień 1 - Aktywna platforma / Strumień 2 - Aktywna platforma / Strumień 3 - Aktywna platforma (dostępne tylko w VRM, podglądzie na żywo i kamerach z zapisem na lokalnej pamięci masowej)

Wyświetla nazwę ustawień platformy w oknie dialogowym **Ustawienia jakości strumienia**. Ta kolumna jest tylko do odczytu i wskazuje, które ustawienia profilu zostaną zapisane w nadajniku.

Uwaga: Ta kolumna jest wyświetlana tylko wtedy, gdy skonfigurowano co najmniej jedną kamerę obsługującą trzeci strumień.

Strumień 1/Profil, Strumień 2/Profil (dostępne tylko w kamerach ONVIF)

Kliknij komórkę, aby przeglądać dostępne tokeny profili podglądu tej kamery ONVIF.

Jeśli zostanie wybrana pozycja **<Automatycznie>**, zostanie automatycznie użyty strumień o najwyższej jakości.

Uwaga: Jeśli masz zainstalowaną starszą wersję VSG, która nie obsługuje dwóch strumieni, opcja **<Użyj strumienia 1>** zostanie automatycznie ustawiona na **Strumień 2/Profil**.

Należy zainstalować najnowszą wersję VSG.

Strumień 1/Rozdzielczość obrazu, Strumień 2/Rozdzielczość obrazu (dostępne tylko w kamerach ONVIF)

Ta kolumna jest tylko do odczytu i wskazuje rozdzielczość obrazu wybranego profilu strumienia.

Obraz bieżący - Strumień (dostępne tylko w VRM, podglądzie na żywo i kamerach z zapisem na lokalnej pamięci masowej)

Kliknij odpowiednią komórkę, aby wybrać strumień przypisany do modułu VRM lub nadajnika z obsługą lokalnego urządzenia pamięci masowej / udostępniającego tylko podgląd bieżący.

Obraz bieżący - ROI (dostępne tylko w VRM, podglądzie na żywo i kamerach z zapisem na lokalnej pamięci masowej)

Kliknij, aby włączyć Region of Interest (ROI). Jest to możliwe tylko wtedy, gdy w kolumnie **Jakość** została wybrana opcja H.264 MP SD ROI lub H.265 MP SD ROI dla strumienia 2 i strumień 2 jest przypisany do bieżącego obrazu.

Uwaga: Jeśli strumień 1 jest używany do podglądu na żywo na jakiejś stacji roboczej, program Operator Client nie może włączyć funkcji ROI dla tej kamery.



jest automatycznie włączony w tabeli

Obraz bieżący - Strumień bieżący (dostępne tylko dla kamer podłączonych przez VSG)

Kliknij komórkę w celu wybrania żądanego strumienia na żywo dla danej kamery.

W przypadku kamer ONVIF dostępne są następujące opcje:

- **Bezpośrednio (z kamery)**
- **Strumień 1 (przez VSG)**
- **Strumień 2 (przez VSG)**

W przypadku kamer Bosch dostępne są następujące opcje:

- **Strumień 1**
- **Strumień 2**

Uwaga: Jeśli wybierzesz urządzenie Video Streaming Gateway do pobierania obrazu na żywo w stacji roboczej, obraz na żywo zostanie pobrany tylko po wybraniu opcji **Bezpośrednio (z kamery)** dla strumienia na żywo.

Obraz bieżący - Profil (dostępne tylko w przypadku kamer ONVIF podłączonych przez VSG)

Kliknij komórkę, aby wyszukać dostępne tokeny profilu na żywo tej kamery ONVIF.

Uwaga: Profil obrazu na żywo można wybrać tylko po wybraniu opcji **Bezpośrednio (z kamery)** w odniesieniu do transmisji strumieniowej na żywo. Jeśli wybierzesz **Strumień 1 (przez VSG)** lub **Strumień 2 (przez VSG)** dla strumienia na żywo, profil obrazu na żywo zostanie automatycznie ustawiony na **<Automatycznie>**.

Zapis – Ustawienie

Kliknij komórkę w celu wybrania żądanego ustawienia zapisu. W oknie dialogowym **Ustawienia zaplanowanego zapisu** można skonfigurować dostępne ustawienia zapisu.

Zapis – ANR

Zaznacz pole wyboru, aby włączyć funkcję ANR. Funkcję tę można włączyć tylko wtedy, gdy nadajnik jest odpowiedniego typu i ma odpowiednie oprogramowanie układowe.

Zapis – Maks. czas trwania (przed wystąpieniem alarmu)

Wyświetla obliczony maksymalny czas przed wystąpieniem alarmu dla tej kamery. Ta wartość jest pomocna przy obliczaniu wymaganej wielkości pamięci dla lokalnego nośnika danych.

**Uwaga!**

Jeśli nadmiarowy VRM jest już skonfigurowany dla jakiegoś nadajnika, w kolumnie **Zapis pomocniczy** nie można zmienić ustawień tego nadajnika.

Zapis pomocniczy - Ustawienie (dostępne tylko wówczas, gdy jest skonfigurowany pomocniczy VRM)

Kliknij, aby przypisać ustawienia zaplanowanego zapisu do podwójnego zapisu dla tego nadajnika. W zależności od konfiguracji może się zdarzyć, że skonfigurowana jakość strumienia dla dodatkowego zapisu jest nieodpowiednia. Wówczas zostanie użyta jakość strumienia skonfigurowana dla podstawowego zapisu.

Zapis pomocniczy – Profil (dostępne tylko w kamerach ONVIF)

Kliknij komórkę, aby przeglądać dostępne tokeny profili zapisywania tej kamery ONVIF.



(widoczne tylko po kliknięciu opcji  **Wszystko**)

Zaznacz pole wyboru, aby włączyć sterowanie PTZ.

Uwaga:

Ustawienia portu opisano w punkcie Port COM1.

Port (widoczne tylko po kliknięciu opcji **Wszystko**)

Kliknij komórkę, aby określić, który port szeregowy nadajnika jest używany do sterowania PTZ. W przypadku podłączenia kamery PTZ do systemu Bosch Allegiant można wybrać opcję **Krosownica Allegiant**. W przypadku takiej kamery nie trzeba używać linii wizyjnej.

Protokół (widoczne tylko po kliknięciu opcji **Wszystko**)

Kliknij komórkę, aby wybrać odpowiedni protokół na potrzeby sterowania PTZ.

Adres PTZ (widoczne tylko po kliknięciu opcji **Wszystko**)

Wprowadź numer adresu na potrzeby sterowania PTZ.

Śledzenie obiektów (widoczne tylko po kliknięciu i włączeniu funkcji **Wizualizacja obiektów na mapie** [menu **Ustawienia > Opcje Przetwarzanie metadanych**])

Umożliwia włączanie/wyłączanie funkcji śledzenia obiektów dla wybranych kamer.

**Uwaga!**

Funkcja śledzenia obiektów jest dostępna wyłącznie dla kamer z platformą CPP6 lub nowszą, dodanych do drzewa logicznego oraz do mapy globalnej.

Zapis – Min. czas przechowywania [w dniach]**Zapis pomocniczy – Min. czas przechowywania [w dniach] (tylko VRM i lokalna pamięć masowa)**

Kliknij komórkę, aby edytować minimalną liczbę dni przechowywania danych wizyjnych z tej kamery. Nagrania młodsze niż podana liczba dni nie są kasowane automatycznie.

Zapis – Maks. czas przechowywania [w dniach]**Zapis pomocniczy – Maks. czas przechowywania [w dniach] (tylko VRM i lokalna pamięć masowa)**

Kliknij komórkę, aby edytować maksymalną liczbę dni przechowywania danych wizyjnych z tej kamery. Automatycznie kasowane są wyłącznie nagrania starsze niż podana liczba dni. 0 = nieograniczone.

Patrz

- Konfigurowanie podwójnego zapisu w tabeli kamery, Strona 303
- Konfigurowanie predefiniowanych położeń i funkcji dodatkowych, Strona 300
- Konfiguracja ustawień portu PTZ, Strona 300
- Konfigurowanie ustawień jakości strumienia, Strona 292
- Kopiowanie i wklejanie w tabelach, Strona 291
- Konfigurowanie funkcji ANR, Strona 302
- Eksportowanie tabeli kamery, Strona 292
- Przypisywanie profilu ONVIF, Strona 303
- Konfigurowanie funkcji ROI, Strona 302

21.2

Strony ustawień zapisu



Okno główne > **Kamery i zapis** >  > kliknąć kartę Harmonogram zapisu (np. **Dzień**)

Umożliwia skonfigurowanie ustawień zapisu.

Wyświetlone Harmonogramy zapisu są konfigurowane na stronie **Harmonogramy**.

Opisano tylko kolumny nie będące częścią tabeli kamery.

- ▶ Kliknąć nazwę kolumny, aby posortować tabelę według tej kolumny.

Zapis ciągły

W kolumnie **Jakość** kliknąć komórkę, aby wyłączyć zapis lub wybrać jakość strumienia 1.

W kolumnie  zaznaczyć pole wyboru, aby włączyć dźwięk.

Zapis obrazu bieżącego / przed zdarzeniem

W kolumnie **Jakość** kliknąć odpowiednią komórkę, aby wybrać jakość strumienia widoku na żywo (wymagane do odtwarzania natychmiastowego) oraz trybu zapisu przed zdarzeniem (wymagane do zapisu ruchu i alarmu) przypisanych do strumienia 2. Jeśli na danym nadajniku aktywna jest funkcja podwójnego strumieniowania, można wybrać strumień 1 do zapisu na żywo lub przed zdarzeniem.

W kolumnie  zaznaczyć pole wyboru, aby włączyć dźwięk.

Zapis ruchu

W kolumnie **Jakość** kliknąć komórkę, aby wyłączyć zapis lub wybrać jakość strumienia 1.

W kolumnie  kliknąć odpowiednią komórkę, aby włączyć dźwięk.

W kolumnie **Przed zdarzeniem [s]** kliknąć odpowiednią komórkę, aby określić żądany czas zapisu (w sekundach) przed wystąpieniem zdarzenia ruchu.

W kolumnie **Po zdarzeniu [s]** kliknąć odpowiednią komórkę, aby określić żądany czas zapisu (w sekundach) po wystąpieniu zdarzenia ruchu.

Zapis alarmowy

W kolumnie **Jakość** kliknąć komórkę i wybrać jakość strumienia 1.

Aby włączyć zapis alarmowy, należy skonfigurować odpowiedni alarm.

W kolumnie  zaznaczyć pole wyboru, aby włączyć dźwięk.

W kolumnie **Przed zdarzeniem [s]** kliknąć odpowiednią komórkę, aby określić długość trwania okresu (w sekundach) przed wystąpieniem alarmu.

W kolumnie **Po zdarzeniu [s]** kliknąć odpowiednią komórkę, aby określić długość trwania okresu (w sekundach) po wystąpieniu alarmu.

Patrz

- Kopiowanie i wklejanie w tabelach, Strona 291

22

Konfiguracja kamer i ustawień zapisu



Uwaga!

W niniejszym dokumencie opisano niektóre funkcje, które nie są dostępne w programie BVMS Viewer.

Szczegółowe informacje na temat poszczególnych wersji systemu BVMS znajdują się na stronie www.boschsecurity.com oraz w Skróconym poradniku wyboru systemu BVMS: [Skrócony poradnik wyboru systemu BVMS](#).

Okno główne > Kamery i zapis

Niniejszy rozdział zawiera informacje o sposobie konfigurowania kamer w systemie BVMS.

Użytkownik konfiguruje różne właściwości kamer oraz ustawienia zapisu.

- Kliknij , aby zapisać ustawienia.
- Kliknij , aby cofnąć ostatnią zmianę.
- Kliknij , aby uaktywnić konfigurację.

Patrz

- strona Kamery, Strona 285
- Okno Ustawienia zaplanowanego zapisu (tylko VRM i lokalna pamięć masowa), Strona 297
- Okno dialogowe Ustawienia jakości strumienia, Strona 293
- Okno dialogowe predefiniowanych położeń i poleceń pomocniczych, Strona 301

22.1

Kopiowanie i wklejanie w tabelach

Użytkownik może skonfigurować jednocześnie wiele obiektów w Tabeli kamer, Tabeli konfiguracji zdarzenia lub Tabeli konfiguracji alarmu.

Istnieje możliwość kopiowania konfigurowalnych wartości w wierszu tabeli do innych wierszy:

- Kopiowanie wszystkich wartości z wiersza do innych wierszy
- Kopiowanie tylko jednej wartości z wiersza do innego wiersza
- Kopiowanie wartości z jednej komórki do całej kolumny

Wartości można kopiować na dwa różne sposoby:

- Kopiowanie do schowka, a następnie wklejenie
- Bezpośrednie kopiowanie i wklejenie

Można określić, do których wierszy mają być kopiowane wartości:

- Kopiowanie we wszystkich wierszach
- Kopiowanie w wybranych wierszach

Aby skopiować i wkleić wszystkie konfigurowalne wartości, należy:

1. Kliknąć prawym przyciskiem myszy wiersz z wymaganymi wartościami i kliknąć **Kopiuj wiersz**.
2. Kliknąć nagłówek wiersza, który ma być zmodyfikowany.
Aby zaznaczyć więcej niż jeden wiersz, nacisnąć klawisz CTRL i kliknąć nagłówki innych wierszy.
3. Kliknąć prawym przyciskiem myszy tabelę i kliknąć **Wklej**.
Wartości zostaną skopiowane.

Aby skopiować i wkleić jedną wartość w wierszu do innego wiersza, należy:

1. Kliknąć prawym przyciskiem myszy wiersz z wymaganymi wartościami i kliknąć **Kopiuj wiersz**.
2. Kliknąć prawym przyciskiem myszy komórkę, która ma być zmodyfikowana i wybrać **Wklej komórkę do**, a następnie kliknąć **Bieżąca komórka**.
Wartość zostanie skopiowana.

Aby bezpośrednio skopiować wszystkie konfigurowalne wartości, należy:

1. Kliknąć nagłówek wiersza, który ma być zmodyfikowany.
Aby zaznaczyć więcej niż jeden wiersz, nacisnąć klawisz CTRL i kliknąć nagłówki innych wierszy.
2. Kliknąć prawym przyciskiem myszy wiersz z wymaganymi wartościami i wybrać **Kopiuj wiersz do**, a następnie kliknąć **Zaznaczone wiersze**.
Wartości zostaną skopiowane.

Aby bezpośrednio skopiować jedną wartość, należy:

1. Kliknąć nagłówek wiersza, który ma być zmodyfikowany.
Aby zaznaczyć więcej niż jeden wiersz, nacisnąć klawisz CTRL i kliknąć nagłówki innych wierszy.
2. Kliknąć prawym przyciskiem myszy komórkę z wymaganą wartością i wybrać **Kopiuj komórkę do**, a następnie kliknąć **Zaznaczenie w kolumnie**.
Wartość zostanie skopiowana.

Aby skopiować wartość z komórki do pozostałych komórek w tej kolumnie, należy:

- ▶ Kliknąć prawym przyciskiem myszy komórkę z wymaganą wartością i wybrać **Kopiuj komórkę do**, a następnie kliknąć **Uzupełnij kolumnę**.
Wartość zostanie skopiowana.

Aby skopiować wiersz, należy:

- ▶ Kliknąć prawym przyciskiem myszy wiersz i kliknąć **Dodaj wstawiony wiersz**.
Wiersz o nowej nazwie zostanie dodany poniżej.

Patrz

- strona Kamery, Strona 285
- Okno Ustawienia zaplanowanego zapisu (tylko VRM i lokalna pamięć masowa), Strona 297
- strona Zdarzenia, Strona 305
- strona Alarmy, Strona 310

22.2

Eksportowanie tabeli kamery

Okno główne > **Kamery i zapis**

LUB

Okno główne > **Kamery i zapis** > Kliknij ikonę, aby zmienić stronę kamer odpowiednio dożądanego



urządzenia pamięci masowej, na przykład

Wyświetla różnego rodzaju informacje o kamerach dostępnych w systemie BVMS.

Tabelę kamery można wyeksportować do pliku CSV.

Aby wyeksportować dane:

1. Kliknij prawym przyciskiem myszy w dowolnym miejscu tabeli, a następnie kliknij **Eksportuj tabelę...**
2. W oknie dialogowym wpisz odpowiednią nazwę pliku.
3. Kliknij przycisk **Zapisz**.
Wybrana tabela kamery zostanie wyeksportowana do pliku csv.

22.3

Konfigurowanie ustawień jakości strumienia

Aby dodać pozycję do ustawień jakości strumienia:

1. Kliknij przycisk , aby dodać nową pozycję do listy.
2. Wprowadź nazwę.

Aby usunąć pozycję ustawień jakości strumienia:

- ▶ Zaznacz wpis na liście i kliknij przycisk , aby usunąć wpis.
Domyślnych pozycji nie można usuwać.

Aby zmienić nazwę pozycji ustawień jakości strumienia:

1. Wybierz z listy określoną pozycję.
2. Wprowadź nową nazwę w polu **Nazwa**.
Nazw domyślnych pozycji nie można zmieniać.
3. Kliknąć **OK**.

Aby skonfigurować ustawienia jakości strumienia:

1. Wybierz z listy określoną pozycję.
2. Wprowadź odpowiednie ustawienia.

22.3.1**Okno dialogowe Ustawienia jakości strumienia**

Okno główne > **Kamery i zapis** > 

Umożliwia konfigurowanie profili jakości strumienia, które można później przypisywać na stronie **Kamery i zapis** do kamer lub w oknie dialogowym **Ustawienia zaplanowanego zapisu**.

Na jakość strumienia składa się rozdzielczość obrazu, częstotliwość odświeżania, maks. szerokość pasma oraz kompresja sygnału wizyjnego.

Jakość strumienia

 Wybierz wstępnie zdefiniowaną jakość strumienia i kliknij ikonę , aby dodać nową jakość strumienia określoną na bazie wstępnie zdefiniowanej jakości. Po wybraniu strumienia i kliknięciu

ikony  ustawienie jakości tego strumienia zostanie skopiowane do węzła najwyższego poziomu bez elementów podrzędnych.



Kliknij, aby usunąć wybraną jakość strumienia. Nie można usuwać ustawień jakości strumienia.

Lista przedstawia wszystkie wstępnie zdefiniowane ustawienia jakości strumienia. Zalecane jest przypisanie do jakości strumienia tej samej nazwy co dla platformy kamery.

Dostępne są następujące profile jakości strumienia:

Image optimized: ustawienia są zoptymalizowane pod kątem jakości obrazu. Taki profil może obciążać sieć.

Bit rate optimized: ustawienia są zoptymalizowane pod kątem małej szerokości pasma. To może zmniejszać jakość obrazu.

Balanced: te ustawienia są kompromisem między optymalną jakością obrazu a optymalną szerokością pasma.

Wymienione poniżej profile jakości strumienia są dostępne począwszy od wersji 9.0 systemu BVMS, aby umożliwić obsługę funkcji Intelligent Streaming kamer Bosch:

Cloud optimized 1/8 FR: ustawienia są zoptymalizowane pod kątem małej szerokości pasma i takie same dla wszystkich typów kamer.

PTZ optimized: ustawienia są zoptymalizowane pod kątem kamer PTZ.

Image optimized quiet / standard / busy

Bit rate optimized quiet / standard / busy

Balanced quiet / standard / busy

Kategorie typów scen:

quiet: ustawienia są zoptymalizowane pod kątem obrazów o niskiej aktywności. 89% sceny statycznej, 10% sceny normalnej, 1% sceny zajętej.

standard: ustawienia są zoptymalizowane pod kątem obrazów o średniej aktywności. 54% sceny statycznej, 35% sceny normalnej, 11% sceny zajętej.

busy: ustawienia są zoptymalizowane pod kątem obrazów o wysokiej aktywności. 30% sceny statycznej, 55% sceny zajętej, 15% sceny zatłoczonej.

Wartości procentowe są powiązane z rozkładem w ciągu dnia.

Domyślnie przypisany jest profil Balanced standard.



Uwaga!

Dla każdej kombinacji platformy kamer (CPP3-CPP7.3) i dla każdej dostępnej rozdzielczości istnieje określone ustawienie, które pozwala ustawić prawidłowe prędkości transmisji dla kamer. Profil należy wybrać ręcznie, z zastosowaniem odpowiedniego typu sceny dla każdej kamery.



Uwaga!

W przypadku instalowania aktualizacji nowe profile należy wybrać ręcznie, aby zostały aktywowane. Stare profile pozostają.

Nazwa

Wyświetla nazwę profilu jakości strumienia. Po dodaniu nowej jakości strumienia można zmienić nazwę.

Rozdzielczość obrazu SD

To ustawienie ma zastosowanie, tylko gdy kodek strumienia ma ustawioną rozdzielczość SD.

Wybierz wymaganą rozdzielczość obrazu. W przypadku jakości HD skonfiguruj jakość SD strumienia 2.

Uwaga: nie ma żadnego wpływu na rozdzielczość, jeśli kodek ma ustawioną rozdzielczość HD lub UHD (dowolną powyżej SD). Za pomocą tego parametru nie można ograniczyć rozdzielczości np. kamery HD do poziomu SD.

Interwał kodowania obrazu

Przesuń suwak lub wprowadź wymaganą wartość.

System pomaga przy obliczaniu odpowiedniej wartości IPS.

Opcja **Interwał kodowania obrazu** pozwala skonfigurować przedział czasowy, po którym obrazy będą kodowane i wysyłane. Jeśli ustawiona jest wartość 1, wszystkie obrazy będą kodowane. Wprowadzenie wartości 4 oznacza, że tylko co czwarty obraz jest kodowany, a kolejne trzy są pomijane. Jest to szczególnie przydatne w sieciach małej szerokości pasma. Im niższa szerokość pasma, tym większa powinna być ta wartość, aby uzyskać jak najlepszą jakość obrazu.

Silnik kodujący otrzymuje na przykład jako dane wejściowe 30 klatek z czujnika. Wymagane wyjście dla widoku na żywo lub zapisu to 15 klatek.

Aby to uzyskać:

- ▶ Ustaw parametr **Interwał kodowania obrazu** na wartość 2.
Nadajnik będzie pomijał co drugą klatkę z czujnika i prześle strumień zakodowany w standardzie H.264 zawierający tylko 15 klatek.

Interwał kodowania obrazu:

- 1 = pełna częstotliwość odświeżania podana w ustawieniach kodeka
- 2 = 50% liczby kl./s podanej w ustawieniach kodeka

Szybkie obliczanie częstotliwości odświeżania umożliwia następujący wzór: $IPS = \text{tryb pracy czujnika} / \text{interwał kodowania obrazu}$

Struktura GOP

W tym miejscu należy wybrać wymaganą strukturę dla grupy obrazów (GOP). W zależności od tego, czy ważniejsze jest uzyskanie jak najmniejszego opóźnienia (tylko ramki IP) lub zużycie jak najmniejszych zasobów pasma, można wybrać między ustawieniami IP, IBP oraz IBBP. (Wybór GOP nie jest dostępny w przypadku niektórych kamer)

Uwaga:

B-ramki są obsługiwane tylko przez kamery o rozdzielczości do 1080p i od wersji oprogramowania układowego 6.40.

Unikaj B-ramek w widoku na żywo i w trybie PTZ — powodują one opóźnienie obrazu na żywo.

Optymalizacja prędkości transmisji

Optymalizacja szybkości transmisji określa, czy priorytet jest nadawany jakości obrazu czy szybkości transmisji.

Ustawienia **Wysoka jakość** lub **Maksymalna jakość** tylko minimalnie oszczędzają przepustowość lub nie oszczędzają jej wcale, ale jakość obrazu jest dobra lub doskonała.

Ustawienia **Niska prędkość transmisji** i **Średnia** oszczędzają przepustowość, ale obraz jest mniej wyraźny.

Jeśli optymalizacja szybkości transmisji jest wyłączona, oczekuje się uśrednionej przepływności 24 h (wyższej niż docelowa szybkość transmisji).

Docelowa prędkość transmisji [Kb/s]

Przesuń suwak lub wprowadź wymaganą wartość.

Użytkownik może ograniczyć przepływność dla encoder, aby zoptymalizować wykorzystanie szerokości pasma sieci. Docelowa przepływność powinna być ustawiona zgodnie z wymaganą jakością obrazu dla typowych scen bez nadmiernego ruchu.

W przypadku obrazów złożonych lub częstych zmian zawartości obrazu z powodu ruchu limit może być chwilowo przekroczony i osiągać wartość wprowadzoną w polu **Maksymalna prędkość transmisji [kb/s]**.

Maksymalna prędkość transmisji [kb/s]

Przesuń suwak lub wprowadź wymaganą wartość.

Maksymalna przepływność określa maksymalną prędkość transmisji, której nie można przekroczyć. Ustawienie ograniczenia przepływności umożliwia dokładne określenie odpowiedniej przestrzeni dyskowej do przechowywania obrazów.

W zależności od ustawienia jakości obrazu dla ramek typu I oraz P, może to powodować pomijanie pojedynczych obrazów.

Wartość wprowadzona w tym polu musi być co najmniej o 10% wyższa od wartości wprowadzonej w polu **Docelowa prędkość transmisji [Kb/s]**. Jeśli wprowadzona wartość będzie zbyt niska, zostanie automatycznie skorygowana.

Odległość ramki I

Pole umożliwia ustawienie odstępu czasu, w którym będą kodowane I-ramki.

Wartość 1 oznacza, że I-ramki są generowane w sposób ciągły. Wartość 10 oznacza, że tylko co dziesiąty obraz jest I-ramką, wartość 60 – że co szósty obraz itd. I-ramki pomiędzy nimi są kodowane jako P-ramki.

Uwaga: w przypadku użycia bardzo długiego GOP (do 255) w połączeniu z niską częstotliwością odświeżania (1 kl/s) odstęp czasowy między I-ramkami jest zbyt duży i nie można wyświetlić odtwarzania. Zalecamy zmniejszenie długości GOP do 30.

Poziom jakości ramki

W tym oknie można wybrać ustawienie pomiędzy wartościami 0 i 100 dla ramek I oraz ramek P. Najniższa wartość powoduje ustawienie najwyższej jakości obrazu i najniższej częstotliwości odświeżania. Najwyższa wartość powoduje ustawienie najwyższej częstotliwości odświeżania i najniższej jakości obrazu.

Im niższa jest dostępna przepustowość transmisji, tym wyżej należy ustawić poziom jakości, aby utrzymać wysoką jakość obrazu.

Uwaga:

Jeśli pomoc techniczna nie przekazała innych informacji, zalecamy wybranie pola wyboru **Auto**. Optymalny stosunek pomiędzy ruchem a definicją obrazu jest regulowany automatycznie.

Ustawienia VIP X1600 XFM4

Umożliwia skonfigurowanie następujących ustawień kodowania H.264 dla modułu nadajnika VIP X 1600 XFM4.

Filtr deblokujący H.264: wybierz, aby podnieść jakość obrazu i poprawić działanie funkcji przewidywania poprzez wygładzenie ostrych krawędzi.

CABAC: wybierz, aby włączyć kompresję o wysokiej wydajności. Zużywa znaczną część dostępnej mocy obliczeniowej.

Patrz

– Konfigurowanie ustawień jakości strumienia, Strona 292

22.4**Konfiguracja właściwości kamery**

Okno główne > **Kamery i zapis** > 

Aby zmienić właściwości kamery:

1. Kliknij komórkę w kolumnie **Kamera** i wpisz nową nazwę kamery.
Nazwa ta jest wyświetlana we wszystkich innych miejscach, gdzie wymienione są kamery.
2. Dokonaj odpowiednich ustawień w innych kolumnach.

Kliknąć poniższy odnośnik do wybranego okna programu, aby uzyskać szczegółowe informacje o różnych polach.

Patrz

– strona Kamery, Strona 285

22.5**Konfigurowanie ustawień zapisu (tylko dla VRM i lokalnych urządzeniach pamięci masowej)**

Okno główne > **Kamery i zapis** > 

Można skonfigurować ustawienia zapisu wszystkich urządzeń dodanych do pozycji Urządzenia VRM na Drzewie urządzeń.

Uwaga: W przypadku zapisu należy upewnić się, że odpowiedni rejestrator VRM lub lokalne urządzenie pamięci masowej zostały prawidłowo skonfigurowane.

VRM: **Urządzenia** > rozwinąć  > 

Lokalne urządzenie pamięci masowej: **Urządzenia** > rozwinąć  > 

Aby dodać pozycję do ustawień zapisu:

1. Kliknij przycisk , aby dodać nową pozycję do listy.
2. Wprowadź nazwę.

Aby usunąć pozycję ustawień zapisu:

- ▶ Wybrać z listy określoną pozycję i kliknąć przycisk  w celu usunięcia tej pozycji.
Pozycji domyślnych nie można usunąć.

Aby zmienić nazwę pozycji ustawień zapisu:

1. Wybierz z listy określoną pozycję.
2. Wprowadź nową nazwę w polu **Nazwa**.
Nazw domyślnych pozycji nie można zmieniać.
3. Kliknąć **OK**.

Aby skonfigurować ustawienia zapisu:

1. Wybierz z listy określoną pozycję.
2. Wykonaj żądane ustawienia i kliknij **OK**.
3. Kliknij  lub .
4. W kolumnie **Zapis** zaznacz żądane ustawienia zapisu dla każdego nadajnika.

Więcej informacji o różnych polach znajduje się w Pomocy ekranowej wybranego okna programu.

Patrz

- Okno Ustawienia zaplanowanego zapisu (tylko VRM i lokalna pamięć masowa), Strona 297

22.6

Okno Ustawienia zaplanowanego zapisu (tylko VRM i lokalna pamięć masowa)

Okno główne > **Kamery i zapis** > 

Umożliwia konfigurację ustawień zaplanowanego zapisu dla wszystkich dostępnych serii urządzeń. Seria urządzeń jest dostępna, gdy co najmniej jeden nadajnik z tej serii został dodany do Drzewa urządzeń. W tabeli **Kamery** można przypisać takie ustawienia zapisu do poszczególnych kamer. Należy użyć Harmonogramów zapisu skonfigurowanych na stronie **Harmonogramy**.

Uwaga: Włączanie lub wyłączanie normalnego zapisu jest dostępne dla wszystkich serii urządzeń.

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, VI1

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

Dostępne ustawienia zapisu

Wybierz wstępnie zdefiniowane ustawienie zapisu, aby zmienić jego właściwości. Można dodawać i usuwać ustawienia zdefiniowane przez użytkownika.

Nazwa:

Wprowadź nazwę dla nowego ustawienia zapisu.

Karta Seria urządzeń

Wybierz żadaną serię urządzeń, aby skonfigurować ustawienia zapisu dla tej serii.

Karta Harmonogram zapisu

Dla wybranej serii urządzeń wybierz harmonogram zapisu, aby skonfigurować ustawienia zapisów.

Zapis

Włącz lub wyłącz zapis normalny (zapis ciągły i przed wystąpieniem alarmu).

Zapis dźwięku

Zaznacz, jeśli chcesz nagrywać audio.

Zapis metadanych

Zaznacz, jeśli chcesz rejestrować metadane.

Tryb zapisu

Wybierz żądany tryb zapisu.

2025-07 | V01 | Configuration Client

Instrukcja konfiguracji

Bosch Security Systems B.V.

Dostępne są następujące opcje:

- **Ciągły**
- **Przed alarmem**

Strumień

Wybierz strumień używany do zapisu normalnego.

Uwaga: Dostępność strumieni zależy od serii urządzenia.

Jakość

Wybierz żadaną jakość strumienia dla zapisu normalnego. Ustawienia jakości można skonfigurować w oknie dialogowym **Ustawienia jakości strumienia**.

Czas trwania (przed alarmem)

Wprowadzić czas zapisu przed alarmem. Czas należy wprowadzić w formacie gg.mm.ss.

Uwaga: Funkcja jest włączana tylko po wybraniu opcji **Przed alarmem**.



Uwaga!

W przypadku ustawień czasu przed wystąpieniem alarmu w granicach od 1 do 10 s alarmy wstępne są automatycznie przechowywane w pamięci RAM nadajnika, o ile jest w niej wolne miejsce. W przeciwnym razie są zapisywane w pamięci masowej.

W przypadku ustawień czasu przed wystąpieniem alarmu przekraczających 10 s alarmy wstępne są przechowywane w pamięci masowej.

Przechowywanie alarmów wstępnych w pamięci RAM nadajnika jest dostępne tylko w przypadku oprogramowania układowego w wersji 5.0 lub nowszej.

Ustawienia zapisu alarmowego

Umożliwia włączanie i wyłączenie zapisu alarmowego tej kamery.

Alarm ruchu

Umożliwia włączanie i wyłączenie zapisu alarmowego wyzwalanego przez ruch.

Strumień

Wybrać strumień, który będzie używany dla zapisu alarmowego.

Uwaga: Dostępność strumieni zależy od serii urządzenia.

Jakość

Wybierz żadaną jakość strumienia dla zapisu alarmowego. Ustawienia jakości można skonfigurować w oknie dialogowym **Ustawienia jakości strumienia**.

Tylko dla urządzeń należących do serii 2 lub 3: w przypadku zaznaczenia opcji **Bez modyfikacji** zapis alarmowy będzie tej samej jakości co zapis ciągły/alarmu wstępnego. Zalecane jest użycie pozycji **Bez modyfikacji**. Wybranie jakości strumienia zapisu alarmowego powoduje zmianę jedynie wartości interwału kodowania obrazu i docelowej przepływności, które są modyfikowane zgodnie z ustawieniami dla wybranej jakości strumienia. Pozostałe stosowane ustawienia jakości są konfigurowane w sekcji ustawień przypisanych do zapisu ciągłego/alarmu wstępnego.

Czas trwania (po alarmie)

Wprowadzić żądany czas zapisu alarmowego. Czas należy wprowadzić w formacie gg.mm.ss.

Patrz

- *Kopiowanie i wklejanie w tabelach, Strona 291*
- *Konfigurowanie ustawień zapisu (tylko dla VRM i lokalnych urządzeniach pamięci masowej), Strona 296*

22.7 Konfiguracja ustawień portu PTZ

Okno główne > **Urządzenia** > rozwinąć  > rozwinąć  > karta **Interfejsy** > karta **Urządzenie peryferyjne**

Okno główne > **Urządzenia** >  >  > karta **Interfejsy** > karta **Urządzenie peryferyjne**
Ustawienia portu można skonfigurować tylko dla nadajnika, w którym sterowanie kamerą jest możliwe oraz włączone.

Przy zastąpieniu nadajnika lub kamery PTZ ustawienia portu nie zostaną zachowane. Należy skonfigurować je ponownie.

Po aktualizacji oprogramowania układowego sprawdzić ustawienia portu.

Aby skonfigurować ustawienia portu nadajnika, należy:

- ▶ Wprowadzić odpowiednie ustawienia.

Ustawienia te obowiązują natychmiast po zapisie. Konfiguracja nie wymaga aktywacji.

Więcej informacji o różnych polach znajduje się w Pomocy ekranowej wybranego okna programu.

22.8 Konfigurowanie predefiniowanych położeń i funkcji dodatkowych

Okno główne > **Kamery i zapis** > 

Można wstępnie zdefiniować i zapisać położenie kamer odnośnie do kamer PTZ, ROI i panoramicznych. W przypadku kamer PTZ można również zdefiniować polecenia pomocnicze.

Uwaga: zanim będzie można wprowadzić ustawienia kamery PTZ, należy skonfigurować ustawienia jej portu. W przeciwnym razie element sterujący funkcją PTZ nie będzie działać w tym oknie dialogowym.

Aby skonfigurować predefiniowane położenie:

1. W tabeli **Kamery** zaznacz odpowiedni nadajnik.
2. Tylko kamery PTZ: aby włączyć sterowanie kamerą PTZ, w kolumnie  zaznaczyć pole wyboru.
3. Kliknij przycisk  .
Pojawi się okno dialogowe **Zdefiniowane pozycje i polecenia dodatkowe**.
4. Można zdefiniować liczbę predefiniowanych położeń, których chcesz użyć.
5. Wybierz położenie, które chcesz zdefiniować.
6. W oknie podglądu użyj kursora myszy, aby przejść do położenia, które chcesz skonfigurować. Przewijaj, aby przybliżać lub oddalać widok, i przeciągaj, aby przesuwać sekcję obrazu.
7. W razie potrzeby wpisz nazwę skonfigurowanego położenia.

8. Kliknąć , aby zapisać predefiniowane położenie.

Uwaga: kliknąć  w odniesieniu do każdego zdefiniowanego położenia. W przeciwnym razie położenie nie zostanie zapisane.

9. Kliknąć **OK**.

Aby wyświetlić już skonfigurowane predefiniowane położenia:

1. W tabeli **Kamery** zaznacz odpowiedni nadajnik.

2. Kliknij przycisk  .

Pojawi się okno dialogowe **Zdefiniowane pozycje i polecenia dodatkowe**.

- Wybierz odpowiednie położenie.

- Kliknij .

Predefiniowane położenie kamery jest wyświetlane w oknie podglądu.

Uwaga:

Predefiniowane położenia kamer PTZ i ROI są zapisane bezpośrednio w aparacie. Predefiniowane położenia kamer panoramicznych są zapisane w BVMS

Kamery PTZ przesuwają się fizycznie do predefiniowanych położzeń. Kamery panoramiczne i ROI wyświetlają tylko część całego pola widzenia kamery.

Aby skonfigurować polecenia pomocnicze do kamer PTZ:

- W tabeli **Kamery** zaznacz odpowiedni nadajnik.

- Kliknij przycisk .

Pojawi się okno dialogowe **Zdefiniowane pozycje i polecenia dodatkowe**.

- Wybierz kartę **Polecenia AUX**.

- Wprowadź odpowiednie ustawienia.

- Kliknij , aby zapisać predefiniowane polecenia.

Więcej informacji o różnych polach znajduje się w Pomocy ekranowej wybranego okna programu.

Patrz

- Okno dialogowe predefiniowanych położzeń i poleceń pomocniczych, Strona 301
- Konfiguracja ustawień portu PTZ, Strona 300
- Konfigurowanie alarmu, Strona 322
- Okno dialogowe Wybierz zawartość Okienka obrazu, Strona 312
- Okno dialogowe Opcje alarmu, Strona 313
- Okno wyboru Wybierz zawartość okienka obrazu (MG), Strona 313

22.9

Okno dialogowe predefiniowanych położzeń i poleceń pomocniczych

Okno główne > **Kamery i zapis** >  > Wybierz kamerę PTZ, ROI lub panoramiczną > 
 Umożliwia konfigurowanie kamery PTZ, ROI lub panoramicznej.

W przypadku kamer ROI i panoramicznych polecenia dodatkowe są niedostępne.

Uwaga: zanim będzie można wprowadzić ustawienia kamery PTZ, należy skonfigurować ustawienia jej portu. W przeciwnym razie element sterujący funkcją PTZ nie będzie działać w tym oknie dialogowym.

Icons (Ikony)

	Kliknij, aby przesunąć kamerę w uprzednio zdefiniowane położenie lub wykonać polecenie.
	Kliknij, aby zapisać uprzednio zdefiniowane położenie lub polecenie.

Karta Zdefiniowane pozycje

Kliknąć, aby wyświetlić tabelę z predefiniowanymi położeniami.

Nr

Wyświetla numer zdefiniowanej pozycji.

Nazwa

Kliknąć komórkę, aby edytować nazwę zdefiniowanej pozycji.

Karta Polecenia AUX (dotyczy tylko kamer PTZ)

Kliknij, aby wyświetlić tabelę z poleceniami dodatkowymi.

Uwaga: jeśli nadajnik ONVIF obsługuje polecenia dodatkowe, są one dostarczane bezpośrednio z nadajnika ONVIF.

Nr

Wyświetla numer polecenia dodatkowego.

Nazwa

Kliknąć komórkę, aby edytować nazwę polecenia.

Kod

Kliknąć komórkę, aby edytować kod polecenia.

Patrz

- Konfiguracja ustawień portu PTZ, Strona 300
- Konfigurowanie predefiniowanych położeń i funkcji dodatkowych, Strona 300

22.10**Konfigurowanie funkcji ROI**

Okno główne > **Kamery i zapis** >

Funkcję ROI można włączyć dla kamery stałopozycyjnej HD.

Strumień 2 należy skonfigurować dla obrazu wideo na żywo, a kodek H.264 MP SD ROI lub H.265 MP SD ROI skonfigurować na strumień 2.

Należy upewnić się, że strumień 2 jest używany dla obrazu wideo na żywo na każdej stacji roboczej, na której jest używana funkcja ROI.

Aby włączyć protokół ROI:

1. W kolumnie **Strumień 2 - Kodek** zaznacz kodek H.264 MP SD ROI lub H.265 MP SD ROI.
2. W kolumnie **Obraz bieżący – Strumień** zaznacz **Strumień 2**.
3. W kolumnie **Obraz bieżący – ROI** kliknij, aby zaznaczyć to pole wyboru.

Aby wyłączyć funkcję ROI:

1. W kolumnie **Obraz bieżący – ROI** kliknij, aby wyczyścić to pole wyboru.
2. W kolumnie **Strumień 2 – Kodek** zaznacz żądany kodek.

Patrz

- strona Kamery, Strona 285

22.11**Konfigurowanie funkcji ANR**

Okno główne > **Kamery i zapis** >

Przed włączeniem funkcji ANR należy dodać do żądanego nadajnika nośnik zapisu nadajnika i skonfigurować ten nośnik.

Należy wyłączyć podwójny zapis nadajnika, aby móc skonfigurować funkcję ANR.

Funkcja ANR działa tylko na nadajnikach z oprogramowaniem układowym w wersji 5.90 lub wyższej.

Nie wszystkie typy nadajników obsługują funkcję ANR, nawet jeśli mają zainstalowaną prawidłową wersję oprogramowania układowego.

Aby włączyć tę opcję:

- ▶ W wierszu żądanej kamery w kolumnie **ANR** zaznacz pole wyboru.

Patrz

- Konfigurowanie podwójnego zapisu w tabeli kamery, Strona 303
- strona Kamery, Strona 285
- Konfigurowanie nośnika zapisu nadajnika, Strona 230

22.12

Konfigurowanie podwójnego zapisu w tabeli kamery



Okno główne > **Kamery i zapis** >

Aby móc skonfigurować podwójny zapis, należy wyłączyć funkcję ANR.

Jeśli zostanie skonfigurowany podwójny zapis dla jednej kamery wielokanałowego nadajnika, system zapewni to samo miejsce docelowe zapisu dla wszystkich kamer tego nadajnika.

Aby przeprowadzić konfigurację:

1. W kolumnie **Zapis pomocniczy** – Cel kliknij komórkę żądanego nadajnika, a następnie żądaną pulę pomocniczego VRM.
Wszystkie kamery danego nadajnika zostaną skonfigurowane automatycznie do zapisywania na wybranym pomocniczym VRM.
2. W kolumnie **Ustawienie** wybierz ustawienia zaplanowanego zapisu.

Patrz

- Konfigurowanie podwójnego zapisu w drzewie urządzeń, Strona 187
- Konfigurowanie funkcji ANR, Strona 302
- Zapis podwójny / awaryjny, Strona 30
- strona Kamery, Strona 285

22.13

Zarządzanie bramą Video Streaming Gateway

Patrz

- Strona Urządzenie Video Streaming Gateway, Strona 198
- Okno dialogowe Dodaj / Edytuj nadajnik Bosch, Strona 202
- Okno dialogowe Dodaj / Edytuj nadajnik ONVIF, Strona 203
- Okno dialogowe Dodaj / Edytuj kamerę JPEG, Strona 205
- Okno dialogowe Dodaj / Edytuj nadajnik RTSP, Strona 206

22.13.1

Przypisywanie profilu ONVIF



Okno główne > **Kamery i zapis** >

Do kamery ONVIF można przypisać profil nośnika ONVIF.

Można go przypisać albo dla obrazu wideo na żywo, albo dla zapisywanego.

Aby przypisać token dla obrazu wideo na żywo:

- ▶ W kolumnie **Obraz bieżący** – **Profil** zaznacz żądany wpis.

Aby przypisać token dla obrazu rejestrowanego:

- ▶ W kolumnie **Zapis** – **Profil** zaznacz żądany wpis.

Patrz

- strona Kamery, Strona 285

23

strona Zdarzenia

Okno główne > **Zdarzenia**

Wyświetla drzewo zdarzeń ze wszystkimi dostępnymi zdarzeniami oraz tabelę konfiguracji zdarzeń dla każdego zdarzenia. Zdarzenia są pogrupowane na podstawie ich typu, na przykład wszystkie zapisy z kamery, takie jak zapis ciągły lub zapis alarmowy, są zgrupowane pod pozycją Tryb zapisu. Dostępne zdarzenia są grupowane poza odpowiadającymi im urządzeniami. Zmiana stanu urządzenia

jest wyświetlana poza  jako . Wszystkie pozostałe zdarzenia są wyświetlane pod grupami urządzeń jako .

Dla każdego zdarzenia można skonfigurować:

- Wyzwolenie alarmu na podstawie harmonogramu (nie jest dostępne dla wszystkich zdarzeń).
- Rejestrowanie zdarzenia na podstawie harmonogramu. Zdarzenie jest wyświetlane na liście zdarzeń Operator Client, jeśli zostało zarejestrowane.
- Wykonanie skryptu poleceń na podstawie harmonogramu (nie jest dostępne dla wszystkich zdarzeń).

- Dla zdarzenia typu : dodawanie danych tekstowych do zapisu.

Jeśli zdarzenie wystąpi, ustawienia są realizowane.

Użytkownik może utworzyć zdarzenie złożone, które łączy kilka zdarzeń z wyrażeniami boolowskimi.

- Kliknij element drzewa, aby wyświetlić odpowiednią tabelę konfiguracji zdarzenia.



Kliknąć, aby utworzyć duplikat zdarzenia. Użyć tej opcji do wygenerowania kilku alarmów dla określonego zdarzenia.



Kliknąć, aby usunąć duplikat lub Zdarzenie złożone.



Kliknąć, aby zmienić nazwę wybranego zdarzenia złożonego.



Kliknąć, aby wyświetlić okno dialogowe służące do tworzenia zdarzeń złożonych używających wyrażen boolowskich innych zdarzeń (maksymalnie 10).

Zdarzenia złożone są dodawane do tabeli konfiguracji zdarzenia.



Kliknąć, aby edytować wybrane zdarzenie złożone.



Kliknąć, aby wyświetlić okno dialogowe służące do tworzenia lub edycji skryptów poleceń.

Aby wyszukać elementy:

- W polu wyszukiwania wpisz ciąg znaków i naciśnij przycisk ENTER aby przefiltrować wyświetlone elementy.
Pojawią się tylko elementy zawierające łańcuch i odpowiadające im elementy nadrzędne (tylko w drzewach). Zostanie podana liczba odfiltrowanych elementów oraz całkowita liczba elementów.

Uwaga: ciąg znaków należy otoczyć cudzysłowem, aby znaleźć go precyzyjnie. Na przykład wpisanie "Camera 1" odfiltruje kamery o tej nazwie, a nie camera 201.

Patrz

- Konfiguracja zdarzeń i alarmów, Strona 318
- Konfiguracja skryptów poleceń, Strona 89
- Okno dialogowe Opcje (menu Ustawienia), Strona 120
- Konfigurowanie migających miejsc aktywnych, Strona 325

23.1 Karta Ustawienia eliminacji odbicia

Uwaga: Z powodu ograniczeń technicznych dla niektórych zdarzeń karta Ustawienia eliminacji odbicia jest niedostępna.

Umożliwia skonfigurowanie ustawień eliminacji odbicia dla wybranego zdarzenia.

Czas eliminacji odbicia

W trakcie określonego czasu, wszystkie późniejsze zdarzenia będą ignorowane.

Priorytet stanu zdarzenia

Do stanu zdarzenia można przypisać ustawienie priorytetu.

Edytuj priorytety

Kliknij, aby wyświetlić okno dialogowe konfiguracji ustawienia priorytetu.

Dodaj ustawienie

Kliknij, aby dodać wiersz konfiguracji ustawienia eliminacji odbicia różniącego się od ustawienia dla wszystkich pozostałych urządzeń.

Usuń ustawienie

Kliknij, aby usunąć zaznaczony wiersz. Aby zaznaczyć wiersz, kliknij lewy nagłówek wiersza.

23.2 Karta ustawień zaawansowanego wyświetlania mapy

Konfiguracja stanów kolorów na mapach jest możliwa tylko po zaznaczeniu opcji **Włącz zaawansowane wyświetlanie stanu (kolorowanie miejsc aktywnych na mapach w zależności od stanu)** lub **Włącz zaawansowane wyświetlanie stanu (kolorowanie miejsc aktywnych na mapach w zależności od alarmu)** w oknie dialogowym **Opcje**.

Dla każdego zdarzenia  lub alarmu można skonfigurować kolor tła i zachowanie (miganie lub

jego brak) miejsc aktywnych. Można np. skonfigurować alarm zdarzenie urządzenia , którego ikona na mapie zacznie migać, gdy stan urządzenia ulegnie zmianie.

Można ponadto skonfigurować priorytet wyświetlania poszczególnych miejsc aktywnych. Jest to niezbędne, jeśli dla tego samego urządzenia występują różne zdarzenia. (1 = najwyższy priorytet) Skonfigurowany kolor zachowuje ważność w przypadku wszystkich miejsc aktywnych o identycznym priorytecie wyświetlania. Można zmieniać kolor, zachowanie i priorytet każdego alarmu lub zdarzenia



: zmodyfikowany kolor i zmienione zachowanie obowiązują w przypadku wszystkich miejsc

aktywnych pozostałych alarmów lub zdarzeń , które mają identyczny priorytet.

Włącz kolorowanie stanów na mapach

To pole wyboru należy zaznaczyć, aby miejsca aktywne urządzenia należące do tego zdarzenia były wyświetlane na mapach z kolorowym tłem i ewentualnym miganiem.

Priorytet wyświetl. na mapie:

Klikając strzałki, można zmieniać priorytet miejsc aktywnych urządzeń należących do tego zdarzenia.

Kolor tła mapy:

Klikając kolorowe pole, można wybrać barwę tła stosowaną w przypadku miejsc aktywnych urządzeń należących do tego zdarzenia.

Uwaga: wszystkie zdarzenia stanu wszystkich urządzeń o tym samym priorytecie mają identyczny kolor tła.

Migające

To pole wyboru należy zaznaczyć, aby włączyć miganie miejsc aktywnych urządzeń należących do tego zdarzenia.

23.3**Karta ustawień konfiguracji zdarzeń****Urządzenie**

Wyświetla nazwę urządzenia lub harmonogramu.

Sieć

Wyświetla adres IP urządzenia sieciowego.

Wyzwól alarm

Należy kliknąć jedną z komórek, aby wybrać harmonogram zapisu lub harmonogram zadań do wyzwalania alarmu.

Jeśli alarm ma być wyzwalany niezależnie od punktu w czasie, należy wybrać ustawienie **Zawsze**.

Aby alarm w ogóle nie był wyzwalany, należy wybrać ustawienie **Nigdy**.

Rejestr zdarzeń

W kolumnie **Harmonogram** należy kliknąć jedną z komórek, aby wybrać harmonogram zapisu lub harmonogram zadań do rejestrowania.

Jeśli zdarzenie ma być rejestrowane niezależnie od punktu w czasie, należy wybrać ustawienie **Zawsze**.

Jeśli zdarzenie w ogóle nie ma być rejestrowane, należy wybrać ustawienie **Nigdy**.

Skrypt

W kolumnie **Skrypt** należy kliknąć jedną z komórek, aby wybrać skrypt poleceń.

W kolumnie **Harmonogram** należy kliknąć jedną z komórek, aby wybrać harmonogram zapisu lub harmonogram zadań do wykonania skryptu poleceń.

Jeśli skrypt poleceń ma być wykonywany niezależnie od punktu w czasie, należy wybrać ustawienie **Zawsze**.

Jeśli skrypt poleceń w ogóle nie ma być wykonywany, należy wybrać ustawienie **Nigdy**.

Zapis danych tekstowych

Można skonfigurować ustawienia w taki sposób, aby dane tekstowe były dodawane do zapisu ciągłego kamery.

Uwaga: ta kolumna jest dostępna tylko w przypadku zdarzeń zawierających dane tekstowe, np.:

Urządzenia interfejsu do ATM/POS-Bridge > Wejście ATM > Wejście danych

23.4**Okno dialogowe Edytor skryptu poleceń**

Okno główne > **Zdarzenia** > 

Umożliwia tworzenie i edycję skryptów poleceń.



Kliknąć, aby zapisać zmienione ustawienia.



Kliknąć, aby przywrócić zapisane ustawienia.



Kliknąć, aby sprawdzić kod skryptu.



Kliknąć, aby utworzyć plik skryptletu.



Kliknąć, aby usunąć plik skryptletu.



Kliknąć, aby wyświetlić okno dialogowe importu pliku skryptletu.

-  Kliknąć, aby wyświetlić okno dialogowe eksportu pliku skryptu.
-  Kliknąć, aby przekształcić istniejący skrypt na inny dostępny język skryptowy. Cały tekst istniejącego skryptu zostanie usunięty.
-  Kliknąć, aby wyświetlić pomoc ekranową dla skryptu API systemu BVMS.
-  Kliknąć, aby wyświetlić pomoc ekranową dla systemu BVMS.
-  Kliknąć, aby zamknąć okno dialogowe **Edytor skryptów poleceń**.

Patrz

- Konfiguracja skryptów poleceń, Strona 89

23.5**Utwórz Zdarzenie złożone / okno dialogowe Edytuj Zdarzenie złożone**

Okno główne > **Zdarzenia** >

Umożliwia tworzenie i edycję zdarzenia złożonego.

Aby wyszukać elementy:

- ▶ W polu wyszukiwania wpisz ciąg znaków i naciśnij przycisk ENTER aby przefiltrować wyświetlone elementy.
Pojawią się tylko elementy zawierające łańcuch i odpowiadające im elementy nadrzędne (tylko w drzewach). Zostanie podana liczba odfiltrowanych elementów oraz całkowita liczba elementów.

Uwaga: ciąg znaków należy otoczyć cudzysłowem, aby znaleźć go precyzyjnie. Na przykład wpisanie "Camera 1" odfiltruje kamery o tej nazwie, a nie camera 201.

Nazwa zdarzenia:

Należy tu wpisać nazwę zdarzenia złożonego.

Stany zdarzenia:

Należy tu wybrać zmianę stanu, która ma wchodzić w skład zdarzenia złożonego.

Obiekty:

Należy tu wybrać co najmniej jeden z dostępnych obiektów należących do wybranego stanu zdarzenia. Ten stan i wybrany obiekt pojawiają się w drzewie zdarzeń złożonych jako bezpośrednie elementy podrzędne głównego operatora.

Zdarzenie złożone:

Umożliwia tworzenie zdarzeń złożonych w drzewie takich zdarzeń. Wszystkie bezpośrednie elementy podrzędne operatora logicznego (AND, OR) są łączone przez ten operator.

Patrz

- Tworzenie zdarzenia złożonego, Strona 321
- Edycja zdarzenia złożonego, Strona 322

23.6**Okno dialogowe Wybierz język skryptu**

Okno główne > **Zdarzenia** >

Umożliwia ustawienie języka skryptu dla skryptów poleceń.

Nie można zmienić języka skryptu dla istniejących skryptów poleceń.

Język skryptu:

Należy tu wybrać odpowiedni język skryptu.

Patrz

– Konfiguracja skryptów poleceń, Strona 89

23.7

Okno dialogowe Edytuj priorytety typu zdarzenia

Okno główne > **Zdarzenia** > karta **Ustawienia eliminacji odbicia** > przycisk **Edytuj priorytety**

W razie potrzeby można skonfigurować priorytety dla różnych zmian stanu rodzaju zdarzenia, na przykład Wirtualne wejście zamknięte czy Wirtualne wejście otwarte. Zmiana stanu o wyższym priorytecie zastępuje czas eliminacji odbicia innej zmiany stanu o niższym priorytecie.

Nazwa priorytetu:

Wprowadzić nazwę ustawienia priorytetu.

Wartość stanu

Wyświetla nazwy stanów wybranego zdarzenia.

Priorytet stanu

Wprowadź wymagany priorytet. 1=najwyższy priorytet, 10=najniższy priorytet.

23.8

Okno dialogowe Wybierz urządzenia

Okno główne > **Zdarzenia** >  lub  > karta **Ustawienia eliminacji odbicia** > przycisk **Dodaj ustawienie**

Wybierz

To pole wyboru należy zaznaczyć obok odpowiedniej pozycji i kliknąć przycisk **OK**, aby dodać wiersz w tabeli **Urządzenia z odmiennymi ustawieniami eliminacji odbicia**.

23.9

Okno dialogowe Zapis danych tekstowych

Okno główne > **Zdarzenia** > w drzewie zdarzeń wybierz element  **Wejście danych** (muszą być dostępne dane tekstowe, np.: **Urządzenia z czytnikiem kart** > **Czytnik kart** > **Karta odrzucona**) > kolumna **Zapis danych tekstowych** > ...

Można skonfigurować kamery, w których przypadku do zapisu ciągłego będą dodawane dane tekstowe.

Patrz

– Wyzwalanie zapisu alarmowego za pomocą danych tekstowych, Strona 324

24

strona Alarmy

Okno główne > **Alarmy**

Wyświetla drzewo zdarzeń oraz tabelę konfiguracji alarmu dla każdego zdarzenia. Wyświetlane są tylko zdarzenia skonfigurowane na stronie **Zdarzenia**.

W tabelach dla każdego zdarzenia określa się, jak wyświetlany jest alarm wyzwolony przez to zdarzenie oraz które kamery są zapisywane i wyświetlane, kiedy alarm wystąpi.

Niektóre zdarzenia są konfigurowane domyślnie jako alarmy, np. błąd systemowy.

Alarmu nie można skonfigurować dla zdarzeń takich jak:

- Zmiana trybu zapisu
- Zmiana stanu alarmowego
- Większość działań użytkownika, np. sterowanie PTZ



Kliknij, aby wyświetlić okno dialogowe **Manager zasobów**.



Wyświetla okno dialogowe umożliwiające skonfigurowanie ustawień alarmu obowiązujących dla danego serwera Management Server.

Aby wyszukać elementy:

- ▶ W polu wyszukiwania wpisz ciąg znaków i naciśnij przycisk ENTER aby przefiltrować wyświetlone elementy.
Pojawią się tylko elementy zawierające łańcuch i odpowiadające im elementy nadrzędne (tylko w drzewach). Zostanie podana liczba odfiltrowanych elementów oraz całkowita liczba elementów.

Uwaga: ciąg znaków należy otoczyć cudzysłowem, aby znaleźć go precyzyjnie. Na przykład wpisanie "Camera 1" odfiltruje kamery o tej nazwie, a nie camera 201.

- ▶ Kliknąć element drzewa, aby wyświetlić odpowiednią tabelę konfiguracji alarmu.

Urządzenie

Wyświetla urządzenie warunku zdarzenia wybranego w oknie Drzewo zdarzeń.

Adres sieciowy

Wyświetla adres IP urządzenia sieciowego.

Identyfikacja alarmu

W kolumnie **Priorytet** kliknąć komórkę, aby wprowadzić priorytet dla wybranego alarmu (**100** jest priorytetem niskim, **1** jest priorytetem wysokim). W kolumnie **Nazwa** kliknij w komórce, aby wprowadzić nazwę alarmu wyświetlanego w programie BVMS, na przykład na liście alarmów. W kolumnie **Kolor** kliknij w komórce, aby wyświetlić okno dialogowe wyboru koloru dla alarmu wyświetlanego w programie Operator Client, na przykład na liście alarmów.

Okienka obrazów alarmowych

W kolumnach **1 - 5** kliknąć pozycję ... w komórce, aby wyświetlić okno dialogowe wyboru kamery. Można wybrać tylko kamerę, która została dodana do okna Drzewo logiczne na stronie **Mapy i struktura**.

Użytkownik może skonfigurować liczbę dostępnych Okienek obrazów alarmowych w oknie dialogowym **Ustawienia alarmowe**.

W kolumnie **Plik dźwiękowy** kliknij ... w komórce, aby wyświetlić okno dialogowe wyboru pliku dźwiękowego odtwarzanego w przypadku alarmu.

Opcje alarmu

Kliknąć pozycję ... w komórce, aby wyświetlić okno dialogowe **Opcje alarmu**.

Patrz

- Obsługa alarmów, Strona 39

24.1 Okno dialogowe Ustawienia alarmowe

Okno główne > Alarmy>



Karta Ustawienia alarmowe

Maks. liczba okienek obrazu dla jednego alarmu:

Wprowadź maksymalną liczbę okienek obrazów alarmowych do wyświetlania w przypadku alarmu.

Uwaga: w przypadku obsługi urządzenia Enterprise System obowiązuje najwyższa maksymalna liczba, która została skonfigurowana w systemie online Management Servers.

Czas automatycznego resetowania:

Wprowadzić liczbę sekund, po upływie których alarm jest automatycznie resetowany.

Dotyczy to tylko alarmów z ustawieniem **Autom. resetuj alarm po upływie ust. czasu (okno dialogowe „Ustawienia alarmowe”)** na stronie Alarmy.

Wielorzędowe wyświetlanie alarmu w oknie obrazu alarmowego

Zaznaczyć pole wyboru, aby włączyć widoku alarmu wielowierszowego w oknie obrazów alarmowych.



Uwaga!

W przypadku istniejących konfiguracji alarmów tryb alarmu wielowierszowego jest włączony, a w przypadku nowych konfiguracji alarmów domyślnie jest on wyłączony i aktywny jest tryb widoku pojedynczego.

Ustaw limit czasu trwania zapisów alarmowych wyzwalanych przez stan:

Zaznacz to pole wyboru, aby włączyć limit czasu trwania zapisów alarmowych wywoływanych przez określony stan. Wprowadź żądaną liczbę minut czasu trwania zapisu alarmowego. Zapis alarmowy jest zatrzymywany automatycznie po upływie zdefiniowanego czasu.

Użytkownik może wprowadzić czas trwania od 1 do 1440 minut.

Jeśli alarm wyzwała zapis ze skonfigurowanym limitem czasu trwania:

- Jeśli alarm jest wyzwalany ponownie przed osiągnięciem limitu czasu, zapis jest kontynuowany, a czas jest ponownie naliczany od 0.
- Jeśli alarm został anulowany przed osiągnięciem limitu czasu, zapis jest kontynuowany do osiągnięcia skonfigurowanego limitu czasu po alarmie.

Karta Grupy monitorów

Kolejność wyświetlania w przypadku tego samego priorytetu alarmu

Zaznacz odpowiednią pozycję dotyczącą sortowania alarmów o tym samym priorytecie według ich znacznika czasu.

Pokaż pusty ekran

Kliknąć, aby skonfigurować system w taki sposób, że na monitorze, który nie jest używany do wyświetlania alarmu, nic nie jest widoczne.

Kontynuuj podgląd bieżącego

Kliknąć, aby skonfigurować system w taki sposób, że na monitorze, który nie jest używany do wyświetlania alarmu, był widoczny podgląd bieżący.

Patrz

- Konfiguracja ustawień dla wszystkich alarmów, Strona 323

24.2

Okno dialogowe Wybierz zawartość Okienka obrazu

Okno główne > **Alarmy** >  lub  > kolumna **Okienka obrazów alarmowych** > kliknąć ... w jednej z kolumn **1-5**

Umożliwia wybranie pozycji z drzewa logicznego, która jest wyświetlana i zapisywana (jeśli jest to kamera) w przypadku wybranego alarmu.

**Uwaga!**

Mapa obszaru wyświetlana w okienku obrazów alarmowych jest zoptymalizowana pod kątem wyświetlania i zawiera tylko początkowy widok oryginalnego pliku mapy.

Wyszukaj element

Po wpisaniu tu tekstu można znaleźć element w drzewie logicznym.

Znajdź

Ten przycisk należy kliknąć, aby odnaleźć kamerę poprzez wyszukanie tekstu w jej opisie.

Bieżący

Ten przycisk należy kliknąć, aby w przypadku alarmu wyświetlany był obraz na żywo z kamery.

Odtwarzanie natychmiastowe

Kliknij, aby skonfigurować system do wyświetlania odtwarzania natychmiastowego z kamery.

Czas przewijania dla odtwarzania alarmu natychmiastowego jest ustawiany na stronie **Funkcje operatora**, patrz *Strona funkcji operatora*, Strona 337.

Wstrzymaj odtwarzanie

To pole wyboru należy zaznaczyć, aby po wstrzymaniu odtwarzania natychmiastowego wyświetlany był obraz z kamery alarmowej. W takiej sytuacji w razie potrzeby można będzie ręcznie wznowić odtwarzanie natychmiastowe.

Odtwarzaj w pętli

To pole wyboru należy zaznaczyć, aby po zapętleniu odtwarzania natychmiastowego wyświetlany był obraz z kamery alarmowej.

Czas trwania zapętlonego odtwarzania natychmiastowego w okienku obrazu alarmowego to czas cofania zapisu plus czas trwania stanu alarmowego plus czas przewijania.

Zapisz z tej kamery

To pole wyboru należy zaznaczyć, aby w przypadku alarmu włączał się zapis alarmowy sygnału z wybranej kamery. Jeśli zostanie wyzwolony alarm, sygnał z kamery jest zapisywany w jakości zapisu alarmowego. Czas trwania zapisu to czas trwania stanu alarmowego plus czas przed wystąpieniem alarmu i czas po wystąpieniu alarmu. To ustawienie ma bezpośredni wpływ na ustawienie zapisu alarmowego w oknie dialogowym **Opcje alarmu** i odwrotnie.

Uwaga: jeśli w odniesieniu do kamery panoramicznej wybrano wstępnie predefiniowane położenie, zapisywany jest nie tylko dany fragment obrazu, ale również pełny widok 360°.

Zdefiniowana pozycja widoku panoramicznego

Jeśli wybrano kamerę panoramiczną, można wybrać predefiniowane położenie kamery. Jeśli użytkownik Operator Client zaakceptuje ten alarm, obraz alarmu jest wyświetlany w predefiniowanym położeniu w widoku przyciętym.

Jeśli wybrano opcję **<brak>**, obraz alarmu jest wyświetlany w widoku panoramicznym.

Patrz

- Strona funkcji operatora, Strona 337

– Konfigurowanie alarmu, Strona 322

24.3

Okno wyboru Wybierz zawartość okienka obrazu (MG)

Okno główne >



Alarmy > lub > kolumna **Opcje alarmu** > Kliknij ... > okno dialogowe **Opcje alarmu** > karta **Grupa monitorów** > Kliknij ... w jednej z kolumn 1–10

Będzie można wybrać kamerę z drzewa logicznego. Obraz z tej kamery zostanie wyświetlony na przypisanym monitorze w przypadku wybranego alarmu.

Wyszukaj element

Po wpisaniu tu tekstu można znaleźć element w drzewie logicznym.

Znajdź

Ten przycisk należy kliknąć, aby odnaleźć kamerę poprzez wyszukanie tekstu w jej opisie.

Zdefiniowana pozycja widoku panoramicznego

Jeśli wybrano kamerę panoramiczną, można wybrać predefiniowane położenie kamery. Jeśli użytkownik Operator Client zaakceptuje ten alarm, obraz alarmu jest wyświetlany w predefiniowanym położeniu w widoku przyciętym.

Jeśli wybierzesz opcję **<brak>**, dekodery wyświetla obraz alarmu w widoku okręgu.

Brak kamery

Kliknij, aby usunąć kamerę z kolumny grupy monitorów.

Uwaga:

Pole widzenia predefiniowanego położenia kamery panoramicznej jest inne dla Operator Client lub Configuration Client i dla dekodera.



Uwaga!

Aby używać predefiniowanych położzeń w kamerach panoramicznych, parametr **Pozycja mocowania** kamery panoramicznej musi mieć wartość **Ściana** lub **Sufit**.

24.4

Okno dialogowe Opcje alarmu



Okno główne > **Alarmy** > lub > kolumna **Opcje alarmu** > ...

Umożliwia skonfigurowanie następujących ustawień alarmów:

- Kamery, które rozpoczynają zapis w przypadku alarmu.
- Włączanie ochrony dla tych zapisów alarmowych.
- Włączanie i konfigurowanie ustawień różniących się czasów trwania alarmu.
- Wyzwalanie poleceń PTZ w przypadku alarmu.
- Powiadomienia wysyłane w przypadku alarmu.
- Sekwencja zadań, która musi zostać wykonana w przypadku alarmu.
- Przypisanie kamer wyświetlanych w grupach monitorów w przypadku alarmu.

Karta Kamery

Nr	Wyświetla numer kamery skonfigurowany na stronie Kamery i zapis .

Nazwa	Wyświetla nazwę kamery skonfigurowaną na stronie Kamery i zapis .
Lokalizacja	Wyświetla lokalizację kamery skonfigurowaną na stronie Mapy i struktura .
Tryb	Zaznaczyć pole wyboru, aby włączyć zapis alarmowy dla wybranej kamery w przypadku alarmu. Jeśli zostanie wyzwolony alarm, sygnał z kamery jest zapisywany w jakości zapisu alarmowego. Czas trwania zapisu to czas trwania stanu alarmowego plus czas przed wystąpieniem alarmu i czas po wystąpieniu alarmu. To ustawienie ma bezpośredni wpływ na ustawienie zapisu alarmowego w oknie dialogowym Wybierz zawartość okienka obrazu i odwrotnie.
Chroń zapis	Zaznaczyć, aby chronić zapisy alarmowe z wybranej kamery. Uwaga: chronione dane wideo nigdy nie zostaną usunięte VRM automatycznie. Należy jednak pamiętać, że zbyt wiele chronionych bloków danych może zapełnić pamięć magazynową kamery i zatrzymać nagrywanie.
Odmienne ustawienia czasu trwania alarmów	To pole wyboru jest automatycznie zaznaczane po zaznaczeniu pola wyboru Tryb , gdy kamera obsługuje funkcję ANR.
Polecenia AUX	Kliknąć komórkę, aby zaznaczyć funkcję dodatkową, która zostanie wykonana w przypadku alarmu. Pozycje z tej listy są dostępne tylko dla kamery PTZ.
Zdefiniowana pozycja	Kliknąć komórkę, aby zaznaczyć uprzednio zdefiniowane położenie, do którego ma przejść kamera w przypadku alarmu. Pozycje z tej listy są dostępne tylko dla kamery PTZ.

Uwaga: nie można skonfigurować obu z tych opcji jednocześnie: **Polecenia AUX** oraz **Zdefiniowana pozycja** dla tej samej kamery i alarmu.

Karta Powiadomienia

E-mail	Zaznacz pole wyboru, aby wysyłać wiadomość e-mail w przypadku alarmu.
Serwer:	Wybierz serwer poczty elektronicznej.
Odbiorcy:	Wprowadzić rozdzielone przecinkami adresy e-mail odbiorców (przykład: nazwa@dostawcauslugi.com).
Tekst:	Wprowadzić tekst powiadomienia.
Informacja:	Zaznaczyć pole wyboru, aby dodać określoną informację do tekstu powiadomienia. Uwaga: W wiadomościach e-mail używana jest data strefy czasowej serwera Management Server.

Karta Etapy pracy

Zapisuj tylko alarm	Zaznacz pole wyboru, aby skonfigurować system w taki sposób, że obraz z kamery jest tylko zapisywany i nie jest wyświetlany w przypadku alarmu. To pole wyboru jest aktywne tylko wtedy, gdy na karcie Kamery zostało zaznaczone pole Tryb .
Autom. resetuj alarm po upływie ust. czasu (okno dialogowe „Ustawienia alarmowe”)	Zaznaczyć pole wyboru, aby alarm był automatycznie resetowany.
Automatycznie resetuj alarm, gdy stan zdarzenia zmieni się ponownie na normalny	W przypadku zaznaczenia tego pola wyboru alarm będzie automatycznie zerowany po zmianie stanu zdarzenia wyzwalającego. Zerowanie automatyczne nie zostanie przeprowadzone w sytuacji, gdy alarm został zaakceptowany bądź odrzucony.
Zapobiegaj resetowaniu alarmów podczas trwania stanu uaktywnienia	Zaznaczenie tego pola wyboru uniemożliwi usunięcie alarmu, dopóki jego przyczyna nie zostanie usunięta.
Pomiń powielone alarmy na liście alarmów	Zaznaczenie tego pola wyboru pozwoli uniknąć występowania alarmów dla zdarzeń tego samego typu i dublowania urządzeń na liście alarmów w programie BVMS Operator Client. Dopóki alarm będzie aktywny (w stanie alarmowym Aktywny lub Przyjęty), na liście alarmów nie będą wyświetlane żadne dodatkowe alarmy dla tego samego typu zdarzenia i urządzenia. Uwaga: – Zdarzenia są nadal zapisywane w rejestrze. – Należy pamiętać, że żadne działanie alarmowe wyzwalane przez ten alarm (na przykład uruchomienie zapisu alarmowego itp.) nie będą ponownie wyzwalane. Jeśli po skasowaniu takiego alarmu dla tego samego urządzenia lub z powodu tego samego typu zdarzenia wyzwolony zostanie nowy alarm, wówczas nowy alarm ponownie pojawi się na liście alarmów, a wszystkie działania alarmowe dla tego alarmu zostaną ponownie wyzwolone. – To pole wyboru jest wstępnie zaznaczone dla alarmów Person Identification.
Pokaż plan działania	Zaznaczyć pole wyboru, aby włączyć sekwencje zadań, które muszą zostać wykonane w przypadku alarmu.
Zasoby...	Kliknąć, aby wyświetlić okno dialogowe Manager zasobów . Wybierz dokument z opisem sekwencji zadań.
Wyświetl pole komentarza	Zaznaczyć pole wyboru, aby włączyć wyświetlanie okna komentarzy w przypadku alarmu. W oknie komentarzy użytkownik może wprowadzić komentarze na temat alarmu.

Wymuszaj przetwarzanie etapów pracy przez operatora	Zaznaczyć pole wyboru, aby wymóc na użytkowniku wykonanie sekwencji zadań. Jeśli pole zostanie zaznaczone, użytkownik nie może zresetować alarmu do czasu, kiedy wprowadzi komentarz na temat alarmu.
Wykonaj następujący Skrypt klienta, kiedy alarm został przyjęty:	Select a Client Command Script that is executed automatically, when the user accepts an alarm.

Karta Grupa monitorów

1...10	W ponumerowanej kolumnie kliknij komórkę. Pojawi się okno dialogowe Wybierz zawartość okienka obrazu . Wybierz kamerę z drzewa logicznego. Obraz z tej kamery zostanie wyświetlony na przypisanym monitorze w przypadku alarmu. Wybierz predefiniowane położenia kamer, jeśli są skonfigurowane. Aby uzyskać więcej informacji, zobacz pomoc online dotyczącą okna dialogowego Wybierz zawartość okienka obrazu (MG).
Usuń tabelę	Kliknij, aby usunąć wszystkie przypisania kamer do grup monitorów.
Menu ekranowe (Ustawienia OSD)	
Nazwa alarmu	Zaznacz pole wyboru, aby skonfigurować system w taki sposób, aby nazwa alarmu była wyświetlana na monitorach jako informacja ekranowa.
Godzina alarmu	Zaznacz pole wyboru, aby skonfigurować system w taki sposób, aby godzina alarmu była wyświetlana na monitorach jako informacja ekranowa.
Data alarmu	Zaznacz pole wyboru, aby skonfigurować system w taki sposób, aby data alarmu była wyświetlana na monitorach jako informacja ekranowa.
Nazwa zaalarmowanej kamery	Zaznacz pole wyboru, aby skonfigurować system w taki sposób, aby nazwa zaalarmowanej kamery była wyświetlana na monitorach jako informacja ekranowa.
Numer zaalarmowanej kamery	Zaznacz pole wyboru, aby skonfigurować system w taki sposób, aby numer zaalarmowanej kamery był wyświetlany na monitorach jako informacja ekranowa.
Tylko na 1. monitorze	Zaznacz pole wyboru, aby skonfigurować system w taki sposób, aby nazwa i godzina były wyświetlane tylko na pierwszym monitorze z grupy monitorów jako informacja ekranowa.

Karta Odmienne ustawienia czasu trwania alarmów

Ustawienia na tej karcie są dostępne tylko wtedy, gdy dla tej kamery jest włączona funkcja ANR.

Użyj ustawień profilu	Kliknij, aby włączyć to ustawienie. Dla tej kamery są używane ustawienia czasów przed i po wystąpieniu alarmu skonfigurowane w oknie dialogowym Ustawienia zaplanowanego zapisu .
Zastąp ustawienia	Kliknij, aby włączyć następujące ustawienia czasów przed i po wystąpieniu alarmu.
Czas trwania (przed alarmem)	Dostępne dla wszystkich zdarzeń.
Czas trwania (po alarmie)	Dostępne tylko dla zdarzeń  .

Karta Poziom zagrożenia

Podnieś poziom zagrożenia do	Wybierz poziom zagrożenia uruchamiany przez ten alarm. Wybierz pozycję Resetuj poziom zagrożenia , jeśli alarm ma wyłączać aktywny poziom zagrożenia. Aplikacja Operator Client wyloguje się, a użytkownik będzie mógł zalogować się ponownie.

Patrz

- Konfiguracja dekodarów do wyświetlania OSD, Strona 233
- Okno wyboru Wybierz zawartość okienka obrazu (MG), Strona 313
- Wyzwalanie zapisu alarmowego za pomocą danych tekstowych, Strona 324
- Konfigurowanie alarmu, Strona 322
- Konfigurowanie dla alarmu czasów trwania okresu przed i po wystąpieniu alarmu, Strona 323

24.5

Okno dialogowe Wybierz zasób

Okno główne > **Alarmy** >  lub  > kolumna **Identyfikacja alarmu** > kolumna **Plik dźwiękowy** > kliknij ...

Umożliwia wybór pliku dźwiękowego odtwarzanego w przypadku alarmu.

Odtwarzanie

Kliknąć, aby odtworzyć wybrany plik dźwiękowy.

Pauza

Kliknąć, aby wstrzymać odtwarzanie wybranego pliku dźwiękowego.

Zatrzymaj

Kliknąć, aby zatrzymać odtwarzanie wybranego pliku dźwiękowego.

Zarządzaj...

Kliknij, aby wyświetlić okno dialogowe **Manager zasobów**.

Patrz

- Konfigurowanie alarmu, Strona 322
- Zarządzanie plikami zasobów, Strona 319

25 Konfiguracja zdarzeń i alarmów

Okno główne > **Zdarzenia**

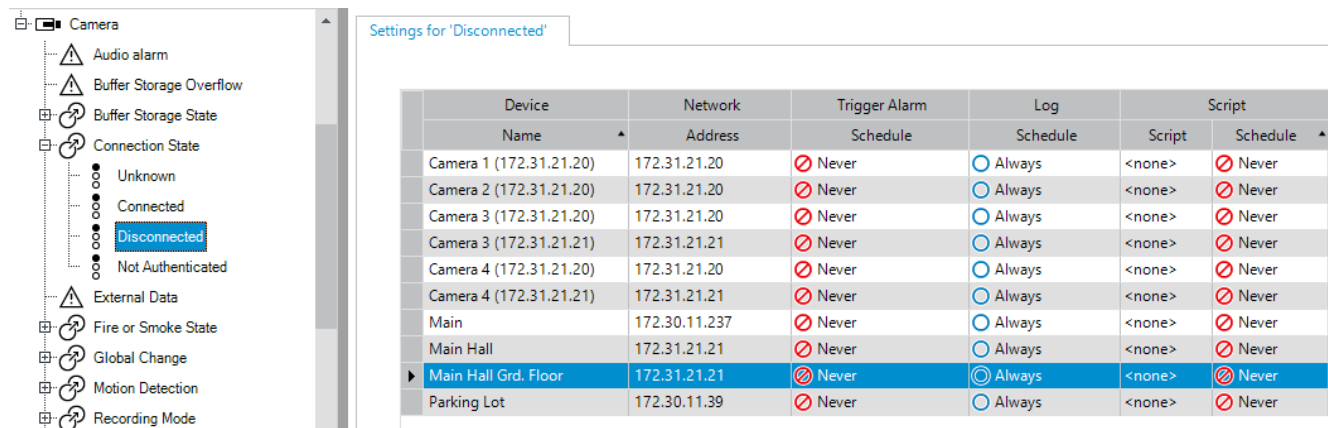
LUB

Okno główne > **Alarmy**

Niniejszy rozdział zawiera informacje o sposobie konfigurowania zdarzeń oraz alarmów w systemie. Dostępne zdarzenia są grupowane poza odpowiadającymi im urządzeniami.

Na stronie **Zdarzenia** można skonfigurować, kiedy zdarzenie w systemie BVMS wyzwoi alarm, wykona Skrypt poleceń i kiedy zostanie zarejestrowane.

Przykład (część tabeli konfiguracji zdarzenia):



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>

Ten przykład oznacza:

Jeśli sygnał wizyjny z wybranej kamery zaniknie, wyzwalany jest alarm, następuje rejestracja zdarzenia, ale skrypt nie jest wykonywany.

Na stronie **Alarmy** użytkownik definiuje sposób, w jaki jest wyświetlany alarm oraz które kamery są wyświetlane i zapisywane w przypadku alarmu.

Niektóre zdarzenia systemu są domyślnie konfigurowane jako alarmy.

- Kliknij , aby zapisać ustawienia.
- Kliknij , aby cofnąć ostatnią zmianę.
- Kliknij , aby uaktywnić konfigurację.

Patrz

- Karta Ustawienia eliminacji odbicia, Strona 306
- Karta ustawień zaawansowanego wyświetlania mapy, Strona 306
- Karta ustawień konfiguracji zdarzeń, Strona 307
- Okno dialogowe Edytor skryptu poleceń, Strona 307
- Utwórz Zdarzenie złożone / okno dialogowe Edytuj Zdarzenie złożone, Strona 308
- Okno dialogowe Wybierz język skryptu, Strona 308
- Okno dialogowe Edytuj priorytety typu zdarzenia, Strona 309
- Okno dialogowe Wybierz urządzenia, Strona 309
- Okno dialogowe Zapis danych tekstowych, Strona 309
- Okno dialogowe Ustawienia alarmowe, Strona 311
- Okno dialogowe Wybierz zawartość Okienka obrazu, Strona 312
- Okno dialogowe Opcje alarmu, Strona 313

25.1 Kopiowanie i wklejanie w tabelach

Użytkownik może jednocześnie skonfigurować wiele obiektów w Tabeli kamer, Tabeli konfiguracji zdarzenia lub Tabeli konfiguracji alarmu za pomocą kilku kliknięć myszą.

Aby uzyskać więcej informacji, patrz *Kopiowanie i wklejanie w tabelach*, Strona 291.

25.2 Usuwanie wiersza tabeli

Okno główne > **Alarmy**

Użytkownik może usunąć wiersz tabeli, który został dodany przez niego lub innego użytkownika, tj. usuwane są duplikaty zdarzeń lub zdarzenia złożone.

Zdarzenia złożone znajdują się w drzewie zdarzeń pod pozycją **Urządzenia systemowe > Zdarzenia złożone**.

Aby usunąć wiersz tabeli:

1. Zaznacz wiersz.

2. Kliknij .

Patrz

- strona *Zdarzenia*, Strona 305

25.3 Zarządzanie plikami zasobów

Aby uzyskać więcej informacji, patrz:

- *Zarządzanie plikami zasobów*, Strona 262.

25.4 Konfigurowanie zdarzenia

Okno główne > **Zdarzenia**

Aby skonfigurować zdarzenie:

1. Wybierz w drzewie zdarzenie lub stan zdarzenia, np. **Urządzenia systemowe > Uwierzytelnianie > Uwierzytelnianie operatora odrzucone**.
Pojawi się odpowiednia tabela konfiguracji zdarzenia.
2. W kolumnie **Wyzwól alarm – Harmonogram** kliknij właściwą komórkę i wybierz odpowiedni harmonogram.
Harmonogram określa, kiedy wyzwalany jest alarm.
Wybierz jeden z harmonogramów zapisu lub harmonogramów zadań skonfigurowanych wcześniej na stronie **Harmonogramy**.
3. W kolumnie **Rejestr zdarzeń – Harmonogram** kliknij właściwą komórkę i wybierz odpowiedni harmonogram.
Harmonogram określa, kiedy nastąpi zarejestrowanie zdarzenia.
4. W kolumnie **Skrypt – Skrypt** kliknij właściwą komórkę i wybierz odpowiedni skrypt poleceń.
5. W kolumnie **Skrypt – Harmonogram** kliknij właściwą komórkę i wybierz odpowiedni harmonogram.
Harmonogram określa, kiedy zdarzenie ma wyzwać wykonanie skryptu poleceń.

Patrz

- strona *Zdarzenia*, Strona 305

25.5 Tworzenie duplikatu zdarzenia

Okno główne > **Zdarzenia**

Użytkownik może utworzyć duplikat zdarzenia, aby wyzwać różne alarmy dla określonego zdarzenia.

Aby utworzyć duplikat zdarzenia:

1. Wybierz w drzewie warunek zdarzenia. Pojawi się odpowiednia tabela konfiguracji zdarzeń.
2. Zaznacz wiersz tabeli.
3. Kliknij . W tabeli zostanie dodany poniżej nowy wiersz z domyślnymi ustawieniami.

Patrz

– strona Zdarzenia, Strona 305

25.6

Rejestracja zdarzeń użytkownika

Okno główne > **Zdarzenia** > rozwiń **Urządzenia systemowe** > **Działania użytkownika**

Użytkownik może skonfigurować sposób rejestracji wielu działań użytkowników osobno dla każdej grupy użytkowników.

Przykład:

Aby rejestrować zdarzenia użytkownika:

1. Wybierz zdarzenie użytkownika, aby skonfigurować sposób jego rejestracji, np. **Logowanie operatora**.
Pojawi się odpowiednia tabela konfiguracji zdarzeń.
Wszystkie grupy użytkowników są wyświetlane w kolumnie **Urządzenie**.
2. O ile jest to możliwe: w kolumnie **Wyzwól alarm – Harmonogram** kliknij właściwą komórkę i wybierz odpowiedni harmonogram.
Harmonogram określa, kiedy wyzwalany jest alarm, który ma powiadomić użytkownika.
Można wybrać jeden z harmonogramów zapisu lub harmonogramów zadań skonfigurowanych w oknie **Harmonogramy**.
3. W kolumnie **Rejestr zdarzeń – Harmonogram** kliknij właściwą komórkę i wybierz odpowiedni harmonogram.
Harmonogram określa, kiedy nastąpi zarejestrowanie zdarzenia.
W podanym przykładzie harmonogram **Dzień** powoduje, że zdarzenie logowania operatora grupy administratorów oraz grupy użytkowników upoważnionych nie jest rejestrowane, podczas gdy zdarzenie logowania operatora grupy użytkowników podglądu na żywo jest rejestrowane.

Patrz

– strona Zdarzenia, Strona 305

25.7

Konfiguracja przycisków zdarzeń użytkownika

Okno główne > **Zdarzenia**

Można skonfigurować przyciski zdarzeń użytkownika dostępne w oprogramowaniu Operator Client. Można ustawić, aby jeden lub więcej przycisków zdarzeń operatora nie było wyświetlanych w oprogramowaniu Operator Client.

Na stronie **Grupy użytkowników** można skonfigurować, aby przyciski zdarzeń użytkownika były dostępne tylko w oprogramowaniu Operator Client odpowiedniej grupy użytkowników.

Aby skonfigurować przyciski zdarzeń użytkownika, należy:

1. Na drzewie wybrać **Urządzenia systemowe** > **Przyciski zdarzeń Operator Client** > **Naciśnięto przycisk zdarzenia**.
Zostaje wyświetlona odpowiednia tabela konfiguracji zdarzeń.
2. Zaznaczyć przycisk zdarzeń użytkownika, aby skonfigurować jego działanie.

3. W kolumnie **Wyzwól alarm – Harmonogram** kliknąć właściwą komórkę i wybrać odpowiedni harmonogram.
Harmonogram określa, kiedy wyzwalany jest alarm, który ma powiadomić użytkownika.
4. W kolumnie **Rejestr zdarzeń – Harmonogram** kliknąć właściwą komórkę i wybrać odpowiedni harmonogram.
Harmonogram określa, kiedy nastąpi zarejestrowanie zdarzenia.
Zaznaczenie opcji **Nigdy** powoduje, że przycisk zdarzeń użytkownika jest niedostępny w aplikacji Operator Client wszystkich grup użytkowników, które posiadają uprawnienia do obsługi przycisku zdarzeń użytkownika.
5. W kolumnie **Skrypt – Skrypt** kliknąć właściwą komórkę i wybrać odpowiedni Skrypt poleceń.
6. W kolumnie **Skrypt – Harmonogram** kliknąć właściwą komórkę i wybrać odpowiedni harmonogram.
Harmonogram określa, kiedy wykonywany jest skrypt poleceń.

Patrz

– strona Zdarzenia, Strona 305

25.8

Tworzenie zdarzenia złożonego



Okno główne > **Zdarzenia** >

Użytkownik tworzy zdarzenie złożone. Można łączyć tylko zmiany stanu i ich obiekty. Obiektami mogą być na przykład harmonogramy i zdarzenia. Istnieje możliwość łączenia zmian stanu oraz ich obiektów z wyrażeniami boolowskimi AND i OR.

Przykład: użytkownik łączy stany połączenia kamery sieciowej i odbiornika. Zdarzenie złożone pojawi się tylko wówczas, gdy obydwa urządzenia utracą połączenie. W tym przypadku dla dwóch obiektów (kamery sieciowej i odbiornika) oraz dwóch stanów **Zanik sygnału wizyjnego** i **Rozłączone** został użyty operator AND.

Create Compound Event

Event name:

Construction Set for Event States and their Objects

Event States:

- Events and Alarms
 - Dvr Devices
 - ONVIF Encoders
 - NVR Devices
 - Encoders/Decoders
 - VRM Devices
 - Allegiant Devices
 - System Devices
 - Compound Events
 - Schedules
 - Virtual Inputs
 - Input State
 - Input Opened
 - Input Closed
 - Input Error
 - Unknown
 - Backup Video Data
 - Alarm State
 - Authentication
 - Operator Client Event Buttons

Objects of Input Opened (1/1):

- Virtual Input 1

Resulting Compound Event will be fired, IF:

Compound Event:

```

AND
├── Virtual Inputs.Input State.Input Opened
└── AND
    └── Virtual Input 1
  
```

OK Cancel

Aby utworzyć zdarzenie złożone:

1. W polu **Nazwa zdarzenia**: wprowadź nazwę zdarzenia złożonego.
2. W polu **Stany zdarzenia**: zaznacz stan zdarzenia.
Dostępne obiekty są wyświetlane w polu **Obiekty**.
3. W polu **Obiekty**: wybierz urządzenie.
Odpowiednie zdarzenie i wybrane urządzenia zostaną dodane do okienka zdarzeń złożonych.
4. W polu **Zdarzenie złożone**: kliknij prawym przyciskiem myszy operację boolowską i zmień ją tam, gdzie to potrzebne.
Operacja boolowska definiuje kombinację bezpośrednich elementów podrzędnych.
5. Kliknąć **OK**.
Nowe zdarzenie złożone zostanie dodane do tabeli konfiguracji zdarzenia. Znajduje się ona w drzewie zdarzeń pod pozycją **Urządzenia systemowe**.

Patrz

– strona Zdarzenia, Strona 305

25.9**Edycja zdarzenia złożonego**

Okno główne > **Zdarzenia**

Użytkownik może zmienić wcześniej utworzone zdarzenie złożone.

Aby edytować zdarzenie złożone:

1. W drzewie zdarzeń rozwiń **Urządzenia systemowe > Stan Zdarzenia złożonego > Zdarzenie złożone jest prawdziwe**.
2. W tabeli konfiguracji zdarzenia w kolumnie **Urządzenie** kliknij prawym przyciskiem myszy żądane zdarzenie złożone, następnie kliknij polecenie **Edytuj**.
Pojawi się okno dialogowe **Edytuj Zdarzenie złożone**.
3. Wprowadź żądane ustawienia.
4. Kliknij przycisk **OK**.
Zdarzenie złożone zostanie zmienione.

Patrz

– strona Zdarzenia, Strona 305

25.10**Konfigurowanie alarmu**

Okno główne > **Alarmy**

Przed skonfigurowaniem alarmu należy skonfigurować wyzwalacz w oknie **Zdarzenia**.

Aby potwierdzić alarm:

1. Wybierz alarm w drzewie, na przykład **Urządzenia systemowe > Uwierzytelnianie > Uwierzytelnianie operatora odrzucone**.
Pojawi się odpowiednia tabela konfiguracji alarmów.
2. W kolumnie **Priorytet** kliknij ... w komórce, aby wprowadzić priorytet dla wybranego alarmu (100 jest priorytetem niskim, 1 jest priorytetem wysokim).
W kolumnie **Nazwa** kliknij ... w komórce, aby wprowadzić nazwę alarmu wyświetlanego w BVMS, na przykład na liście alarmów.
W kolumnie **Kolor** kliknij ... w komórce, aby wyświetlić okno dialogowe wyboru koloru dla alarmu wyświetlanego w Operator Client, na przykład na liście alarmów.
3. W kolumnach 1-5 kliknij ... w komórce, aby wyświetlić okno dialogowe **Wybierz zawartość okienka obrazu**.
Wprowadź żądane zmiany.

4. W kolumnie **Plik dźwiękowy** kliknij ... w komórce, aby wyświetlić okno dialogowe wyboru pliku dźwiękowego odtwarzanego w przypadku alarmu.
5. W kolumnie **Opcje alarmu** kliknij ... w komórce, aby wyświetlić okno dialogowe **Opcje alarmu**.
6. Wprowadź żądane zmiany.

Więcej informacji o różnych polach znajduje się w Pomocy ekranowej wybranego okna programu.

Patrz

- Konfigurowanie zdarzenia, Strona 319
- strona Alarmy, Strona 310
- Okno dialogowe Wybierz zawartość Okienka obrazu, Strona 312
- Okno dialogowe Opcje alarmu, Strona 313

25.11

Konfiguracja ustawień dla wszystkich alarmów

Okno główne > **Alarmy**

Użytkownik może wprowadzić następujące ustawienia alarmów obowiązujące dla danego serwera Management Server:

- Liczba Okienek obrazu na alarm
- Czas automatycznego resetowania
- Czas zapisu alarmowego uruchamianego ręcznie
- Wyświetlanie alarmów wielowierszowych w oknie obrazów alarmowych
- Limit czasu trwania zapisów alarmowych wywoływanych przez określony stan
- Konfigurowanie zachowania wszystkich grup monitorów

Aby skonfigurować wszystkie alarmy, należy:

1. Kliknąć .
Zostanie wyświetlone okno dialogowe **Ustawienia alarmu**.
2. Wprowadzić odpowiednie ustawienia.
 - ▶ Kliknąć **OK**.

Więcej informacji o różnych polach znajduje się w Pomocy ekranowej wybranego okna programu.

Patrz

- Okno dialogowe Ustawienia alarmowe, Strona 311

25.12

Konfigurowanie dla alarmu czasów trwania okresu przed i po wystąpieniu alarmu

Aby skonfigurować ustawienia czasów trwania okresu przed i po wystąpieniu alarmu, potrzebna jest kamera obsługująca funkcję ANR z oprogramowaniem układowym w wersji 5.90 lub nowszym.

Okno główne > **Kamery i zapis** > 

- ▶ Kliknij żądaną kamerę, aby włączyć funkcję **ANR**.

Okno główne > **Zdarzenia**

- ▶ Skonfiguruj żądane zdarzenie dla aktywowanej kamery ANR.

Okno główne > **Alarmy**

1. Skonfiguruj alarm dla tego zdarzenia.

2. Wybierz  lub .

3. W kolumnie **Opcje alarmu** kliknij ...

Pojawi się okno dialogowe **Opcje alarmu**.

4. W kolumnie **Tryb** zaznacz pole wyboru włączonej kamery ANR, aby włączyć zapis alarmowy. Pole wyboru w kolumnie **Odmienne ustawienia czasu trwania alarmów** zostanie zaznaczone automatycznie.
5. Kliknij kartę **Odmienne ustawienia czasu trwania alarmów**.
6. Skonfiguruj odpowiednio czas trwania alarmu.

Patrz

- Okno dialogowe Opcje alarmu, Strona 313

25.13

Wyzwalanie zapisu alarmowego za pomocą danych tekstowych

Okno główne > **Alarmy**

Zapis alarmowy można wyzwoić za pomocą danych tekstowych.

Przed skonfigurowaniem alarmu należy skonfigurować zdarzenie, które zawiera te dane tekstowe.

Przykład: **Zdarzenia** > w drzewie zdarzeń wybierz element  (muszą być dostępne dane tekstowe, np.: **Urządzenia z czytnikiem kart** > **Czytnik kart** > **Karta odrzucona**)



Uwaga!

Dla wybranego zdarzenia ustaw czas opóźnienia aktywacji na 0.

Dzięki temu żadne dane tekstowe nie zostaną utracone.

Aby skonfigurować zapis alarmowy:

1. Wybrać alarm w drzewie, na przykład **Urządzenia interfejsu do ATM/POS-Bridge** > **Wejście ATM** > **Wejście danych**.
Pojawi się odpowiednia tabela konfiguracji alarmów.
2. Wprowadzić żądane zmiany.
3. W kolumnie **Opcje alarmu** kliknąć ... w komórce, aby wyświetlić okno dialogowe **Opcje alarmu**.
4. Kliknąć kartę **Kamery** i kliknąć, aby zaznaczyć pole wyboru **Tryb**.

Patrz

- Okno dialogowe Opcje alarmu, Strona 313
- Okno dialogowe Zapis danych tekstowych, Strona 309

25.14

Dodawanie danych tekstowych do zapisu ciągłego

Okno główne > **Zdarzenia** > w drzewie zdarzeń wybierz element  **Wejście danych** (muszą być dostępne dane tekstowe, np.: **Urządzenia z czytnikiem kart** > **Czytnik kart** > **Karta odrzucona**) > kolumna **Zapis danych tekstowych** > ...

Do zapisu ciągłego można dodawać dane tekstowe.

25.15

Ochrona zapisu alarmowego

Okno główne > **Alarmy**

Przed skonfigurowaniem alarmu należy skonfigurować zdarzenie w oknie **Zdarzenia**.

**Uwaga!**

W przypadku zabezpieczenia zapisu alarmu z kamery, chronione dane wizyjne nigdy nie zostaną automatycznie przez funkcję VRM. Należy jednak pamiętać, że zbyt wiele chronionych bloków danych może zapełnić pamięć magazynową kamery i zatrzymać nagrywanie. Ochronę danych wizyjnych należy wyłączyć ręcznie w programie Operator Client.

Aby skonfigurować zapis alarmowy:

- Wybrać alarm w drzewie, na przykład **Urządzenia interfejsu do ATM/POS-Bridge > Wejście ATM > Wejście danych**.
Pojawi się odpowiednia tabela konfiguracji alarmów.
- Wprowadzić żądane zmiany.
- W kolumnie **Opcje alarmu** kliknąć ... w komórce, aby wyświetlić okno dialogowe **Opcje alarmu**.
- Kliknąć kartę **Kamery** i kliknąć, aby zaznaczyć pole wyboru **Tryb**.
- Zaznaczyć pole wyboru **Chroń zapis**.

Patrz

- Okno dialogowe **Opcje alarmu**, Strona 313

25.16**Konfigurowanie migających miejsc aktywnych****Uwaga!**

Migające miejsce aktywne można skonfigurować wyłącznie dla zdarzenia LUB alarmu.

Okno główne > **Zdarzenia**

LUB

Okno główne > **Alarmy**

Dla każdego zdarzenia  lub alarmu można skonfigurować kolor tła i zachowanie (miganie lub jego brak) miejsc aktywnych. Można np. skonfigurować alarm zdarzenie urządzenia , którego ikona na mapie zacznie migać, gdy stan urządzenia ulegnie zmianie.

Można ponadto konfigurować priorytet wyświetlania poszczególnych miejsc aktywnych. Jest to niezbędne, jeśli dla tego samego urządzenia występują różne zdarzenia. (1 = najwyższy priorytet) Skonfigurowany kolor zachowuje ważność w przypadku wszystkich miejsc aktywnych o identycznym priorytecie wyświetlania. Można zmieniać kolor, zachowanie i priorytet każdego alarmu lub zdarzenia



: zmodyfikowany kolor i zmienione zachowanie obowiązują w przypadku wszystkich miejsc

aktywnych pozostałych alarmów lub zdarzeń , które mają identyczny priorytet.

Konfiguracja stanów kolorów na mapach jest możliwa tylko po zaznaczeniu opcji **Włącz zaawansowane wyświetlanie stanu (kolorowanie miejsc aktywnych na mapach w zależności od stanu)** lub **Włącz zaawansowane wyświetlanie stanu (kolorowanie miejsc aktywnych na mapach w zależności od alarmu)** w oknie dialogowym **Opcje**.

Aby skonfigurować migające miejsce aktywne dla zdarzenia:

- Wybierz w drzewie stan zdarzenia (), np. **Nadajniki / Odbiorniki > Przekaznik nadajnika > Stan przekaznika > Przekaznik otwarty**.
Pojawi się odpowiednia tabela konfiguracji zdarzenia.

2. Kliknij przycisk **Włącz kolorowanie stanów na mapach**.
3. Wprowadź wymagany priorytet w polu **Priorytet wyświetl. na mapie**.
4. Kliknij pole **Kolor tła mapy**, aby wybrać żądany kolor.
5. W razie potrzeby kliknij przycisk **Migające**, aby włączyć miganie.

Aby skonfigurować migające miejsce aktywne dla alarmu:

Patrz rozdział *Identyfikacja alarmu*, Strona 310, strona *Alarmy*, Strona 310.



Uwaga!

Miejsce aktywne miga tylko wówczas, gdy alarm znajduje się na liście alarmów.

Ikony urządzeń na mapie będą migać w kolorze skonfigurowanym dla alarmu lub zdarzenia.

Patrz

- strona *Zdarzenia*, Strona 305
- Okno dialogowe *Opcje* (menu *Ustawienia*), Strona 120

25.17

Zdarzenia i alarmy w systemach kontroli dostępu

Dodatkowe informacje na temat zdarzeń i alarmów w systemach kontroli dostępu.

Zdarzenie żądania dostępu

Zdarzenie to pozwala operatorowi systemu BVMS ręcznie udzielać lub odmawiać dostępu danej osobie za pośrednictwem systemu kontroli dostępu. Dla danego zdarzenia można skonfigurować zapis alarmowy, zapis danych tekstowych lub informacje dodatkowe.

Zdarzenia żądania dostępu są przesyłane do systemu BVMS tylko wtedy, gdy w każdym czytniku systemu kontroli dostępu jest ustawiona opcja **Dodatkowa weryfikacja**. W przypadku konfiguracji zdarzeń w systemie BVMS zdarzenia **Zażądano dostępu** wysyłane przez czytniki zawsze wyzwalają alarm w systemie BVMS.



Uwaga!

Zaleca się ustawienie najwyższego priorytetu (1) dla alarmów **Zażądano dostępu**. Dzięki temu alarmy będą się automatycznie wyświetlać w wyskakujących okienkach i zwracać na siebie konieczną uwagę operatora.

25.18

Zdarzenia i alarmy dla programu Person Identification

Okno główne > **Zdarzenia**

Dodatkowe informacje o zdarzeniach i alarmach dla programu Person Identification.

Wykryto nieautoryzowaną osobę

Dla każdej kamery można określić, które grupy osób mają prawo i zakaz dostępu do konkretnego obszaru.

Uwaga: Grupy autoryzowanych i nieautoryzowanych osób można konfigurować tylko pod warunkiem posiadania uprawnienia **Zmień ustawienia zdarzenia**.

Aby skonfigurować zdarzenie Wykryto nieautoryzowaną osobę

1. Zaznaczyć odpowiednią kamerę w obszarze **Video Analytics**.
2. Zaznaczyć zdarzenie **Wykryto nieautoryzowaną osobę**.
3. Wybrać kartę **Wykryto nieautoryzowaną osobę**.

4. Kliknąć przycisk ... w komórce **Nieautoryzowane** lub **Upoważniony**.
Zostanie wyświetlone okno dialogowe **Autoryzacja w kamerze**.
5. Przeciągnąć i upuścić skonfigurowane grupy osób do odpowiednich pól.
6. Kliknąć przycisk **OK**.
W odnośnej kamerze skonfigurowane grupy osób będą teraz ustawione jako autoryzowane lub nieautoryzowane.

26

strona Grupy użytkowników

**Uwaga!**

Program BVMS Viewer zapewnia tylko podstawowe funkcje. Funkcje zaawansowane udostępnia program BVMS Professional. Aby uzyskać szczegółowe informacje na temat różnych wersji systemu BVMS, należy odwiedzić witrynę www.boschsecurity.com i zobaczyć skrócony poradnik wyboru systemu BVMS: [Skrócony poradnik wyboru systemu BVMS](#).

Okno główne > Grupy użytkowników

Umożliwia konfigurowanie grup użytkowników, Enterprise User Groups i Dostępu Enterprise.

Domyślnie dostępne są następujące grupy użytkowników:

- **Grupa administratorów** (z jednym użytkownikiem admin).

Mapowanie Identity provider (IdP)

Umożliwia mapowanie grup IdP na grupy użytkowników BVMS.

Grupy podwójnej autoryzacji i grupy użytkowników przypisane do par logowania nie są objęte mapowaniem.

Uwaga: Ta sama grupa IdP nie może być mapowana wiele razy.

Aby zmapować grupy IdP na grupy użytkowników BVMS, należy:

1. Kliknąć **Dodaj**.
Zostanie wyświetlone okno dialogowe **Dodaj/Edytuj skojarzone grupy IdP**.
2. Wprowadzić nazwę i wartość oświadczenia, a następnie kliknąć **Dodaj**.
Niezbędne dane można uzyskać od zewnętrznego dostawcy tożsamości.
Uwaga: W polach *** Nazwa roszczenia** i *** Wartość roszczenia** rozróżniana jest wielkość liter.
3. Kliknąć przycisk **OK**, aby zapisać zmiany.
4. Jeżeli użytkownik należy do kilku zmapowanych grup, kolejność na liście określa kolejność wybierania grupy użytkowników BVMS. Kolejność można dostosować za pomocą przycisków góra/dół.



5. Kliknij , aby uaktywnić konfigurację.

Karta Grupy użytkowników

Należy ją kliknąć, aby wyświetlić dostępne strony umożliwiające konfigurację uprawnień standardowej grupy użytkowników.

Karta Enterprise User Groups

Należy ją kliknąć, aby wyświetlić dostępne strony umożliwiające konfigurację uprawnień grupy Enterprise User Group.

Karta Dostęp Enterprise

Należy ją kliknąć, aby wyświetlić dostępne strony umożliwiające dodanie i konfigurację dostępu Enterprise Access.

Opcje użytkownika / grupy użytkowników

Ikona	Opis
	Kliknij, aby usunąć wybraną pozycję.
	Kliknij, aby dodać nową grupę lub konto.

Ikona	Opis
	Należy kliknąć, aby dodać nowego użytkownika do wybranej grupy użytkowników. W razie potrzeby można zmienić domyślną nazwę użytkownika.
	Kliknij, aby dodać nową grupę podwójnej autoryzacji.
	Należy kliknąć, aby dodać nową parę logowania dla podwójnej autoryzacji.
	Wyświetla okno dialogowe kopiowania uprawnień z wybranej grupy użytkowników do innej grupy użytkowników.
	Należy kliknąć, aby wyświetlić dostępną stronę umożliwiającą konfigurację właściwości użytkownika.
	Należy kliknąć, aby wyświetlić dostępną stronę umożliwiającą konfigurację właściwości pary logowania.
	Należy kliknąć, aby wyświetlić dostępne strony umożliwiające konfigurację uprawnień grupy podwójnej autoryzacji.

Aktywacja zmian nazwy użytkownika i hasła



Kliknij, aby uaktywnić zmiany hasła.



Kliknij, aby uaktywnić zmiany nazwy użytkownika.



Uwaga!

Zmiany nazwy użytkownika i hasła są odwracane po cofnięciu konfiguracji.

Uprawnienia w systemie Enterprise System

Dla systemu Enterprise System można skonfigurować następujące uprawnienia:

- Uprawnienia dotyczące obsługi programu Operator Client, od których zależy interfejs obsługi systemu Enterprise System, na przykład interfejs użytkownika monitora alarmowego. Należy użyć grupy użytkowników Enterprise User Group. Konfigurację należy przeprowadzić na serwerze Enterprise Management Server.
- Uprawnienia dotyczące urządzeń, które powinny być dostępne do korzystania z serwera Enterprise Management Server, są definiowane na każdym serwerze Management Server. Użyj kont Enterprise Accounts. Konfigurację należy przeprowadzić na każdym serwerze Management Server.

Uprawnienia na pojedynczym serwerze Management Server

W celu zarządzania dostępem do jednego serwera Management Servers należy użyć standardowej grupy użytkowników. Wszystkie uprawnienia są konfigurowane na tym serwerze Management Server w tej grupie użytkowników.

Dla standardowych grup użytkowników i dla grup Enterprise User Groups można skonfigurować grupy użytkowników podwójnej autoryzacji.

Typ	Zawiera	Dostępne ustawienia konfiguracyjne	Gdzie jest konfigurowana?
Grupa użytkowników	Użytkownicy	– Uprawnienia do obsługi i uprawnienia dotyczące urządzeń	– Management Server
Enterprise User Group	Użytkownicy	– Uprawnienia dotyczące obsługi – Dla każdego serwera Management Server: nazwy odpowiednich kont dostępowych Enterprise z poświadczeniami logowania	– Enterprise Management Server
Enterprise Account	-	– Uprawnienia dotyczące urządzeń – Klucz konta	– Management Server
Grupa użytkowników podwójnej autoryzacji	Grupy użytkowników	– Zobacz grupy użytkowników	– Zobacz grupy użytkowników
Podwójna autoryzacja Enterprise	Enterprise User Groups	– Patrz Enterprise User Groups	– Patrz Enterprise User Groups

Aby wyszukać elementy:

- ▶ W polu wyszukiwania wpisz ciąg znaków i naciśnij przycisk ENTER aby przefiltrować wyświetlone elementy.
Pojawią się tylko elementy zawierające łańcuch i odpowiadające im elementy nadrzędne (tylko w drzewach). Zostanie podana liczba odfiltrowanych elementów oraz całkowita liczba elementów.
- Uwaga:** ciąg znaków należy otoczyć cudzysłowem, aby znaleźć go precyzyjnie. Na przykład wpisanie "Camera 1" odfiltruje kamery o tej nazwie, a nie camera 201.

26.1

strona Właściwości grupy użytkowników

Okno główne > **Grupy użytkowników** > karta **Grupy użytkowników** >  > karta **Uprawnienia do obsługi** > karta **Właściwości grupy użytkowników**
lub

Okno główne > **Grupy użytkowników** > karta **Enterprise User Groups** >  > karta **Uprawnienia do obsługi** > karta **Właściwości grupy użytkowników**

Funkcja ta umożliwia skonfigurowanie następujących ustawień dla wybranej grupy użytkowników:

- Harmonogram logowania
- Wybór powiązanej grupy użytkowników LDAP

Właściwości grupy użytkowników

Opis:

Wprowadzić opis grupy użytkowników.

Język

Wybierz język programu Operator Client.

Harmonogram logowania

Wybrać harmonogram zadań lub zapisu. Użytkownicy wybranej grupy mogą logować się do systemu tylko w czasie zdefiniowanym przez ten harmonogram.

Właściwości LDAP

Szukaj grup

Kliknąć, aby wyświetlić dostępne powiązane grupy użytkowników LDAP na liście **Przypisana grupa LDAP**. Aby wybrać powiązaną grupę LDAP, w oknie dialogowym **Ustawienia serwera LDAP** należy wprowadzić odpowiednie ustawienia.

Przypisana grupa LDAP

Wybrać grupę LDAP z listy **Przypisana grupa LDAP**, której użytkownik chce używać w systemie.

Patrz

- Wybieranie skojarzonej grupy LDAP, Strona 357
- Przypisywanie grupy LDAP, Strona 117
- Konfiguracja uprawnień logowania użytkownika, Strona 357

26.2

strona Właściwości użytkowników

Okno główne > **Grupy użytkowników** > **Grupy użytkowników** karta



lub

Okno główne > **Grupy użytkowników** > karta **Enterprise User Groups**



Umożliwia skonfigurowanie nowego użytkownika w standardowej grupie użytkowników lub w grupie użytkowników Enterprise User Group.

W przypadku zmiany hasła użytkownika, który jest zalogowany, lub usunięcia takiego użytkownika, użytkownik ten może kontynuować pracę z programem Operator Client. Jeśli po zmianie hasła lub usunięciu użytkownika nastąpi przerwanie połączenia z serwerem Management Server (na przykład po uaktywnieniu konfiguracji), taki użytkownik nie może automatycznie połączyć się ponownie z serwerem Management Server bez wylogowania/zalogowania w programie Operator Client.

Konto jest włączone

Zaznaczenie tego pola wyboru pozwala aktywować konto.

Uwaga: Każde nowe konto użytkownika jest domyślnie wyłączone. Aby można było aktywować konto użytkownika, należy najpierw ustawić mu hasło.

Pełna nazwa

Wprowadź pełną nazwę użytkownika.

Opis

Wprowadzić opis użytkownika.

Przy następnym logowaniu użytkownik musi zmienić hasło

Zaznaczenie tego pola wyboru spowoduje wymuszenie na użytkownikach ustawiania nowego hasła podczas następnego logowania.

Wprowadź nowe hasło

Wprowadź hasło dla nowego użytkownika.

Potwierdź hasło

Wprowadzić ponownie nowe hasło.

**Uwaga!**

Aby uaktywnić zmiany wprowadzone w tym oknie dialogowym, kliknij ikonę .

**Uwaga!**

Zaleca się przypisać określone hasło do wszystkich nowych użytkowników i wymusić zmianę hasła przez użytkownika przy logowaniu.

**Uwaga!**

Klienci Web Client, aplikacji Bosch iOS oraz klienci SDK nie mogą zmienić hasła przy logowaniu.

Zastosuj

Kliknąć, aby zastosować ustawienia.



Kliknąć , aby uaktywnić hasło.

Informacje dodatkowe

Po uaktualnieniu systemu BVMS do wersji 9.0.0.x ustawienia **Właściwości użytkowników** są następujące:

- Opcja **Konto jest włączone** jest ustawiona.
- Opcja **Przy następnym logowaniu użytkownik musi zmienić hasło** nie jest ustawiona.

26.3

strona Właściwości pary logowania

Okno główne > Grupy użytkowników > karta Grupy użytkowników > Nowa grupa podwójnej

autoryzacji >

lub

Okno główne > Grupy użytkowników > karta Enterprise User Groups > Nowa grupa

podwójnej autoryzacji Enterprise >

Umożliwia przekształcenie pary grup użytkowników w grupę podwójnej autoryzacji. Użytkownicy pierwszej grupy użytkowników są tymi, którzy muszą się zalogować w pierwszym oknie logowania; użytkownicy z drugiej grupy użytkowników potwierdzają logowanie.

Wybierz parę logowania

Na każdej liście zaznaczyć grupę użytkowników.

Wymuszaj podwójną autoryzację

Zaznaczyć pole wyboru, aby każdy użytkownik logował się tylko razem z użytkownikiem z drugiej grupy użytkowników.

**Uwaga!**

Użytkownicy należący do grupy podwójnej autoryzacji nie mogą logować się do Operator Client za pomocą funkcji logowania jednokrotnego.

Patrz

– Dodawanie pary logowania do grupy podwójnej autoryzacji, Strona 355

26.4**strona Uprawnienia kamery****Uwaga!**

Program BVMS Viewer zapewnia tylko podstawowe funkcje. Funkcje zaawansowane udostępnia program BVMS Professional. Aby uzyskać szczegółowe informacje na temat różnych wersji systemu BVMS, należy odwiedzić witrynę www.boschsecurity.com i zobaczyć skrócony poradnik wyboru systemu BVMS: [Skrócony poradnik wyboru systemu BVMS](#).

Okno główne > **Grupy użytkowników** > karta **Grupy użytkowników** >  > karta **Uprawnienia urządzenia** > karta **Uprawnienia kamery**
lub

Okno główne > **Grupy użytkowników** > karta **Dostęp Enterprise** >  > karta **Uprawnienia urządzenia** > karta **Uprawnienia kamery**

Umożliwia skonfigurowanie uprawnień dostępu do funkcji wybranej kamery lub do grupy kamer dla wybranej grupy użytkowników.

Jeśli zostaną dodane nowe komponenty, uprawnienia kamer muszą zostać skonfigurowane po ich instalacji.

Dostęp do kamery można anulować na stronie **Kamera**.

Kamera

Wyświetla nazwę kamery skonfigurowaną na stronie **Kamery i zapis**.

Lokalizacja

Wyświetla lokalizację kamery skonfigurowaną na stronie **Mapy i struktura**.

Dostęp

Zaznaczyć pole wyboru, aby umożliwić dostęp do kamery.

Obraz bieżący

Zaznaczyć pole wyboru, aby umożliwić wyświetlanie obrazu bieżącego.

Dźwięk bieżący

Zaznaczyć pole wyboru, aby umożliwić odtwarzanie fonii na żywo.

Nagrywanie ręczne

To pole wyboru należy zaznaczyć, aby uaktywnić funkcję zapisu alarmowego uruchamianego ręcznie. Użytkownik może zaznaczyć to pole wyboru lub usunąć jego zaznaczenie tylko wtedy, gdy na stronie **Funkcje operatora** uaktywniono funkcję zapisu alarmowego uruchamianego ręcznie.

Odtwarzaj obraz

To pole wyboru należy zaznaczyć, aby umożliwić odtwarzanie obrazu.

Użytkownik może zaznaczyć to pole wyboru lub usunąć jego zaznaczenie tylko wtedy, gdy na stronie **Funkcje operatora** uaktywniono funkcję odtwarzania.

Odtwarzaj dźwięk

Zaznaczyć pole wyboru, aby umożliwić odtwarzanie dźwięku.

Użytkownik może zaznaczyć to pole wyboru lub usunąć jego zaznaczenie tylko wtedy, gdy na stronie **Funkcje operatora** uaktywniono funkcję odtwarzania.

Dane tekstowe

Zaznaczyć pole wyboru, aby umożliwić wyświetlanie metadanych.

Użytkownik może zaznaczyć to pole wyboru lub usunąć jego zaznaczenie tylko wtedy, gdy na stronie **Funkcje operatora** uaktywniono opcję wyświetlania metadanych.

Eksport

To pole wyboru należy zaznaczyć, aby uaktywnić funkcję eksportowania danych wizyjnych.

Użytkownik może zaznaczyć to pole wyboru lub usunąć jego zaznaczenie tylko wtedy, gdy na stronie **Funkcje operatora** uaktywniono opcję eksportowania danych wizyjnych.

PTZ/ROI

Zaznacz pole wyboru, aby zezwolić na obsługę PTZ lub ROI tej kamery.

Użytkownik może zaznaczyć to pole wyboru lub usunąć jego zaznaczenie tylko wtedy, gdy na stronie **Funkcje operatora** uaktywniono opcję sterowania funkcjami PTZ lub ROI kamery. Ponadto należy skonfigurować funkcje PTZ lub ROI w tabeli kamery.

Aux

Zaznaczyć pole wyboru, aby umożliwić wykonywanie funkcji dodatkowych.

Użytkownik może zaznaczyć to pole wyboru lub usunąć jego zaznaczenie tylko wtedy, gdy na stronie **Funkcje operatora** uaktywniono opcję sterowania funkcjami PTZ kamery.

Ustaw zdefiniowane pozycje

To pole wyboru należy zaznaczyć, aby umożliwić użytkownikowi ustawienie zaprogramowanych położeń dla kamery PTZ.

Można także ustawić wstępne położenie obszaru zainteresowania (ROI), jeśli ta funkcja jest włączona i autoryzowana.

Użytkownik może zaznaczyć to pole wyboru lub usunąć jego zaznaczenie tylko wtedy, gdy na stronie **Funkcje operatora** uaktywniono opcję sterowania funkcjami PTZ kamery.

Obraz odniesienia

Zaznaczyć pole wyboru, aby umożliwić aktualizację obrazu odniesienia tej kamery.

Privacy overlay

Zaznacz pole wyboru, aby włączyć opcję Privacy overlay dla tej kamery w trybie podglądu na żywo i odtwarzania.

26.5

Strona Priorytetu sterowania

Okno główne > **Grupy użytkowników** > karta **Grupy użytkowników** >  > karta **Uprawnienia urządzenia** > karta **Priorytetu sterowania**
lub

Okno główne > **Grupy użytkowników** > karta **Dostęp Enterprise** >  > karta **Uprawnienia urządzenia** > karta **Priorytetu sterowania**

Priorytety sterowania

Aby zmniejszyć priorytet w zakresie przejmowania kontroli nad funkcjami sterowania PTZ oraz liniami połączeń urządzenia Bosch Allegiant, należy przesunąć odpowiedni suwak w prawo. Użytkownik o większych uprawnieniach może przejąć na wyłączność kontrolę nad kamerą PTZ lub nad liniami połączeń. Limit czasu dla blokady funkcji sterowania PTZ należy określić w polu **Limit czasu w min..** Ustawieniem domyślnym jest 1 minuta.

Limit czasu w min.

Należy tu określić limit czasu (w minutach).

Patrz

– Konfigurowanie różnych priorytetów, Strona 359

26.6

Okno dialogowe Kopiuj uprawnienia grupy użytkowników

Okno główne > **Grupy użytkowników** > karta **Grupy użytkowników**  > 
LUB

Okno główne > **Grupy użytkowników** > karta **Enterprise User Groups**  > 

Umożliwia wybranie uprawnień grupy użytkowników w celu skopiowania do wybranych grup użytkowników.

Kopiuj z:

Wyświetla wybraną grupę użytkowników. Jej uprawnienia zostaną skopiowane do innej grupy użytkowników.

Ustawienia do skopiowania

Zaznaczyć pole wyboru, aby wybrać żądane uprawnienia grupy użytkowników do skopiowania.

Kopiuj do:

Zaznaczyć pole wyboru, aby określić grupę użytkowników, do której będą skopiowane uprawnienia wybranej grupy użytkowników.

Patrz

– Kopiowanie uprawnień grupy użytkowników, Strona 361

26.7

strona Uprawnienia odbiornika

Okno główne > **Grupy użytkowników** > **Grupy użytkowników** karta >  > **Uprawnienia urządzenia** karta > **Uprawnienia - odbiorniki** karta
lub

Okno główne > **Grupy użytkowników** > **Dostęp Enterprise** karta >  > **Uprawnienia urządzenia** karta > **Uprawnienia - odbiorniki** karta

Umożliwia skonfigurowanie odbiorników, do których mają dostęp użytkownicy z tej grupy.

Odbiornik

Wyświetla dostępne odbiorniki.

Zaznaczyć pole wyboru, aby nadać grupie użytkowników dostęp do odbiornika.

Grupa monitorów

Zaznaczanie tego pola wyboru pozwala udzielić użytkownikom z wybranej grupy użytkowników dostępu do tej grupy monitorów.

26.8 strona Zdarzenia i alarmy

Okno główne > **Grupy użytkowników** > karta **Grupy użytkowników** >  > karta **Uprawnienia urządzenia** > karta **Zdarzenia i alarmy**
lub

Okno główne > **Grupy użytkowników** > karta **Dostęp Enterprise** >  > karta **Uprawnienia urządzenia** > karta **Zdarzenia i alarmy**

Umożliwia skonfigurowanie uprawnień do drzewa zdarzeń, na przykład użytkownik może wskazać zdarzenia, do użycia których grupa użytkowników ma mieć uprawnienia lub nie.

Nie można zmienić tych ustawień dla domyślnej grupy użytkowników.

Dla każdego zdarzenia jest co najmniej jedno urządzenie. Na przykład dla zdarzenia **Zanik sygnału wizyjnego** urządzeniami są dostępne kamery. Dla zdarzenia typu **Tworzenie kopii zapasowej zakończone**, odpowiednim urządzeniem jest **Sterowana czasem kopia bezpieczeństwa**.

Urządzeniem może być proces programowy.

1. Rozwiń element drzewa i kliknij żądane pola wyboru, aby włączyć zdarzenia. W kolumnie **Dostęp** zaznacz pole wyboru urządzenia, aby włączyć zdarzenia z tego urządzenia. Dostęp do urządzeń jest konfigurowany na stronie **Kamera** oraz stronie **Uprawnienia kamery**.
2. Aby jednocześnie włączyć lub wyłączyć wszystkie zdarzenia, zaznacz lub usuń zaznaczenie pola wyboru **Zdarzenia i alarmy**.

26.9 Strona Dane uwierzytelniające

Okno główne > **Grupy użytkowników** > karta **Dostęp Enterprise** >  > karta **Uprawnienia urządzenia** > karta **Poświadczenia**

Dane uwierzytelniające konta Enterprise Account są konfigurowane na serwerze Management Server. Użytkownik konfiguruje Dostęp Enterprise na każdym serwerze Management Server, który jest częścią systemu Enterprise System. Serwer Enterprise Management Server używa tych danych uwierzytelniających w celu przyznania dostępu do urządzeń danego serwera Management Server użytkownikowi programu Operator Client, który loguje się jako użytkownik grupy użytkowników Enterprise User Group.

Opis:

Wprowadź opis żadanego konta Enterprise Account.

Zasady silnych kluczy

Pole wyboru **Zasady silnych kluczy** jest wstępnie zaznaczone dla wszystkich nowo utworzonych grup użytkowników.

Zalecamy zachować to ustawienie w celu zwiększenia ochrony przed nieautoryzowanym dostępem komputera.

Mają zastosowanie następujące reguły:

- Minimalna długość klucza skonfigurowana na stronie **Zasady konta** dla grupy użytkowników.
- Nie należy używać jednego z poprzednich kluczy.
- Należy zastosować co najmniej jedną dużą literę (od A do Z).
- Należy zastosować co najmniej jedną cyfrę (od 0 do 9).
- Należy zastosować co najmniej jeden znak specjalny (np. !) \$ # %).

Wprowadź nowy klucz: / Potwierdź klucz:

Wprowadź i potwierdź klucz dla tego serwera Management Server.

Patrz

– Tworzenie konta Enterprise Account, Strona 353

26.10**strona Drzewo logiczne**

Okno główne > **Grupy użytkowników** > karta **Grupy użytkowników** >  > karta **Uprawnienia urządzenia** > karta **Drzewo logiczne** karta lub

Okno główne > **Grupy użytkowników** > **Dostęp Enterprise** karta >  > **Uprawnienia urządzenia** karta > **Drzewo logiczne** karta

Umożliwia skonfigurowanie okna Drzewo logiczne dla każdej grupy użytkowników.

Aby skonfigurować uprawnienia:

- ▶ Zaznacz lub usuń zaznaczenie w odpowiednich polach wyboru.
Zaznaczenie elementu poniżej węzła powoduje automatyczne zaznaczenie tego węzła.
Zaznaczenie węzła powoduje automatyczne zaznaczenie wszystkich elementów poniżej.

Kamera

Zaznaczyć pole wyboru, aby nadać użytkownikom wybranej grupy użytkowników dostęp do odpowiednich urządzeń.

Dostęp do kamery można anulować na stronie **Uprawnienia kamery**.

Grupa monitorów

Zaznaczanie tego pola wyboru pozwala udzielić użytkownikom z wybranej grupy użytkowników dostępu do tej grupy monitorów.

Patrz

– Konfigurowanie uprawnień dla urządzenia, Strona 358

26.11**Strona funkcji operatora**

Okno główne > **Grupy użytkowników** > karta **Grupy użytkowników** >  > karta **Uprawnienia do obsługi** > karta **Funkcje operatora** lub

Okno główne > **Grupy użytkowników** > karta **Enterprise User Groups** >  > karta **Uprawnienia do obsługi** > karta **Funkcje operatora**

Umożliwia skonfigurowanie różnych uprawnień dla wybranej grupy użytkowników.

Sterowanie funkcjami PTZ kamer kopułkowych

Zaznaczyć to pole wyboru, aby umożliwić sterowanie kamerą.

Strona **Priorytety sterowania**: w polu **Priorytety sterowania** można określić priorytet dla funkcji przejmowania kontroli nad kamerą.

Linie połączeń Allegiant

Zaznacz to pole wyboru, aby umożliwić dostęp do linii połączeń urządzenia Bosch Allegiant.

Strona **Priorytety sterowania**: w polu **Priorytety sterowania** można określić priorytet dla funkcji przejmowania kontroli nad liniami połączeń urządzenia Bosch Allegiant.

Drukuj i zapisz

Zaznaczenie tego pola wyboru umożliwia drukowanie i zapisywanie obrazów wideo, map i dokumentów.

Wyświetlanie alarmu

Zaznaczyć pole wyboru, aby umożliwić wyświetlanie alarmów. W przypadku wybrania tej opcji jednocześnie wyłączane jest **Przetwarzanie alarmów**.

Przetwarzanie alarmów

Zaznaczyć pole wyboru, aby umożliwić przetwarzanie alarmów.

Przerwij działanie wygaszacza ekranu systemu Windows w razie wystąpienia alarmu

W przypadku zaznaczenia tego pola wyboru komunikat o alarmie będzie wyświetlany nawet w sytuacji, gdy aktywny jest wygaszacz ekranu. Opcja ta zostanie zignorowana, jeśli warunkiem wyłączenia wygaszacza ekranu jest podanie nazwy użytkownika i hasła.

Włączanie/wyłączanie analizy zawartości obrazu (Video Analysis)

Zaznaczyć pole wyboru, aby umożliwić użytkownikom wybranej grupy włączanie / wyłączanie analizy zawartości obrazu.

Odtwarzanie

To pole wyboru należy zaznaczyć, aby umożliwić korzystanie z różnych funkcji odtwarzania.

Eksportuj wideo

To pole wyboru należy zaznaczyć, aby umożliwić eksportowanie danych wizyjnych.

Eksportuj do formatów niemacierzystych

Zaznaczyć pole wyboru, aby zezwolić na eksportowanie danych wideo do formatu nie natywnego.

Chroń wideo

Zaznaczyć pole wyboru, aby umożliwić ochronę danych wizyjnych.

Anuluj ochronę wideo

Zaznaczenie tego pola wyboru umożliwia zabezpieczanie i odbezpieczanie danych wizyjnych.

Ogranicz wideo (ograniczone wideo jest widoczne tylko dla użytkowników posiadających to uprawnienie)

To pole wyboru należy zaznaczyć, aby umożliwić ograniczanie dostępu do danych wizyjnych.

Anuluj ograniczenie wideo

Zaznaczenie tego pola wyboru umożliwia narzucanie i anulowanie ograniczeń dostępu do danych wizyjnych.

Uwaga!

VRM

W razie potrzeby można skonfigurować uprawnienia użytkownika do zastrzegania i zdejmowania zastrzeżenia danych wizyjnych w systemie BVMS.

Tylko użytkownik posiadający uprawnienie **Ogranicz wideo (ograniczone wideo jest widoczne tylko dla użytkowników posiadających to uprawnienie)** widzi zastrzeżony materiał wizyjny na skali czasu w programie Operator Client. W przeciwnym zastrzeżony zakres czasu jest wyświetlany z adnotacją **Brak zapisu**.



**Uwaga!****DIVAR AN**

W razie potrzeby należy skonfigurować uprawnienia użytkownika do zastrzegania i zdejmowania zastrzeżenia danych wizyjnych na urządzeniu DIVAR AN. Należy utworzyć konto użytkownika w systemie BVMS z identycznymi danymi uwierzytelniającymi i skonfigurować odpowiednio uprawnienia do zastrzegania i zdejmowania zastrzeżenia danych wizyjnych.

Nie wpływa to na wyświetlanie danych wizyjnych o ograniczonym dostępie i trzeba je skonfigurować osobno na urządzeniu DIVAR AN.

Usuń obraz

Zaznaczyć pole wyboru, aby umożliwić usuwanie danych wizyjnych.

Dostęp do wideo, które zostały nagrane w czasie, kiedy ta grupa użytkowników nie była upoważniona do zalogowania

Zaznaczyć pole wyboru, aby umożliwić dostęp do opisanych danych wizyjnych.

Dostęp do Rejestru

Zaznaczyć pole wyboru, aby umożliwić dostęp do rejestru.

Wymaż dane tekstowe z rejestru (służy do usuwania informacji związanych z osobami)

Zaznaczyć to pole wyboru, aby zezwolić na kasowanie danych tekstowych z wpisów rejestru.

Przyciski zdarzeń operatora

Zaznaczyć pole wyboru, aby uaktywnić przyciski zdarzeń użytkownika w oprogramowaniu Operator Client.

Zamknij Operator Client

Zaznaczyć pole wyboru, aby umożliwić zamknięcie oprogramowania Operator Client.

Minimalizuj Operator Client

To pole wyboru należy zaznaczyć, aby umożliwić minimalizowanie okna programu Operator Client.

Interkom foniczny

Zaznaczyć pole wyboru, aby umożliwić użytkownikowi rozmowę przez głośniki nadajnika z funkcją wejścia i wyjścia fonicznego.

Zapis alarmowy uruchamiany ręcznie

To pole wyboru należy zaznaczyć, aby uaktywnić funkcję zapisu alarmowego uruchamianego ręcznie.

Ustaw obraz odniesienia

Należy zaznaczyć to pole wyboru, aby umożliwić aktualizację obrazu odniesienia w Operator Client.

Ustaw wybór obszaru dla obrazu odniesienia

Zaznaczyć pole wyboru, aby umożliwić zaznaczanie obszaru na obrazie z kamery w celu aktualizacji obrazu odniesienia w module Operator Client.

Zmień hasło

Zaznacz to pole wyboru, aby umożliwić użytkownikowi programu Operator Client zmianę hasła logowania.

Uzbrój obszary centrali alarmowej

To pole wyboru należy zaznaczyć, aby umożliwić użytkownikowi programu Operator Client uzbrajanie obszarów skonfigurowanych w centrali alarmowej, która wchodzi w skład konfiguracji systemu BVMS.

Wymuś uzbrojenie obszarów centrali alarmowej

To pole wyboru należy zaznaczyć, aby umożliwić użytkownikowi programu Operator Client wymuszanie uzbrajania obszarów skonfigurowanych w centrali alarmowej, która wchodzi w skład konfiguracji systemu BVMS.

Rozbrój obszary centrali alarmowej

To pole wyboru należy zaznaczyć, aby umożliwić użytkownikowi programu Operator Client rozbrajanie obszarów skonfigurowanych w centrali alarmowej, która wchodzi w skład konfiguracji systemu BVMS.

Wycisz dzwonki dla obszarów centrali alarmowej

To pole wyboru należy zaznaczyć, aby umożliwić użytkownikowi programu Operator Client wyłączanie syren alarmowych w obszarach skonfigurowanych w centrali alarmowej, która wchodzi w skład konfiguracji systemu BVMS.

Pomiń punkty centrali alarmowej

To pole wyboru należy zaznaczyć, aby umożliwić użytkownikowi programu Operator Client zmianę stanu punktu skonfigurowanego w centrali alarmowej na stan **Punkt pominięty**. Punkt pomijany nie może wysyłać alarmu. Po przywróceniu stanu **Punkt niepominięty** oczekujący alarm jest wysyłany, o ile nadal jest dostępny.

Odblokuj drzwi centrali alarmowej

To pole wyboru należy zaznaczyć, aby umożliwić użytkownikowi programu Operator Client odblokowanie drzwi skonfigurowanych w centrali alarmowej.

Zabezpiecz i cofnij zabezpieczenie drzwi centrali alarmowej

To pole wyboru należy zaznaczyć, aby umożliwić użytkownikowi programu Operator Client uzbrajanie i rozbrajanie drzwi skonfigurowanych w centrali alarmowej.

Cykl drzwi centrali alarmowej

To pole wyboru należy zaznaczyć, aby umożliwić użytkownikowi programu Operator Client uruchamianie drzwi skonfigurowanych w centrali alarmowej.

Przestaw drzwi KD

Zaznaczyć pole wyboru, aby zezwolić użytkownikowi Operator Client na dostęp do stanu drzwi (uzbrojone, zablokowane, odblokowywane).

Zadecyduj o dostępie

Zaznaczyć to pole wyboru, aby pozwolić użytkownikowi aplikacji Operator Client podejmować decyzje o dostępie.

Zarządzanie osobami

Zaznaczyć to pole wyboru, aby zezwolić użytkownikowi Operator Client na zarządzanie osobami do obsługi alarmów Person Identification.

Resetuj poziom zagrożenia

Zaznaczyć to pole wyboru, aby pozwolić użytkownikowi aplikacji Operator Client na resetowanie poziomu zagrożenia, jeśli aplikacja Operator Client znajduje się w trybie poziomu zagrożenia.

Importowanie/eksportowanie ulubionych i zakładek

Zaznaczyć to pole wyboru, aby pozwolić użytkownikowi aplikacji Operator Client na importowanie i eksportowanie elementów ulubionych i zakładek.

Kolejność wyświetlania w przypadku tego samego priorytetu alarmu

Wybierz odpowiednią wartość, aby skonfigurować kolejność okienek obrazów alarmowych w oknie Wyświetlanie alarmu programu Operator Client.

Czas przewijania do tyłu odtwarzania natychmiastowego:

Wprowadzić liczbę sekund dla alarmu odtwarzania natychmiastowego.

Powtarzanie dźwięku alarmu:

Zaznacz pole wyboru i wprowadź liczbę sekund, po których dźwięk alarmu jest powtarzany.

Ogranicz dostęp do zapisanych obrazów do ostatnich n minut:

Zaznacz pole wyboru, aby ograniczyć dostęp do zapisanych obrazów.

Z listy wybierz żadaną liczbę minut.

Wymuś automatyczne wylogowanie operatora po tym czasie braku aktywności:

Zaznacz to pole wyboru, aby włączyć automatyczne wylogowanie z programu Operator Client po czasie wybranym w ustawieniach.

Patrz

– Wylogowanie w przypadku braku aktywności, Strona 43

26.12

strona Priorytety

Okno główne > Grupy użytkowników > karta Grupy użytkowników >  > karta Uprawnienia do obsługi > karta Priorytety
LUB

Okno główne > Grupy użytkowników > karta Enterprise User Groups >  > karta Uprawnienia do obsługi > karta Priorytety

Umożliwia takie skonfigurowanie blokady funkcji sterowania PTZ, aby obowiązywała tylko przez określony czas. Można też określić priorytety dla funkcji sterowania PTZ i wyświetlania alarmów przychodzących.

Automatyczne zachowanie okna podręcznego

Przesunąć suwak, aby regulować wartość priorytetu Okna obrazu podglądu bieżącego lub Okna obrazu odtwarzania. Wartość ta jest wymagana dla przychodzących alarmów, aby system mógł zdecydować, czy alarm jest automatycznie wyświetlany w oknie Obrazów alarmowych.

Na przykład: Jeśli dla okna obrazu w trybie podglądu bieżącego suwak zostanie przesunięty na 50, dla okna obrazu w trybie odtwarzania na 70, a przychodzący alarm ma priorytet 60, alarm jest wyświetlany automatycznie tylko wtedy, jeśli okno obrazu w trybie odtwarzania jest aktywne. Alarm nie jest wyświetlany automatycznie, jeśli aktywne jest okno obrazu w trybie podglądu bieżącego.

Patrz

– Konfigurowanie różnych priorytetów, Strona 359

26.13

strona Interfejs użytkownika

Okno główne > Grupy użytkowników > karta Grupy użytkowników >  > karta Uprawnienia do obsługi > karta Interfejs użytkownika
lub

Okno główne > Grupy użytkowników > karta Enterprise User Groups >  > karta Uprawnienia do obsługi > karta Interfejs użytkownika

Umożliwia skonfigurowanie interfejsu 4 monitorów używanego przez program Operator Client. Można skonfigurować tryb wielomonitorowy obejmujący do 4 monitorów. W przypadku każdego monitora ustawia się wyświetlaną treść, np. Monitor 2 wyświetla tylko okienka obrazu podglądu bieżącego, a Monitor 1 i Monitor 2 wykorzystują format obrazu 16:9 dla kamer HD.

Monitor sterowania

Pozwala wybrać monitor, który ma być używany jako monitor sterowania.

Maks. liczba wierszy okienek obrazu podczas odtwarzania

Pozwala wybrać maksymalną liczbę wierszy w okienkach obrazów wyświetlanych w oknie Odtwarzanie obrazów na monitorze sterowania.

Monitor alarmowy

Pozwala wybrać monitor alarmowy, który może obsługiwać tryb podglądu bieżącego i tryb alarmowy lub tylko tryb alarmowy.

Monitor 1–4

Zaznacz wymaganą opcję na listach odpowiadających poszczególnym monitorom.

- W przypadku monitora sterowania opcja **Sterowanie** jest wstępnie wybrana i nie można jej zmienić.
- Dla monitora alarmowego można wybrać jedną z poniższych opcji:
 - **Zawartość wideo podglądu bieżącego i alarmowego**
 - **Zawartość tylko alarmów**
- W przypadku pozostałych monitorów można wybrać jedną z poniższych opcji:
 - **Wideo tylko podglądu bieżącego**
 - **Mapa i dokument**
 - **Dwie mapy i dokument**
 - **Wideo pełnoekranowego podglądu bieżącego**
 - **Obraz Quad podglądu bieżącego**

Maks. liczba wierszy okienek obrazu

Pozwala wybrać maksymalną liczbę wierszy w okienkach obrazów wyświetlanych w oknie obrazu na odpowiednim monitorze.

Uwaga: ta opcja jest dostępna tylko dla następujących widoków:

- **Sterowanie**
- **Zawartość tylko alarmów**
- **Zawartość wideo podglądu bieżącego i alarmowego**
- **Wideo tylko podglądu bieżącego**

Pozostałe widoki mają stały układ posiadający stałą liczbę wierszy okienek obrazów i nie można ich zmieniać.

Format okienek obrazu

Dla każdego monitora wybierz wymagany format obrazu dla początkowego uruchomienia Operator Client. Dla kamer HD zastosować format 16:9.

Przywróć ustawienia domyślne

Kliknij, aby przywrócić ustawienia domyślne na tej stronie. Wszystkim opcjom na liście zostaną przywrócone ustawienia domyślne.

26.14

Strona Dostęp do serwera

Okno główne > **Grupy użytkowników** > karta **Enterprise User Groups** >  > karta **Dostęp do serwera**

Dostęp do serwera jest konfigurowany na serwerze Enterprise Management Server.

Należy wprowadzić nazwę konta Enterprise Account oraz hasło dla każdego serwera Management Server należącego do systemu Enterprise System. To konto jest skonfigurowane na każdym serwerze Management Server.

Management Server

Wyświetla nazwę serwera Management Server, który został skonfigurowany na tym serwerze Enterprise Management Server.

Adres sieciowy

Podaje prywatny adres IP lub nazwę DNS serwera Management Server.

Numer serwera

Podaje numer serwera Management Server. Klawiatura Bosch IntuiKey wykorzystuje ten numer do wybrania żądanego serwera Management Server.

Dostęp

Zaznacz to pole wyboru, aby przyznać dostęp do serwera Management Server. Ten serwer Management Server stanie się teraz serwerem Enterprise Management Server.

Enterprise Account

Wpisać nazwę konta Enterprise Account, które zostało skonfigurowane na danym serwerze Management Server.

Uwierzytelnianie

W oknie dialogowym **Ustawienia uwierzytelniania** zaznaczyć odpowiednią opcję uwierzytelniania.

Interfejs API konfiguracji

Zaznaczyć pole wyboru, jeśli token dostępu ma zezwalać na dostęp do usługi Interfejs API konfiguracji w programie Management Server.

Opis serwera

Umożliwia wyświetlanie opisu danego serwera.

Dalsze kolumny są widoczne, jeśli zostały dodane do listy serwerów.

Patrz

- Tworzenie grupy lub konta, Strona 352
- Tworzenie Enterprise System, Strona 85
- Konfigurowanie funkcji listy serwerów dla systemu Enterprise System, Strona 85
- Uwierzytelnianie za pomocą tokenów, Strona 87

26.15

Strona Konfigurowanie uprawnień

**Uwaga!**

W niniejszym dokumencie opisano niektóre funkcje, które nie są dostępne w programie BVMS Viewer.

Szczegółowe informacje na temat poszczególnych wersji systemu BVMS znajdują się na stronie www.boschsecurity.com oraz w Skróconym poradniku wyboru systemu BVMS: [Skrócony poradnik wyboru systemu BVMS](#).

Okno główne > **Grupy użytkowników** > karta **Grupy użytkowników** >  > karta **Uprawnienia do obsługi** > karta **Uprawnienia konfiguracji**
LUB

Okno główne > **Grupy użytkowników** > karta **Enterprise User Groups** >  > karta **Uprawnienia do obsługi** > karta **Uprawnienia konfiguracji**
Umożliwia skonfigurowanie uprawnień różnych użytkowników dla programu Configuration Client.

Drzewo urządzeń

W tej sekcji można określić uprawnienia na stronie **Urządzenia**. Zaznacz pole wyboru przy odpowiednim uprawnieniu.

Mapy i struktura

W tej sekcji można określić uprawnienia na stronie **Mapy i struktura**. Zaznacz pole wyboru przy odpowiednim uprawnieniu.

Harmonogramy

W tej sekcji można określić uprawnienia na stronie **Harmonogramy**. Zaznacz pole wyboru przy odpowiednim uprawnieniu.

Kamery i zapis

W tej sekcji można określić uprawnienia na stronie **Kamery i zapis**. Zaznacz pole wyboru przy odpowiednim uprawnieniu.

Zdarzenia

W tej sekcji można określić uprawnienia na stronie **Zdarzenia**. Zaznacz pole wyboru przy odpowiednim uprawnieniu.

Alarmy

W tej sekcji można określić uprawnienia na stronie **Alarmy**. Zaznacz pole wyboru przy odpowiednim uprawnieniu.

Grupy użytkowników

W tej sekcji można określić uprawnienia do konfigurowania grup użytkowników. Zaznacz pole wyboru przy odpowiednim uprawnieniu.

**Uwaga!**

Ze względów bezpieczeństwa pola wyboru **Konfiguruj grupy użytkowników/Enterprise Accounts**, **Konfiguruj użytkowników** i **Konfiguruj użytkowników Enterprise** wzajemnie się wykluczają.

**Uwaga!**

Po przypisaniu uprawnień **Konfiguruj użytkowników** i **Konfiguruj użytkowników Enterprise** na stronie **Uprawnienia grupy użytkowników** należy przypisać grupy użytkowników, w których nowi użytkownicy mogą być dodawani i konfigurowani.

Audit Trail

W tej sekcji można określić, czy użytkownik ma prawo korzystać z funkcji Audit Trail oraz eksportować dane z funkcji Audit Trail.

Zaznacz pole wyboru przy odpowiednim uprawnieniu.

Polecenia menu

W tej sekcji można określić uprawnienia do konfigurowania poleceń menu. Zaznacz pole wyboru przy odpowiednim uprawnieniu.

Raporty

W tej sekcji można określić uprawnienia do konfigurowania raportów. Zaznacz pole wyboru przy odpowiednim uprawnieniu.

**Uwaga!**

Jeśli chcesz skorzystać z usługi Interfejs API konfiguracji Management Server, musisz wybrać opcje

Uprawnienia konfiguracji:

- Zmień właściwości urządzenia
- Wywołaj menedżera uaktywnienia

**Uwaga!**

W celu skonfigurowania ustawień w obszarze **Ustawienia zaufanych certyfikatów** trzeba zaznaczyć uprawnienie **Konfiguruj grupy użytkowników/Enterprise Accounts**.

26.16 Strona Uprawnienia grup użytkowników

Okno główne > **Grupy użytkowników** > karta **Grupy użytkowników** >  > karta **Uprawnienia do obsługi** > karta **Uprawnienia grupy użytkowników**
LUB

Okno główne > **Grupy użytkowników** > karta **Enterprise User Groups** >  > karta **Uprawnienia do obsługi** > karta **Uprawnienia grupy użytkowników**

Umożliwia przypisanie grup użytkowników, do których użytkownicy należący do konkretnej grupy użytkowników mogą dodawać nowych użytkowników.



Uwaga!

Uprawnienia do grupy użytkowników można przypisać wyłącznie grupie użytkowników, której uprzednio przypisano uprawnienia do konfigurowania użytkowników. Uprawnienia te przypisuje się na stronie **Uprawnienia konfiguracji**.



Uwaga!

Użytkownicy należący do grupy użytkowników standardowych nie mogą dodawać nowych użytkowników do grupy administratorów. To pole wyboru jest nieaktywne.

Patrz

– Strona Konfigurowanie uprawnień, Strona 343

26.17 Strona zasad kont

Okno główne > **Grupy użytkowników** > karta **Grupy użytkowników** >  > karta **Bezpieczeństwo** > karta **Zasady konta**
lub

Okno główne > **Grupy użytkowników** > karta **Enterprise User Groups** >  > karta **Bezpieczeństwo** > karta **Zasady konta**

Umożliwia skonfigurowanie ustawień dla użytkowników i haseł.

Zasady silnych haseł

Zaznacz to pole wyboru, aby włączyć politykę haseł.

Aby uzyskać więcej informacji, patrz *Konfigurowanie użytkowników, uprawnień i dostępu Enterprise*, Strona 351.



Uwaga!

Ustawienie **Zasady silnych haseł** dotyczy użytkowników tylko wówczas, gdy to pole wyboru jest zaznaczone w odpowiedniej grupie użytkowników.
Zalecamy zachować to ustawienie w celu zwiększenia ochrony przed nieautoryzowanym dostępem komputera.

Minimalna długość hasła

To ustawienie określa minimalną liczbę znaków, jaką musi zawierać hasło do konta użytkownika.
Zaznacz pole wyboru, aby włączyć to ustawienie i wprowadzić minimalną liczbę znaków.

Maksymalny wiek hasła w dniach

To ustawienie określa okres czasu (w dniach), przez jaki można używać hasła, zanim system zażąda od użytkownika jego zmiany.

Zaznacz pole wyboru, aby włączyć to ustawienie i wprowadzić maksymalną liczbę dni.

Liczba używanych haseł w historii

To ustawienie określa liczbę niepowtarzalnych nowych haseł, jakie muszą zostać powiązane z kontem użytkownika, zanim będzie można ponownie użyć starego hasła.

Zaznacz pole wyboru, aby włączyć to ustawienie i wprowadzić minimalną liczbę haseł.

Maksymalna liczba prób nieprawidłowego logowania

To ustawienie określa wyłączenie konta po określonej liczbie nieprawidłowych prób logowania.

Zaznacz pole wyboru, aby włączyć to ustawienie i wprowadzić maksymalną liczbę prób.

Jeśli pole wyboru **Maksymalna liczba prób nieprawidłowego logowania** jest zaznaczone, możesz określić następujące dwa ustawienia:

Czas trwania blokady konta

To ustawienie określa, przez ile minut wyłączone konto pozostaje wyłączone, zanim zostanie automatycznie włączone.

Zaznacz pole wyboru, aby włączyć to ustawienie i wprowadzić liczbę minut.

Resetuj licznik blokad konta po

To ustawienie określa, ile minut musi upłynąć od chwili błędnego logowania, zanim licznik błędnego logowania zostanie wyzerowany.

Zaznacz pole wyboru, aby włączyć to ustawienie i wprowadzić liczbę minut.

**Uwaga!**

Jeśli maksymalna liczba nieprawidłowych prób logowania przekroczy określony próg, konto jest wyłączone.

Jeśli pole **Czas trwania blokady konta** nie jest zaznaczone, konto musi zostać wyłączone ręcznie.

Jeśli pole wyboru **Czas trwania blokady konta** jest zaznaczone, konto automatycznie zostaje włączone po określonym czasie.

**Uwaga!**

Licznik nieprawidłowych prób logowania jest zerowany:

Po pomyślnym zalogowaniu.

Lub po określonym czasie, jeśli pole wyboru **Resetuj licznik blokad konta po** jest zaznaczone.

Wyłącz klienta offline

Zaznaczenie tego pola wyboru pozwala wyłączyć funkcję logowania do klienta w trybie offline.

Informacje dodatkowe

W przypadku systemu BVMS począwszy od wersji 9.0 domyślnie zastosowanie mają następujące ustawienia **Zasady konta**:

- Pole wyboru **Zasady silnych haseł** jest wstępnie zaznaczone.
- Pole wyboru **Minimalna długość hasła** jest wstępnie zaznaczone. Wartość domyślna wynosi 10.
- Pole wyboru **Maksymalny wiek hasła w dniach** wstępnie nie jest zaznaczone. Wartość domyślna wynosi 90.
- Pole wyboru **Liczba używanych haseł w historii** wstępnie nie jest zaznaczone. Wartość domyślna wynosi 10.
- Pole wyboru **Maksymalna liczba prób nieprawidłowego logowania** wstępnie nie jest zaznaczone. Wartość domyślna wynosi 1.
- Pole wyboru **Wyłącz klienta offline** wstępnie nie jest zaznaczone.

Od wersji BVMS 10.0.1 poniższe ustawienia **Zasady konta** są wybierane domyślnie dla wszystkich grup użytkowników:

- **Maksymalna liczba prób nieprawidłowego logowania**
- **Czas trwania blokady konta**
- **Resetuj licznik blokad konta po**

26.17.1

Tryb offline programu Operator Client

W trybie offline można korzystać z programu Operator Client w następujące sposoby:

- Program Operator Client obsługuje podgląd na żywo, odtwarzanie i eksportowanie bez połączenia z serwerem Management Server.
- Jeśli stacja robocza miała już wcześniej nawiązane połączenie z serwerem Management Server, każdy użytkownik może zawsze zalogować się za jej pośrednictwem w trybie offline.

Tryb offline wymaga systemu BVMS w wersji 3.0 lub nowszej.

Nawet jeśli stacja robocza z programem Operator Client nie ma połączenia z serwerem Management Server, można nadal kontynuować pracę. Są wtedy dostępne niektóre główne funkcje, np. podgląd na żywo i odtwarzanie materiału wideo.

Począwszy od wersji 5.5 systemu BVMS stacja robocza z programem Operator Client może działać offline z użyciem konfiguracji systemu BVMS w wersji 5.0.5.



Uwaga!

Po zmianie hasła na serwerze Management Server w okresie, kiedy aplikacja Operator Client jest w trybie offline, nie zostanie ono propagowane do tej wersji aplikacji Operator Client.

Gdy aplikacja Operator Client działa w trybie online, użytkownik musi zalogować się przy użyciu nowego hasła.

Gdy aplikacja Operator Client działa w trybie offline, użytkownik musi zalogować się przy użyciu starego hasła. Zmiana zostanie wprowadzona dopiero po aktywowaniu nowej konfiguracji i przesłaniu jej do stacji roboczej aplikacji Operator Client.



Uwaga!

W przypadku wywołania kamery na wyświetlacz w grupie monitorów ze stacją roboczą i klawiaturą Bosch Intuikey, gdy stacja robocza jest offline, klawiatura nie wyśle dźwięku błędu.

26.17.1.1

Praca w trybie offline

Gdy program Operator Client nie ma połączenia z serwerem Management Server, w oknie Drzewo



logiczne na serwerze Management Server wyświetlana jest odpowiednia ikona nakładki. Można kontynuować pracę z programem Operator Client nawet jeśli rozłączenie trwa dłużej, ale niektóre funkcje nie są dostępne.

W przypadku ponownego ustanowienia połączenia z serwerem Management Server zostanie wyświetlona odpowiednia ikona nakładki.

Jeśli w serwerze Management Server została aktywowana nowa konfiguracja, na Drzewie logicznym ikony tego serwera Management Server zostanie wyświetlona odpowiednia ikona i na kilka sekund zostanie wyświetlone okno dialogowe. Należy zaakceptować lub odrzucić nową konfigurację.

Jeśli program Operator Client jest skonfigurowany w taki sposób, aby w określonym momencie nastąpiło wylogowanie, to wylogowanie będzie miało miejsce nawet wtedy, gdy w danym momencie nie będzie ponownie ustanowione połączenie z serwerem Management Server.

Kiedy użytkownik programu Operator Client zaloguje się za pomocą funkcji Server Lookup w trybie offline, zostanie wyświetlona lista serwerów dostępna przy ostatnim udanym logowaniu. Tryb offline oznacza w tym przypadku, że stacja robocza z programem Operator Client nie ma połączenia sieciowego z serwerem zawierającym listę serwerów.

Funkcje niedostępne przy braku połączenia

Gdy program Operator Client nie ma połączenie z serwerem Management Server, następujące funkcje są niedostępne:

- Lista alarmów:
Obejmuje to obsługę alarmów. Lista alarmów jest pusta i zostaje automatycznie zapełniona po ponownym nawiązaniu połączenia.
- System Allegiant:
Obsługa linii połączeń jest niedostępna. W starszych wersjach zanik obsługi linii połączeń powodował automatyczne zamykanie widoku z kamer Allegiant i wyświetlanie okna z odpowiednim komunikatem. W systemie BVMS w wersji 3.0 będzie pojawiać się bardziej przyjazne okienko obrazu z informacją o tymczasowym braku możliwości wyświetlania obrazu z danej kamery.
- MG:
Nie można przeciągać kamer na element sterujący MG. Jest on wyłączony i zostaje automatycznie włączony po ponownym nawiązaniu połączenia.
- Priorytety PTZ:
Bez połączenia z serwerem Management Server program Operator Client działający w trybie offline może nawiązać połączenie z kamerą PTZ, o ile nie jest ona zablokowana. Priorytety kamery kopułkowej zostają automatycznie zaktualizowane po ponownym nawiązaniu połączenia.
- Wejście:
Nie można przełączać wejść.
- Rejestr:
Rejestr jest niedostępny i nie można go otworzyć. Otwarte okno wyszukiwania w rejestrze nie zostanie automatycznie zamknięte. Można używać dotychczasowych wyników wyszukiwania i je eksportować.
- Pakiet Operator Client SDK:
Nie można przetwarzać funkcji pakietu Operator Client SDK z użyciem interfejsu IServerApi. Tworzenie interfejsu RemoteClientApi jest niemożliwe.
Nie działają niektóre metody dostępne tylko na poziomie interfejsu API programu klienckiego, np. ApplicationManager (należy w zamian użyć metody GetUserName()).
- Zmiana hasła:
Operator nie może zmieniać swojego hasła.
- Przekaznik:
Nie można przełączać przekazników.
- Skrypt serwera:
Następujące metody serwera z interfejsu IServerApi będą wprawdzie przetwarzane, ale nie można ich wysyłać do programu klienckiego:
 - AlarmManager
 - AnalogMonitorManager
 - CameraManager
 - CompoundEventManager
 - DecoderManager
 - DeviceManager
 - DomeCameraManager

- EventManager
- InputManager
- LicenseManager
- Rejestr
- MatrixManager
- RecorderManager
- RelayManager
- ScheduleManager
- SendManager
- SequenceManager
- VirtualInputManager
- Nakładki stanu:
Nie są dostępne żadne nakładki stanu kamer, wejść ani przekaźników.

Nakładka stanu urządzenia

Stany urządzeń (kropka zapisu, obraz zbyt zaszumiony, obraz zbyt ciemny...) są przetwarzane przez serwer Management Server. Przy braku połączenia między komputerem klienckim a serwerem aktualizowanie stanów na komputerze klienckim jest niemożliwe. Nowa nakładka stanu będzie zawierać informację wizualną sygnalizującą, że obecnie wszystkie stany urządzeń są niedostępne. Gdy komputer kliencki odzyska połączenie z serwerem, nakładki stanu zostaną automatycznie zaktualizowane.

-  Stan nieznany.
Nakładka stanu urządzenia wyświetlana w oknie Drzewo logiczne lub na mapie, gdy komputer kliencki nie ma połączenia z serwerem Management Server.

Przyczyny braku połączenia

Możliwe przyczyny braku połączenia między komputerem z programem Operator Client a serwerem Management Server:

- Uszkodzenie połączenia fizycznego.
- Hasło zalogowanego użytkownika zostało zmienione podczas działania w trybie offline.
- Podczas gdy dany komputer z programem Operator Client działał w trybie offline, serwer Management Server przyznał licencję przechodnią stacji roboczej innemu komputerowi z programem Operator Client działającemu w trybie online.
- Program Operator Client i oprogramowanie serwera Management Server różnią się wersjami (dotyczy oprogramowania serwera Management Server w wersjach starszych niż 5.5).

26.18

Uprawnienia do logowania na stronie typu aplikacji

Okno główne > Grupy użytkowników > karta Grupy użytkowników >  > karta Uprawnienia do aplikacji > karta Uprawnienia logowania zależnie od typu aplikacji
LUB

Okno główne > Grupy użytkowników > karta Enterprise User Groups >  > karta Uprawnienia do aplikacji > karta Uprawnienia logowania zależnie od typu aplikacji

Umożliwia skonfigurowanie różnych uprawnień użytkowników dla różnych aplikacji.

Operator Client lub Cameo SDK (bezpośrednio do serwera Management Server)

Zaznacz to pole wyboru, aby umożliwić bezpośrednie logowanie do serwera Management Server w aplikacji Operator Client lub do aplikacji Cameo SDK.

Operator Client (do lokalizacji Unmanaged Site)

Zaznacz pole wyboru, aby umożliwić logowanie do aplikacji Operator Client przez połączenie z unmanaged site.

Configuration Client

Zaznacz to pole wyboru, aby zezwolić na logowanie do aplikacji Configuration Client.

Interfejs API konfigurowania

Zaznacz to pole wyboru, aby zezwolić na logowanie do aplikacji **Interfejs API konfigurowania**.

Dostęp mobilny przez oprogramowanie Video Security Client

Zaznacz to pole wyboru, aby zezwolić na dostęp mobilny z aplikacji Video Security Client.

Zestaw SDK / interfejs API serwera programu BVMS

Zaznacz to pole wyboru, aby zezwolić na logowanie do aplikacji SDK serwera BVMS.

BVMS Client SDK (umożliwia łączność z aplikacją Operator Client)

Zaznacz to pole wyboru, aby zezwolić niektórym grupom użytkowników na logowanie do aplikacji SDK klienta.

26.19

Strona ustawień zarządzania zagrożeniami

Okno główne > **Grupy użytkowników** > karta **Grupy użytkowników** >  > karta **Zarządzanie zagrożeniami** > karta **Ustawienia**

Umożliwia skonfigurowanie, czy członkostwo w grupie powinno zmieniać się stosownie do różnych poziomów zagrożenia.

Uwaga: w przypadku alarmu o poziomie zagrożenia aktualny użytkownik Operator Client zostaje wylogowany, a aplikacja Operator Client zrestartuje się. Użytkownik musi ponownie zalogować się do aplikacji Operator Client w trybie poziomu zagrożenia. W zależności od konfiguracji grupy użytkowników odpowiedni użytkownik otrzyma uprawnienia skonfigurowanej grupy użytkowników właściwe dla aktywnego poziomu zagrożenia.

Aby skonfigurować poziom zagrożenia dla grupy użytkowników:

1. Wybierz odpowiednią grupę użytkowników.
2. W odpowiednim menu rozwijanym poziomu zagrożenia wybierz grupę użytkowników, która powinna być aktywna na tym poziomie zagrożenia.

27

Konfigurowanie użytkowników, uprawnień i dostępu Enterprise

**Uwaga!**

Program BVMS Viewer zapewnia tylko podstawowe funkcje. Funkcje zaawansowane udostępnia program BVMS Professional. Aby uzyskać szczegółowe informacje na temat różnych wersji systemu BVMS, należy odwiedzić witrynę www.boschsecurity.com i zobaczyć skrócony poradnik wyboru systemu BVMS: [Skrócony poradnik wyboru systemu BVMS](#).

Okno główne > Grupy użytkowników

Ten rozdział zawiera informacje na temat sposobu konfigurowania grup użytkowników, grup użytkowników Enterprise User Group i dostępu Enterprise.

Wszystkie uprawnienia dotyczące urządzeń i obsługi konfiguruje się dla grup użytkowników, a nie dla pojedynczego użytkownika.

Mają zastosowanie następujące reguły:

- Użytkownik BVMS może być członkiem tylko jednej grupy użytkowników BVMS lub Enterprise User Group. Użytkownik LDAP może być członkiem kilku grup użytkowników LDAP.
- Nie można zmienić ustawień domyślnej grupy użytkowników.
- Ta grupa użytkowników ma dostęp do wszystkich urządzeń z całego drzewa logicznego oraz jest przypisana do harmonogramu **Zawsze**.
- Do dostępu do grup użytkowników domeny Windows służą grupy LDAP.

- Kliknij , aby zapisać ustawienia.

- Kliknij , aby cofnąć ostatnią zmianę.

- Kliknij , aby uaktywnić konfigurację.

Zasady silnych haseł

Aby ułatwić ochronę komputera przed nieautoryzowanym dostępem, zaleca się używanie silnych haseł do kont użytkowników.

W związku z tym polityka silnych haseł jest domyślnie włączona dla wszystkich nowo utworzonych grup użytkowników. Dotyczy to grupy użytkowników będących administratorami, a także grup użytkowników standardowych, grup użytkowników Enterprise i Dostępu Enterprise.

Mają zastosowanie następujące reguły:

- Minimalna długość hasła dla grupy użytkowników jest skonfigurowana na stronie **Zasady konta**.
- Nie należy używać jednego z poprzedniej haseł.
- Należy zastosować co najmniej jedną dużą literę (od A do Z).
- Należy zastosować co najmniej jedną cyfrę (od 0 do 9).
- Należy zastosować co najmniej jeden znak specjalny (np. !, \$, #, %).

Przy pierwszym uruchomieniu programu Configuration Client przez użytkownika-administrатора, zostanie wyświetlone okno dialogowe **Naruszono politykę haseł** z prośbą o ustawienie hasła dla konta użytkownika administratora. Bezwzględnie zaleca się zachowanie tego ustawienia i ustawienie dla konta użytkownika administratora silnego hasła, zgodnego z zasadami polityki haseł.

Podczas tworzenia nowych grup użytkowników w programie Configuration Client ustawienie polityki silnych haseł jest domyślnie włączone. Jeśli hasła dla nowych kont użytkowników odpowiedniej grupy użytkowników nie zostaną ustawione, nie będzie można aktywować konfiguracji. Zostanie wyświetlone okno dialogowe **Naruszono politykę haseł** zawierające wszystkich użytkowników, dla których nie ustawiono hasła.

Aby aktywować konfigurację, ustaw brakujące hasła.

Patrz

- Strona zasad kont, Strona 345
- strona Właściwości grupy użytkowników, Strona 330
- strona Właściwości użytkowników, Strona 331
- strona Właściwości pary logowania, Strona 332
- strona Uprawnienia kamery, Strona 333
- Strona Priorytety sterowania, Strona 334
- Okno dialogowe Kopiuj uprawnienia grupy użytkowników, Strona 335
- strona Uprawnienia odbiornika, Strona 335
- strona Zdarzenia i alarmy, Strona 336
- Okno dialogowe Ustawienia serwera LDAP (menu Ustawienia), Strona 116
- Strona Dane uwierzytelniające, Strona 336
- strona Drzewo logiczne, Strona 337
- Strona funkcji operatora, Strona 337
- strona Priorytety, Strona 341
- strona Interfejs użytkownika, Strona 341
- Strona Dostęp do serwera, Strona 342

27.1 Tworzenie grupy lub konta

Okno główne > **Grupy użytkowników**

Można utworzyć standardową grupę użytkowników, grupę Enterprise User Group lub konto Enterprise Account.

Aby dostosować uprawnienia grupy użytkowników do własnych potrzeb, należy utworzyć nową grupę użytkowników i zmienić jej ustawienia.

27.1.1 Tworzenie grupy użytkowników standardowych

Okno główne > **Grupy użytkowników**

Aby utworzyć grupę użytkowników standardowych:

1. Kliknij kartę **Grupy użytkowników**.
2. Kliknij .
Zostanie wyświetlone okno dialogowe **Nowa grupa użytkowników**.
3. Wpisz nazwę i opis.
4. Kliknij przycisk **OK**.
Nowa grupa zostanie dodana do odpowiedniego drzewa.
5. Kliknij nową grupę użytkowników prawym przyciskiem myszy i kliknij pozycję **Zmień nazwę**.
6. Wpisz żądaną nazwę i naciśnij klawisz ENTER.

Patrz

- strona Właściwości grupy użytkowników, Strona 330
- Strona funkcji operatora, Strona 337
- strona Priorytety, Strona 341
- strona Interfejs użytkownika, Strona 341

27.1.2 Tworzenie grupy Enterprise User Group

Okno główne > **Grupy użytkowników**

Użytkownik wykonuje zadanie polegające na utworzeniu konta Enterprise User Group dla Enterprise System na serwerze Enterprise Management Server.

Celem utworzenia grupy użytkowników Enterprise User Group wraz z użytkownikami jest skonfigurowanie ich uprawnień dotyczących obsługi. Te uprawnienia dotyczące obsługi są dostępne w aplikacji Operator Client, która jest połączona z serwerem zarządzającym Enterprise Management Server. Przykładem uprawnienia dotyczącego obsługi jest interfejs użytkownika monitora alarmowego.

Aby utworzyć grupę Enterprise User Group:

1. Kliknij kartę **Enterprise User Groups**.
Uwaga: Karta **Enterprise User Groups** jest dostępna tylko wówczas, gdy występuje odpowiednia licencja oraz co najmniej jeden komputer z serwerem Management Server został skonfigurowany w oknie **Urządzenia > System Enterprise > Lista serwerów/książka adresowa**.
2. Kliknij .
Zostanie wyświetlone okno dialogowe **Nowa grupa użytkowników Enterprise User Group**.
3. Wpisz nazwę i opis.
4. Kliknij przycisk **OK**.
Grupa Enterprise User Group zostanie dodana do odpowiedniego drzewa.
5. Kliknij nową grupę Enterprise prawym przyciskiem myszy i kliknij pozycję **Zmień nazwę**.
6. Wpisz żadaną nazwę i naciśnij klawisz ENTER.
7. Na stronie **Uprawnienia do obsługi** skonfiguruj według potrzeb uprawnienia dotyczące obsługi oraz dostęp do serwera dla skonfigurowanych komputerów typu Management Server.

Patrz

- strona *Właściwości grupy użytkowników*, Strona 330
- *Strona funkcji operatora*, Strona 337
- strona *Priorytety*, Strona 341
- strona *Interfejs użytkownika*, Strona 341
- *Strona Dostęp do serwera*, Strona 342

27.1.3

Tworzenie konta Enterprise Account

Okno główne > Grupy użytkowników



Uwaga!

Przed dodaniem Enterprise Account należy skonfigurować co najmniej jedno urządzenie w Drzewie urządzeń.

Użytkownik wykonuje zadanie polegające na utworzeniu konta Enterprise Account na serwerze Management Server. Należy powtórzyć to zadanie dla każdego serwera Management Server, który jest częścią systemu Enterprise System.

Celem utworzenia konta Enterprise Account jest skonfigurowanie uprawnień dotyczących urządzeń dla aplikacji Operator Client korzystającej z systemu Enterprise System.

Aby utworzyć grupę Enterprise Account:

1. Kliknąć kartę **Dostęp Enterprise**.
2. Kliknąć .
Zostanie wyświetlone okno dialogowe **Nowe konto Enterprise Account**.
3. Wpisać nazwę i opis.

4. Pole wyboru **Przy następnym logowaniu użytkownik musi zmienić hasło** jest wstępnie zaznaczone dla wszystkich nowo utworzonych kont użytkowników.
Wpisać klucz z zachowaniem zasad polityki kluczy, a następnie go potwierdzić.
5. Kliknąć przycisk **OK**.
Nowe konto Enterprise Account zostanie dodane do odpowiedniego drzewa.
6. Kliknąć prawym przyciskiem myszy nowe konto Enterprise Account, a następnie kliknąć opcję **Zmień nazwę**.
7. Wpisać żadaną nazwę i naciśnij klawisz ENTER.
8. Na stronie **Uprawnienia urządzenia** skonfigurować według wymagań dane uwierzytelniające oraz uprawnienia urządzeń.

Patrz

- Zasady silnych haseł, Strona 351
- Strona Dane uwierzytelniające, Strona 336
- strona Drzewo logiczne, Strona 337
- strona Zdarzenia i alarmy, Strona 336
- Strona Priorytety sterowania, Strona 334
- strona Uprawnienia kamery, Strona 333
- strona Uprawnienia odbiornika, Strona 335

27.2

Tworzenie użytkownika

Okno główne > **Grupy użytkowników** > karta **Grupy użytkowników**>
lub

Okno główne > **Grupy użytkowników** > karta **Enterprise User Groups**

Podczas dodawania nowego użytkownika jest on przypisywany do istniejącej grupy użytkowników standardowych lub grupy Enterprise User Group.



Uwaga!

Użytkownik, który chce obsługiwać klawiaturę Bosch IntuiKey podłączoną do odbiornika, musi posiadać nazwę użytkownika złożoną tylko z cyfr oraz hasło. Nazwa użytkownika może składać się z maks. 3 cyfr, natomiast hasło może zawierać maks. 6 cyfr.

Aby utworzyć użytkownika:

1. Wybierz grupę i kliknij przycisk  lub kliknij prawym przyciskiem myszy żadaną grupę, a następnie kliknij opcję **Nowy użytkownik**.
Nowy użytkownik zostanie dodany do drzewa **Grupy użytkowników**.
2. Kliknąć nowego użytkownika prawym przyciskiem myszy i kliknąć **Zmień nazwę**.
3. Wpisać żadaną nazwę i naciśnąć klawisz ENTER.
4. Na stronie **Właściwości użytkowników** wprowadzić nazwę użytkownika oraz opis.
5. Pole wyboru **Przy następnym logowaniu użytkownik musi zmienić hasło** jest wstępnie zaznaczone dla wszystkich nowo utworzonych kont użytkowników.
Wprowadzić hasło zgodnie z zasadami polityki haseł, a następnie je potwierdzić.
6. Kliknąć przycisk **Zastosuj**, aby zastosować ustawienia.
7. Zaznaczyć pole wyboru **Konto jest włączone**, aby aktywować konto.
8. Kliknąć , aby uaktywnić hasło.
9. Kliknij , aby uaktywnić konfigurację.

Uwaga: po dodaniu nowego użytkownika zawsze trzeba aktywować konfigurację.

Patrz

- strona Właściwości użytkowników, Strona 331
- Zasady silnych haseł, Strona 351
- strona Grupy użytkowników, Strona 328

27.3

Tworzenie grupy użytkowników podwójnej autoryzacji

Okno główne > **Grupy użytkowników** > karta **Grupy użytkowników**>

lub

Okno główne > **Grupy użytkowników** > karta **Enterprise User Groups**

Można utworzyć podwójną autoryzację grupy użytkowników standardowych lub Enterprise User Group.

Podwójna autoryzacja nie jest dostępna dla dostępu Enterprise.

Użytkownik zaznacza dwie grupy użytkowników. Członkowie tych grup użytkowników są członkami nowej grupy podwójnej autoryzacji.

Aby utworzyć grupę podwójnej autoryzacji:

1. Kliknij przycisk .
Kolejno zostaną wyświetlone okna dialogowe **Nowa grupa podwójnej autoryzacji** i **Nowa grupa podwójnej autoryzacji Enterprise**.
2. Wpisać nazwę i opis.
3. Kliknąć przycisk **OK**.
Nowa grupa podwójnej autoryzacji zostanie dodana do odpowiedniego drzewa.
4. Kliknąć prawym przyciskiem myszy nową grupę podwójnej autoryzacji, a następnie opcję **Zmień nazwę**.
5. Wpisać żadaną nazwę i nacisnąć klawisz ENTER.



Uwaga!

Użytkownicy należący do grupy podwójnej autoryzacji nie mogą logować się do Operator Client za pomocą funkcji logowania jednokrotnego.

Patrz

- Dodawanie pary logowania do grupy podwójnej autoryzacji, Strona 355
- strona Właściwości grupy użytkowników, Strona 330
- Strona funkcji operatora, Strona 337
- strona Priorytety, Strona 341
- strona Interfejs użytkownika, Strona 341

27.4

Dodawanie pary logowania do grupy podwójnej autoryzacji

Okno główne > **Grupy użytkowników** > karta **Grupy użytkowników** >  **Nowa grupa podwójnej autoryzacji**

Okno główne > **Grupy użytkowników** > karta **Enterprise User Groups** >  **Nowa grupa podwójnej autoryzacji Enterprise**

Aby dodać parę logowania do grupy podwójnej autoryzacji:

1. Zaznacz żadaną grupę podwójnej autoryzacji i kliknij przycisk  lub kliknij prawym przyciskiem myszy grupę, a następnie kliknij opcję **Nowa para logowania**.
Zostanie wyświetlone odpowiednie okno dialogowe.
2. Wybierz grupę użytkowników na każdej liście.
Użytkownicy pierwszej grupy użytkowników są tymi, którzy muszą się zalogować w pierwszym oknie logowania, użytkownicy z drugiej grupy użytkowników potwierdzają logowanie.
Istnieje możliwość wybrania tej samej grupy na obydwu listach.
3. Dla każdej listy zaznaczyć pole wyboru **Wymuszaj podwójną autoryzację**, jeśli jest to wymagane.
W przypadku zaznaczenia tego pola wyboru każdy użytkownik pierwszej grupy będzie mógł zalogować się jedynie z użytkownikiem drugiej grupy.
Gdy to pole wyboru nie jest zaznaczone, każdy użytkownik pierwszej grupy może zalogować się sam, jednak posiada jedynie uprawnienia dostępu swojej grupy.
4. Kliknij przycisk **OK**.
Nowa para logowania zostanie dodana do odpowiedniej grupy podwójnej autoryzacji.
5. Kliknij prawym przyciskiem myszy nową parę logowania, a następnie kliknij opcję **Zmień nazwę**.
6. Wpisz żadaną nazwę i naciśnij klawisz ENTER.

**Uwaga!**

Użytkownicy należący do grupy podwójnej autoryzacji nie mogą logować się do Operator Client za pomocą funkcji logowania jednokrotnego.

Patrz

- Tworzenie grupy użytkowników podwójnej autoryzacji, Strona 355
- strona Właściwości pary logowania, Strona 332

27.5**Konfigurowanie grupy administratorów**

Okno główne > **Grupy użytkowników** > karta **Grupy użytkowników**  Grupa administratorów
Umożliwia dodanie nowych użytkowników o statusie administrator, zmianę ich nazwy lub usunięcie ich z Grupy administratorów.

Aby dodać nowego administratora do grupy administratorów:

1. Kliknij przycisk  lub kliknij prawym przyciskiem myszy grupę administratorów i kliknij **Dodaj nowego użytkownika**.
Nowy użytkownik o statusie administrator zostanie dodany do grupy administratorów.
2. Na stronie **Właściwości użytkowników** wprowadź nazwę użytkownika oraz opis.
3. Pole wyboru **Przy następnym logowaniu użytkownik musi zmienić hasło** jest wstępnie zaznaczone dla wszystkich nowo utworzonych kont użytkowników.
Wpisz hasło z zachowaniem zasad polityki haseł, a następnie je potwierdź.
4. Kliknij przycisk **Zastosuj**, aby zastosować ustawienia.
5. Kliknij , aby uaktywnić hasło.

Aby zmienić nazwę danego administratora:

1. Kliknij prawym przyciskiem myszy żadanego administratora i kliknij **Zmień nazwę**.
2. Wpisz żadaną nazwę i naciśnij klawisz ENTER.



3. Kliknij , aby uaktywnić zmianę nazwy użytkownika.

Aby usunąć danego administratora z grupy administratorów:

- ▶ Kliknij prawym przyciskiem myszy żądanego administratora, a następnie kliknij przycisk **Usuń**.
Użytkownik zostanie usunięty z grupy administratorów.

Uwaga:

Użytkownika o statusie administratora można usunąć z grupy administratorów tylko wtedy, gdy istnieje inny użytkownik o statusie administrator.

Jeśli w grupie administratorów znajduje się tylko jeden administrator, nie można go usunąć.

Patrz

- strona Grupy użytkowników, Strona 328
- strona Właściwości użytkowników, Strona 331
- Zasady silnych haseł , Strona 351

27.6

Wybieranie skojarzonej grupy LDAP

Okno główne > **Grupy użytkowników** > karta **Grupy użytkowników** >  > karta **Uprawnienia do obsługi** > karta **Właściwości grupy użytkowników**
lub

Okno główne > **Grupy użytkowników** > karta **Enterprise User Groups** >  > karta **Uprawnienia do obsługi** > karta **Właściwości grupy użytkowników Enterprise User Group**

Grupy LDAP są konfigurowane w standardowych grupach użytkowników lub Enterprise User Groups.

Aby wybrać skojarzoną grupę LDAP:

1. Kliknąć przycisk **Szukaj grup**.
2. Na liście **Przypisana grupa LDAP** wybrać odpowiednią grupę LDAP.

Kliknąć poniższy odnośnik do wybranego okna programu, aby uzyskać szczegółowe informacje o różnych polach.

Patrz

- Okno dialogowe Ustawienia serwera LDAP (menu Ustawienia), Strona 116
- strona Właściwości grupy użytkowników, Strona 330

27.7

Konfiguracja uprawnień logowania użytkownika

Okno główne > **Grupy użytkowników** > karta **Grupy użytkowników** >  > karta **Uprawnienia do obsługi** > karta **Właściwości grupy użytkowników**
lub

Okno główne > **Grupy użytkowników** > karta **Enterprise User Groups** >  > karta **Uprawnienia do obsługi** > karta **Właściwości grupy użytkowników Enterprise User Group**

Użytkownik może ograniczyć możliwość logowania się członków grupy użytkowników lub grupy użytkowników Enterprise User Group do swoich komputerów w określonych przedziałach czasowych. Nie można zmienić tych ustawień dla domyślnej grupy użytkowników.

Aby skonfigurować logowanie, należy:

1. Kliknąć kartę **Właściwości grupy użytkowników**.

2. Na liście **Harmonogram logowania** zaznaczyć harmonogram.

27.8

Konfigurowanie uprawnień dotyczących obsługi

Okno główne > **Grupy użytkowników** > karta **Grupy użytkowników** >  > karta **Uprawnienia do obsługi** > karta **Właściwości grupy użytkowników**
lub

Okno główne > **Grupy użytkowników** > karta **Enterprise User Groups** >  > karta **Uprawnienia do obsługi** > karta **Właściwości grupy użytkowników Enterprise User Group**

- Użytkownik może skonfigurować uprawnienia dotyczące obsługi, np. dostęp do rejestru czy ustawienia interfejsu użytkownika.
- W przypadku domyślnej grupy użytkowników nie można zmieniać tych ustawień.
- Uprawnienia dotyczące obsługi są konfigurowane w standardowych grupach użytkowników lub grupach użytkowników Enterprise User Group.

Więcej informacji o różnych polach znajduje się w Pomocy ekranowej wybranego okna programu. Kliknąć poniższy odnośnik do wybranego okna programu, aby uzyskać szczegółowe informacje o różnych polach.

Patrz

- strona *Właściwości grupy użytkowników*, Strona 330
- Strona *funkcji operatora*, Strona 337
- strona *Priorytety*, Strona 341
- strona *Interfejs użytkownika*, Strona 341
- Strona *Dostęp do serwera*, Strona 342

27.9

Konfigurowanie uprawnień dla urządzenia

Okno główne > **Grupy użytkowników** > karta **Grupy użytkowników** > karta **Uprawnienia urządzenia**
lub

Okno główne > **Grupy użytkowników** > karta **Dostęp Enterprise** > karta **Uprawnienia urządzenia**
Użytkownik może niezależnie ustawić uprawnienia dla wszystkich urządzeń w oknie *Drzewo logiczne*.

Po przesunięciu dozwolonych urządzeń do folderu, który nie jest dozwolony dla danej grupy użytkowników, należy ustawić uprawnienia dla tego folderu, aby udzielić dostępu do zawartych w nim urządzeń.

- W przypadku domyślnej grupy użytkowników nie można zmieniać tych ustawień.
- Uprawnienia dotyczące urządzeń są konfigurowane w standardowych grupach użytkowników lub na kontach Enterprise Account.

Więcej informacji o różnych polach znajduje się w Pomocy ekranowej wybranego okna programu. Kliknąć poniższy odnośnik do wybranego okna programu, aby uzyskać szczegółowe informacje o różnych polach.

Patrz

- strona *Drzewo logiczne*, Strona 337
- strona *Zdarzenia i alarmy*, Strona 336
- Strona *Priorytety sterowania*, Strona 334
- strona *Uprawnienia kamery*, Strona 333
- strona *Uprawnienia odbiornika*, Strona 335

27.10

Konfigurowanie różnych priorytetów

Problem	Możliwa przyczyna	Działanie
1. Brak dźwięku	Wzmacniacz	Sprawdzić, czy wszystkie elementy elektroniczne są włączone, trasowanie sygnału jest prawidłowe, źródło aktywne, głośność ustawiona, a żaden kanał nie jest wyciszony itp. W razie potrzeby napraw, skorygować lub wymienić elementy. Jeśli nadal nie ma dźwięku, problem może dotyczyć okablowania.
	Gniazda połączeniowe	Sprawdź, czy podłączono właściwe przewody do wzmacniacza. Odtwórz cichy sygnał przez wzmacniacz. Podłącz głośnik testowy równolegle do niesprawnej linii. Jeśli poziom dźwięku zanikł lub jest bardzo niski, linia ma zwarcie (może to być silne przetarcie, zgniecenie lub brak połączenia). Używając głośnika testowego, sprawdź kolejne połączenia i złącza wzdłuż linii, aż zlokalizujesz i usuniesz usterkę. Zachować prawidłową polaryzację.
2. Przerwany dźwięk, np. trzaski lub zniekształcenia	Uszkodzone połączenie	Sprawdź wszystkie połączenia przy wzmacniaczu i głośnikach — powinny być czyste i solidnie połączone. Jeśli problem nie ustępuje, sprawdź okablowanie. Zobacz problem 1.
3. Stały hałas, np. brzęczenie, syczenie lub buczenie	Uszkodzone źródło lub inne urządzenie elektroniczne	Jeśli hałas występuje, ale nie jest odtwarzany żaden materiał, należy kolejno sprawdzić wszystkie komponenty, by zlokalizować źródło problemu. Najprawdopodobniej nastąpiło przerwanie toru sygnałowego.
	Nieprawidłowe uziemienie systemu lub pętla masy	Sprawdź i popraw uziemienie systemu.
4. Brak dźwięku po podłączeniu mikrofonu do INPUT 1–2	Mikrofon wymaga zasilania fantomowego.	Upewnić się, że mikrofon podłączono do INPUT 1–2. Upewnić się, że w tym kanale ustawiono PHANTOM na WL . Zasilanie phantom nie jest dostępne na INPUT 3–6.
	Kanał wejściowy jest wyciszony lub poziom sygnału jest zbyt niski.	Wybrać kanał i sprawdzić, czy nie jest wyciszony. Jeśli nie jest wyciszony, stopniowo zwiększaj poziom, aż pojawi się dźwięk.
5. Dźwięk zniekształcony, przednia dioda LED jest WYŁ., ekran LCD wskazuje LIMIT	Zbyt wysoki poziom sygnału wejściowego	Zredukuj poziom sygnału wejściowego lub głośników, aby zapobiec przekroczeniu limitu.
	Nieprawidłowa struktura wzmocnienia lub przesterowane źródło sygnału (mikser/ przedwzmacniacz)	Sprawdź ustawienia poziomu sygnału źródła za pomocą wskaźnika VU na ekranie LCD. Jeśli wskaźnik VU jest pełny lub system wskazuje CLIP lub LIMIT, poziom źródła lub wejścia jest zbyt wysoki.

Problem	Możliwa przyczyna	Działanie
6. Mikrofon generuje sprzężenie akustyczne przy zwiększonym poziomie sygnału wejściowego	Nieprawidłowa struktura wzmocnienia	Zredukować poziom wejściowy mikrofonu. Ustawienie mikrofonu blisko źródła dźwięku zwiększa wzmocnienie przed sprzężeniem.
	Tryb ustawiony na MUSIC	Zmień tryb na LIVE lub SPEECH.
	Mikrofon znajduje się zbyt blisko przedniej części głośnika	W miarę możliwości ustaw głośniki za mikrofonem. Jeśli używany jest oddzielny głośnik jako monitor, należy skierować go w stronę tylnej części mikrofonu.
7. Menu DSP zablokowane	Włączono funkcję LOCK menu. Na ekranie LCD pojawia się symbol blokady.	Nacisnąć pokrętkę MASTER VOLUME lub przyciski wyboru wejścia, aby odblokować.
8. Aplikacja QuickSmart Mobile nie wykrywa głośnika	Włącz Bluetooth®	Upewnić się, że Bluetooth® jest włączony w głośniku. Android: Upewnić się, że włączono usługi lokalizacji. Usuń głośnik z ustawień urządzenia iOS/Android (czasem: „ZAPOMNIJ”). Uruchomić ponownie parowanie. >Upewnić się, że telefon/tablet ma odpowiednią wersję systemu i najnowsze aktualizacje. Upewnić się, że zainstalowano najnowszą wersję aplikacji QuickSmart Mobile. Upewnić się, że do głośnika nie jest podłączony inny telefon/tablet.
9. Nieudane odblokowanie za pomocą kodu PIN	Wprowadzono nieprawidłowy kod PIN	Spróbować ponownie wprowadzić kod PIN LUB Przytrzymać przycisk funkcyjny dla INPUT 2 i pokrętkę MASTER VOLUME przez co najmniej 15 sekund, aby zresetować głośnik do ustawień domyślnych.
10. Dźwięk zniekształcony lub przerywany podczas korzystania z QuickSmart Link	Nieprawidłowy lub zbyt długi przewód	Używać ekranowanych przewodów CAT5 (lub lepszych) o długości nieprzekraczającej 100 m (328 ft).
	Podłączono sprzęt sieciowy (przełączniki/routery)	Poprawna praca jest możliwa tylko przy bezpośrednim połączeniu maksymalnie dwóch systemów EKX.

Okno główne > **Grupy użytkowników** > karta **Grupy użytkowników**
LUB

Okno główne > **Grupy użytkowników** > karta **Enterprise User Groups**
LUB

Okno główne > **Grupy użytkowników** > karta **Dostęp Enterprise**
Można konfigurować następujące priorytety:

- W przypadku standardowych grup użytkowników i grup **Enterprise User Groups**: można konfigurować priorytety alarmów dla trybu podglądu na żywo i trybu odtwarzania.
- W przypadku standardowych grup użytkowników i dostępu **Dostęp Enterprise**: można konfigurować priorytety przejmowania sterowania funkcjami PTZ i przejmowania linii połączeń urządzenia Bosch Allegiant.
Można konfigurować czas obowiązywania blokady sterowania funkcjami PTZ, np. użytkownik o wyższym priorytecie może przejąć sterowanie kamerą od użytkownika o niższym priorytecie i zablokować sterowanie kamerą na ten okres.

Aby skonfigurować priorytety dla trybu podglądu bieżącego i trybu odtwarzania, należy:

1. Wybrać standardową grupę użytkowników lub grupę Enterprise User Group.
2. Kliknąć **Uprawnienia do obsługi**.
3. Kliknąć kartę **Priorytety**.
4. W polu **Automatyczne zachowanie okna podręcznego** przesunąć suwak w żądane położenie.

Aby skonfigurować priorytety dla funkcji PTZ i linii połączeń urządzenia Allegiant, należy:

1. Wybrać standardową grupę użytkowników lub grupę Enterprise Account.
2. Kliknąć kartę **Uprawnienia urządzenia**.
3. Kliknąć kartę **Priorytety sterowania**.
4. W polu **Priorytety sterowania** przesunąć suwak w żądane położenie.
5. Na liście **Limit czasu w min.** zaznaczyć żądaną pozycję.

Patrz

- Strona Priorytety sterowania, Strona 334
- strona Priorytety, Strona 341

27.11

Kopiowanie uprawnień grupy użytkowników

Okno główne > **Grupy użytkowników** > karta **Grupy użytkowników**
LUB

Okno główne > **Grupy użytkowników** > karta **Enterprise User Groups**
LUB

Okno główne > **Grupy użytkowników** > karta **Dostęp Enterprise**

Użytkownik może skopiować uprawnienia z jednej grupy lub konta do innej grupy lub konta.

Wcześniej należy skonfigurować przynajmniej 2 grupy lub konta.

Aby skopiować uprawnienia:

1. Na drzewie Grupy użytkowników zaznacz grupę użytkowników lub konto.

2. Kliknij  .

Zostanie wyświetlone okno dialogowe **Kopiuje uprawnienia grupy użytkowników**.

3. Wybierz odpowiednie uprawnienia oraz odpowiednią grupę docelową lub konto docelowe.
4. Kliknąć **OK**. Uprawnienia danej grupy zostaną skopiowane do innej grupy lub konta. Okno dialogowe zostanie zamknięte.

28

Strona Audit Trail

**Uwaga!**

Program BVMS Viewer zapewnia tylko podstawowe funkcje. Funkcje zaawansowane udostępnia program BVMS Professional. Aby uzyskać szczegółowe informacje na temat różnych wersji systemu BVMS, należy odwiedzić witrynę www.boschsecurity.com i zobaczyć skrócony poradnik wyboru systemu BVMS: [Skrócony poradnik wyboru systemu BVMS](#).

Okno główne > **Audit Trail**

Funkcja Audit Trail umożliwia śledzenie wszystkich zmian w konfiguracji systemu oraz eksportowanie danych do pliku CSV.

Warunki wstępne:

1. Zainstaluj bazę danych funkcji Audit Trail, zaznaczając ją w instalatorze programu BVMS (opcjonalna funkcja instalatora).
2. Masz następujące uprawnienia: **Pokaż stronę ścieżki Audit Trail**.
3. Funkcja Audit Trail jest włączona w oknie **Ustawienia > Opcje > Audit Trail**.

Zalecenia:

- Nie włączaj funkcji Audit Trail od samego początku, ponieważ ilość protokolowanych informacji będzie ogromna.
- Zamiast tego wykonaj początkową konfigurację systemu, utwórz raporty dla procesu przekazywania do użytku i dopiero potem włącz funkcję Audit Trail, aby protokolować późniejsze zmiany.
- Zamierzając importować konfiguracje, wyłączaj funkcję Audit Trail.

Aby rozwinąć / zwinąć dane funkcji Audit Trail:

1. Kliknij przycisk , aby rozwinąć jeden węzeł danych.
2. Kliknij przycisk , aby zwinąć jeden węzeł danych.
3. Kliknij przycisk **Rozwiń wszystko / Zwiń wszystko**, aby rozwinąć / zwinąć wszystkie wczytane węzły danych.

Aby wczytać dane funkcji Audit Trail:

- ▶ Kliknij **Wczytaj więcej**.

Uwaga: Kliknięcie przycisku **Wczytaj więcej** spowoduje wczytanie tylko 10 węzłów danych naraz.

Aby wyeksportować dane funkcji Audit Trail:

- ▶ Kliknij przycisk **Eksport**, aby zapisać wczytane dane do pliku CSV.

Uwaga: Zostaną wyeksportowane tylko wczytane dane.

Patrz

- Okno dialogowe **Opcje** (menu **Ustawienia**), Strona 120
- Strona **Konfigurowanie uprawnień**, Strona 343

28.1 Protokołowanie szczegółów w funkcji Audit Trail

Uwaga: Jeśli w bazie danych nie ma wystarczającej ilości miejsca, najstarsze pozycje będą automatycznie usuwane. Po upływie czasu przechowywania te wpisy są automatycznie usuwane.

Tabela Audit Trail zawiera następujące kolumny:

Działanie	Modyfikacja, którą zainicjował użytkownik.
Utworzono	Do konfiguracji programu BVMS został dodany nowy obiekt, na przykład kamera lub użytkownik.
Zmodyfikowano	Zmodyfikowano obiekt istniejący w konfiguracji, na przykład nazwa wyświetlana kamery.
Usunięto	Usunięto obiekt istniejący w konfiguracji.
Element listy dodany	Do listy został dodany obiekt, na przykład do puli systemu VRM dodano kamerę.
Element listy usunięty	Z listy został usunięty obiekt, na przykład usunięto kamerę z puli systemu VRM lub z programu VSG.
Typ obiektu	Typ zmienionego obiektu konfiguracyjnego.
Obiekt	Zmodyfikowany obiekt, np. kamera, użytkownik lub harmonogram.
Adres sieciowy	Adres sieciowy obiektu, jeśli jest dostępny.
Kontekst obiektu 1 / Kontekst obiektu 2	Kontekst zmodyfikowanego elementu, zazwyczaj element nadrzędny obiektu. Na przykład: Dodano lokalizację docelową urządzenia iSCSI. Kontekstem urządzenia 1 jest element nadrzędny urządzenia iSCSI, a kontekstem 2 system VRM, do którego należy urządzenie iSCSI.
Właściwość	Nazwa zmodyfikowanej właściwości.
Stara wartość	Wartość sprzed zainicjowania zmiany.
Nowa wartość	Nowa wartość ustawiona podczas modyfikacji.
Kontekst 1 / Kontekst 2	Dodatkowy kontekst opisujący modyfikację. Na przykład: Jeśli zmienisz ustawienia kamery w oknie opcji alarmu w konfiguracji alarmu, kamera zostanie dodana jako kontekst.

28.2 Okno dialogowe filtrów w funkcji Audit Trail

Okno dialogowe filtrów umożliwia filtrowanie lub wyszukiwanie określonych informacji w bazie danych funkcji Audit Trail.

Okno dialogowe zawiera następujące predefiniowane filtry:

- Kategoria
- Działanie
- Przedział czasowy

Jeśli w oknie dialogowym filtrów wybierzesz kilka kategorii działań, wszystkie te sekcje będą uwzględniane w wyszukiwaniu.

Dodatkowo w polu wyszukiwania tekstowego można wpisać ciągi znaków, które spowodują wyfiltrowanie określonych użytkowników, urządzeń, ustawień itd. Jeżeli wpiszesz wiele wyszukiwanych terminów, wynik będzie musiał zawierać wszystkie te wyrazy. Z pomocą cudzysłowów można wpisywać szukane terminy, które mają zawierać spacje. Na przykład: "Camera 1".

Przykład:

Wybierasz kategorie **Urządzenia i Mapy i struktura**, a następnie w polu wyszukiwania tekstowego wpisujesz nazwę kamery "Cam1" i nazwę użytkownika "X".

Wynik: W bazie danych funkcji Audit Trail zostaną odnalezione wszystkie zmiany dokonane przez użytkownika "X" w obiektach konfiguracyjnych kamery "Cam1", które znajdują się w sekcji

Urządzenia lub Mapy i struktura.

Aby używać filtra Audit Trail:

1. Kliknij przycisk **Filtr**.
Zostanie wyświetlone okno dialogowe filtrów funkcji Audit Trail.
2. Po skonfigurowaniu filtrów kliknij przycisk **Zastosuj**.
3. Kliknij przycisk , aby usunąć jeden obiekt filtra.
4. Kliknij przycisk **Resetuj wszystkie filtry**, aby zresetować całą konfigurację filtrów.

29 Konfigurowanie wizyjnego systemu wykrywania pożaru

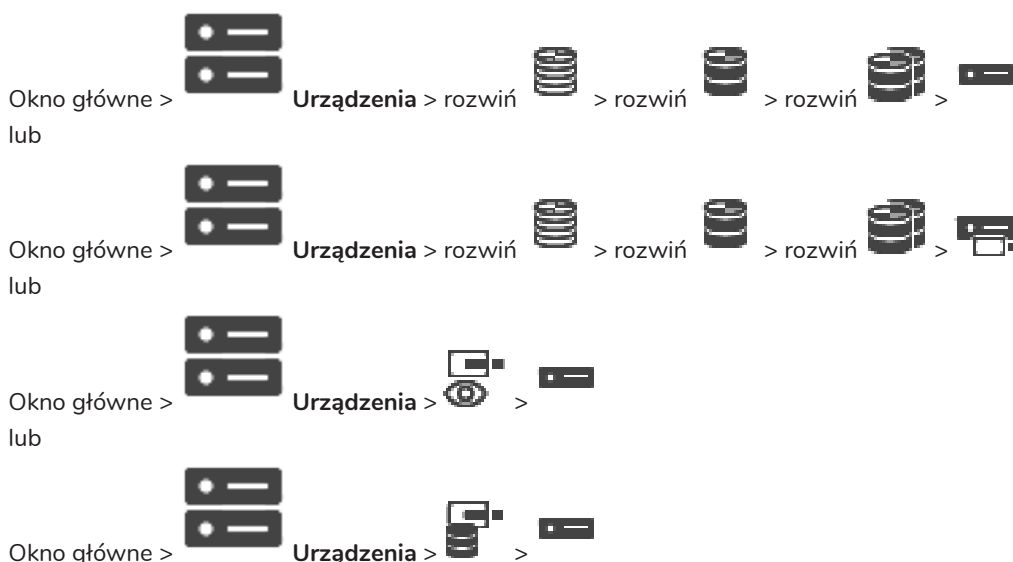
Aby skonfigurować wizyjny system wykrywania pożaru, należy:

1. Skonfigurować wykrywanie pożaru w kamerze wykrywania pożaru.
W tej konfiguracji należy użyć sieciowej strony kamery.
Aby uzyskać szczegółowe informacje na temat konfigurowania kamery wykrywania pożaru, patrz
 - Konfigurowanie kamery wykrywania pożaru, Strona 365
2. Dodać tę kamerę wykrywania pożaru do systemu. Do puli VRM można dodać kamerę wykrywania pożaru jako nadajnik udostępniający tylko podgląd na żywo lub nadajnik z pamięcią lokalną.
Aby uzyskać szczegółowe informacje o dodawaniu kamery, patrz
 - Dodawanie nadajnika do puli VRM, Strona 218
 - Dodawanie nadajnika udostępniającego tylko podgląd bieżący, Strona 218
 - Dodawanie nadajnika z pamięcią lokalną, Strona 218
3. Skonfigurować zdarzenie alarmu pożarowego dla tej kamery.
 - Konfiguracja zdarzenia alarmu pożarowego, Strona 367
4. Skonfigurować alarm dla tego zdarzenia alarmu pożarowego.
 - Konfigurowanie alarmu pożarowego, Strona 368

Patrz

- Dodawanie nadajnika do puli VRM, Strona 366
- Dodawanie nadajnika udostępniającego tylko podgląd bieżący, Strona 218
- Dodawanie nadajnika z pamięcią lokalną, Strona 218
- Konfiguracja zdarzenia alarmu pożarowego, Strona 367
- Konfigurowanie alarmu pożarowego, Strona 368

29.1 Konfigurowanie kamery wykrywania pożaru



Aby skonfigurować wizyjny alarm pożarowy, należy najpierw skonfigurować wykrywanie pożaru w kamerze wykrywania pożaru.

Szczegółowe informacje na ten temat można znaleźć w instrukcji obsługi kamery wykrywania pożaru.

Aby przeprowadzić konfigurację, należy:

1. Kliknąć prawym przyciskiem myszy ikonę urządzenia, a następnie przycisk **Pokaż stronę sieciową w przeglądarce**.

2. Kliknąć **Konfiguracja**.
3. W okienku nawigacji rozwinąć **Alarm** i kliknąć przycisk **Wykrywanie pożaru**.
4. Wprowadzić odpowiednie ustawienia.

29.2 Dodawanie nadajnika do puli VRM

Aby dodać nadajniki do puli VRM, patrz *Dodawanie nadajników poprzez skanowanie*, Strona 177.

Patrz

- Dodawanie urządzenia, Strona 125

29.3 Dodawanie nadajników poprzez skanowanie

Aby dodać nadajniki poprzez skanowanie:

1. Kliknij prawym przyciskiem myszy , a następnie kliknij **Skanuj w poszukiwaniu nadajników**.
Zostanie wyświetlone okno dialogowe **BVMS Scan Wizard**.
2. Wybierz wymagane nadajniki oraz żadaną pulę VRM, a następnie kliknij **Przypisz**, aby przypisać nadajniki do puli VRM.
3. Kliknij **Dalej >>**.
Zostanie wyświetlone okno dialogowe kreatora **Uwierzytelnianie urządzeń**.
4. Wpisać hasło w przypadku każdego urządzenia, które jest nim chronione.
Jeśli przez kilka sekund nie wprowadzisz żadnego znaku w polu hasła lub klikniesz poza tym polem, sprawdzenie hasła następuje automatycznie.
Jeśli hasło do wszystkich urządzeń jest identyczne, można wpisać je w pierwszym polu **Hasło**.
Następnie kliknij to pole prawym przyciskiem myszy i kliknij polecenie **Kopiuj komórkę do kolumny**.

Udane logowanie jest oznaczane w kolumnie **Stan** ikoną .

Nieudane próby logowania są oznaczane ikoną .

5. Kliknąć **Zakończ**.
Urządzenie zostanie dodane do drzewa urządzeń.

Ikona  oznacza błąd, którym należy się zająć. Więcej informacji o charakterze błędu uzyskasz z etykiety narzędzia.

29.4 Dodawanie urządzeń podglądu bieżącego poprzez skanowanie

Aby poprzez skanowanie dodać urządzenia Bosch tylko z podglądem bieżącym:

1. Kliknij prawym przyciskiem myszy , a następnie kliknij **Skanuj w poszukiwaniu nadajników tylko podglądu bieżącego**.
Zostanie wyświetlone okno dialogowe **BVMS Scan Wizard**.
2. Zaznacz pola wyboru odpowiadające urządzeniom, które mają zostać dodane.
3. Kliknij **Dalej >>**.
Zostanie wyświetlone okno dialogowe kreatora **Uwierzytelnianie urządzeń**.

4. Wpisać hasło w przypadku każdego urządzenia, które jest nim chronione.
Jeśli przez kilka sekund nie wprowadzisz żadnego znaku w polu hasła lub klikniesz poza tym polem, sprawdzenie hasła następuje automatycznie.
Jeśli hasło do wszystkich urządzeń jest identyczne, można wpisać je w pierwszym polu **Hasło**.
Następnie kliknij to pole prawym przyciskiem myszy i kliknij polecenie **Kopiuj komórkę do kolumny**.



Udane logowanie jest oznaczane w kolumnie **Stan** ikoną



Nieudane próby logowania są oznaczane ikoną

5. Kliknąć **Zakończ**.
Urządzenie zostanie dodane do drzewa urządzeń.

Ikona  oznacza błąd, którym należy się zająć. Więcej informacji o charakterze błędu uzyskasz z etykiety narzędzia.

29.5

Dodawanie nadajników z obsługą lokalnego urządzenia pamięci masowej poprzez skanowanie



Okno główne > **Urządzenia** > rozwinąć

Umożliwia dodawanie i konfigurowanie nadajników służących do nagrywania na lokalnych urządzeniach pamięci masowej.

Aby poprzez skanowanie dodać nadajniki z obsługą lokalnego urządzenia pamięci masowej:

1. W oknie Drzewo urządzeń kliknij prawym przyciskiem myszy , a następnie kliknij **Skanuj w poszukiwaniu nadajników z pamięcią lokalną**.
Zostanie wyświetlone okno dialogowe **BVMS Scan Wizard**.
2. Zaznacz pola wyboru odpowiadające urządzeniom, które mają zostać dodane.
3. Kliknij **Dalej >>**.
Zostanie wyświetlone okno dialogowe kreatora **Uwierzytelnianie urządzeń**.
4. Wpisać hasło w przypadku każdego urządzenia, które jest nim chronione.
Jeśli przez kilka sekund nie wprowadzisz żadnego znaku w polu hasła lub klikniesz poza tym polem, sprawdzenie hasła następuje automatycznie.
Jeśli hasło do wszystkich urządzeń jest identyczne, można wpisać je w pierwszym polu **Hasło**.
Następnie kliknij to pole prawym przyciskiem myszy i kliknij polecenie **Kopiuj komórkę do kolumny**.



Udane logowanie jest oznaczane w kolumnie **Stan** ikoną



Nieudane próby logowania są oznaczane ikoną

5. Kliknąć **Zakończ**.
Urządzenie zostanie dodane do drzewa urządzeń.

29.6

Konfiguracja zdarzenia alarmu pożarowego



Okno główne > **Zdarzenia**

Aby przeprowadzić konfigurację, należy:

1. Wybrać na drzewie **Nadajniki / Odbiorniki > Kamera > Stan pożaru lub dymu > Wykryto pożar lub dym**.
Pojawi się odpowiednia tabela konfiguracji zdarzeń.
2. W kolumnie **Wyzwól alarm – Harmonogram** kliknij właściwą komórkę i wybierz odpowiedni harmonogram.
Harmonogram określa, kiedy wyzwalany jest alarm.
Wybrać jeden z harmonogramów zapisu lub harmonogramów zadań skonfigurowanych wcześniej na stronie **Harmonogramy**.
3. Wprowadzić żądane zmiany.

Uwaga: takiej samej procedury można użyć w przypadku innych zdarzeń alarmu pożarowego.

29.7

Konfigurowanie alarmu pożarowego

Okno główne > **Alarmy**

Aby przeprowadzić konfigurację, należy:

1. Na drzewie wybrać **Nadajniki / Odbiorniki > Kamera > Stan pożaru lub dymu > Wykryto pożar lub dym**.
Pojawi się odpowiednia tabela konfiguracji alarmów.
2. Wprowadzić żądane zmiany.

30

Konfigurowanie MIC IP 7000 podłączonego do zasilacza VIDEOJET connect 7000

Aby zapewnić prawidłowe działanie kamery MIC IP 7000 podłączonej do zasilacza VIDEOJET connect 7000, należy wykonać następujące konfiguracje.

Przed dodaniem kamery MIC IP do systemu BVMS należy wykonać następujące czynności:

1. Zresetować kamerę MIC IP 7000 i zasilacz VIDEOJET connect 7000 do domyślnych ustawień fabrycznych na stronie internetowej każdego urządzenia.
2. Skonfigurować kamerę MIC IP 7000 w wariantcie **MIC IP Starlight 7000 HD – VJC-7000**.
3. Skonfigurować kamerę MIC IP 7000 i zasilacz VIDEOJET connect 7000 zgodnie z dokumentacją dołączoną do urządzeń.
4. Jeśli użytkownik chce używać ANR, należy uruchomić narzędzie konfiguracji ANR dla zasilacza VIDEOJET connect 7000.

To zadanie trzeba wykonać na komputerze, który należy do tej samej sieci co zasilacz VIDEOJET connect 7000.

Narzędzie konfiguracji ANR można znaleźć w katalogu produktu na stronie zasilacza VIDEOJET connect 7000.

Należy wykonać tę procedurę, aby dodać i skonfigurować kamerę MIC IP 7000 w systemie BVMS:

1. W drzewie urządzeń dodać tylko kamerę MIC IP 7000.
Urządzenia VIDEOJET connect 7000 nie można dodać do systemu BVMS.
2. Kliknąć dodaną kamerę prawym przyciskiem myszy, a następnie wybrać opcję **Edytuj nadajnik**.
Pojawi się okno dialogowe **Edytuj nadajnik**.
Informacje o wydajności urządzenia są pobierane automatycznie zgodnie ze skonfigurowanym powyżej wariantem.
3. W razie potrzeby skonfigurować ANR na stronie **Kamery i zapis**.

31 Rozwiązywanie problemów

Niniejszy rozdział zawiera informacje o usuwaniu znanych problemów występujących podczas działania systemu BVMS Configuration Client.

Problemy podczas instalacji

Problem	Przyczyna	Rozwiązanie
Instalator wyświetla nieprawidłowe znaki.	Ustawienia języka w systemie Windows są nieprawidłowe.	Ustawienie żądanego języka w systemie Windows, Strona 372
Konfiguracja zostaje zatrzymana i pojawia się komunikat informujący, że instalacja serwera OPC nie jest możliwa.	Pliki serwera OPC nie mogą być nadpisywane.	Należy odinstalować składnik OPC Core Components Redistributable i ponownie rozpocząć konfigurację systemu BVMS.
Nie można odinstalować oprogramowania poprzez uruchomienie programu instalacyjnego.		Kliknij przycisk Control Panel > Add/Remove Programs i odinstaluj program BVMS.

Problemy natychmiast po uruchomieniu aplikacji

Problem	Przyczyna	Rozwiązanie
System BVMS wyświetla nieprawidłowy język.	System Windows nie został przełączony na żądany język.	Wybieranie wersji językowej modułu Configuration Client, Strona 73 lub Wybieranie wersji językowej modułu Operator Client, Strona 73
Okno dialogowe logowania do programu Operator Client wskazuje zły język.	Mimo zmiany języka dla programu Operator Client w Configuration Client, język okna dialogowego logowania do programu Operator Client zależy od ustawień języka w systemie Windows.	Ustawienie żądanego języka w systemie Windows, Strona 372

Problemy związane z wersją językową interfejsu użytkownika

Problem	Przyczyna	Rozwiązanie
Niektóre opisy tekstowe pojawiające się w oknach programu Configuration Client lub Operator Client są wyświetlane w obcym języku (zazwyczaj angielskim).	Management Server jest często instalowany na komputerze pracującym pod kontrolą anglojęzycznego systemu operacyjnego. Dlatego podczas generowania bazy danych systemu BVMS na takim komputerze wiele	Nie należy podejmować prób samodzielnego rozwiązania tego problemu.

Problem	Przyczyna	Rozwiązanie
	elementów tekstowych interfejsu użytkownika jest kopiowanych w angielskiej wersji językowej. Dzieje się tak nawet jeśli komputer z zainstalowanym programem Operator Client pracuje pod kontrolą systemu Windows w innej niż angielska wersja językowa. Aby rozwiązać ten problem, Management Server należy zainstalować na komputerze z systemem Windows w żądanej wersji językowej.	

Problemy z klawiaturą Bosch IntuiKey

Problem	Przyczyna	Rozwiązanie
Klawiatura Bosch IntuiKey wyzwała alarm, a na wyświetlaczu przycisków ekranowych jest widoczny komunikat Off Line.	Połączenie ze stacją roboczą zostało zerwane. Kabel uległ uszkodzeniu lub został odłączony albo stacja robocza została zresetowana.	Przywracanie połączenia z klawiaturą Bosch IntuiKey, Strona 372

Problemy z ustawieniami sterowania zapisem karty dźwiękowej

Problem	Przyczyna	Rozwiązanie
Sprzężenia zwrotne występują podczas używania mikrofonu Interkomu.	W oknie sterowania zapisem z użyciem karty dźwiękowej musi być zaznaczona opcja odpowiadająca mikrofonowi (opcja miksowania dźwięku stereofonicznego i wszystkie inne opcje nie powinny być zaznaczone). Podczas uruchamiania programu Operator Client sprawdzany jest jego plik konfiguracyjny i odpowiednio modyfikowane są ustawienia sterowania zapisem. Ten plik konfiguracyjny zawiera domyślny wpis, który może być niezgodny z konfiguracją systemu. Ustawienia domyślne są przywracane za każdym	W takiej sytuacji należy zmienić odpowiednie ustawienie w pliku konfiguracyjnym programu Operator Client tak, aby wybierana była opcja odpowiadająca mikrofonowi.

Problem	Przyczyna	Rozwiązanie
	razem, gdy program Operator Client jest uruchamiany po raz kolejny.	

Awarie Configuration Client

Problem	Przyczyna	Rozwiązanie
Configuration Client ulega awarii.	Jeśli istnieje wiele kamer skonfigurowanych w pliku Allegiant, które nie są połączone z systemem Bosch Video Management System, można zmniejszyć ich liczbę. Zapobiega to niepotrzebnym obciążeniom systemu.	Patrz <i>Zmniejszenie liczby kamer systemu Allegiant</i> , Strona 372.

31.1 Ustawienie żadanego języka w systemie Windows

Aby zmienić język interfejsu ekranowego instalatora systemu BVMS, należy wybrać żadaną wersję językową w systemie Windows. Aby uaktywnić zmiany ustawień języka, komputer jest ponownie uruchamiany po wykonaniu poniższych czynności.

Aby ustawić żądany język, należy:

1. Kliknąć menu **Start**, wybrać **Panel sterowania**, a następnie kliknąć dwukrotnie ikonę **Opcje regionalne i językowe**.
2. Kliknąć kartę **Zaawansowane** i w polu **Język dla programów nie obsługujących kodu Unicode** wybrać żądany język.
3. Kliknąć przycisk **OK**.
4. W każdym z kolejnych okienek komunikatów kliknąć przycisk **Tak**.
Komputer użytkownika zostanie uruchomiony ponownie.

31.2 Przywracanie połączenia z klawiaturą Bosch IntuiKey

1. Powtórnie podłączyć kabel lub zaczekać, aż stacja robocza przejdzie w tryb online.
Komunikat Off Line zniknie.
2. Kliknąć klawisz ekranowy Terminal, aby przejść do systemu BVMS.

31.3 Zmniejszenie liczby kamer systemu Allegiant

Aby edytować plik Allegiant, wymagane jest oprogramowanie Allegiant Master Control Software.

Aby zmniejszyć liczbę kamer systemu Allegiant, należy:

1. Uruchomić oprogramowanie Master Control Software.
2. Otworzyć plik Allegiant.
3. Kliknąć kartę Camera.
4. Zaznaczyć kamery, które nie są wymagane.
5. W menu Edit kliknąć pozycję Delete.
6. Zapisać plik. Rozmiar pliku pozostaje niezmienny.
7. Ostatni krok należy powtórzyć dla monitorów, które nie są potrzebne. Kliknąć kartę Monitors.
8. Należy importować ten plik do systemu Bosch Video Management System (patrz *Dodawanie urządzenia*, Strona 125).

31.4 Używane porty

W tej sekcji są wymienione porty wszystkich składników systemu BVMS, które muszą być otwarte w sieci LAN. Tych portów nie należy otwierać do Internetu! Do operacji w Internecie należy używać bezpiecznych połączeń, na przykład VPN.

W każdej tabeli są wymienione lokalne porty, które muszą być otwarte na komputerze z zainstalowanym serwerem lub na routerze/poziom 3, który jest podłączony do tego sprzętu.

Na zaporze sieciowej systemu Windows należy skonfigurować dla każdego otwartego portu reguły ruchu przychodzącego.

Zezwól na połączenia wychodzące dla wszystkich aplikacji systemu BVMS.

Management Server / porty Enterprise Management Server

Serwer (nasłuchujący)	Protokół	Porty wejściowe	Klient (zapytujący)	Adnotacja
Management Server	UDP	123	Nadajnik	TimeServer NTP
Management Server	TCP	5322	Operator Client	Połączenie SSH
Management Server	TCP	5422	Operator Client	Usługa dostawcy autoryzacji
Management Server	TCP	5389	Urządzenie ONVIF	Serwer proxy urządzenia ONVIF, powiadomienie o zdarzeniu
Management Server	TCP	5390	Operator Client, Configuration Client	.NET Remoting
Management Server	TCP	5391	Klienci Operator Client, Configuration Client, NVR	Port zdalny dla wszystkich usług NVR
Management Server	TCP	5392	Operator Client, Configuration Client, Aplikacja BVMS SDK	WCF, gateway.push.apple.com
Management Server	TCP	5393	Operator Client, VRM	Data-Access-Service
Management Server	TCP	5394	Operator Client	Port zdalny dla aplikacji Operator Client
Management Server	TCP	5395	Configuration Client, Operator Client	Preferencje użytkownika, transfer plików
Management Server	TCP	5396	Configuration Client, aplikacje klienckie WCF	Punkt wejścia mex (normalnie wyłączony)
Management Server	TCP	5397	Operator Client dla NoTouchDeployment	Port NoTouchDeployment
Management Server	TCP	5398	Klient API konfiguracji	Komunikacja wewnętrzna między komponentem AKKA.Net i CS

Serwer (nasłuchujący)	Protokół	Porty wejściowe	Klient (zapytujący)	Adnotacja
Management Server	UDP	12544	Klient SNMP	BVMS, port get SNMP
Management Server	TCP	162	SNMP	
Management Server	TCP	5389 - 5396	Porty BVMS	
Management Server	TCP, UDP	135	BRS DCOM	BRS
Management Server	TCP	808	BRS WebService (DIBOS)	Serwer centralny połączony z Dibos na tym porcie przy użyciu WCF
Management Server	TCP	1756 / 1757	RCP	1757 dla dodatkowego VRM

Dodatkowe elementy centralne

Serwer (nasłuchujący)	Protokół	Porty wejściowe	Klient (zapytujący)	Adnotacja
Configuration Client	UDP	1024 - 65535	Nadajnik, VRM	Strumień wizyjny
Configuration API	TCP	5399	Klient REST interfejsu API	Configuration API
Management Server	TCP	5443	PID	Połączenie PID, dostęp przez HTTPS
Monitorowanie stacji roboczej	TCP	5410	Operator Client, Management Server	
Monitorowanie stacji roboczej	TCP	5411	Usługa GRPC	
Usługa metadanych	TCP	5460	Usługa GRPC	

Porty Video Recording Manager

Serwer (nasłuchujący)	Protokół	Porty wejściowe	Klient (zapytujący)	Adnotacja
VRM	TCP	554 / 555	Klient RTSP	Pobieranie pierwotnego/ dodatkowego strumienia RTSP
VRM	TCP	40023	Klient Telnet	Telnet (tylko lokalny host z VRM 4.x)
VRM	TCP	40080 / 40081	Klient VRM	Port HTTP vj_generic.dll

Serwer (nasłuchujący)	Protokół	Porty wejściowe	Klient (zapytujący)	Adnotacja
VRM	TCP	41080 / 41081	Klient VRM	HTTP vj_generic.dll (tylko lokalny host)
VRM	TCP	1756 / 1757	Management Server, Configuration Client	przez RCP+, (1757 dla dodatkowego klienta RCP+ VRM)
VRM	UDP	1757	Management Server, Operator Client	Skanowanie celu Broadcast
VRM	UDP	1758	Management Server, Configuration Client	Odpowiedź funkcji skanowania
VRM	UDP	1759	Management Server, Configuration Client	Wykrywanie sieci, skanowanie celu Multicast
VRM	UDP	1760		
VRM	UDP	1800 / 1900	Management Server, Operator Client	Skanowanie celu Multicast
VRM	TCP	80	Operator Client	Odtwarzanie z głównego VRM przez http
VRM	TCP	443	Operator Client	Odtwarzanie z głównego VRM przez https
VRM	TCP	81	Operator Client	Odtwarzanie z podrzędnego urządzenia VRM przez http
VRM	TCP	444	Operator Client	Odtwarzanie z podrzędnego urządzenia VRM przez https

Porty Bosch Video Streaming Gateway

Serwer (nasłuchujący)	Protokół	Porty wejściowe	Klient (zapytujący)	Adnotacja
Bosch Video Streaming Gateway	TCP	8080 - 8086	VRM, Management Server, Configuration Client, Operator Client	HTTP
Bosch Video Streaming Gateway	TCP	8443 - 8449	VRM, Management Server, Configuration Client, Operator Client	HTTPS
Bosch Video Streaming Gateway	TCP	8756 - 8762	VRM, Management Server, Configuration Client	RCP+
Bosch Video Streaming Gateway	TCP	8443-8449	VRM, Management Server, Configuration Client, Operator Client	HTTPS

Serwer (nasłuchujący)	Protokół	Porty wejściowe	Klient (zapytujący)	Adnotacja
Bosch Video Streaming Gateway	UDP	1757	Klient VRM	Skanowanie celu Broadcast
Bosch Video Streaming Gateway	UDP	1758	Klient VRM	Odpowiedź funkcji skanowania
Bosch Video Streaming Gateway	UDP	1759	Klient VRM	Wykrywanie sieci, skanowanie celu Multicast
Bosch Video Streaming Gateway	UDP	1800, 1900	VRM Configuration Client	Wykrywanie sieci, skanowanie celu Multicast
Bosch Video Streaming Gateway	UDP	1064-65535	Nadajnik, VRM	Strumienie wizyjne

Porty pamięci masowej iSCSI

Skonfiguruj port przesyłający dalej na routerze podłączonym do urządzenia.

Serwer (nasłuchujący)	Protokół	Porty wejściowe	Klient (zapytujący)	Adnotacja
System pamięci masowej iSCSI	TCP	3260	Nadajnik, VRM, Configuration Client, Operator Client	System pamięci masowej iSCSI

Porty DVR

Skonfiguruj port przesyłający dalej na routerze podłączonym do urządzenia.

Serwer (nasłuchujący)	Protokół	Porty wejściowe	Klient (zapytujący)	Adnotacja
DVR	TCP	80	Management Server, Configuration Client, Operator Client	Dostęp przez HTTP
DVR	TCP	443	Management Server, Configuration Client, Operator Client	Dostęp przez HTTPS

Porty kamery ONVIF / kamery / nadajnika

Skonfiguruj Przekierowanie Portów na routerze podłączonym do urządzenia.

Serwer (nasłuchujący)	Protokół	Porty wejściowe	Klient (zapytujący)	Adnotacja
Nadajnik	TCP	80	Management Server, VSG, Configuration Client, Operator Client	Dostęp przez HTTP

Serwer (nasłuchujący)	Protokół	Porty wejściowe	Klient (zapytujący)	Adnotacja
Nadajnik	TCP	443	Management Server, VSG, Configuration Client, Operator Client	Dostęp przez HTTPS
Nadajnik	UDP	123	Management Server, VRM	SNTP
Nadajnik	UDP	161	Management Server, VRM	SNMP
Nadajnik	TCP	554	Operator Client, aplikacja BVMS SDK, VSG	Strumieniowanie RTSP
Nadajnik	TCP	3260	Nadajnik (wyjściowy)	Rejestrowanie iSCSI
Nadajnik	TCP	1756	Dekoder, Management Server, Operator Client	Połączenia wychodzące dla kamer Bosch
Nadajnik	UDP	1757	Dekoder, Management Server, Operator Client	Skanowanie celu Broadcast
Nadajnik	UDP	1758	Dekoder, Management Server, Operator Client	Odpowiedź funkcji skanowania
Nadajnik	UDP	1800	Dekoder, Management Server, Operator Client	Wykrywanie sieci, skanowanie celu Multicast
Nadajnik	UDP	1900		SSDP (opcjonalny port nadajnika)
Nadajnik	TCP	21		FTP (opcjonalny port nadajnika)
Nadajnik	UDP	3702		UPNP (opcjonalny port nadajnika)
Nadajnik	UDP	9554		SRTSP (opcjonalny port nadajnika)
Nadajnik	UDP	15344 / 15345		RTSP send (opcjonalne porty nadajnika)

Porty dekodera BVMS

Skonfiguruj Przekierowanie Portów na routerze podłączonym do urządzenia.

Serwer (nasłuchujący)	Protokół	Porty wejściowe	Klient (zapytujący)	Adnotacja
Dekoder	TCP	1756	Aplikacja Management Server, Operator Client, Configuration Client, BVMS SDK	Połączenia wychodzące dla kamer Bosch
Dekoder	UDP	1757	Management Server, Operator Client	Skanowanie celu Broadcast
Dekoder	UDP	1758	Management Server, Operator Client	Odpowiedź funkcji skanowania

Serwer (nasłuchujący)	Protokół	Porty wejściowe	Klient (zapytujący)	Adnotacja
Dekoder	UDP	1800	Management Server, Operator Client	Wykrywanie sieci, skanowanie celu Multicast
Dekoder	TCP	80	Operator Client	Dostęp przez HTTP
Dekoder	TCP	443	Operator Client	Dostęp przez HTTPS
Dekoder	UDP	1024-65535	Nadajnik	Porty strumieniowania
Dekoder	UDP	123	Management Server, VRM	SNTP
Dekoder	UDP	161	Management Server, VRM	SNMP

Porty BVMSOperator Client / Cameo SDK

Serwer (nasłuchujący)	Protokół	Porty wejściowe	Klient (zapytujący)	Adnotacja
Operator Client	TCP	5394	Aplikacja BVMS SDK, BIS	WCF
Operator Client	UDP	1024-65535	Nadajnik, VRM	Strumienie wizyjne
Operator Client	TCP	40082		
Operator Client	TCP	41756		

Porty adaptera urządzeń LPR, BVMS

Serwer (nasłuchujący)	Protokół	Porty wejściowe	Klient (zapytujący)	Adnotacja
Adapter urządzenia BVMS	TCP	31000	Klient kamery LPR	VRC

Porty AMS / Access Management System

Serwer (nasłuchujący)	Protokół	Porty wejściowe	Klient (zapytujący)	Adnotacja
AMS	TCP	62904	Management Server	Dostęp przez HTTPS

Transkoder

Serwer (nasłuchujący)	Protokół	Porty wejściowe	Klient (zapytujący)	Adnotacja
	UDP	5080		
	UDP	5443		
	UDP	5756		

31.5

Włączanie rejestrowania zdarzeń ONVIF

**Uwaga!**

Należy pamiętać, że ta funkcja wkrótce zostanie wyłączona.

Należy korzystać z narzędzia ONVIF Camera Event Driver Tool do łatwego mapowania zdarzeń ONVIF.

Patrz *Uruchamianie narzędzia ONVIF Camera Event Driver Tool za pomocą Configuration Client*, Strona 208.

Można włączyć rejestrowanie zdarzeń ONVIF, np. w przypadku napotkania problemów z odbiorem zdarzeń systemu BVMS. Rejestrowanie pomaga więc w wykryciu źródła problemu.

Aby włączyć rejestrowanie:

1. Otworzyć plik `%programfiles%\Bosch\VMS\AppData\Server\CentralServer\BVMSLogCfg.xml` w odpowiednim edytorze, np. Notepad. Uruchomić aplikację Notepad jako administrator.
2. Przejść do wiersza zawierającego następujący ciąg:
`Add logging for onvif events of a device by network address`
Krótkie objaśnienie znajduje się w wierszach komentarza.
3. Jako nazwę narzędzia do rejestrowania wpisać `OnvifEvents.<Networkaddress>`.
Wpisać tylko `OnvifEvents` w celu rejestrowania zdarzeń dotyczących wszystkich urządzeń ONVIF.
4. Jako wartość poziomu wpisać `DEBUG` dla wszystkich zdarzeń przychodzących i wychodzących.
Wpisać `INFO` dla wszystkich zdarzeń wychodzących.
Wpisać `WARN` lub `ERROR`, aby wyłączyć rejestrowanie.

Uwaga: Aktywacja może wymagać ponownego uruchomienia serwera centralnego.

W poniższych wierszach podano przykład rejestrowania wszystkich zdarzeń przychodzących i wychodzących, które dotyczą urządzenia 172.11.122.22:

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

**Pomoc techniczna**

Nasza **pomoc techniczna** jest dostępna na stronie www.boschsecurity.com/xc/en/support/.

Bosch Security and Safety Systems oferuje pomoc techniczną w następujących obszarach:

- [Aplikacje i narzędzia](#)
- [Modelowanie statystyk budynku](#)
- [Gwarancja](#)
- [Rozwiązywanie problemów](#)
- [Naprawy i wymiana](#)
- [Bezpieczeństwo produktów](#)

**Akademia Bosch Building Technologies**

Odwiedź witrynę Akademii Bosch Building Technologies, aby uzyskać dostęp do **kursów**

szkoleniowych, samouczków wideo i dokumentów: www.boschsecurity.com/xc/en/support/training/

Patrz

- Uruchamianie narzędzia ONVIF Camera Event Driver Tool za pomocą Configuration Client, Strona 208
- Konfigurowanie tabeli odwzorowań ONVIF, Strona 241
- Mapowanie zdarzeń ONVIF, Strona 42

Słowniczek

Alarm

Zdarzenie, które jest skonfigurowane w celu wyzwolenia alarmu. Jest to określona sytuacja (wykryty ruch, dzwonek drzwiowy, zanik sygnału itp.) wymagająca natychmiastowej uwagi. Alarm może powodować wyświetlenie obrazu bieżącego, obraz zapisanego, planu działania, strony sieciowej lub mapy.

ANR

Automatyczne uzupełnianie sieciowe. Wbudowana procedura kopiująca brakujące dane wizyjne z nadajnika/odbiornika wizyjnego do sieciowego rejestratora wizyjnego po awarii sieci. Skopiowane dane wizyjne idealnie wypełniają lukę, która powstała po awarii sieci. Dlatego nadajnik/odbiornik wymaga lokalnej pamięci masowej dowolnego typu. Pojemność zapisu na urządzeniu lokalnej pamięci masowej jest obliczana według następującego wzoru: (szerokość pasma x szacowany czas przestoju sieci + margines bezpieczeństwa) x (1 + 1/prędkość wykonywania kopii zapasowej). Wymagana jest obliczona w ten sposób pojemność zapisu, ponieważ zapis ciągły musi być kontynuowany podczas procesu kopiowania.

Awaryjny VRM

Oprogramowanie w środowisku systemu BVMS. Przejmuje zadania przypisane do podstawowego lub pomocniczego VRM w przypadku ich awarii.

Bankomat

Automatyczne urządzenie służące przede wszystkim do wypłaty gotówki.

BIS

Building Integration System – system automatyki budynkowej

Brama Video Streaming Gateway (VSG)

Wirtualne urządzenie umożliwiające integrację kamer Bosch, ONVIF, JPEG, nadajników RTSP.

B-ramka

Dwukierunkowa ramka. Część metody kompresji sygnału wizyjnego.

centrala alarmowa

Ogólna nazwa podstawowego urządzenia wchodzącego w skład systemu bezpieczeństwa firmy Bosch do ochrony przed włamaniami (kradzieżami). Do centrali alarmowej podłącza się klawiatury, moduły, czujki i inne urządzenia.

Cyfrowy rejestrator wizyjny

Cyfrowy rejestrator wizyjny

czas opóźnienia aktywacji

Przedział czasu rozpoczynający się od wystąpienia zdarzenia. Zazwyczaj w trakcie tego przedziału czasu nie jest akceptowane żadne inne zdarzenie tego samego typu. Zapobiega to na przykład generowaniu dużej liczby zdarzeń przez czujki. W przypadku zdarzeń o wielu stanach dla każdego ze stanów można ustawić inny priorytet. Poniższe przykłady pozwalają lepiej zrozumieć pojęcie czasu eliminacji odbicia. W przykładzie 1 opisano zdarzenia tworzące ten sam stan: występuje zdarzenie Informacje o systemie i rozpoczyna się odliczanie skonfigurowanego czasu eliminacji odbicia. W tym czasie występuje kolejne, takie samo zdarzenie. Drugie zdarzenie Informacje o systemie nie zostanie zaakceptowane jako nowe zdarzenie. W przykładzie 2 opisano zdarzenia tworzące różne stany o takim samym priorytecie: występuje zdarzenie Wykryto ruch i rozpoczyna się odliczanie skonfigurowanego czasu eliminacji odbicia. W tym czasie wystąpiło zdarzenie związane z zatrzymaniem ruchu o takim samym priorytecie. Zdarzenie związane z zatrzymaniem ruchu nie zostanie zaakceptowane jako nowe zdarzenie. W przykładzie 3 także opisano zdarzenia tworzące różne stany o takim samym priorytecie: wirtualne wejście jest w stanie włączonym. Obie zmiany mają takie same priorytety stanów. W określonym punkcie czasu wirtualne wejście jest wyłączane i rozpoczyna się odliczanie czasu eliminacji odbicia. W trakcie czasu eliminacji odbicia wirtualne wejście zostaje włączone. Ta zmiana stanu nie jest akceptowana jako nowe zdarzenie, ponieważ ma taki sam priorytet. Gdy czas eliminacji odbicia dobiegnie końca, wirtualne wejście jest w innym stanie. Podczas procesu włączania pobierana jest sygnatura czasowa zakończenia odliczania czasu eliminacji odbicia i nie zaczyna się nowe odliczanie. W przykładzie 4 opisano zdarzenia o różnych priorytetach tworzące różne stany: występuje zdarzenie wykrycia ruchu i rozpoczyna się odliczanie

skonfigurowanego czasu eliminacji odbicia. W tym czasie wystąpiło zdarzenie związane z zatrzymaniem ruchu o wyższym priorytecie. Zdarzenie związane z zatrzymaniem ruchu jest akceptowane jako nowe, ale odliczanie czasu eliminacji odbicia nie rozpoczyna się na nowo. W przykładzie 5 także opisano zdarzenia o różnych priorytetach tworzące różne stany: wirtualne wejście jest w stanie wyłączonym. Priorytet stanu dla włączenia wynosi „5”, a dla wyłączenia „2”. W określonym punkcie czasu wirtualne wejście jest włączane (priorytet „5”) i rozpoczyna się odliczanie czasu eliminacji odbicia. W trakcie czasu eliminacji odbicia, wirtualne wejście zostaje wyłączone (priorytet „2”). Ta zmiana stanu jest akceptowana jako nowe zdarzenie, ponieważ ma wyższy priorytet. Kontynuowane jest odliczanie czasu eliminacji odbicia związanego z pierwszym włączeniem. W trakcie czasu eliminacji odbicia, kolejne zmiany nie są akceptowane.

Czas prezentowania sekwencji

Określony czas, przez który wyświetlany jest obraz z kamery w oknie obrazu do momentu wyświetlenia obrazu z następnej kamery podczas wyświetlania sekwencji obrazów z kamer.

Czas przewijania do tyłu

Liczba sekund, kiedy Okienko obrazu zostaje przełączone na tryb odtwarzania natychmiastowego.

Dane tekstowe

Dane o dacie i godzinie transakcji w punkcie sprzedaży lub bankomacie albo numer konta przechowywane z odpowiadającym im obrazem, które zapewniają dodatkowe informacje do analizy.

dekoder

Zamienia strumień cyfrowy na strumień analogowy.

DNS

Domain Name System. Serwer DNS zamienia adres URL (np. www.myDevice.com) na adres IP w sieciach, które używają protokołu TCP/IP.

Dokument

Pliki dokumentów obsługiwane przez system BVMS to: HTM, URL, MHT, HTML, TXT.

Dostęp Enterprise

Dostęp Enterprise jest funkcją systemu BVMS, która składa się z jednego lub wielu kont Enterprise Account. Każde konto Enterprise Account obejmuje uprawnienia do urządzeń określonego serwera Management Server.

Drzewo logiczne

Drzewo ze spersonalizowaną strukturą wszystkich urządzeń. Drzewo logiczne w aplikacji Operator Client służy do wyboru kamer i innych urządzeń. W aplikacji Configuration Client skonfigurowane jest „Pełne Drzewo logiczne” (na stronie Mapy i struktura) i jest ono dostosowane do każdej grupy użytkowników (na stronie Grupy użytkowników).

Drzewo urządzeń

Hierarchiczna lista wszystkich urządzeń dostępnych w systemie.

DTP

Urządzenie DTP (Data Transform Processor) przekształca dane szeregowe z urządzeń ATM do postaci w zdefiniowanym formacie i przesyła je przez sieć Ethernet do systemu BVMS. Należy zapewnić ustawienie na urządzeniu DTP filtra przekształcania. To zadanie jest wykonywane przez oddzielne oprogramowanie dostarczone przez producenta urządzenia DTP.

dupleks

Termin definiujący kierunek transmisji danych między dwiema lokalizacjami. W trybie półdupleksu dane mogą być przesyłane w obu kierunkach jedynie na przemian. Z kolei w trybie pełnego duplexu możliwa jest jednoczesna transmisja danych w obu kierunkach.

DWF

Design Web Format. Format pliku służący do wyświetlania rysunków technicznych na monitorze komputerowym.

DynDNS

Dynamic Domain Name System. Usługa hostingu DNS przechowująca w bazie danych adresy IP. Dynamiczny DNS umożliwia połączenie z urządzeniem przez sieć Internet przy użyciu nazwy hosta urządzenia. Patrz DNS.

Emulacja poleceń CCL

Emulacja poleceń CCL (Command Console Language) jest używana do sterowania krosownicą Allegiant. Zestawu tych poleceń można używać do przełączania

kamery sieciowej BVMS / nadajnika na dekodery sieciowy BVMS. Poleceń CCL nie można używać do bezpośredniego sterowania starymi kamerami analogowymi ani krosownicą Allegiant.

Główny rejestrator VRM

Synonim urządzenia VRM.

grupa monitorów

Zestaw monitorów dołączonych do odbiorników. Grupa monitorów może służyć do przetwarzania alarmów w określonym obszarze fizycznym. Na przykład instalacja z trzema fizycznie oddzielnymi sterownikami może posiadać trzy grupy monitorów. Monitory w grupie monitorów są logicznie skonfigurowane w rzędy i kolumny oraz mogą być ustawione na różne układy, np. na podgląd obrazów w trybie pełnoekranowym lub w widoku poczwórnym.

Grupa użytkowników

Grupy użytkowników służą do definiowania wspólnych atrybutów użytkownika, takich jak pozwolenia, uprawnienia oraz priorytet funkcji PTZ. Stając się członkiem grupy, użytkownik automatycznie nabywa wszystkie atrybuty grupy.

Grupa użytkowników Enterprise

Grupa użytkowników Enterprise User Group to grupa użytkowników, która została skonfigurowana na serwerze Enterprise Management Server. Grupa użytkowników Enterprise User Group definiuje użytkowników, którzy mają uprawnienia do jednoczesnego dostępu do wielu komputerów typu serwer zarządzający. Określa uprawnienia dotyczące obsługi dostępne dla tych użytkowników.

GSM

Globalny system komunikacji bezprzewodowej. Standard cyfrowych telefonów komórkowych.

H.264

Standard kodowania (kompresji) cyfrowego dźwięku i obrazu w zastosowaniach multimedialnych. Ten standard obejmuje różne profile, które mogą być zależne od producenta. Dostępne są następujące profile: Baseline, Baseline+, główny. Profil Baseline (nieużywany w systemie Bosch Video Management System) obsługuje rozdzielczość 2 CIF. Baseline+ obsługuje rozdzielczość 4 CIF i zapewnia lepszą jakość obrazu od profilu Baseline. Main Profile obsługuje rozdzielczość 4 CIF i oferuje wysokowydajny algorytm kompresji o nazwie CABAC

(Context-adaptive binary arithmetic coding). Ma on zastosowanie w kodowaniu obrazu wysokiej jakości przeznaczonego do zapisu.

H.265

H.265 jest standardem kompresji wideo zdefiniowane przez ISO2 i ITU3 i ratyfikowanym 29 października 2014. Jest on uznawany za następcę standardu MPEG-4 AVC (Advanced Video Codec), nazywanego też H.264, używanego do adresowania kompresji z rozdzielczości 4K i ultra HD do maks. 36 megapikseli.

Harmonogram zadań

Służy do planowania zadań, które pojawiają się w systemie Bosch Video Management System, na przykład wykonanie skryptu poleceń. Na karcie Zdarzenia użytkownik przypisuje harmonogramy zadań do zdarzeń. Do planowania zdarzeń można także użyć harmonogramów zapisu. Za pomocą standardowego harmonogramu zadań można konfigurować przedziały czasowe dla każdego dnia tygodnia, dni świątecznych oraz dni wolnych od pracy. Przy powtarzającym się harmonogramie zadań użytkownik może konfigurować powtarzające się przedziały czasowe. Mogą one powtarzać się codziennie, co tydzień, co miesiąc lub co rok.

Harmonogram zapisu

Służy do harmonogramowania zapisu oraz niektórych zdarzeń, takich jak rozpoczęcie tworzenia kopii zapasowej lub ograniczanie logowania. Harmonogramy zapisu nie mogą zawierać luk lub zachodzić na siebie. Określa on także jakość zapisu obrazu.

Interkom

Służy do rozmowy przez głośniki nadajnika. Nadajnik musi posiadać wejście i wyjście foniczne. Funkcja interkomu może być przydzielana grupie użytkowników.

IQN

Kwalifikowana nazwa iSCSI. Nazwa inicjatora w formacie IQN jest wykorzystywana w celu zapewnienia adresów dla węzłów inicjujących połączenie iSCSI i lokalizacji docelowych. Dzięki mapowaniu IQN można utworzyć grupę inicjującą, która kontroluje dostęp do numerów LUN lokalizacji docelowej iSCSI, oraz zapisywać nazwy początkowe wszystkich nadajników i urządzeń VRM w tej grupie

inicjującej. Tylko urządzenia, których nazwy inicjatora są dodane do grupy inicjującej, mają dostęp do LUN. Patrz LUN i iSCSI.

I-ramka

Ramka Intra. Część metody kompresji sygnału wizyjnego. Zawiera informacje o pełnym obrazie – w przeciwieństwie do P-ramek lub B-ramek, które zawierają informacje o zmianach w stosunku do poprzedniego lub następnego obrazu.

iSCSI

Internet Small Computer System Interface. Protokół używany do zarządzania pamięcią masową za pośrednictwem sieci TCP/IP. Dzięki niemu dostęp do zapisanych danych można uzyskać z dowolnej lokalizacji w sieci. Wraz z nastaniem ery dominacji sieci Gigabit Ethernet zmalały koszty rozwiązań pamięci masowej opartych na serwerach zgodnych ze standardem iSCSI podłączanych do sieci w charakterze zdalnych macierzy dysków twardych. Zgodnie z terminologią używaną w odniesieniu do standardu iSCSI serwer udostępniający przestrzeń dyskową nosi nazwę „węzła docelowego połączenia iSCSI”, a klient łączący się z serwerem i korzystający z jego zasobów jest nazywany „węzłem inicjującym połączenie iSCSI”.

JPEG

Joint Photographic Experts Group. Proces kodowania obrazów nieruchomych.

Kamera PTZ

Kamera z funkcją obrotu, pochylenia i zoomu.

Konto Enterprise

Konto Enterprise Account to autoryzacja, która umożliwia użytkownikowi programu Operator Client łączenie się z urządzeniami serwera zarządzającego wchodzącego w skład systemu Enterprise System. Na koncie Enterprise Account skonfigurowane są wszystkie uprawnienia dotyczące urządzeń tego serwera zarządzającego. Program Operator Client może łączyć się jednocześnie ze wszystkimi serwerami Management Server należącymi do danego systemu Enterprise System. Kontrola dostępu odbywa się z użyciem członkostwa w grupie Enterprise User Group albo z użyciem uprawnień urządzenia skonfigurowanych dla danego serwera Management Server na koncie Enterprise Account.

Korygowanie zniekształceń

Używanie oprogramowania do konwertowania obrazu kolistego z obiektywu typu „rybie oko” z zakłóceniem radialnym na obraz prostoliniowy do wyświetlania w widoku normalnym (prostowanie koryguje zakłócenia).

Krosownica Allegiant

Rodzina analogowych systemów krosownic wizyjnych firmy Bosch.

LDAP

Lightweight Directory Access Protocol. Protokół sieciowy w sieciach TCP/IP umożliwiający dostęp do katalogów. Katalogiem może być na przykład lista grup użytkowników oraz ich uprawnienia dostępu. System Bosch Video Management System używa tego protokołu, aby uzyskać dostęp do tych samych grup użytkowników co MS Windows lub inny system zarządzania użytkownikami.

Linia połączenia

Wyjścia analogowe krosownicy analogowej dołączone do nadajnika. Dzięki temu w systemie Bosch Video Management System jako źródło sygnału wizyjnego mogą być używane krosownice.

Lista alarmów

Okno w systemie Bosch Video Management System, w którym wyświetlana jest lista aktywnych alarmów.

LUN

Logical Unit Number. Numer używany w środowisku iSCSI do adresowania poszczególnych dysków lub partycji wirtualnych (woluminów). Takie partycje są częścią macierzy dyskowej RAID (węzła docelowego połączenia iSCSI).

MHT

Nazywane także „Archiwum sieciowym”. Format pliku, w ramach którego mogą być zapisane wszystkie pliki HTML oraz pliki obrazów. Aby uniknąć problemów, zaleca się utworzenie plików MHT za pomocą przeglądarki Internet Explorer w wersji 7.0 lub nowszej.

Miejsce aktywne

Reagująca na wskaźnik myszy ikona na mapie. Miejsca aktywne konfiguruje się w programie Configuration Client. Miejscami aktywnymi mogą być np. kamery, przekaźniki czy wejścia. Operator używa ich do lokalizowania i wybierania urządzeń w

budynku. Po skonfigurowaniu miejsc aktywnych mogą one być wyświetlane z migającym kolorem tła, gdy wystąpi określone zdarzenie stanu lub alarm.

Monitorowanie sieci

Pomiar parametrów związanych z pracą sieci i porównanie ich wartości z konfigurowalnymi progami.

Nadajnik

Zmienia strumień analogowy na cyfrowy, np. w celu integracji kamer analogowych z systemem cyfrowym, takim jak Bosch Video Management System. Niektóre nadajniki mogą korzystać z lokalnego urządzenia pamięci masowej, np. karty pamięci lub dysku twardego podłączanego za pośrednictwem magistrali USB. Dane wizyjne często można także zapisywać i przechowywać w urządzeniach iSCSI. Kamery sieciowe są wyposażone we wbudowany nadajnik.

Nadmiarowy VRM

Oprogramowanie w środowisku systemu BVMS. Specjalny przypadek pomocniczego VRM. Zapewnia, że zapisywanie wykonywane przez podstawowy VRM jest dodatkowo równocześnie wykonywane przez inne urządzenie docelowe iSCSI z takimi samymi ustawieniami zapisywania.

Numer logiczny

Numery logiczne są niepowtarzalnymi identyfikatorami przypisanymi do każdego urządzenia w systemie ułatwiającymi identyfikację. Numery logiczne są niepowtarzalne tylko w ramach określonego typu urządzenia. Typowym zastosowaniem numerów logicznych są skrypty poleceń.

Obraz odniesienia

Obraz odniesienia jest stale porównywany z obrazem bieżącym. Jeśli aktualny obraz różni się od obrazu odniesienia w wybranych obszarach, wyzwalany jest alarm. Umożliwia to wykrywanie sabotażu, który w innym wypadku pozostałby niewykryty, np. jeśli kamera została obrócona.

obrazy/s

Obrazy na sekundę. Liczba obrazów transmitowanych lub zapisywanych w ciągu sekundy.

Obszar

Grupa urządzeń wykrywających podłączonych do systemu bezpieczeństwa.

Odtwarzanie natychmiastowe

Odtwarza zapisane obrazy z wybranej kamery w Okienku obrazu na ekranie podglądu bieżącego. Czas rozpoczęcia (liczba sekund w przeszłości lub czas przewijania) może być konfigurowany.

OID

Identyfikator obiektu. Termin używany w środowisku SNMP. Określa zmienną MIB.

Okienko obrazu

Służy do wyświetlania obrazu na żywo lub zarejestrowanego obrazu z pojedynczej kamery, mapy miejsca, dokumentu, sekwencji, grupy monitorów, aplikacji zewnętrznej lub okna roboczego mapy.

Okno obrazów alarmowych

Okno obrazu służące do wyświetlania jednego lub więcej Okienek obrazów alarmowych.

Okno obrazu

Przestrzeń dla Okienek obrazu o wyglądzie określonym układem Okienek obrazu.

okno robocze mapy

Okno robocze mapy to obszar ekranu używany do wyświetlania określonej części globalnej mapy geolokalizacji.

ONVIF

Open Network Video Interface Forum. Globalny standard sieciowych urządzeń wizyjnych. Urządzenia zgodne z normą ONVIF mogą wymieniać bieżący obraz, dźwięk, metadane i sygnały sterujące. Ponadto użytkownik zyskuje gwarancję, że będą one automatycznie wykrywane i podłączane do aplikacji sieciowych, takich jak systemy zarządzania sygnałem wizyjnym.

Operator Client

Komponent systemu Bosch Video Management System, który zapewnia interfejs użytkownika do monitorowania i obsługi systemu.

Oprogramowanie Master Control Software

Oprogramowanie używane jako interfejs pomiędzy systemem Bosch Video Management System a urządzeniem systemu Allegiant. Używana jest wersja 2.8 lub nowsza.

Pasek okienka obrazu

Pasek narzędzi okienka obrazu.

PID

Urządzenie PID (Person Identification Device). Wyodrębnia cechy osób widocznych na obrazie, na przykład twarz. Za pomocą specjalnych algorytmów stara się zidentyfikować osobę w strumieniu wizyjnym.

Pliki map

System BVMS obsługuje następujące pliki map: PNG i JPG.

Pliki map obszarów

System BVMS obsługuje następujące pliki map obszarów: PNG, JPG, PDF i DWF.

podwójna autoryzacja

Zasada bezpieczeństwa, która wymaga zalogowania się do aplikacji Operator Client przez dwóch różnych użytkowników. Obaj użytkownicy muszą być członkami normalnej grupy użytkowników systemu Bosch Video Management System. Dodatkowo ta grupa użytkowników (lub te grupy użytkowników, jeśli użytkownicy są członkami różnych grup użytkowników) musi być częścią grupy podwójnej autoryzacji. Grupa podwójnej autoryzacji ma własne prawa dostępu w systemie Bosch Video Management System. Grupa ta powinna mieć więcej uprawnień dostępu niż normalna grupa użytkowników, do której należy użytkownik. Przykład: Użytkownik A jest członkiem grupy użytkowników o nazwie Grupa A. Użytkownik B jest członkiem Grupy B. Dodatkowo grupa podwójnej autoryzacji jest skonfigurowana z Grupą A oraz Grupą B jako członkami. W przypadku użytkowników Grupy A podwójna autoryzacja jest opcjonalna, natomiast w przypadku użytkowników Grupy B jest obowiązkowa. Po zalogowaniu się użytkownika Grupy A zostaje wyświetlone drugie okno dialogowe w celu potwierdzenia logowania. W tym oknie dialogowym może zalogować się drugi użytkownik, jeśli jest dostępny. W przeciwnym wypadku użytkownik A może kontynuować i uruchomić aplikację Operator Client. Ma wówczas tylko prawa dostępu Grupy A. Podczas logowania się użytkownika Grupy B także wyświetlane jest drugie okno dialogowe logowania. Drugi użytkownik musi zalogować się w tym oknie dialogowym. Jeśli tego nie zrobi, użytkownik B nie uruchomi aplikacji Operator Client.

Podwójne strumieniowanie

Podwójne strumieniowanie umożliwia jednoczesne kodowanie przychodzącego strumienia danych zgodnie z dwoma różnymi, indywidualnie skonfigurowanymi profilami. Tworzone są dwa strumienie danych: jeden dla zapisu obrazu bieżącego i zapisu przed wystąpieniem zdarzenia, a drugi dla zapisu ciągłego, zapisu ruchu i zapisu alarmowego.

pomijanie / wyłączanie pomijania

Pominięcie urządzenia oznacza zignorowanie wszelkich alarmów, jakie może ono wygenerować. Zazwyczaj funkcję tę stosuje się w niektórych okolicznościach wymagających złagodzenia ochrony, takich jak konserwacja. Wyłączenie pomijania oznacza zaprzestanie ignorowania takich urządzeń.

Pomocniczy VRM

Oprogramowanie w środowisku systemu BVMS. Zapewnia, że zapisywanie wykonywane przez jeden lub wiele podstawowych urządzeń VRM jest dodatkowo równocześnie wykonywane przez inne urządzenie docelowe iSCSI. Ustawienia zapisywania mogą być inne niż dla podstawowego VRM.

Port

1) W komputerze oraz urządzeniach telekomunikacyjnych port jest określonym złączem do fizycznego dołączenia innego urządzenia, zwykle za pomocą gniazda lub wtyku. Standardowo komputer osobisty posiada jeden lub więcej portów szeregowych oraz jeden port równoległy. 2) W przypadku programowania port jest „logicznym miejscem połączenia”, a w szczególności sposobem, w jaki program klienta określa dany program serwera na komputerze w sieci, korzystając z protokołu internetowego TCP/IP. Aplikacje wyższego poziomu, które używają protokołu TCP/IP, takie jak protokół sieciowy, protokół Hypertext Transfer Protocol, posiadają porty z przypisanymi numerami. Są one ogólnie znanymi portami, które zostały przypisane przez organizację Internet Assigned Numbers Authority (IANA). Innym procesom aplikacji numery przydzielane są dynamicznie przy każdym połączeniu. Przy pierwszym uruchomieniu usługi (program serwera) jest ona łączona z wyznaczonym numerem portu. Ponieważ każdy program klienta chce używać tego serwera, także on musi zgłosić chęć połączenia z wyznaczonym numerem portu. Numery portów zawierają się w zakresie od 0 do 65535. Porty od 1 do 1023 są zarezerwowane dla określonych usług

uprzywilejowanych. Dla usługi HTTP domyślnie zdefiniowany jest port 80 i nie musi być określony w adresie Uniform Resource Locator (URL).

P-ramka

Ramka przewidywana. Część metody kompresji sygnału wizyjnego.

Prostowanie obrazu w kamerze

Prostowanie jest wykonywane automatycznie w kamerze.

punkt

Urządzenie wykrywające podłączone do systemu bezpieczeństwa. Punkty są wyświetlane na klawiaturze numerycznej osobno z niestandardowym tekstem. Może on opisywać pojedyncze drzwi, czujnik ruchu, czujnik dymu lub obszar chroniony, np. PIĘTRO czy GARAŻ.

Punkt sprzedaży

Stanowisko kasowe typu detalicznego.

RAID

Redundant array of independent disks – Macierz dyskowa. Służy do połączenia dwóch lub więcej dysków do pracy jako jeden napęd. Na takim napędzie dane są współdzielone lub replikowane. Macierz pomaga osiągnąć większą pojemność, niezawodność i prędkość.

RCP

Remote Control Protocol

Rejestr

Miejsce rejestrowania wszystkich zdarzeń w systemie Bosch Video Management System.

ROI

Obszar zainteresowania. Celem użycia funkcji ROI jest zapisanie szerokości pasma podczas powiększania fragmentu obrazu z kamery, w przypadku gdy jest to kamera stałopozycyjna. Fragment ten zachowuje się jak obraz z kamery PTZ.

Rozdzielczość obrazu

Liczba pikseli w poziomie oraz w pionie przesyłanych z sygnałem wizyjnym. 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 = kodowane 1280 x 720 1080p = kodowane 1920 x 1080

RTP

Skrót od „Real-time Transport Protocol”. Protokół transmisyjny do przesyłania obrazu i dźwięku w czasie rzeczywistym.

RTSP

Skrót od „Real Time Streaming Protocol”. Protokół sieciowy umożliwiający kontrolę nad ciągłą transmisją dźwięku i obrazu lub oprogramowania w sieciach IP.

Seria urządzeń

Nadajniki / kamery sieciowe firmy Bosch mogą należeć do jednej z poniższych serii urządzeń: Seria urządzeń 1, Seria urządzeń 2, Seria urządzeń 3. Urządzenia z serii 1 mogą nagrywać tylko strumień 1. Urządzenia z serii 2 mogą nagrywać strumień 1 lub 2. Urządzenia z serii 3 mogą nagrywać tylko strumień 1, 2 lub I-Frame.

Server Lookup

Metoda dostępu dla użytkownika programów Configuration Client lub Operator Client pozwalająca sekwencyjnie łączyć się z wieloma punktami dostępowymi systemu. Punktem dostępowym systemu może być serwer Management Server lub Enterprise Management Server.

Server Enterprise Management Server

Serwer Enterprise Management Server jest serwerem zarządzającym BVMS Management Server hostującym konfigurację grup Enterprise User Group. Potrzebna co najmniej jedna grupa użytkowników Enterprise User Group odwołująca się do jednego lub wielu komputerów z serwerami. Role serwera Enterprise Management Server i serwera Management Server można połączyć w ramach jednej konfiguracji.

Serwer zarządzający

Serwer BVMS zarządzający urządzeniami.

Sieciowy rejestrator wizyjny (NVR)

Sieciowy rejestrator wizyjny firmy Bosch, czyli komputer w środowisku systemu Bosch Video Management System przechowujący dane foniczne i wizyjne, pełniący funkcję awaryjnego lub zapasowego rejestratora NVR. Rejestrator ten różni się od rejestratora VIDOS NVR, który można zintegrować z systemem Bosch Video Management System.

Skimming

Sabotaż czytnika kart. Urządzenie w postaci nałożonego fałszywego czytnika czyta podstępnie dane z paska magnetycznego karty użytkownika.

Skrypt poleceń

Makro, które może zaprogramować administrator w celu utworzenia automatycznych działań, takich jak pozycjonowanie kamery PTZ lub wysyłanie wiadomości e-mail. System Bosch Video Management System oferuje określony zestaw poleceń przeznaczonych dla tej funkcji. Skrypty poleceń dzielą się na skrypty klienta oraz skrypty serwera. Skrypty klienta są używane na stacjach roboczych klienta w celu wykonania określonych zadań, które mogą być uruchomione na stacji roboczej klienta. Skrypty serwera są wykonywane automatycznie przez zdarzenie, które zostało wyzwolone w systemie. Pobierają argumenty dostarczane przez zdarzenie, takie jak data i czas. Skrypt poleceń może składać się z wielu scriptletów. Użytkownik może stworzyć skrypt poleceń, używając następujących języków skryptów: C#, VB.Net. Skrypty poleceń są wykonywane automatycznie w odpowiedzi na zdarzenia lub alarmy, zgodnie z harmonogramem (tylko skrypty serwera), lub ręcznie – z poziomu okna Drzewo logiczne, ikon lub map.

SNMP

Simple Network Management Protocol. Protokół sieciowy, który umożliwia uzyskanie informacji z urządzeń sieciowych (GET) w celu ustawienia ich parametrów (SET) oraz otrzymywania powiadomień o określonych zdarzeniach (EVENT).

Stacja robocza

W środowisku BVMS: osobny komputer, na którym jest zainstalowany program Operator Client. Komputer ten jest skonfigurowany w programie Configuration Client jako stacja robocza, aby umożliwić korzystanie ze specjalnych funkcji.

Stacja robocza Operator Client

Komputer w środowisku systemu Bosch Video Management System służący do oglądania obrazów na żywo, odtwarzania wideo i ustawiania konfiguracji. Na tym komputerze jest instalowany program Operator Client.

System Enterprise

Enterprise System to funkcja systemu Bosch Video Management System, która umożliwia użytkownikowi aplikacji Operator Client uzyskiwanie jednoczesnego dostępu do wielu komputerów typu serwer zarządzający.

TCP

Skrót od „Transmission Control Protocol” (nazwa protokołu komunikacyjnego).

TCP/IP

Transmission Control Protocol / Internet Protocol. Jest także nazywany zestawem protokołów komunikacyjnych transmisji danych. Zestaw protokołów komunikacyjnych używany do przesyłania danych w sieci IP.

Trap

Termin środowiska SNMP dla niewywoływanego komunikatu z monitorowanego urządzenia (agent) do sieciowego systemu monitoringu (manager) o zdarzeniu w tym urządzeniu.

Tryb podglądu bieżącego

Funkcja aplikacji Operator Client. Służy do wyświetlania na żywo obrazu.

UDP

User Datagram Protocol. Protokół bezpołączeniowy używany do wymiany danych przez sieć IP. Protokół UDP jest bardziej wydajny od protokołu TCP przy transmisji obrazu ze względu na mniejszą nadmiarowość.

Unmanaged Site

Element drzewa urządzeń na serwerze BVMS, który może zawierać sieciowe urządzenia wizyjne, takie jak cyfrowe rejestratory wizyjne. Urządzenia te nie są zarządzane przez serwer zarządzający systemem. Użytkownik programu Operator Client może nawiązywać na żądanie połączenia z urządzeniami lokalizacji unmanaged site.

URL

Skrót od „Uniform Resource Locator” – standard nazewniczy umożliwiający jednoznaczne identyfikowanie serwerów i zgromadzonych w nich zasobów

VCA

Analiza zawartości obrazu: analiza komputerowa strumieni wizyjnych mająca na celu określenie, co dzieje się w monitorowanej scenie. Patrz także Intelligent Video Analytics

Video Analytics

Analiza obrazu to proces programowy, w którym porównuje się obraz z kamery z zapisanymi obrazami określonych osób lub obiektów. W przypadku dopasowania oprogramowanie wyzwoli alarm.

VRM

Video Recording Manager. Pakiet oprogramowania w systemie Bosch Video Management System, którego zadaniem jest zarządzanie przechowywaniem danych wizyjnych (MPEG-4 SH++, H.264 i H.265) zawierających audio i metadane na sieciowych urządzeniach iSCSI. Oprogramowanie VRM korzysta z bazy danych zawierającej informacje o źródle zapisu oraz listę powiązanych napędów iSCSI. Jest ono uruchamiane jako usługa zainstalowana na komputerze przyłączonym do sieci systemu Bosch Video Management System. Samo oprogramowanie VRM nie przechowuje danych wideo, lecz przekazuje do nadajników informacje o dostępnych pojemnościach urządzeń iSCSI, zapewniając jednocześnie równowagę obciążenia pomiędzy wieloma urządzeniami iSCSI. Odtwarzanie strumieni VRM z urządzenia iSCSI do klientów Operator Client.

wieloscieżkowość

Wykorzystanie techniki wieloscieżkowości pamięci komputera.

wieloscieżkowość

Technika przechowywania danych w pamięci komputera polegająca na zdefiniowaniu wielu ścieżek fizycznych łączących serwer danych z docelową lokalizacją pamięci (przy użyciu różnych sterowników, przełączników magistral itp.) w celu zapewnienia odporności na awarie lub zrównoważenia obciążenia (nadmiarowości, wydajności).

Wirtualne wejście

Służy do przekazywania zdarzeń z systemów innych producentów do systemu Bosch Video Management System.

zakresy

Zakres to termin używany w polu kamer ONVIF. Parametr ten służy do badania urządzenia ONVIF. Zwykle zawiera on identyfikator URI, np.: onvif://www.onvif.org/<ścieżka>. Parametr <ścieżka> może mieć np. postać video_encoder lub audio_encoder. Jedno urządzenie ONVIF może zawierać wiele zakresów. Identyfikator URI wskazuje obszar zadań urządzenia.

Zdarzenie

Warunek lub stan, który jest zwykle połączony z alarmem i/lub działaniem. Zdarzenia mogą pochodzić z różnych źródeł, takich jak kamery, archiwizatory, katalogi, wejścia cyfrowe itp. Obejmują stany

rozpoczęcia zapisu, stany zaniku sygnału, komunikaty o zapełnieniu dysku, logowanie użytkownika, wyzwacze wejścia cyfrowego itp.

Zdarzenie złożone

Połączenie różnych zdarzeń. Połączenia używają wyrażen boolowskich, tj. AND oraz OR. Użytkownik może łączyć tylko zmiany stanów, na przykład zmianę stanu połączenia na „rozłączony” lub „uaktywnienie harmonogramu”.

znacznik

Używany w celu zapisywania przedziału czasowego bieżącego i zarejestrowanego obrazu. Umożliwia oznaczenie konkretnych scen w celu ich późniejszego przeanalizowania. Ponadto użytkownik może udostępniać wyniki swoich analiz innym użytkownikom, eksportując znacznik.

Bosch Security Systems B.V.

Torenallee 49

5617 BA Eindhoven

Netherlands

www.boschsecurity.com

© Bosch Security Systems B.V., 2025